AZƏRBAYCAN RESPUBLİKASI
ELM VƏ TƏHSİL NAZİRLİYİ

Azərbaycan Kibertəhlükəsizlik
Təşkilatları Assosiasiyası

Sosial mühəndislik

fənni üzrə mühazirələr toplusu

Müəlliflər: Orxan Məmmədov, Dr. Təbriz Cəfərov, Vüqar Qədimov

Bu vəsait Azərbaycan Respublikasının Elm və Təhsil Nazirliyinin maliyyə dəstəyi ilə həyata keçirilən "İnformasiya təhlükəsizliyi ixtisası üzrə elmi-metodiki tədris (çap və onlayn) vəsaitlərinin hazırlanması" layihəsi çərçivəsində hazırlanmışdır.

Nəşrin məzmununa görə donor məsuliyyət daşımır.

AZƏRBAYCAN RESPUBLİKASI ELM VƏ TƏHSİL NAZİRLİYİ

AZƏRBAYCAN RESPUBLİKASI DAXİLİ İŞLƏR NAZİRLİYİ
POLİS AKADEMİYASI

AZƏRBAYCAN KİBERTƏHLÜKƏSİZLİK TƏŞKİLATLARI ASSOSİASİYASI

Sosial mühəndislik

fənni üzrə mühazirələr toplusu

Bakı - 2025

AZƏRBAYCAN RESPUBLİKASI DAXİLİ İŞLƏR NAZİRLİYİ
POLİS AKADEMİYASI

AZƏRBAYCAN RESPUBLİKASI ELM VƏ TƏHSİL NAZİRLİYİ

AZƏRBAYCAN KİBERTƏHLÜKƏSİZLİK TƏŞKİLATLARI ASSOSASİYASI

Müəlliflər:
Orxan Məmmədov, Dr. Təbriz Raufoğlu (Cəfərov), Vüqar Qədimov. **Sosial mühəndislik. Mühazirələr toplusu, 2025**

Sosial mühəndislik fənni üzrə mühazirələr toplusunun hazırlanmasının əsas məqsədi sosial mühəndisliyin ali təhsilin bakalavriat səviyyəsində öyrətmək, bu sahədə elmi-metodiki boşluqları doldurmaq və azərbaycandilli elmi ədəbiyyatın inkişafına töhfə verməkdir. Bu mühazirələr toplusu, sosial mühəndisliyin əsas prinsiplərini, onun təhlükəsizlik sistemlərinə təsirini və hücumların qarşısının alınması yollarını əhatə edir. Təhsilalanlara sosial mühəndislik texnikalarını, kiberdələduzluq və psixoloji manipulyasiya üsullarını daha dərindən öyrənmək imkanı yaradılacaqdır.

Sosial mühəndislik texnikalarının təşkilatlar və şəxslər üçün yaratdığı risklər, eləcə də onların informasiya təhlükəsizliyinə təsiri geniş şəkildə təhlil ediləcəkdir.

Eyni zamanda, sosial mühəndislik hücumlarına qarşı fərdi və təşkilati müdafiə mexanizmlərinin gücləndirilməsi üzrə praktiki tövsiyələr veriləcəkdir. Təhsilalanlar real hadisələr və nümunələr əsasında sosial mühəndislik hücumlarını təhlil edərək, onların qarşısını almaq üçün strateji və texnoloji həllər öyrənəcəklər. Praktik təhlillər və simulyasiyalar vasitəsilə tələbələrin sosial mühəndislik hücumlarına qarşı daha effektiv müdafiə üsulları inkişaf etdirmələri üçün imkan yaradılacaqdır. Bu yanaşma həm elmi-nəzəri biliklərin artırılmasına, həm də tələbələrin analitik düşünmə və praktiki bacarıqlarının inkişafına xidmət edəcəkdir. Təhsilalanlar sosial mühəndislik hücumlarının texnoloji və psixoloji aspektlərini kompleks şəkildə mənimsəyərək, təhlükəsizlik sahəsində daha hazırlıqlı mütəxəssislərə çevriləcəklər.

Sosial mühəndislik
Mühazirələr toplusu

Azərbaycan Respublikası Daxili İşlər Nazirliyi, Polis Akademiyası, Bakı, 2025.

MÜNDƏRİCAT:

§ 1. Sosial mühəndisliyin anlayışı, mahiyyəti və yaranma tarixi

Giriş

Sosial mühəndislik, kibertəhlükəsizlik sahəsində çoxşaxəli və mürəkkəb bir anlayışdır. Bu, insanların psixoloji zəifliklərindən istifadə edərək, onların məlumatlarını və ya resurslarını manipulyasiya etmək məqsədini güdən bir texnikadır. Sosial mühəndislik, kibercinayətkarların texnoloji müdaxilələrdən daha çox insan davranışlarına yönəlməsi ilə xarakterizə olunur. Belə hücumlar, adətən texnoloji vasitələrdən istifadə olunmadan həyata keçirilir və insanların düşüncələrinə və davranışlarına təsir etməklə məqsədlərinə çatırlar.

Son onilliklər ərzində texnologiyanın inkişafı ilə kibertəhlükəsizlik sahəsində ciddi irəliləyişlər əldə edilmişdir. Lakin texniki təhlükəsizlik tədbirləri nə qədər güclü olsa da, sosial mühəndislik, insanların psixoloji zəifliklərindən faydalanaraq, bu tədbirləri aşmaq üçün təsirli bir vasitə olaraq qalmışdır. Bu, insanları manipulyasiya etməklə məlumatları əldə etmək və ya təhlükəsizlik sistemlərinə daxil olmaq üçün istifadə olunan bir təcrübədir.

Sosial mühəndislik hücumları, yalnız texnoloji biliklərə deyil, həm də insan davranışları və psixologiyası haqqında geniş məlumata malik olan şəxslər tərəfindən həyata keçirilir. Bu cür hücumlar çox vaxt qurbanların emosional reaksiyalarını hədəf alır və onları təhlükəsizlik tədbirlərindən yayınmağa məcbur edir. Beləliklə, sosial mühəndislik, texniki hücumlarla müqayisədə daha geniş miqyaslı və fərqli bir təhdid yaradır.

Bu mühazirə, sosial mühəndisliyin təməl anlayışlarını, onun mahiyyətini və yaranma tarixini dərindən araşdıracaqdır. Həmçinin, sosial mühəndisliyin cəmiyyətə və təşkilatlara olan təsirlərini və bu hücumlara qarşı mübarizə metodlarını nəzərdən keçirəcəkdir. Sosial mühəndislik, yalnız kibertəhlükəsizlik mütəxəssisləri üçün deyil, həm də geniş ictimaiyyət üçün mühüm bir mövzudur, çünki hər bir şəxs bu cür hücumların potensial qurbanı ola bilər.

Geniş perspektivdən baxdıqda, sosial mühəndislik, insanların təbii olaraq qarşılıqlı fəaliyyətə açıq və etibar etməyə meyilli olması üzərində qurulmuşdur. Bu, xüsusilə internet və sosial medianın sürətlə yayıldığı müasir dövrdə, kibercinayətkarlar üçün geniş imkanlar yaradır. Sosial mühəndislik texnikalarının köməyi ilə hücum edən şəxslər qurbanlarının zəifliklərindən faydalanaraq məlumatları əldə etmək üçün onları manipulyasiya edirlər. Bu, şəxslərin, şirkətlərin və hətta dövlət qurumlarının təhlükəsizliyinə ciddi zərər verə bilər.

Beləliklə, bu mühazirə vasitəsilə sosial mühəndisliyin əsas anlayışlarını, metodlarını və tarixini ətraflı öyrənərək, bu təhlükənin qarşısını almaq və ya minimuma endirmək üçün hansı tədbirlərin görülməli olduğunu dərk edəcəyik. Sosial mühəndisliyin kökləri və inkişafı, bu təhdidin niyə bu qədər yayılmış olduğunu və nə üçün bu qədər təhlükəli olduğunu daha yaxşı başa düşməyə kömək edəcəkdir.

Sosial mühəndislik anlayışı

Sosial mühəndislik, kibertəhlükəsizlik sahəsində diqqətəlayiq bir mövzu olaraq son illərdə böyük əhəmiyyət kəsb edir. Texnoloji təhlükəsizlik tədbirləri nə qədər güclü olsa da, insan faktorunu manipulyasiya edərək bu tədbirləri aşmaq mümkündür. Məhz bu məqamda sosial mühəndislik öz aktuallığını qoruyur. Sosial mühəndislik, çoxşaxəli və mürəkkəb bir anlayış kimi, həm texnologiya ilə, həm də insan psixologiyası ilə sıx əlaqəlidir. Bu səbəbdən, bu konsepti tam dərk etmək üçün onun müxtəlif aspektlərini və yanaşmalarını araşdırmaq vacibdir.

Bu hissədə, sosial mühəndisliyin nə olduğunu daha dəqiq anlamaq üçün onun müxtəlif tərifləri nəzərdən keçirəcəyik. Fərqli perspektivlərdən yanaşaraq, sosial mühəndisliyin necə işlədiyini və niyə bu qədər təsirli olduğunu daha yaxşı anlamaq mümkündür. Sosial mühəndislik təkcə kibercinayətkarlıqla məhdudlaşmır, həm də insan davranışlarını manipulyasiya etmək üçün geniş spektrdə tətbiq olunan metodlar toplusudur. Bu metodlar, həm fərdi, həm də təşkilati səviyyədə geniş şəkildə istifadə edilə bilər.

Sosial mühəndislik anlayışına dair fərqli yanaşmalar, bu fenomenin müxtəlif aspektlərini üzə çıxarır. Bu fərqlər, sosial mühəndisliyin mürəkkəbliyini və onun tətbiq sahələrinin genişliyini göstərir. Hər bir tərif, sosial mühəndisliyin müəyyən bir aspektini vurğulayır və beləliklə, bu təcrübənin çoxölçülü xarakterini başa düşmək üçün müxtəlif perspektivlər təqdim edir.

Növbəti addımda, sosial mühəndisliyin müxtəlif tərifləri və yanaşmalarını təhlil edərək onların oxşar və fərqli cəhətlərini müəyyən edəcəyik. Sosial mühəndisliyin anlayışını daha yaxşı mənimsəmək və onun real dünyadakı tətbiqlərini anlamaq üçün bizə daha dərin bir anlayış verəcəkdir.

1: Klassik yanaşma

Tərif: Sosial mühəndislik, bir şəxsin və ya təşkilatın məlumatlarını əldə etmək və ya təhlükəsizlik sistemini aşmaq üçün insanların etibarını qazanmaq və onları manipulyasiya etmək prosesidir[1].

Xüsusiyyətlər:

- **Oxşar cəhətləri:** Anlayış sosial mühəndisliyin əsas xüsusiyyətlərini əks etdirir, yəni insanların etibarının qazanılması və manipulyasiya edilməsi.
- **Fərqli cəhətləri:** Tərif əsasən məlumat əldə etmək və təhlükəsizlik sistemlərini aşmaq kimi konkret məqsədlərə fokuslanır.

2: Psixoloji yanaşma

Tərif: Sosial mühəndislik, insan psixologiyasından və emosional zəifliklərdən faydalanaraq, qurbanları aldadaraq məlumatları ələ keçirmək və ya onları müəyyən davranışlara məcbur etmək sənətidir[2].

Xüsusiyyətlər:

[1] The art of deception: controlling the human element of security - Kevin D. Mitnick, William L. Simon
[2] Sosial mühəndislik nədir? - cybersign.az/xeber/xeber_1

- **Oxşar cəhətləri:** Hər iki tərif, insanların etibarını qazanmaq və manipulyasiya etmək üzərində qurulmuşdur.
- **Fərqli cəhətləri:** Bu tərif, insan psixologiyası və emosional zəifliklərə xüsusi diqqət yetirir, bu da sosial mühəndisliyin psixoloji aspektlərini vurğulayır.

3: Texnoloji yanaşma

Tərif: Sosial mühəndislik, texnoloji sistemlərə müdaxilə etmək və ya məlumatları oğurlamaq üçün texnologiyadan istifadə edərək insanları manipulyasiya etmək üçün tətbiq olunan taktikaların və metodların toplusudur[3].

Xüsusiyyətlər:

- **Oxşar cəhətləri:** Bu tərif də manipulyasiya və məlumat əldə etmək üzərində fokuslanır.
- **Fərqli cəhətləri:** Tərifdə texnologiya mühüm rol oynayır və texnoloji vasitələrin sosial mühəndislikdə necə istifadə edildiyi vurğulanır.

4: Holistik yanaşma

Tərif: Sosial mühəndislik, qurbanların etibarını qazanmaq, insan psixologiyasını və texnologiyanı manipulyasiya etmək yolu ilə şəxsi və ya təşkilati məlumatları əldə etmək və ya onların davranışlarını dəyişdirmək üçün tətbiq olunan mürəkkəb və çoxşaxəli strategiyalar toplusudur[4].

Xüsusiyyətlər:

- **Oxşar cəhətləri:** Bu tərif də digər təriflər kimi manipulyasiya və məlumat əldə etmək üzərində qurulmuşdur.
- **Fərqli cəhətləri:** Tərif, sosial mühəndisliyin həm insan psixologiyasını, həm də texnologiyanı necə birləşdirdiyini vurğulayır, bu da onu daha geniş və mürəkkəb bir tərif halına gətirir.

5: Etik yanaşma

Tərif: Sosial mühəndislik, insanların və təşkilatların məlumatlarını qorumaq və təhlükəsizlik tədbirlərini yaxşılaşdırmaq məqsədilə onların zəifliklərini müəyyən etmək üçün istifadə edilən etik metodlardan ibarətdir[5].

Oxşar cəhətlər

- **Manipulyasiya:** Bütün təriflər, manipulyasiya elementini ehtiva edir, bu da sosial mühəndisliyin əsas xüsusiyyətlərindən biridir.
- **Məlumat əldə etmək:** Hər bir tərif, məlumatların əldə edilməsini və ya qorunan resurslara giriş əldə edilməsini vurğulayır.
- **İnsan psixologiyası:** Bir çox tərif, insan psixologiyasını manipulyasiya etməyin əhəmiyyətini qeyd edir.

Fərqli cəhətlər

- **Texnologiya:** Bəzi təriflər texnologiyanın sosial mühəndislikdə oynadığı rolu vurğulayır, digərləri isə əsasən insan psixologiyasına diqqət yetirir.

[3] Social engineering: understanding and auditing - global information assurance certification paper - Chris Jones, 2003
[4] "Sosyal mühendislik ve oltalama saldırılarını anlamak: derinlemesine bir analiz" - Ceren Çubukçu Çerasi
[5] Social engineering: the science of human hacking - Christopher Hadnagy

- **Etik aspektlər:** Bəzi tərifl ər sosial mühəndisliyin etik cəhətlərini qeyd edir, digərləri isə əsasən zərərli niyyətlərə fokuslanır.
- **Komplekslik:** Tərifl ər arasında sosial mühəndisliyin necə tətbiq olunduğunu və hansı strategiyaların istifadə olunduğunu vurğulayan fərqlər var. Bəzi tərifl ər daha sadə, digərləri isə daha mürəkkəb və genişdir.

Təklif olunan anlayış: Holistik yanaşma

Tərif: Sosial mühəndislik, qurbanların etibarını qazanmaq, insan psixologiyasını və texnologiyanı manipulyasiya etmək yolu ilə şəxsi və ya təşkilati məlumatları əldə etmək və ya onların davranışlarını dəyişdirmək üçün tətbiq olunan mürəkkəb və çoxşaxəli strategiyalar toplusudur.

Səbəblər:

- **Bütün aspektləri əhatə edir:** Bu tərif sosial mühəndisliyin həm texnoloji, həm də insan psixologiyası aspektlərini nəzərə alır. Bu yanaşma, sosial mühəndisliyin kompleks və çoxşaxəli bir hücum növü olduğunu vurğulayır.
- **Strateji genişlik:** Holistik yanaşma sosial mühəndisliyin yalnız bir hissəsini deyil, tam bir strategiya olaraq qəbul edir və sosial mühəndislik hücumlarının mürəkkəbliyini və onların müxtəlif formalarını əhatə edir.
- **Reallığa daha uyğun:** Müasir dövrdə sosial mühəndislik hücumları həm insan zəifliklərindən, həm də texnoloji vasitələrdən istifadə edir. Tərif, bu iki əsas elementin birləşdirilməsini əks etdirir və sosial mühəndisliyin təbiətini daha dəqiq əks etdirir.

Holistik sözü yunanca holos (“bütöv”) sözündən yaranıb və bütöv yanaşma, sistemli baxış mənasını ifadə edir[6]. Holistik yanaşma, bir mövzunu və ya problemi onun yalnız ayrı-ayrı hissələri ilə deyil, bütövlükdə dəyərləndirməyə əsaslanır. Holistik yanaşma sosial mühəndisliyi təkcə texnoloji və psixoloji aspektlər çərçivəsində deyil, həm də qurbanın davranışlarını formalaşdıran kompleks bir strategiya kimi nəzərdən keçirir. Bu yanaşma, hücum edən şəxsin yalnız məlumat əldə etməklə kifayətlənmədiyini, eyni zamanda qurbanın etibarını qazanaraq onu istənilən hərəkətləri etməyə təşviq etdiyini vurğulayır. İnsan psixologiyasının manipulyasiya edilməsi, texnologiyanın istismar edilməsi və davranışların dəyişdirilməsi strategiyanın əsas elementləridir. Holistik yanaşma tək bir üsula deyil, çoxşaxəli və əlaqəli texnikalara əsaslanaraq sosial mühəndisliyin effektivliyini artırır. Aşağıda bu yanaşmanın əsas tərkib hissələri və onların praktiki tətbiqləri ətraflı izah olunur.

1. Qurbanların etibarını qazanmaq

Holistik yanaşmanın ilk tərkib hissəsi, qurbanların etibarını qazanmaqdır. Sosial mühəndisliyin effektiv olması üçün hücum edən şəxsin qurbanla etibarlı bir əlaqə qurması vacibdir. Adətən hücum edən şəxsin özünü etibarlı bir şəxs və ya təşkilat kimi təqdim etməsi ilə həyata keçirilir. Etibar qazanıldıqdan sonra, qurbanın məlumatlarını ifşa etməsi və ya müəyyən hərəkətləri etməsi daha asan olur.

Bu tərkib hissəsi sosial mühəndisliyin əsas məqsədlərindən birini təşkil edir: insanların təbii olaraq etimad göstərməyə meyilli olması. Etibar qazanma texnikaları

[6] Holistic definition & meaning - www.merriam-webster.com/dictionary/holistic

arasında sadə yalanlar, yalançı adlar və ya uydurma şəxsiyyətlərdən istifadə kimi metodlar yer alır.

2. İnsan psixologiyasını manipulyasiya etmək

Holistik yanaşmanın ikinci tərkib hissəsi insan psixologiyasını manipulyasiya etməkdir. Sosial mühəndislik, insanların emosional zəifliklərini, qorxularını, ehtiyaclarını və arzu etdikləri şeyləri istifadə edərək, onları manipulyasiya edir. Belə bir manipulyasiya texnikaları fərdi səviyyədə tətbiq oluna bilər, məsələn, bir şəxsiyyətin narahatlığını artıraraq onu müəyyən hərəkətlərə vadar etmək kimi.

Bu tərkib hissəsi sosial mühəndisliyin psixoloji aspektini vurğulayır. Hücum edən şəxslər qurbanların qərar vermə proseslərini manipulyasiya etmək üçün müxtəlif emosional taktikalardan istifadə edirlər. Məsələn, təcili yardım çağırışı və ya təhdid altında olma hissi yaratmaq, qurbanların məlumatları ifşa etməsinə səbəb ola bilər.

3. Texnologiyanı manipulyasiya etmək

Holistik yanaşmanın üçüncü tərkib hissəsi texnologiyanın manipulyasiya edilməsidir. Sosial mühəndislik təkcə insan davranışları ilə məhdudlaşmır; eyni zamanda, texnologiyanı manipulyasiya etmək üçün müxtəlif metodlardan istifadə edilir. Phishing hücumları, zərərli proqramlar və saxta veb-saytlar kimi texnologiyaya əsaslanan hücum metodlarını əhatə edir.

Bu tərkib hissəsi sosial mühəndisliyin texnoloji aspektini vurğulayır. Hücum edən şəxslər, texnoloji vasitələrdən istifadə edərək qurbanları aldadaraq onların fərdi məlumatlarını və ya sistemlərə giriş hüquqlarını əldə edirlər. Bu texnologiya əsaslı manipulyasiya, xüsusilə müasir dövrdə sosial mühəndisliyin nə qədər təsirli ola biləcəyini göstərir.

4. Şəxsi və ya təşkilati məlumatları əldə etmək

Holistik yanaşmanın növbəti tərkib hissəsi şəxsi və ya təşkilati məlumatları əldə etməkdir. Sosial mühəndislik hücumlarının əsas məqsədi, məlumatların ələ keçirilməsidir. Bu məlumatlar şəxslərin fərdi məlumatları, maliyyə məlumatları, şifrə və ya təhlükəsizlik sistemlərinə giriş hüquqları ola bilər. Təşkilati səviyyədə isə bu məlumatlar korporativ sənədlər, məxfi məlumatlar və ya işçilərin şəxsi məlumatları ola bilər.

Bu tərkib hissəsi sosial mühəndisliyin məqsədini aydın şəkildə ifadə edir: hücum edən şəxs, qurbanların məlumatlarını əldə etmək üçün müxtəlif manipulyasiya texnikalarından istifadə edir. Bu, sosial mühəndisliyin effektivliyini artıran əsas faktorlardan biridir.

5. Davranışları dəyişdirmək

Holistik yanaşmanın son tərkib hissəsi davranışları dəyişdirməkdir. Sosial mühəndislik yalnız məlumatları əldə etməklə kifayətlənmir; həm də qurbanın davranışını müəyyən bir şəkildə dəyişdirmək məqsədini güdür. Davranışlar arasında müəyyən bir hərəkəti yerinə yetirmək, bir sənədi imzalamaq, bir sistemə giriş təmin etmək və ya bir təhlükəsizlik tədbirini aşmaq ola bilər.

Bu tərkib hissəsi sosial mühəndisliyin qurban üzərindəki təsirini vurğulayır. Hücum edən şəxslər, qurbanın psixologiyasını manipulyasiya edərək, onun müəyyən bir davranış

göstərməsinə nail olurlar. Belə davranışlar, hücum edən şəxsin son məqsədinə çatmaq üçün vacibdir.

Holistik yanaşma sosial mühəndisliyi kompleks və çoxşaxəli bir proses kimi dəyərləndirir, burada həm insan psixologiyası, həm texnologiya, həm də manipulyasiya strategiyaları bir araya gətirilir. Etibar qazanmaq, psixoloji manipulyasiya və texnologiyanın istismarı strategiyanın əsas elementlərini təşkil edir. Hücum edən şəxslər qurbanların emosional zəifliklərini və təhlükəsizlik sistemlərindəki boşluqları aşkar edərək hədəflərinə çatmağa çalışırlar. Buna görə də, sosial mühəndisliklə mübarizə aparmaq üçün həm fərdi, həm də təşkilati səviyyədə güclü təhlükəsizlik tədbirləri və maarifləndirmə proqramları həyata keçirilməlidir. Holistik yanaşmanın dərk edilməsi, kibertəhlükəsizlik sahəsində daha effektiv müdafiə mexanizmlərinin inkişafına töhfə verir.

Sosial mühəndisliyin mahiyyəti

Sosial mühəndislik, informasiya təhlükəsizliyi kontekstində ən mürəkkəb və təsirli manipulyasiya üsullarından biri hesab olunur. Sosial mühəndislik təkcə kibercinayətkarlar tərəfindən deyil, həm də hüquq-mühafizə orqanları, təhlükəsizlik ekspertləri və hətta biznes sahəsində müştəri münasibətlərinin idarə edilməsi üçün istifadə olunur.

Bu metodun əsas mahiyyəti insan faktorunun zəifliyindən maksimum dərəcədə istifadə edərək onu kibertəhlükəsizlik sistemlərində açıq qapı kimi görməkdir. Çox vaxt insanları texnoloji sistemlərdən daha asan aldatmaq mümkündür, çünki insanlar emosional reaksiyalara meyillidirlər, tez-tez qorxu, maraq, tələsiklik və ya inam hisslərinə əsaslanaraq qərarlar qəbul edirlər. Sosial mühəndislik manipulyasiyası adətən iki əsas elementdən ibarətdir: etibarın əldə edilməsi və emosional manipulyasiya[7].

1. Etibarın əldə edilməsi

Sosial mühəndislik hücumlarının effektiv olması üçün ilk və ən vacib addımlardan biri etibarın əldə edilməsidir. Hücum edən şəxs qurbanı manipulyasiya edə bilməsi üçün əvvəlcə onun inamını qazanması lazımdır. İnsanlar adətən tanıdıqları, etibar etdikləri və ya qanuni görünən mənbələrdən gələn sorğulara daha müsbət yanaşırlar. Buna görə də, sosial mühəndislər özlərini qurbanın tanıdığı və ya hörmət etdiyi bir şəxs və ya qurum kimi təqdim edirlər.

Etibarın əldə edilməsi üçün istifadə olunan üsullar:

- **Mənbənin legitim görünməsi -** hücum edən şəxslər özlərini tanınmış şirkətlərin, dövlət qurumlarının, hüquq-mühafizə orqanlarının və ya iş yoldaşlarının nümayəndəsi kimi qələmə verə bilərlər. Məsələn, bir sosial mühəndis hücumçusu özünü bank işçisi kimi təqdim edərək müştəridən onun kart məlumatlarını tələb edə bilər.
- **İctimaiyyətə açıq məlumatlardan istifadə -** açıq mənbə kəşfiyyatı vasitəsilə qurban haqqında toplanan məlumatlar etibar yaratmaq üçün istifadə olunur. Məsələn,

[7] Sosial mühədislik nədir? / Qlobal internetin təhlükəsizliyi - Emin Muhammadi

hücum edən şəxs qurbanın sosial media hesablarından onun maraq dairəsini və peşəkar fəaliyyətini öyrənərək, onunla eyni mövzularda söhbət açaraq etibarını qazana bilər.

- **Təhlükəsizlik və rəsmi prosedurlardan istifadə -** hücum edən şəxslər bəzi hallarda rəsmi protokollara bənzər taktikalar istifadə edirlər. Məsələn, bir iş yerindəki sosial mühəndis hücumu zamanı hücum edən şəxs özünü İT mütəxəssisi kimi təqdim edərək işçidən şifrəsini dəyişdirməsini və ya daxili sistemlərə giriş icazəsi verməsini tələb edə bilər.

Etibarın əldə edilməsi sosial mühəndisliyin təməl sütunlarından biridir. Qurbanın şübhələnməməsi və istənilən məlumatı təqdim etməsi üçün bu mərhələnin uğurla həyata keçirilməsi vacibdir.

2. Emosional manipulyasiya

Sosial mühəndislik manipulyasiyasının ikinci əsas elementi emosional manipulyasiyadır. İnsanlar rasionallıqdan çox, emosiyalar əsasında qərar verməyə meyillidirlər. Hücum edən şəxslər bu zəiflikdən istifadə edərək qurbanları qorxu, tələsiklik, maraq, həvəs, həyəcan və ya təhdid hissi altında qərar verməyə vadar edirlər.

Emosional manipulyasiya üçün istifadə olunan texnikalar:

- **Qorxu və tələş yaratmaq -** Qurbanın təcili qərar qəbul etməsini təmin etmək üçün hücum edən şəxslər onu həyəcanlandıran və ya qorxudan ssenarilər yaradırlar. Məsələn, "Bank hesabınızdan şübhəli əməliyyat aşkar olundu, dərhal şifrənizi yeniləyin" kimi mesajlarla qurbanın panikaya düşməsi və tələsik hərəkət etməsi təmin edilir.
- **Təcili hərəkətə sövq etmək -** hücum edən şəxslər qurbanın düşünmək üçün kifayət qədər vaxtının olmamasını istəyirlər. Məsələn, bir fişinq hücumu zamanı "Əgər 24 saat ərzində hesabınızı təsdiqləməsəniz, bağlanacaq" kimi mesajlar istifadə edilə bilər.
- **Maraq və cazibə yaratmaq -** İnsanlar maraq və ya mükafat vəd edən mesajlara qarşı həssasdırlar. Məsələn, "Siz lotereyada qalib gəldiniz! Mükafatınızı almaq üçün buraya klikləyin" kimi mesajlar emosional manipulyasiyanın bir formasıdır.
- **Sosial təzyiq və iyerarxiyadan istifadə etmək -** hücum edən şəxslər qurbanı müəyyən hərəkətləri yerinə yetirməyə məcbur etmək üçün sosial təzyiqdən istifadə edə bilərlər. Məsələn, bir iş yerində rəhbərlik adından gələn bir e-poçtla işçilərə yeni təhlükəsizlik qaydalarına uyğun şifrələrini dəyişdirmələri və ya linkə daxil olmaları tələb oluna bilər.

Etibarın əldə edilməsi və emosional manipulyasiya sosial mühəndisliyin iki əsas sütunudur. Hücum edən şəxslər əvvəlcə qurbanın inamını qazanaraq onu rahat hiss etdirirlər və daha sonra emosional manipulyasiya üsulları ilə onu tez qərar verməyə məcbur edirlər. Bu kombinasiyanın effektivliyi, insanların psixoloji və sosial davranışlarını düzgün analiz etmək və onları istənilən formada yönləndirmək qabiliyyətindən asılıdır. Buna görə də sosial mühəndislik hücumlarına qarşı mübarizə aparmaq üçün şəxslər və təşkilatlar bu texnikaları anlamalı və onların təsirinə düşməmək üçün təhlükəsizlik tədbirlərini gücləndirməlidirlər.

Sosial mühəndisliyin yaranma tarixi

Sosial mühəndislik anlayışı, insanları manipulyasiya etməklə informasiya əldə etməyə əsaslanan bir yanaşmadır və bu metodun tarixi qədim dövrlərə qədər uzanır. İnsanlar tarix boyu başqalarını aldatmaq, etibar qazanmaq və gizli məlumatları əldə etmək üçün müxtəlif üsullardan istifadə ediblər. Müasir sosial mühəndislik isə texnologiyanın inkişafı ilə yeni ölçülər qazanmış və kibertəhlükəsizlik sahəsində əsas risklərdən birinə çevrilmişdir. Texnikalar təkcə şəxsləri deyil, böyük korporasiyaları və dövlət qurumlarını da hədəf alaraq təhlükəsizlik sistemlərinə ciddi təsir göstərə bilər.

Sosial mühəndislik anlayışı zamanla inkişaf edərək müxtəlif formalar almışdır. Tarix boyu insanlar etibar qazanmaq və məlumat əldə etmək üçün manipulyasiya üsullarından istifadə ediblər. Erkən dövrlərdə bu üsullar daha çox sosial və psixoloji manipulyasiyaya əsaslanırdı. XX əsrdə texnologiyanın inkişafı ilə birlikdə telefon və elektron fırıldaqçılıq metodları ortaya çıxdı. 1990-cı illərdə internetin sürətli yayılması sosial mühəndislik hücumlarının daha geniş miqyasda həyata keçirilməsinə imkan yaratdı. 2000-ci illərdə sosial medianın populyarlaşması ilə hədəflənmiş hücumlar artdı və şəxslərin onlayn izləri sosial mühəndislər üçün dəyərli resurslara çevrildi. Müasir dövrdə isə süni intellekt və “deepfake” texnologiyalarının tətbiqi bu hücumları daha mürəkkəb və təhlükəli hala gətirmişdir.

1. **Erkən dövr: sosial manipulyasiyanın tarixi kökənləri:** Sosial mühəndislik ilk dəfə texnologiyadan asılı olmadan tətbiq edilən manipulyasiya texnikalarına əsaslanırdı. Tarixin müxtəlif dövrlərində fırıldaqçılar, casuslar və dələduzlar insanların emosional zəifliklərindən istifadə edərək onları manipulyasiya etmişlər.

- **Qədim Misir və Roma:** Qədim dövrlərdə krallar, sərkərdələr və hökmdarlar informasiya əldə etmək üçün casuslardan istifadə edirdilər. Bu casuslar düşmən əsgərləri və saray adamları arasında etibar qazanaraq strateji məlumatları toplayırdılar.
- **Orta əsrlərdə casusluq və sui-qəsd:** Orta əsrlərdə siyasi intriqalar və casusluq sistemləri geniş yayılmışdı. Hökmdarlar düşmənlərini aldadaraq və ya onların yaxın adamlarını manipulyasiya edərək informasiya əldə edirdilər.
- **Dini manipulyasiya:** Tarixin müxtəlif dövrlərində dini liderlər, təriqətlər və ya sektalar insanları manipulyasiya edərək onların inanc sistemlərini və davranışlarını dəyişdirməyə çalışmışdır.

Bu erkən dövr nümunələri göstərir ki, sosial mühəndislik yalnız texnologiya ilə məhdudlaşmır, əksinə insan təbiətinin bir hissəsi kimi uzun müddət istifadə edilən bir konsepsiyadır.

2. **20-ci əsr: telefon və elektron fırıldaqçılığın yüksəlişi:** 1960-cı illərdə telefon fırıldaqçılığı sosial mühəndisliyin erkən texnoloji tətbiqlərindən biri oldu. "Phone phreakers" adlanan şəxslər, telefon şəbəkələrinin zəifliklərindən istifadə edərək pulsuz zənglər etməyə və sistemlərə müdaxilə etməyə çalışırdılar.

- **John Draper (Captain Crunch):** John Draper adlı məşhur "phone phreaker" xüsusi səs tonlarından istifadə edərək telefon sistemlərini aldada bilirdi. O, "Captain Crunch" ləqəbini, istifadə etdiyi fırıldaqçılıq metodlarından biri olan - "Captain Crunch"

dənli səhər yeməyi qutusundan çıxan fitin 2600 Hz tezliyində səs çıxarma xüsusiyyətinə görə götürmüşdür.[8]

3. **1980-ci illər: Kevin Mitnick və sosial mühəndislik metodlarının təkamülü:** 1980-ci illərdə sosial mühəndislik texnikaları daha mürəkkəb və məqsədyönlü şəkildə istifadə olunmağa başladı. Xüsusilə Kevin Mitnick kimi hackerlər, insanların zəifliklərindən istifadə edərək təhlükəsizlik sistemlərinə müdaxilə etməyə başladılar.

- **Kevin Mitnick:** O, telefon operatorlarını, şirkət işçilərini və hətta təhlükəsizlik mütəxəssislərini manipulyasiya edərək konfidensial məlumatları əldə etməyi bacarırdı. Mitnick-in sosial mühəndislik texnikaları arasında uydurma şəxsiyyətlərdən istifadə etmək, şirkətlərin daxili məlumatlarını telefon zəngləri ilə toplamaq və işçiləri şübhələndirmədən təhlükəsizlik sistemlərini aşmaq var idi[9].
- **IBM və AT&T hücumları:** Mitnick, IBM və AT&T kimi nəhəng texnologiya şirkətlərinin sistemlərinə uğurla sızaraq onların məxfi sənədlərini ələ keçirmişdir[10].

4. **1990-cı illər: İnternetin yüksəlişi və sosial mühəndislik hücumlarının artması:** 1990-cı illərdə internetin geniş yayılması ilə sosial mühəndislik metodları daha geniş kütlələrə təsir etməyə başladı. İnternet vasitəsilə məlumatın asanlıqla əldə edilməsi, hakerlərə və fırıldaqçılara yeni imkanlar yaratdı.

- **Phishing hücumlarının başlanğıcı:** İnternet vasitəsilə göndərilən saxta e-poçtlar və veb-saytlar insanların bank hesablarına, şəxsi məlumatlarına və hətta hökumət sistemlərinə sızmaq üçün istifadə olunmağa başladı.
- **Morris Worm (1988):** Robert Morris tərəfindən yazılan ilk kompüter qurd virusu, internetin ilk geniş miqyaslı təhlükəsizlik hadisələrindən biri kimi tarixə düşdü. Bu virus, kompüterlər arasında sürətlə yayılaraq sistemlərə ciddi ziyan vurdu və internetin təhlükəsizlik zəifliklərini aşkar etdi[11].

5. **2000-ci illər: sosial mediyanın yüksəlişi və hədəflənmiş hücumlar:** 2000-ci illərdə sosial media platformalarının populyarlığının artması ilə sosial mühəndislik hücumları yeni bir səviyyəyə çatdı. İnsanlar öz şəxsi həyatları ilə bağlı məlumatları sosial mediada daha çox paylaşdıqca, hakerlər və fırıldaqçılar bu məlumatlardan istifadə edərək daha hədəflənmiş hücumlar həyata keçirməyə başladılar.

- **"Facebook", "LinkedIn" və "X" (red.-Twitter) üzərindən sosial mühəndislik:** Hakerlər qurbanların sosial media hesablarını araşdıraraq onların maraq dairələrini, dostlarını və iş yoldaşlarını təyin edərək saxta dostluq təklifləri və ya phishing hücumları ilə onları manipulyasiya edirdilər[12].
- **"Advanced persistent threats" (APT):** 2000-ci illərdə təşkilatlara qarşı uzunmüddətli və kompleks sosial mühəndislik hücumları (APT hücumları) artmağa başladı. Bu hücumlar, əsasən dövlət və korporativ şəbəkələrə qarşı həyata keçirilirdi[13].

[8] Hall of fame: Captain Crunch - Jochen Kressin
[9] Kevin Mitnick - en.wikipedia.org/wiki/Kevin_Mitnick
[10] Top 10 best and most famous hackers in the world - Ellis Steward
[11] YouTube - The first internet worm (Morris Worm) - Computerphile
[12] Sosial şəbəkələrdə təhlükəsizlik problemlər - Şıxəliyev R.H.
[13] Advanced persistent threats (qabaqcıl davamlı təhdid qrupları) - cert.az/news/2024/etx-advanced-persistent-threats

6. **Müasir dövrdə sosial mühəndislik: "AI" və "Deepfake" texnologiyalarının tətbiqi:** Son illərdə süni intellekt (AI) və deepfake texnologiyalarının inkişafı sosial mühəndislik texnikalarının daha təhlükəli hala gəlməsinə səbəb olub.

- **Deepfake və vishing:** Səs və video manipulyasiya texnologiyaları sayəsində hakerlər real şəxslərin səsini və görüntüsünü təqlid edərək qurumlara və şəxslərə qarşı hücumlar təşkil edirlər[14].
- **Korporativ hədəflənmiş hücumlar:** Müasir dövrdə sosial mühəndislik hücumları yalnız şəxslərə qarşı deyil, həm də iri şirkətlərə qarşı həyata keçirilir. CEO fraud, Business Email Compromise (BEC) və digər metodlar maliyyə fırıldaqları üçün geniş istifadə edilir[15].

Sosial mühəndislik tarix boyu müxtəlif formalarda mövcud olmuş və texnologiyanın inkişafı ilə paralel şəkildə təkamül etmişdir. Qədim dövrlərdən başlayaraq, telefon və internet dövrünə qədər bu metodun əsas prinsipləri dəyişməz qalmış, lakin tətbiq sahələri və üsulları zamanla mürəkkəbləşmişdir. Müasir dövrdə süni intellekt və avtomatlaşdırılmış sistemlər sosial mühəndislik hücumlarını daha da təhlükəli hala gətirir.

Sosial mühəndisliyin cəmiyyətdə təsiri

Sosial mühəndislik texnikalarının cəmiyyətə təsiri son illərdə daha da güclənmişdir. İnformasiya texnologiyalarının inkişafı və rəqəmsal platformaların geniş yayılması sosial mühəndisliyin tətbiq sahələrini artırmış, bu metodun effektivliyini daha da artırmışdır. Müasir dövrdə sosial mühəndislik yalnız şəxslərə deyil, həm də təşkilatlara, dövlət qurumlarına və hətta bütöv cəmiyyətlərə təsir göstərir. Təsir həm şəxsi təhlükəsizlik, həm də milli təhlükəsizlik baxımından ciddi narahatlıq doğurur.

Sosial mühəndisliyin cəmiyyətə təsirini üç əsas istiqamət üzrə təhlil etmək mümkündür:

1. **Fərdi səviyyədə sosial mühəndisliyin təsiri**

Fərdi istifadəçilər sosial mühəndisliyin ən çox hədəfə alınan qrupudur. Hücum edən şəxslər, insanların şəxsi (fərdi) məlumatlarını əldə etmək, onların davranışlarını manipulyasiya etmək və maliyyə fırıldaqçılığı həyata keçirmək üçün müxtəlif texnikalardan istifadə edirlər.

2. **Təşkilatlar və şirkətlər üzərində sosial mühəndisliyin təsiri**

Sosial mühəndislik təkcə fərdi istifadəçiləri deyil, eyni zamanda biznes sektorunu və iri korporasiyaları da ciddi şəkildə hədəfə alır. Təşkilatlar, texniki müdafiə tədbirlərini gücləndirsə də, insan faktorunu istismar edən sosial mühəndislik hücumları hələ də effektiv olaraq qalır.

3. **Sosial mühəndisliyin milli təhlükəsizlik və siyasi manipulyasiya vasitəsi kimi istifadəsi**

[14] Finance worker pays out $25 million after video call with deepfake 'chief financial officer' - Heather Chen, Kathleen Magramo

[15] Business email compromise (BEC) nedir? BEC saldırıları nasıl engellenir? - uzmanposta.com/blog/bec/

Müasir dövrdə sosial mühəndislik texnikaları milli təhlükəsizlik üçün ciddi təhdid yaradır. Xüsusilə kiber müharibə və informasiya müharibəsi çərçivəsində bu metoddan geniş istifadə olunur. Dövlətlər, korporativ casusluq, siyasi manipulyasiya və kütləvi ictimai rəyin formalaşdırılması üçün sosial mühəndislik texnikalarından faydalanırlar.

Sosial mühəndislik texnikaları cəmiyyətin bütün səviyyələrinə təsir edərək şəxslərin, təşkilatların və dövlətlərin təhlükəsizliyini risk altına qoyur. Bu metodların inkişafı və genişlənməsi kibertəhlükəsizlik sistemlərinin yalnız texniki həllərlə məhdudlaşmamalı olduğunu, insan faktorunun qorunmasının vacibliyini göstərir. Xüsusilə fərdi məlumatların oğurlanması, şirkətlərin daxili sistemlərinə müdaxilə və milli təhlükəsizliyə təhdid yaradan informasiya manipulyasiyası bu sahənin nəzarət və müdafiə tədbirlərinin gücləndirilməsini zəruri edir. Sosial mühəndisliyin təsirlərini minimuma endirmək üçün həm fərdi, həm də ictimai səviyyədə maarifləndirmə, kibertəhlükəsizlik tədbirlərinin təkmilləşdirilməsi və hüquqi çərçivələrin gücləndirilməsi vacibdir.

Gələcəkdə texnologiyaların inkişafı ilə bu metodların daha mürəkkəb formalarının ortaya çıxacağı gözlənilir və buna qarşı effektiv müdafiə strategiyalarının yaradılması cəmiyyətin informasiya təhlükəsizliyini qorumaq üçün mühüm rol oynayacaqdır.

Nəticə

Sosial mühəndislik, informasiya təhlükəsizliyi sahəsində ən mürəkkəb və təsirli manipulyasiya metodlarından biridir. Onun əsas mahiyyəti insan psixologiyasından və sosial qarşılıqlı əlaqələrdən istifadə edərək məlumatların əldə edilməsinə yönəlib. Bu metodun təhlükəli tərəfi ondan ibarətdir ki, texnoloji müdafiə sistemləri nə qədər inkişaf etsə də, insan faktorundan istifadə etməklə onları aşmaq mümkündür. Hücum edən şəxslər yalnız şəxslərə deyil, təşkilatlara və hətta dövlətlərə qarşı da bu metoddan geniş şəkildə istifadə edirlər. Onlar hədəflərinin zəif cəhətlərini araşdıraraq psixoloji və emosional reaksiyalardan faydalanaraq manipulyasiya edirlər. Bu manipulyasiya üsulları arasında “phishing”, “spear phishing”, “pretexting”, “doxxing” və digər texnikalar xüsusi yer tutur. Hücum edən şəxslər əsasən qurbanın diqqətini yayındırmaq, onu tələsik qərar verməyə vadar etmək və bu prosesdə şəxsi məlumatlarını açıqlamasına nail olmaq üçün müxtəlif üsullardan istifadə edirlər.

Sosial mühəndisliyin tarixi qədim dövrlərə dayanır, lakin texnologiyanın inkişafı ilə onun yeni və daha təhlükəli formaları meydana çıxmışdır. Qədim zamanlardan etibarən insanlar müxtəlif manipulyasiya üsulları ilə başqalarını aldatmağa çalışırdılar. Lakin 20-ci əsrdə telefon fırıldaqçılığı və sosial manipulyasiya metodları daha geniş yayılmağa başladı. 1980-ci illərdə Kevin Mitnick kimi hakerlər sosial mühəndisliyin gücünü artıraraq bu metodun kibercinayətkarlıqda nə qədər effektiv olduğunu sübut etdilər. 1990-cı illərdə internetin inkişafı ilə sosial mühəndislik hücumlarının miqyası genişləndi və daha mürəkkəb formalar aldı.

Müasir dövrdə sosial mühəndislik hücumları süni intellekt və “deepfake” texnologiyalarının inkişafı ilə daha təhlükəli hala gəlmişdir. Hücum edən şəxslər “deepfake” vasitəsilə real şəxslərin səsini və görüntüsünü təqlid edərək, qurumları və

şəxsləri aldatmağa nail olurlar. Xüsusilə, bu texnologiyalar bank dələduzluqları, siyasi manipulyasiya və hətta dövlət səviyyəsində casusluq üçün istifadə edilə bilər. Bundan əlavə, sosial media platformaları və media vasitəsilə ictimai rəyə təsir göstərmək və dezinformasiya yaymaq sosial mühəndisliyin ən mürəkkəb formalarındandır. Bu cür manipulyasiya texnikaları, informasiya müharibələrinin və kibermünaqişələrin əsas silahına çevrilmişdir.

Sosial mühəndislik hücumlarının qarşısını almaq üçün təkcə texnoloji tədbirlər yetərli deyil, eyni zamanda şəxslərin və təşkilatların məlumatlılığı artırılmalı, insan faktoru zəifliklərə qarşı davamlı olmalıdır. Kibertəhlükəsizlik təlimləri, şəxsi və təşkilati təhlükəsizlik protokolları və hüquqi tənzimləmələr bu cür hücumlarla mübarizədə mühüm rol oynayır.

Eyni zamanda, dövlətlər və beynəlxalq təşkilatlar sosial mühəndislik hücumlarının təsirini minimuma endirmək üçün kibertəhlükəsizlik üzrə qanunvericiliyi və beynəlxalq əməkdaşlığı gücləndirməlidirlər. Sosial mühəndislik hücumlarına qarşı qlobal səviyyədə koordinasiyalı fəaliyyət planı hazırlanmalıdır. Təşkilatlar və dövlətlər rəqəmsal maarifləndirmə proqramlarını genişləndirməli, fərdləri və işçiləri kiber təhlükələrə qarşı hazırlamalıdırlar.

Gələcəkdə sosial mühəndislik hücumlarının daha mürəkkəb və daha çətin aşkarlanan formalarının yaranacağı gözlənilir. Xüsusilə, süni intellektin inkişafı və avtomatlaşdırılmış manipulyasiya texnologiyalarının ortaya çıxması sosial mühəndislik hücumlarının daha genişmiqyaslı və daha effektiv hala gəlməsinə səbəb ola bilər. Bu səbəbdən, təşkilatlar və dövlətlər sosial mühəndislik texnikalarına qarşı mübarizədə daha çevik və innovativ yanaşmalar inkişaf etdirməlidirlər. İnformasiya təhlükəsizliyinin gücləndirilməsi, kibertəhlükəsizlik mədəniyyətinin formalaşdırılması və insan faktorunun qorunması sosial mühəndislik hücumlarına qarşı ən effektiv müdafiə vasitələrindən biri olacaqdır.

Nəticə olaraq, sosial mühəndislik texnikaları təkcə texniki biliklərə deyil, həm də psixoloji manipulyasiyaya əsaslandığından, onunla mübarizə yalnız texnoloji həllərlə məhdudlaşmamalıdır. İnsanların maarifləndirilməsi, etik standartların gücləndirilməsi və kibertəhlükəsizlik tədbirlərinin genişləndirilməsi bu hücumların təsirini azaltmaq üçün vacibdir. Hər bir fərd və təşkilat sosial mühəndislik hücumlarına qarşı diqqətli olmalı, açıq məlumatlarını minimuma endirməli və kiberfırıldaqçılara qarşı ayıq davranmalıdır. Yalnız bu yolla sosial mühəndislik hücumlarının təsirini azalda və informasiya təhlükəsizliyini qoruya bilərik.

§ 2. Sosial mühəndislik hücumlarının təsnifatı və növləri.

Giriş

Sosial mühəndislik hücumları, insanların zəifliklərindən istifadə edərək, onların fərdi məlumatlarını əldə etmək və ya müəyyən davranışlara sövq etmək məqsədilə tətbiq olunan metodların geniş spektrini əhatə edir. Bu hücumlar yalnız şəxsləri deyil, həm də korporativ və dövlət səviyyəsində qurumları hədəf alır. Hücum edən şəxslər insan psixologiyasını, sosial dinamikaları və texnoloji platformaları manipulyasiya edərək, şəxsləri və təşkilatları aldatmağa çalışırlar. Texnikalar sosial media, elektron poçt, telefon zəngləri və hətta fiziki qarşılıqlı əlaqələr vasitəsilə həyata keçirilə bilər.

İnsanların məlumatlara qarşı laqeydliyi, sürətli qərar vermə meyli, sosial norma və qaydalara riayət etmə vərdişləri bu hücumların uğurlu olmasına səbəb ola bilər. Buna görə də, sosial mühəndislik hücumlarının müxtəlif aspektlərini öyrənmək və onların təsnifatını anlamaq, kibertəhlükəsizlik baxımından olduqca vacibdir.

Müasir dövrdə sosial mühəndislik hücumlarının təsnifatı və növlərini anlamaq, həm şəxsi təhlükəsizlik, həm də təşkilatların müdafiə tədbirləri baxımından olduqca əhəmiyyətlidir. Texnologiyanın inkişafı ilə bu hücumlar daha da mürəkkəbləşmiş və təsir dairəsi genişləmişdir. Müxtəlif sosial mühəndislik hücumları fərqli hədəf auditoriyalara, fərqli taktikalara və müxtəlif hücum vektorlarına əsaslanır. Məsələn, bəzi hücumlar sosial mediada istifadəçiləri aldatmaq üçün aparılırsa, digərləri dövlət qurumlarının və korporasiyaların daxili sistemlərinə sızmaq məqsədilə həyata keçirilə bilər.

Sosial mühəndislik hücumları ümumiyyətlə iki əsas kateqoriyaya bölünür: insan əsaslı və texnologiya əsaslı hücumlar. İnsan əsaslı hücumlar birbaşa insanlarla qarşılıqlı əlaqə qurmağa yönəlmiş taktikaları əhatə edir, məsələn, “pretexting” və ya “tailgating”. Texnologiya əsaslı hücumlar isə elektron poçt, sosial media və digər rəqəmsal platformalar vasitəsilə həyata keçirilən hücumları əhatə edir, məsələn, “phishing” və “vishing”.

Sosial mühəndislik hücumlarının təsnifatı və onların xüsusiyyətlərini təhlil edərək, bu hücumların necə fəaliyyət göstərdiyini və hansı şəraitdə daha effektiv olduğunu anlamaq mümkündür. Bu, eyni zamanda, şəxslərin və təşkilatların bu cür hücumlara qarşı daha yaxşı qorunmasını təmin etmək üçün vacib bir addımdır. Hücum növlərinin detallı öyrənilməsi onların qarşısının alınması və profilaktik tədbirlərin effektivliyinin artırılmasına kömək edəcəkdir.

Bu mühazirədə sosial mühəndislik hücumlarının əsas növləri və təsnifatı geniş şəkildə təhlil ediləcək, onların fərqli xüsusiyyətləri və tətbiq metodları izah ediləcəkdir. Məqsəd sosial mühəndisliyin təhlükələrini və bu hücumların qarşısının alınması üçün ən yaxşı təcrübələri təqdim etməkdir.

Hücumların təsnifatı

Sosial mühəndislik hücumlarının təsnifatı onların tətbiq sahələri, istifadə olunan metodologiyalar və məqsədlərinə görə qruplaşdırılması deməkdir. Bu təsnifat, belə hücumların təbiətini daha yaxşı başa düşmək və onlara qarşı təsirli müdafiə tədbirlərini müəyyən etmək üçün vacibdir. Hücumların təsnif edilməsi, həm fərdi, həm də təşkilati səviyyədə potensial risklərin dəyərləndirilməsi üçün nəzəri və praktiki əsaslar yaradır. Yanaşma yalnız sosial mühəndisliyin çoxşaxəli təbiətini dərk etməyə deyil, həm də müxtəlif təhlükəsizlik səviyyələrində bu cür hücumların effektiv idarə olunmasına imkan verir.

Təsnifatın məqsədi, sosial mühəndislik hücumlarının müxtəlif növlərini sistematik şəkildə izah etməklə yanaşı, onların tətbiq sahələri və təhdid modellərini aydınlaşdırmaqdır. Hücumların fərqli xüsusiyyətlərinin müəyyən edilməsi, onların dərin öyrənilməsi və təsirlərinin qiymətləndirilməsi həm fərdi istifadəçilər, həm də təşkilatlar üçün daha güclü müdafiə tədbirlərinin hazırlanmasını təmin edir.

Hücumların texniki və psixoloji aspektlərinin öyrənilməsi qurbanların davranış modellərinin, emosional zəifliklərinin və təhlükəsizlik tədbirlərinin pozulma mexanizmlərinin dərk edilməsinə yardım edir. Hücumların təsnifatında texnologiyanın manipulyasiyası, insan psixologiyasından istifadə və ya hər iki amilin birləşdirilməsi xüsusi diqqət mərkəzindədir. Bu yanaşma, hücumların mürəkkəbliyini və müxtəlif səviyyələrdə təsirlərini daha dərindən anlamağa şərait yaradır.

Hücumların təsnifatında hüquqi çərçivələr də mühüm əhəmiyyət kəsb edir. Hücumların hüquqi təsirləri, əsasən şəxsi məlumatların məxfiliyinin qorunması, kiberməkanda məxfi resurslara qanunsuz girişin qarşısının alınması və şəxsi hüquqların pozulmasının aşkar edilməsi ilə bağlı qanunvericiliklə tənzimlənir. Təşkilatların və şəxslərin hüquqları qorunmaqla yanaşı, bu çərçivələr potensial hücumların qarşısını almaq üçün normativ baza rolunu oynayır. Belə təsnifatlar həm də beynəlxalq kibertəhlükəsizlik qanunvericiliyində bir çox ölkələr tərəfindən tətbiq olunan standartların əsasını təşkil edir.

1. Texnoloji əsaslı hücumlar

Texnoloji əsaslı sosial mühəndislik hücumları, rəqəmsal mühitdə texnologiyanın manipulyasiya edilməsinə və qurbanların zəifliklərindən istifadə edilməsinə əsaslanır. Bu hücumlar, texnoloji vasitələrdən istifadə etməklə qurbanların şəxsi məlumatlarını əldə etmək, sistemlərə qanunsuz giriş təmin etmək və ya texnoloji resursları manipulyasiya etmək məqsədini güdür. Hücumlar adətən proqram təminatları, internet üzərindən yayılan aldatma üsulları, zərərli e-poçtlar və mobil cihazlar vasitəsilə həyata keçirilir. Metodlar geniş miqyaslı təsir gücünə malikdir və şəxsləri, korporasiyaları, hətta dövlət qurumlarını hədəf ala bilər.

Texnoloji əsaslı hücumlar qurbanların rəqəmsal mühitdəki davranışlarına əsaslanaraq həyata keçirilir. Hücum edən şəxslər, çox vaxt e-poçtlar, mesajlar, veb-saytlar və ya sosial media vasitəsilə qurbanlarla əlaqə qururlar. Belə hücumlar zamanı qurbanlara texniki dəstək nümayəndəsi, bank işçisi və ya tanınmış bir təşkilatın

nümayəndəsi kimi təqdim edilə bilər. Taktika, qurbanların diqqətini yayındıraraq onları məlumatlarını açıqlamağa və ya müəyyən zərərli hərəkətləri yerinə yetirməyə sövq edir.

Texnoloji əsaslı hücumların əsas məqsədi şəxsi və ya korporativ məlumatları qanunsuz ələ keçirməkdir. Məlumatlar arasında şifrələr, bank hesabları, şəxsi məlumat bazaları və ya texnoloji resurslara giriş hüquqları yer alır. Bundan əlavə, bu cür hücumlar vasitəsilə qurbanların cihazlarına zərərli proqramlar yüklənərək onların məxfi məlumatları sızdırıla bilər.

Bu hücumların tətbiq sahələri çox genişdir və müxtəlif formalarda özünü göstərə bilər:

- **"Phishing",** rəqəmsal mühitdə ən çox yayılan sosial mühəndislik hücumlarından biridir və əsasən saxta e-poçtlar və ya veb saytlar vasitəsilə həyata keçirilir. Bu hücum növündə hücum edən şəxslər qurbanların şəxsi və ya korporativ məlumatlarını qanunsuz ələ keçirmək üçün etibar yaratmağa çalışır. Onlar adətən tanınmış bir təşkilatın adından saxta bir e-poçt göndərir, bu e-poçtda qurbanın təhlükəsizlik səbəbilə dərhal tədbir görməsini tələb edirlər. Tədbirlər arasında şəxsi məlumatların təsdiqi, şifrənin yenilənməsi və ya bank hesablarına giriş yer ala bilər[16].

"Phishing" hücumlarında əsas məqsəd qurbanın diqqətini yayındıraraq onu saxta bir veb-sayta yönləndirməkdir. Veb-sayt, vizual olaraq orijinal bir təşkilatın saytına bənzəyir, lakin məlumatların oğurlanması üçün xüsusi hazırlanmışdır. Qurban burada fərdi məlumatlarını daxil etdikdə, bu məlumatlar birbaşa hücum edən şəxslərin əlində olur. Hücum edən şəxslər, əldə etdikləri bu məlumatlarla qurbanın maliyyə resurslarına giriş əldə edə, şəxsi hesablarını ələ keçirə və ya daha genişmiqyaslı hücumlar üçün istifadə edə bilərlər.

Bu hücum növü xüsusilə maliyyə qurumlarına, onlayn ticarət platformalarına və sosial media hesablarına qarşı tətbiq olunur. Hücum edən şəxslərin əsas taktikası qurbanı emosional vəziyyətə salmaqdır. Onlar təcili təhlükə, itki və ya cəza kimi mövzuları vurğulamaqla qurbanları sürətli və düşünülməmiş qərarlar verməyə sövq edirlər. Məsələn, bir bankın adından gələn saxta e-poçt, qurbanın hesabının dondurulduğunu iddia edə bilər və qurbanı bu problemi həll etmək üçün müəyyən bir bağlantıya klikləməyə məcbur edər.

"Phishing" hücumları yalnız şəxsləri deyil, həm də korporativ təşkilatları hədəfə alır. Təşkilatlar üzərində edilən hücumlar zamanı işçilərdən məxfi məlumatların təqdim edilməsi tələb olunur və ya onların kompüterlərinə zərərli proqram yüklənməsi üçün aldatıcı bağlantılar göndərilir. Bu kimi hallar, təşkilatların təhlükəsizlik sistemlərinə icazəsiz giriş imkanı yaradır və nəticədə böyük maliyyə itkilərinə və məlumat sızmalarına səbəb ola bilər.

- **"Smishing",** mobil telefonlara göndərilən aldadıcı SMS mesajları vasitəsilə həyata keçirilən sosial mühəndislik hücumudur. Bu hücum növündə hücum edən şəxslər, qurbanları aldadaraq fərdi və ya maliyyə məlumatlarını təqdim etməyə məcbur etməyi

[16] Phishing (oltalama) nedir? Phishing saldırısı nasıl engellenir? - uzmanposta.com/blog/phishing-nedir/

hədəfləyirlər. “Smishing” termini "SMS" və "phishing" sözlərinin birləşməsindən yaranıb və əsasən qurbanın diqqətini yayındıraraq onu manipulyasiya etməyə yönəlib[17].

Bu cür hücumlarda qurbanlara göndərilən mesajlar adətən tanınmış qurumların adından gəlmiş kimi göstərilir. Mesajlarda qurbanın dərhal hərəkət etməsini tələb edən ifadələr yer alır. Məsələn, "hesabınız bloklanıb, yenidən aktivləşdirmək üçün bu bağlantıya klikləyin" və ya "təcili ödəniş tələb olunur, əks halda xidmətiniz dayandırılacaq" kimi mətnlər daxil edilir.

“Smishing” hücumlarında təqdim edilən bağlantılar qurbanı saxta bir veb-sayta yönləndirir. Saytlar, qurbanın fərdi məlumatlarını daxil etməsi üçün hazırlanmışdır. Qurban məlumatları daxil etdikdən sonra, məlumatlar birbaşa hücum edən şəxslərin nəzarətinə keçir. hücum edən şəxslər məlumatlardan maliyyə əməliyyatları aparmaq, qurbanın bank hesabını boşaltmaq və ya onun şəxsiyyətini təqlid etmək üçün istifadə edə bilərlər.

“Smishing”in başqa bir forması zərərli proqramların yayılmasıdır. Mesajlarda təqdim edilən bağlantıya kliklədikdə qurbanın telefonuna zərərli proqram yüklənir. Bu proqramlar vasitəsilə hücum edən şəxslər qurbanın cihazını nəzarət altına ala bilər, onun fərdi məlumatlarına və hətta telefon danışıqlarına giriş əldə edə bilərlər.

Hücumun nəticələri həm şəxslər, həm də təşkilatlar üçün ciddi problemlər yaradır. Şəxslər üçün bu, maliyyə itkiləri, fərdi məlumatların sızması və hüquqi çətinliklərlə nəticələnə bilər. Təşkilatlar üçün isə “smishing”, işçilər vasitəsilə daxili sistemlərə icazəsiz giriş təmin edərək məlumat sızmalarına və reputasiya zədələnməsinə səbəb ola bilər.

- **“Spear phishing”,** adi phishing hücumlarından fərqli olaraq, fərdiləşdirilmiş və müəyyən bir şəxsi və ya qurumu hədəf alan bir hücum növüdür. Bu hücumda hücum edən şəxslər, qurbanın fərdi məlumatlarını toplayaraq, daha etibarlı görünən və məqsədli saxta e-poçtlar və ya mesajlar hazırlayırlar[18].

“Spear phishing” hücumları adətən yüksək vəzifəli şəxslərə, təşkilat rəhbərlərinə və ya korporativ sistemlərə giriş hüququ olan işçilərə yönəlir. Mesajlar çox vaxt qurbanın adını, təşkilat daxilindəki mövqeyini və digər şəxsi məlumatlarını ehtiva edir ki, bu da hücumu daha etibarlı göstərir. Məsələn, hücum edən şəxs qurbanın birbaşa rəhbərinin adından saxta bir e-poçt göndərərək təcili olaraq maliyyə sənədlərinə giriş tələb edə bilər.

“Spear phishing”in təhlükəsi, onun fərdiləşdirilmiş və hədəfli olmasıdır ki, bu da adi “phishing” hücumlarına nisbətən daha yüksək uğur ehtimalı yaradır.

- **“Watering hole attack”,** müəyyən bir qrup və ya təşkilatı hədəf alan mürəkkəb bir sosial mühəndislik hücumudur. Bu hücum növündə hücum edən şəxslər, qurbanların tez-tez ziyarət etdiyi etibarlı veb-saytları müəyyən edir və həmin saytları zərərli kodlarla manipulyasiya edirlər. Qurbanlar zərərli veb-saytlara daxil olduqda, onların cihazlarına avtomatik olaraq zərərli proqram yüklənir və ya fərdi məlumatları oğurlanır[19].

---

[17] Smishing nedir ve nasıl korunulur? - www.kaspersky.com.tr/resource-center/threats/what-is-smishing-and-how-to-defend-against-it

[18] What is spear phishing? - Matthew Kosinski

[19] What is a watering hole attack? - www.fortinet.com/resources/cyberglossary/watering-hole-attack

Hücumun adı, vəhşi heyvanların su mənbələrinə getdiyi yerləri pusquda gözləyən yırtıcılarla müqayisədən götürülüb. Hücum edən şəxslər, əvvəlcə hədəf qrupun hansı veb-saytlardan istifadə etdiyini araşdırır, sonra həmin saytları manipulyasiya edərək zərərli kodlar yerləşdirirlər. Zərərli kodlar qurbanın cihazına daxil olduqda, hücum edən şəxslər fərdi məlumatlara, giriş məlumatlarına və ya korporativ sistemlərə nəzarət əldə edirlər.

"Watering hole" attack hücumları çox vaxt böyük təşkilatlara, dövlət qurumlarına və ya həssas sənaye sahələrində fəaliyyət göstərən şirkətlərə qarşı həyata keçirilir. Hücumun effektivliyi qurbanların tez-tez istifadə etdiyi etibarlı veb-saytlara əsaslandığı üçün metod diqqət çəkmədən geniş miqyasda məlumat oğurluğuna səbəb ola bilər.

Bu hücum növünə qarşı müdafiə tədbirləri arasında aşağıdakılar xüsusi əhəmiyyət daşıyır:

- Zərərli proqramların qarşısını alan təhlükəsizlik proqram təminatlarından istifadə.
- Veb-saytların müntəzəm olaraq təhlükəsizlik yoxlamasından keçirilməsi.
- Qurbanların şübhəli fəaliyyətləri aşkar edə bilməsi üçün kibertəhlükəsizlik təlimlərinin keçirilməsi.

"Watering hole" attack hücumları, təhlükəsizlik sistemlərinin zəifliyindən və qurbanların etibar etdiyi veb-saytlardan sui-istifadə edərək geniş miqyaslı zərərə səbəb ola bilən ciddi bir təhdiddir. Bu səbəbdən, təşkilatlar və şəxslər bu cür hücumların qarşısını almaq üçün qabaqlayıcı tədbirlər görməlidirlər.

- **"Domain spoofing",** sosial mühəndislik hücumları arasında geniş yayılmış bir metoddur və qurbanları aldatmaq üçün saxta veb-saytların yaradılmasına əsaslanır. Bu hücumda hücum edən şəxslər tanınmış bir domenin və ya təşkilatın adını təqlid edərək, onlara çox bənzəyən saxta domenlər qeydiyyatdan keçirirlər. Məqsəd, qurbanları bu saxta domenlərə yönləndirərək onların fərdi məlumatlarını, şifrələrini və ya maliyyə detallarını ələ keçirməkdir[20].

"Domain spoofing" çox vaxt "phishing" hücumlarında istifadə edilir və adətən aşağıdakı şəkildə həyata keçirilir:

- Hücum edən şəxslər, məşhur bir təşkilatın domen adına çox bənzər bir domen adı yaradırlar. Məsələn, "google.com" əvəzinə "goggle.com" və ya "paypa1.com" (sondakı "1" hərfin əvəzinə rəqəm) kimi domenlər qeydiyyatdan keçirilir.
- Qurbanlara e-poçtlar, SMS-lər və ya sosial media mesajları vasitəsilə bu domenlərə daxil olmaq üçün çağırış edilir. Mesajlarda adətən "hesabınızı təsdiqləyin", "şifrənizi yeniləyin" və ya "təhlükəsizlik səbəbiylə daxil olun" kimi təcili hərəkət tələb edən ifadələr yer alır.
- Qurbanlar saxta domenlərə daxil olduqda, onların şəxsi məlumatları birbaşa hücum edən şəxslərin nəzarətinə keçir.

- **"Man-in-the-middle (MitM) attack",** iki tərəf arasında gedən məlumat mübadiləsinə gizli şəkildə müdaxilə edərək həmin məlumatları qanunsuz ələ keçirməyə və ya manipulyasiya etməyə əsaslanan bir hücum növüdür. Hücum edən şəxs qurban ilə

[20] Website and email spoofing - www.cloudflare.com/ru-ru/learning/ssl/what-is-domain-spoofing/

onun ünsiyyət qurduğu tərəf arasında yerləşərək ünsiyyəti nəzarət altına alır və ya dəyişdirir. Bu növ hücum, məlumatların məxfiliyini və bütövlüyünü ciddi şəkildə pozur[21].

"Man-in-the-middle" hücumlarında hücum edən şəxslər, adətən, iki əsas mərhələni yerinə yetirirlər:

- Müdaxilə: hücum edən şəxs, qurbanın cihazı ilə qarşı tərəf arasında bir bağlantı yaradır. Bu, ictimai "Wi-Fi" şəbəkələri, zəif şifrələnmiş əlaqələr və ya saxta "Wi-Fi" nöqtələri vasitəsilə edilə bilər.
- Məlumatların ələ keçirilməsi və manipulyasiya: hücum edən şəxs qurban tərəfindən göndərilən və alınan məlumatları oxuyur, dəyişdirir və ya qeyd edir. Məsələn, bir istifadəçinin bank hesabına daxil olmaq üçün təqdim etdiyi şifrələr və ya maliyyə əməliyyatları barədə məlumatlar bu yolla oğurlana bilər.

"MitM" hücumları, çox vaxt qurbanın fərdi və ya maliyyə məlumatlarının qanunsuz ələ keçirmək ilə nəticələnir. Əldə edilə bilən məlumatlar arasında şifrələr, bank hesab detalları, onlayn ödəmə platformalarına giriş məlumatları və hətta məxfi korporativ məlumatlar yer alır.

"Man-in-the-middle" hücumları müxtəlif sahələrdə həyata keçirilə bilər:

- İctimai "Wi-Fi" şəbəkələri: Hücum edən şəxslər zəif qorunan "Wi-Fi" şəbəkələrindən istifadə edərək məlumat mübadiləsini ələ keçirirlər.
- Saxta "HTTPS" sertifikatları: Hücum edən şəxs istifadəçini təhlükəsiz görünən, lakin zərərli bir veb-sayta yönləndirərək onun məlumatlarını oğurlaya bilər.
- Zəif Şifrələmə Sistemləri: Məlumat mübadiləsində istifadə olunan zəif şifrələmə protokolları hücumun uğurla həyata keçirilməsinə şərait yaradır.

- **"Credential stuffing",** sosial mühəndislik hücumlarının bir növüdür və əvvəllər sızdırılmış istifadəçi adı və şifrələrin avtomatik olaraq bir neçə onlayn platformada yoxlanılmasına əsaslanır. Bu hücum növü, şəxslərin eyni şifrələri bir neçə müxtəlif hesabda istifadə etməsi zəifliyindən faydalanır. Hücum edən şəxslər, bir platformadan əldə edilən giriş məlumatlarını digər platformalarda sınaqdan keçirərək, qurbanın müxtəlif hesablarına qanunsuz giriş əldə etməyə çalışırlar[22].

2. Psixoloji əsaslı hücumlar

Psixoloji əsaslı hücumlar, insanın emosional və psixoloji zəifliklərindən istifadə edərək həyata keçirilən sosial mühəndislik hücumlarıdır. Bu hücum növündə əsas məqsəd, qurbanın qərar qəbul etmə qabiliyyətini təsir altına almaq, onu manipulyasiya edərək müəyyən məlumatları açıqlamağa və ya təhlükəsizlik qaydalarını pozmağa sövq etməkdir. Hücum edən şəxslər insanın təbii davranışlarını və emosional reaksiyalarını analiz edərək onları istismar edir və bu manipulyasiya prosesində müxtəlif taktikalar tətbiq olunur.

Psixoloji əsaslı hücumlar, adətən aşağıdakı metodlarla həyata keçirilir:

[21] Man in the middle (MITM) attack - www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/
[22] Credential stuffing vs. brute force attacks - www.cloudflare.com/ru-ru/learning/bots/what-is-credential-stuffing/

➢ Emosional təcillik yaratmaq: Hücum edən şəxs qurbanın dərhal qərar verməsini təmin etmək üçün təcili vəziyyətlər yaradır. Məsələn, bir bankın adından gələn saxta mesajda "Hesabınız təhlükə altındadır, dərhal tədbir görün" kimi ifadələr yer alır.

➢ Qorxu və təhlükə hissi: Qurbanları qorxuya salmaq və onların rasional düşünməsinə mane olmaq üçün təhdidlər və ya təhlükələrdən istifadə edilir. Məsələn, "Vergi borcunuz var, ödənişi etməsəniz, məhkəmə ilə üzləşəcəksiniz" kimi saxta mesajlar.

➢ İnam qazanmaq: Hücum edən şəxslər, etibarlı bir şəxs və ya qurum kimi özlərini təqdim edərək qurbanların etibarını qazanmağa çalışırlar. Məsələn, bir işçinin rəhbərinin adından göndərilən e-poçtlarla iş məlumatları tələb oluna bilər.

➢ Maraq oyandırmaq: Hücum edən şəxslər, qurbanların marağını cəlb edən "hədiyyələr", "kampaniyalar" və ya "eksklüziv təkliflər" vasitəsilə məlumatlar əldə etməyə çalışırlar.

Psixi əsaslı hücumlara əsasən aşağıdakı növləri misal göstərmək olar:

- **"Pretexting",** sosial mühəndislik hücumlarının ən effektiv metodlarından biridir və qurbanın etimadını qazanmaq üçün yalançı şəxsiyyət və ya qurum adı ilə manipulyasiyaya əsaslanır. Bu hücum növündə hücum edən şəxs özünü qurbanın etibar etdiyi bir şəxs və ya qurumun nümayəndəsi kimi təqdim edir. Məqsəd, qurbanı müəyyən məlumatları könüllü şəkildə açıqlamağa məcbur etməkdir[23].

Hücum edən şəxs əvvəlcə qurban və ya onun iş yeri haqqında məlumat toplayır. Daha sonra həmin məlumatlardan istifadə edərək, real şəxs və ya qurumun adından çıxış edir. Məsələn, bir işçinin telefonuna zəng edərək, "Mən İT şöbəsindənəm, sisteminizdə nasazlıq var. Şifrənizi təsdiqləyərək problemi aradan qaldırmalıyıq" deyə bilər. Qurban, bu təklifə inanaraq öz şifrəsini açıqlayır və bu məlumat birbaşa hücum edən şəxsin nəzarətinə keçir.

- **"Baiting",** qurbanın marağını və diqqətini çəkərək onun davranışlarını manipulyasiya etməyə əsaslanan bir sosial mühəndislik hücumudur. Bu metodda hücum edən şəxslər, cazibədar təkliflər və vədlər təqdim edərək qurbanları müəyyən hərəkətləri etməyə sövq edir. Əsas məqsəd, qurbanın şəxsi məlumatlarını oğurlamaq, onun cihazına zərərli proqram yükləmək və ya sistemlərinə qanunsuz giriş əldə etməkdir[24].

Hücum edən şəxslər, qurbanın emosiyalarını və maraq dairələrini manipulyasiya edərək "əlçatmaz mükafatlar", "pulsuz xidmətlər" və ya "eksklüziv təkliflər" təklif edirlər. Təklif adətən elektron poçt, mesajlaşma platformaları, sosial media və ya saxta veb-saytlar vasitəsilə göndərilir. Təklifin həyata keçirilməsi üçün qurbanın bir bağlantıya klikləməsi və ya məlumatlarını təqdim etməsi tələb olunur.

Məsələn, qurban bir e-poçt alır: "Təbrik edirik! Pulsuz kupon qazandınız. Bu hədiyyəni əldə etmək üçün bu linkə klikləyin." Linkə daxil olduqda qurban, ya zərərli bir veb-sayta yönləndirilir, ya da onun cihazına zərərli proqram yüklənir.

- **"Quid pro quo",** sosial mühəndislik hücumlarının bir növü olaraq, hücum edən şəxsin qurbanı müəyyən bir xidmət və ya fayda qarşılığında şəxsi və ya korporativ

[23] Pretexting definition - www.imperva.com/learn/application-security/pretexting/
[24] Baiting in social engineering: how hackers trick you & staying safe - M. Salman Nadeem

məlumatları təqdim etməyə sövq etdiyi bir metoddur. Bu taktika, qurbanın ehtiyaclarını və ya çətin vəziyyətlərini manipulyasiya etməyə əsaslanır. Hücumun məqsədi, qurbanın məlumatlarına icazəsiz giriş əldə etməkdir[25].

Hücum edən şəxs əvvəlcə qurbanın ehtiyaclarını və ya zəifliklərini müəyyən edir. Daha sonra, birbaşa əlaqə saxlayaraq qurbanın problemlərini həll etmək və ya fayda təqdim etmək təklifi ilə yaxınlaşır. Məsələn:

- Texniki dəstək: Hücum edən şəxs özünü bir İT mütəxəssisi kimi təqdim edərək, "Kompüterinizdə problem var. Həll etmək üçün giriş məlumatlarınıza ehtiyacım var" deyir.
- Maddi faydalar: Hücum edən şəxs, qurbanın məlumatlarını təqdim etməsi müqabilində bir mükafat və ya güzəşt təklif edir, məsələn, "Şifrənizi təsdiqləsəniz, hesabınıza əlavə bonuslar yüklənəcək."

3. Fiziki hücumlar

Fiziki hücumlar, təhlükəsizlik tədbirlərini fiziki səviyyədə aşaraq məxfi məlumatlara və ya xüsusi ərazilərə icazəsiz giriş əldə etməyi nəzərdə tutur. Bu cür hücumlar adətən korporativ mühitlərdə tətbiq olunur, lakin fərdi şəxsləri də hədəf ala bilər. Hücum edən şəxslər, insan davranışlarındakı boşluqlardan və təhlükəsizlik sistemlərindəki zəifliklərdən istifadə edərək öz məqsədlərinə çatırlar. Nəticədə, məlumatların qorunması və ərazi təhlükəsizliyi ciddi şəkildə pozula bilər.

- **"Tailgating",** hücum edən şəxs təşkilatın mühafizə olunan məkanına icazəsiz daxil olması üçün digər bir şəxsin arxasınca keçməsinə əsaslanan bir hücum növüdür. Bu metod, adətən, qapı kartları və ya digər giriş icazəsi tələb edən yerlərdə tətbiq olunur. Hücum edən şəxs, özünü unudulmuş və ya itirilmiş bir kartın sahibi kimi göstərərək və ya sadəcə işçi kimi davranaraq təhlükəsizlik baryerlərini aşır. Hücum edən şəxs, bir işçinin arxasında qapıya yaxınlaşır və "Kartımı evdə unutmuşam, keçməyimə kömək edərsiniz?" deyə bir bəhanə ilə giriş əldə edir[26].
- **"Dumpster diving",** təşkilatların və ya şəxslərin zibil qutularında məxfi sənədlərin, məlumatların və ya cihazların axtarılması metodudur. Hücum edən şəxslər, kağız sənədlər, disklər və ya digər məlumat daşıyıcıları vasitəsilə istifadə üçün yararlı məlumatları əldə etməyə çalışırlar. Hücum edən şəxs, bir təşkilatın zibil qutusunda məxfi sənədləri, bank məlumatlarını və ya müştəri qeydlərini tapmağa çalışır[27].
- **"Shoulder Surfing",** hücum edən şəxs birbaşa qurbanın çiyni arxasından baxaraq onun məxfi məlumatlarını oğurlamağa çalışdığı bir hücum metodudur. Bu cür hücum adətən ictimai yerlərdə və ya sıx ofis mühitlərində həyata keçirilir. Hücum edən şəxs, qurbanın bankomatda "PIN" kodunu daxil etdiyi zamanı yaxından müşahidə edir.

4. Qarışıq (hibrid) hücumlar

Qarışıq hücumlar, texnoloji və psixoloji metodların birləşdirilməsi yolu ilə həyata keçirilən mürəkkəb sosial mühəndislik hücumlarıdır. Bu hücumlar bir neçə mərhələdən ibarət olur və fərqli yanaşmaların kombinasiyası ilə qurbanın məlumatlarını əldə etmək

[25] What is a quid pro quo attack & how to avoid becoming a victim - Tyler Therpsiri
[26] Tailgating hücumu nədir? - cybersign.az/xeber/tailgating-hucumu-nedir
[27] Dumpster diving - it.ufl.edu/security/learn-security/social-engineering/dumpster-diving/

və ya sistemlərə icazəsiz giriş təmin etmək məqsədi daşıyır. Hibrid hücumlar həm insan davranışlarındakı zəifliklərdən, həm də texnoloji boşluqlardan istifadə edir və çox vaxt daha genişmiqyaslı nəticələrə səbəb olur.

- **"Phishing" və "pretexting" birləşməsi,** Bu yanaşma, "phishing" və "pretexting" metodlarının birlikdə tətbiq olunduğu bir hücum növüdür. Hücum edən şəxs əvvəlcə qurbanı saxta bir e-poçt vasitəsilə aldatmağa çalışır. E-poçtda qurbanın təcili tədbir görməsini tələb edən məlumatlar yer alır, məsələn: "Hesabınız təhlükə altındadır, texniki dəstək üçün bu telefon nömrəsinə zəng edin."

Qurban, bu e-poçtdakı təlimatlara əməl edərək telefon nömrəsinə zəng etdikdə, hücum edən şəxs onu daha da manipulyasiya edir. Özünü bir mütəxəssis kimi təqdim edən hücum edən şəxs, qurbanın giriş məlumatlarını və ya digər məxfi məlumatlarını açıqlamasına nail olur.

- **Texniki və fiziki manipulyasiyaların birləşdirilməsi,** Bu metodda hücum edən şəxs, texnoloji vasitələrdən istifadə edərək məlumat toplamağa çalışır və eyni zamanda fiziki səviyyədə manipulyasiyalar həyata keçirir. Məsələn, bir təşkilatın şəbəkə sistemlərinə giriş əldə etmək üçün hücum edən şəxs:

➢ Saxta bir e-poçt göndərərək işçiləri manipulyasiya edir və onların şəbəkə məlumatlarını ələ keçirir.

➢ Daha sonra təşkilatın binasına fiziki olaraq daxil olaraq, məlumat daşıyıcı cihazları (USB və ya kompüter avadanlıqları) manipulyasiya edir.

Hücumların məqsədi

Sosial mühəndislik hücumları müxtəlif məqsədlərə xidmət edə bilər və bu məqsədlər adətən hücumun növünə və hədəfinə görə dəyişir. Hücumların məqsədi şəxslərdən və ya təşkilatlardan məlumat toplamaq, maliyyə qazancı əldə etmək, resurslara qanunsuz giriş təmin etmək və ya ictimai rəyin manipulyasiya edilməsi ola bilər. Hər bir məqsəd müəyyən bir strategiya və texnika ilə həyata keçirilir, ciddi hüquqi və maliyyə nəticələrinə səbəb ola bilər.

Hücum edən şəxslər, məlumatları ələ keçirmək, resursları manipulyasiya etmək və ya ictimai etimadı zədələmək üçün qurbanların zəifliklərindən istifadə edirlər. Bu zəifliklər, adətən, insanların emosional reaksiyalarına və ya texniki boşluqlara əsaslanır. Hücumların təsiri yalnız şəxslər üçün deyil, eyni zamanda təşkilatlar və cəmiyyət üçün də böyük zərər yarada bilər.

Hücumların məqsədləri, həm fərdi, həm də qlobal miqyasda təhlükəsizlik tədbirlərinin hazırlanmasını tələb edən mühüm bir aspektdir. Bu səbəbdən, sosial mühəndislik hücumlarının məqsədlərini və onların mümkün nəticələrini anlamaq, bu cür təhdidlərə qarşı daha təsirli müdafiə mexanizmləri inkişaf etdirmək üçün vacibdir.

1. Məlumat toplama

Məlumat toplama, sosial mühəndislik hücumlarının əsas məqsədlərindən biridir və digər hücum növlərinin uğurlu həyata keçirilməsi üçün baza rolunu oynayır. Bu prosesdə hücum edən şəxslər, qurbanlar haqqında müxtəlif məlumatları ələ keçirmək üçün fərqli

metodlardan istifadə edirlər. Toplanan məlumatlar qurbanın şəxsi məlumatları, korporativ sistemlərə giriş üçün tələb olunan şifrələr, əlaqə vasitələri və ya digər həssas məlumatlar ola bilər[28].

Hücum edən şəxslər, məlumat toplama mərhələsində qurbanların zəifliklərini müəyyən etmək və bu zəifliklərdən istifadə edərək onları manipulyasiya etmək üçün strategiyalar hazırlayırlar. Məlumatların toplanması, adətən, çox mərhələli bir prosesdir və həm texniki vasitələrdən, həm də psixoloji manipulyasiyalardan istifadə etməklə həyata keçirilir. Bu mərhələdə əldə edilən məlumatlar daha genişmiqyaslı hücumların həyata keçirilməsi üçün əsas təşkil edir.

Məsələn, bir təşkilatın işçiləri haqqında məlumat toplamaqla hücum edən şəxslər onların vəzifələrini, istifadə etdikləri sistemləri və ya şəxsi maraqlarını öyrənə bilər. Bu məlumatlar, daha sonra işçilərin aldadılması və ya təşkilatın sistemlərinə icazəsiz giriş əldə etmək üçün istifadə edilə bilər. Məlumat toplama, yalnız şəxslərin deyil, həm də təşkilatların təhlükəsizliyini ciddi şəkildə təhdid edə bilən mühüm bir mərhələdir.

Bu mərhələyə qarşı effektiv mübarizə üçün şəxslər və təşkilatlar məlumatlarını qorumaq, şübhəli sorğulara cavab verməmək və təhlükəsizlik tədbirlərini gücləndirmək üçün diqqətli olmalıdırlar.

2. Resurslara giriş

Resurslara giriş, sosial mühəndislik hücumlarının əsas məqsədlərindən biri olaraq, qurbanın fiziki, texnoloji və ya maliyyə resurslarına icazəsiz çıxış əldə etməyə yönəlmiş fəaliyyətlərdən ibarətdir. Hücum edən şəxslər, təşkilatların və ya şəxslərin istifadə etdiyi sistemlərə, məlumat bazalarına, cihazlara və hətta fiziki məkanlara giriş təmin etmək üçün manipulyasiya texnikalarından istifadə edirlər. Bu məqsədlə həyata keçirilən hücumlar adətən çox mərhələli olur və həm texnoloji, həm də psixoloji metodlarla dəstəklənir[29].

Resurslara giriş hücumları, qurbanın sistemlərini zəiflədir və onların icazəsiz şəkildə idarə edilməsinə şərait yaradır. Hücumlar nəticəsində əldə edilən resurslar müxtəlif məqsədlər üçün istifadə edilə bilər, məsələn:

- Məxfi sənədlərin oğurlanması,
- Məlumatların dəyişdirilməsi və ya silinməsi,
- Şəbəkə infrastrukturlarının pozulması,
- Qurbanın resurslarından digər hücumlar üçün vasitə kimi istifadə edilməsi.

Məsələn, bir təşkilatda çalışan işçinin şifrəsinin oğurlanması ilə hücum edən şəxs, həmin işçinin səlahiyyətlərinə uyğun olaraq daxili sistemlərə giriş təmin edə bilər. Bu giriş vasitəsilə hücum edən şəxs, həm təşkilatın, həm də müştərilərin məlumatlarına zərər verə bilər.

Resurslara giriş hücumları təşkilatların təhlükəsizlik infrastrukturunu sarsıda, böyük maliyyə itkilərinə səbəb ola və onların nüfuzuna ciddi zərər vura bilər. Bu hücumlara qarşı mübarizə üçün güclü autentifikasiya sistemlərinin tətbiqi, giriş hüquqlarının məhdudlaşdırılması və şübhəli fəaliyyətlərin monitorinqi mühüm əhəmiyyət daşıyır. Həm

[28] Sosial mühəndislik hücum texnikası nədir?! - cert.az/news/2019/sosial-muhendislik-texnikasi-nedir
[29] Sosial mühəndislik nüfuz testləri - allsafe.az/bizim-xidmetler/nufuzetme-sinaqlari/sosial-muhendislik-nufuz-testleri/

şəxslər, həm də təşkilatlar öz resurslarını qorumaq üçün müasir texnoloji təhlükəsizlik tədbirlərini və effektiv təhlükəsizlik protokollarını tətbiq etməlidirlər.

3. Maliyyə fırıldaqları

Maliyyə fırıldaqları, sosial mühəndislik hücumlarının ən çox rast gəlinən məqsədlərindən biridir və qurbanların maliyyə resurslarına icazəsiz çıxış əldə etməyə və ya birbaşa maliyyə qazancı əldə etməyə yönəlmiş fəaliyyətləri əhatə edir. Hücum edən şəxslər, şəxsi və ya korporativ maliyyə məlumatlarını oğurlamaq, qanunsuz maliyyə əməliyyatları həyata keçirmək və ya qurbanları aldatmaq üçün müxtəlif texnikalardan istifadə edirlər[30].

Maliyyə fırıldaqları əsasən şəxsləri, təşkilatları və hətta dövlət qurumlarını hədəf alır. Bu hücumlar həm qurbanların texnoloji zəifliklərindən, həm də onların emosional reaksiyalarından faydalanmaqla həyata keçirilir. Hücum edən şəxslər, adətən, qurbanı təcili və ya cazibədar bir təkliflə manipulyasiya edərək onların davranışlarını idarə edirlər.

4. İctimai manipulyasiya

İctimai manipulyasiya, sosial mühəndislik hücumlarının psixoloji və kütləvi təsirə yönəlmiş bir formasıdır. Bu hücum növü, qurbanların qərar qəbul etmə prosesinə təsir edərək onların davranışlarını, fikirlərini və ya münasibətlərini manipulyasiya etməklə həyata keçirilir. Əsas məqsəd, şəxsləri və ya geniş ictimaiyyəti müəyyən bir istiqamətə yönəltmək, məlumatları sızdırmağa məcbur etmək və ya emosional reaksiyalardan istifadə edərək istədiyi nəticəni əldə etməkdir[31].

İctimai manipulyasiya adətən kütləvi təsir gücünə malik platformalarda, məsələn, sosial media, xəbər saytları və ya ictimai tədbirlər vasitəsilə həyata keçirilir. Bu metod həm ayrı-ayrı şəxsləri, həm də böyük sosial qrupları hədəf ala bilər.

Əsas məqsədləri:

- Kütləvi təsir: Fikirləri formalaşdırmaq və ya müəyyən bir fikri geniş ictimaiyyət arasında yaymaq. Məsələn, saxta xəbərlər və ya dezinformasiyalar vasitəsilə ictimai rəyə təsir göstərmək.
- Davranışların idarə olunması: İctimai təzyiq və ya emosional manipulyasiya vasitəsilə insanları müəyyən bir hərəkət etməyə təşviq etmək.
- Siyasi və iqtisadi təsir: Seçkilərə, bazar davranışlarına və ya ictimai sabitliyə təsir göstərmək məqsədilə manipulyasiya.

İctimai manipulyasiya, cəmiyyətin qərarlarına və davranışlarına birbaşa təsir edən təhlükəli bir sosial mühəndislik üsuludur. Bu cür hücumlara qarşı ictimai şüurun artırılması, texnoloji təhlükəsizlik tədbirlərinin tətbiqi və dəqiq məlumatlara əsaslanan maarifləndirmə kampaniyalarının təşkili vacibdir.

[30] Sosial mühəndislik hücumları - Tacir Alıyev
[31] Sosial mühəndislik hücumlarının psixoloji aspektləri: manipulyasiya üsullarının təhlili - Ranar Ramazanov

Hücumların tətbiq sahələri

Sosial mühəndislik hücumları fərqli tətbiq sahələrində həyata keçirilir və müxtəlif hədəf qruplarını əhatə edir. Bu hücumların tətbiq sahələri, hədəflərin xüsusiyyətlərinə və Hücum edən şəxslərin məqsədlərinə uyğun olaraq dəyişir. Şəxslər, korporativ təşkilatlar, dövlət qurumları və hətta internet üzərindən geniş ictimai kütlələr bu hücumların əsas hədəfi ola bilər. Hər bir tətbiq sahəsi, özünəməxsus metodologiyalar və yanaşmalarla fərqlənir.

Fərdi hədəflərə yönəlmiş hücumlar

Fərdi hədəflərə yönəlmiş sosial mühəndislik hücumları, fərdi məlumatların qanunsuz ələ keçirilməsi, maliyyə resurslarına çıxış əldə edilməsi və ya müəyyən davranışlara məcbur edilməyə yönəlir. Hücum edən şəxslər şəxslərin emosional zəifliklərindən və texnoloji biliklərinin kifayət qədər olmamasından istifadə edirlər. Sosial media və digər platformalar vasitəsilə məlumat toplayaraq, qurbanlara saxta təkliflər və təhdidlər göndərirlər.

Məsələn, “phishing” hücumları zamanı qurbanlara "Hesabınızda problem var, bu linkə klikləyin" kimi saxta mesajlar göndərilir və fərdi məlumatlar qanunsuz ələ keçirilir. Bu hücumların nəticəsində fərdi məlumatların sızması, maliyyə itkiləri və şəxsi təhlükəsizliyin pozulması kimi problemlər yaranır.

Bu cür hücumların qarşısını almaq üçün şəxslər güclü şifrələrdən istifadə etməli, iki faktorlu identifikasiyanı aktiv etməli və şübhəli mesajlara diqqətlə yanaşmalıdırlar. Təhlükəsizlik tədbirlərinə riayət etmək və diqqətli olmaq şəxslərin bu hücumlara qarşı qorunmasını təmin edir.

Korporativ hücumlar

Korporativ hücumlar, təşkilatların məxfi məlumatlarını, maliyyə resurslarını və ya sistemlərini hədəf alan sosial mühəndislik metodlarıdır. Hücum edən şəxslər, adətən, işçilərin zəifliklərindən istifadə edərək, saxta e-poçtlar, telefon zəngləri və ya digər manipulyasiya üsulları ilə məlumatlara çıxış əldə etməyə çalışırlar. Məsələn, rəhbərlik adından göndərilən saxta bir e-poçt vasitəsilə maliyyə əməliyyatları təsdiqlənir və ya daxili sistemlərə giriş təmin edilir.

Bu hücumların nəticəsi olaraq, təşkilatların məlumatlarının sızması, maliyyə itkiləri və reputasiya problemləri yaranır. Hücumların qarşısını almaq üçün işçilərin təhlükəsizlik mövzusunda maarifləndirilməsi, güclü təhlükəsizlik protokollarının tətbiqi və davamlı monitorinq vacibdir. Təşkilatlar müasir təhlükəsizlik tədbirləri ilə bu cür təhdidlərin qarşısını ala bilərlər.

Dövlət və ictimai hücumlar

Dövlət və ictimai hücumlar, hökumət qurumlarını, ictimai təşkilatları və ya geniş kütləni hədəf alan sosial mühəndislik metodlarından istifadə edilir. Bu hücumların məqsədi, milli təhlükəsizliyə zərər vurmaq, ictimai sabitliyi pozmaq, məxfi dövlət məlumatlarını ələ keçirmək və ya ictimai fikri manipulyasiya etməkdir. Hücum edən şəxslər dezinformasiya yaymaq, məlumat sızdırmaq və ya ictimai təzyiq yaratmaq üçün texnoloji və psixoloji metodlardan istifadə edirlər.

Məsələn, saxta məlumatların yayılması yolu ilə seçki nəticələrinə təsir etmək və ya ictimai etibarın sarsıdılması dövlətə və cəmiyyətə ciddi problemlər yarada bilər. Hücum edən şəxslər, həmçinin dövlət qurumlarının elektron sistemlərinə sızaraq milli təhlükəsizliklə bağlı məlumatları oğurlaya və ya məhv edə bilərlər.

Bu cür hücumların nəticələri genişmiqyaslı və təhlükəlidir, çünki onlar yalnız konkret qurumlara deyil, bütöv cəmiyyətə təsir göstərə bilər. Belə hücumlarla mübarizə aparmaq üçün güclü kibertəhlükəsizlik tədbirləri, ictimai maarifləndirmə və dezinformasiyanın qarşısını almağa yönəlmiş strategiyalar tətbiq edilməlidir. Dövlət və ictimai hücumların qarşısını almaq milli təhlükəsizliyin qorunmasında əsas rol oynayır.

Hücumların təhlükə səviyyələri

Sosial mühəndislik hücumları təsir dərəcələrinə və nəticələrinin ciddiliyinə görə müxtəlif təhlükə səviyyələrinə bölünür. Hücumun təhlükə səviyyəsi, onun hədəfi, məqsədi və yaratdığı potensial zərərlərlə müəyyən edilir. Aşağı, orta və yüksək təhlükə səviyyəli hücumlar fərqli xüsusiyyətlərə malikdir və hər biri fərqli nəticələr doğurur.

Aşağı təhlükə səviyyəli hücumlar, adətən, şəxsləri və ya kiçik qrupları hədəf alır və onların məlumatlarına və ya resurslarına minimal təsir göstərir. Bu cür hücumlar çox vaxt zərərsiz görünən manipulyasiya üsulları ilə həyata keçirilir. Məsələn, bir şəxsin sosial media hesabına giriş əldə etmək üçün onun məlumatlarının təxmin edilməsi və ya kiçik məbləğdə maliyyə itkilərinə səbəb olan "phishing" cəhdləri bu kateqoriyaya daxildir. Belə hücumlar genişmiqyaslı təhlükə yaratmasa da, şəxsi və maliyyə baxımından narahatlıq doğura bilər.

Orta təhlükə səviyyəli hücumlar daha mürəkkəb və geniş təsirə malikdir. Bu hücumlar şəxsləri, kiçik təşkilatları və ya müəyyən ictimai qrupları hədəf alır. Hücum edən şəxslər, adətən, daha çox məlumat toplamaq və ya zərərli proqram təminatı vasitəsilə qurbanların cihazlarını nəzarət altına almağa çalışırlar. Məsələn, korporativ sistemlərə zərər vermək üçün işçilərin zəifliklərindən istifadə edərək məlumat sızdıran hücumlar orta səviyyəli təhlükə hesab edilir. Bu cür hücumlar həm şəxslər, həm də təşkilatlar üçün ciddi problemlər yarada bilər və onların təhlükəsizlik tədbirlərini gücləndirməsini tələb edir.

Yüksək təhlükə səviyyəli hücumlar ən ciddi nəticələrə səbəb olan və çox genişmiqyaslı təsirə malik hücumlar hesab olunur. Bu hücumların hədəfi, adətən, dövlət qurumları, böyük korporasiyalar və ya geniş ictimaiyyət olur. Hücum edən şəxslər, milli təhlükəsizliyə, iqtisadi sabitliyə və ya ictimai rəylərə ciddi təsir göstərə bilən kompleks metodlardan istifadə edirlər. Məsələn, dövlət qurumlarının məxfi məlumatlarına sızmaq, böyük maliyyə fırıldaqları həyata keçirmək və ya ictimai panika yaratmaq məqsədilə geniş yayılmış dezinformasiya kampaniyaları yüksək təhlükə səviyyəli hücumlara aiddir. Bu cür hücumlar yalnız bir təşkilatı və ya fərdi deyil, bütöv bir ölkəni və ya cəmiyyəti təhlükə altına sala bilər.

Hücumların təhlükə səviyyələrini anlamaq və onlara uyğun müdafiə tədbirləri tətbiq etmək həm şəxslər, həm də təşkilatlar üçün vacibdir. Aşağı səviyyəli hücumlar daha sadə

tədbirlərlə aradan qaldırıla bilsə də, orta və yüksək səviyyəli hücumlara qarşı daha güclü və kompleks təhlükəsizlik strategiyaları tələb olunur. Təhlükəsizlik tədbirlərinin hər səviyyəyə uyğun olaraq planlaşdırılması, sosial mühəndislik hücumlarının təsirini minimuma endirməyə imkan yaradır.

Nəticə

Bu mühazirə, sosial mühəndislik hücumlarının təsnifatını və növlərini sistematik şəkildə izah edərək, onların əsas xüsusiyyətlərini və təhlükə mənbələrini anlamağa kömək edir. Sosial mühəndislik hücumları yalnız texnoloji zəifliklərdən deyil, həm də insan davranışlarının zəifliklərindən istifadə etməklə həyata keçirilir. Bu səbəbdən, hücumların müxtəlif formalarını və onların təsir mexanizmlərini anlamaq, həm fərdi, həm də təşkilati təhlükəsizliyin təmin edilməsi baxımından mühüm əhəmiyyət daşıyır.

Hücumların təsnifatı onların təbiətini və hədəflərini daha dəqiq müəyyən etməyə imkan verir, bu da təhlükəsizlik tədbirlərinin effektiv şəkildə planlaşdırılmasını asanlaşdırır. Aşağı təhlükə səviyyəli hücumlardan tutmuş yüksək təhlükə səviyyəli hücumlara qədər hər biri fərqli yanaşmalar və strategiyalar tələb edir. Bu cür hücumlara qarşı mübarizə yalnız texnoloji həllərlə məhdudlaşmamalı, insan amilinə də xüsusi diqqət yetirilməlidir.

Təhlükəsizlik tədbirləri həm texnoloji, həm də insani səviyyədə gücləndirilməlidir. Texnologiya baxımından güclü autentifikasiya sistemləri, məlumat şifrələmə, şəbəkə monitorinqi və antivirus proqramlarının tətbiqi əsas rol oynayır. Bununla yanaşı, insani səviyyədə maarifləndirmə və təlimlər, psixoloji manipulyasiyaların tanınması və təhlükəsizlik vərdişlərinin inkişaf etdirilməsi vacibdir. Təşkilatlar və şəxslər, təhlükəsizlik sahəsində davamlı təkmilləşmə üçün əməkdaşlıq etməli və məlumat mübadiləsini artırmalıdır.

Sosial mühəndislik hücumlarına qarşı mübarizə təkcə fərdi və ya təşkilati səviyyədə deyil, qlobal miqyasda da aparılmalıdır. Beynəlxalq əməkdaşlıq, hüquqi çərçivələrin gücləndirilməsi və məlumatların qorunması üzrə standartların tətbiqi bu mübarizənin mühüm hissəsidir. Hücumların qarşısını almaq üçün texnologiya və insan faktorunun birlikdə işlədiyi kompleks bir yanaşma zəruridir. Bu istiqamətdə hökumətlər, beynəlxalq təşkilatlar və kibertəhlükəsizlik ekspertləri birgə işləyərək daha güclü müdafiə mexanizmləri və qabaqlayıcı strategiyalar hazırlamalıdır.

Nəticədə, sosial mühəndislik hücumlarının qarşısını almaq yalnız müdafiə tədbirlərini gücləndirməklə deyil, həm də davamlı maarifləndirmə və təhlükəsizlik mədəniyyətinin formalaşdırılması ilə mümkündür. Bu yanaşma, həm şəxslərin, həm də təşkilatların təhlükəsizliyini təmin etməklə yanaşı, daha geniş bir təhlükəsizlik mühiti yaratmağa kömək edəcəkdir. Sosial mühəndislik hücumlarının kompleks təbiətini anlamaq və onlara qarşı sistemli tədbirlər görmək, daha təhlükəsiz bir rəqəmsal gələcək üçün mühüm addımdır. Gələcəkdə süni intellekt və avtomatlaşdırılmış təhlükəsizlik sistemlərinin sosial mühəndislik hücumlarına qarşı istifadəsi bu sahədə yeni imkanlar yarada bilər və daha effektiv müdafiə mexanizmlərinin qurulmasını təmin edəcəkdir.

§ 3. Sosial mühəndisliyin mərhələləri və həyata keçirilməsi

Giriş

Sosial mühəndislik, insan psixologiyasının zəif tərəflərindən istifadə edərək məlumatların oğurlanması, sistemlərə icazəsiz girişin təmin edilməsi və ya müəyyən davranışlara məcbur etmə məqsədi daşıyan mürəkkəb manipulyasiya texnikasıdır. Bu metod, texnoloji boşluqlardan daha çox insanın qərar qəbul etmə prosesindəki boşluqlara əsaslanır. Sosial mühəndislik, qurbanın diqqətsizliklərini, emosional reaksiyalarını və ya etimadını istismar edərək onu məlumat ifşa etməyə və ya təhlükəli hərəkətlərə məcbur edir. Hücum edən şəxslər, qurbanın fərdi xüsusiyyətlərini və zəifliklərini təhlil edərək hər mərhələdə fərqli strategiyalardan istifadə edirlər.

Bu proses bir neçə ardıcıl mərhələdən ibarətdir və hər mərhələ özünəməxsus məqsədlər və texnikalarla həyata keçirilir. Əvvəlcə qurban haqqında məlumatların toplanması ilə başlayan sosial mühəndislik hücumu, etibar qazandıqdan sonra manipulyasiya vasitəsilə qurbanın davranışlarını idarə etmək məqsədini güdür. Nəticədə, qurbanın fərdi məlumatlarının qanunsuz ələ keçirilməsi, maliyyə resurslarının istismarı və ya təşkilatın təhlükəsizlik sistemlərinin pozulması kimi ciddi nəticələr ortaya çıxır. Bu prosesin effektivliyi, hücum edən şəxs hər mərhələni diqqətlə planlaşdırması və icra etməsindən asılıdır.

Sosial mühəndislik hücumları ayrı-ayrı şəxslərdən tutmuş böyük təşkilatlara qədər müxtəlif səviyyələrdə tətbiq oluna bilər. Hücum edən şəxslər, texnoloji vasitələrlə yanaşı, insanın təbii davranışlarını manipulyasiya etmək üçün psixoloji metodlardan da istifadə edir. Bu səbəbdən, sosial mühəndislik yalnız texniki bir problem deyil, həm də insani və psixoloji bir çağırışdır. Hücum edən şəxslər, qurbanlarının psixoloji vəziyyətlərindən, sosial əlaqələrindən və informasiya paylaşımı vərdişlərindən istifadə edərək onlara təsir göstərirlər. Belə ki, qorxu, tələskənlik, inam və maraq kimi emosional amillər hücumun uğurlu olmasında əsas rol oynayır.

Sosial mühəndislik hücumlarının ən təhlükəli tərəfi onların geniş spektrdə tətbiq oluna bilməsidir. Hücum edən şəxslər, fərdi qurbanları hədəfə alaraq şəxsi məlumatları ələ keçirdikləri kimi, iri təşkilatlara və dövlət qurumlarına qarşı da məqsədyönlü kampaniyalar apara bilərlər. Xüsusilə, korporativ casusluq, dövlət sirrlərinin sızdırılması və ya maliyyə fırıldaqçılığı kimi hallarda sosial mühəndislik üsulları geniş istifadə olunur.

Bu hücumların qarşısını almaq üçün onların həyata keçirilmə mərhələlərini başa düşmək vacibdir. Bu mərhələlərin hər biri sosial mühəndislik hücumlarının uğurlu olmasında mühüm rol oynayır. Hücum edən şəxslər qurbanlarının zəifliklərini anlamaq və onları effektiv şəkildə manipulyasiya etmək üçün strategiyalarını diqqətlə planlaşdırırlar. Bu mühazirədə sosial mühəndisliyin həyata keçirilmə mərhələləri və hər mərhələdə istifadə olunan əsas metodlar təhlil ediləcək. Məqsədimiz, bu təhlükənin nə qədər mürəkkəb və geniş yayılmış olduğunu başa düşmək və effektiv müdafiə tədbirlərini müəyyən etməkdir.

Sosial mühəndisliyin mərhələləri

Sosial mühəndislik, insan davranışlarındakı zəifliklərdən istifadə etməklə həyata keçirilən, planlı və bir neçə ardıcıl mərhələdən ibarət olan mürəkkəb bir prosesdir. Hücumun uğurlu olması üçün hər mərhələ diqqətlə planlaşdırılır, sistematik şəkildə həyata keçirilir və hər biri özünəməxsus məqsədlərə xidmət edir. Bu mərhələlər, qurbanın diqqətsizliklərindən, emosional zəifliklərindən və ya təcrübəsizliyindən faydalanaraq hücum edən şəxs hədəflərinə çatmasına şərait yaradır.

Sosial mühəndisliyin əsas məqsədi, qurbanın qərar qəbul etmə prosesinə təsir etmək və onu müəyyən hərəkətləri yerinə yetirməyə məcbur etməkdir. Bu proses, texnoloji və psixoloji yanaşmaları birləşdirərək qurbanın manipulyasiya edilməsinə yönəlir. Hər bir mərhələ, qurbanın zəif tərəflərinin daha yaxşı istifadə edilməsi və hücum edən şəxsin planlarının reallaşması üçün vacib bir addımdır. Hücumun effektivliyi, bu mərhələlərin nə dərəcədə dəqiqliklə və peşəkar şəkildə həyata keçirilməsindən asılıdır.

Hər mərhələ, sosial mühəndisliyin təbii axarını təşkil edir və sonrakı mərhələnin uğurla həyata keçirilməsi üçün əsas yaradır. Məlumat toplama ilə başlayan bu proses, etibar qazandıqdan sonra manipulyasiya və nəticə əldə etmə ilə davam edir. Bu sistemli yanaşma, hücumların daha təsirli olmasını təmin edir və qurbanın hücumu erkən mərhələdə müəyyən etməsini çətinləşdirir. Sosial mühəndisliyin bu təbiəti, onun təhlükəsizlik tədbirlərini pozmaq və insan faktorundan istifadə etmək baxımından ən təsirli hücum metodlarından biri olmasına səbəb olur.

Sosial mühəndislik aşağıdakı mərhələlərdən ibarətdir[32]:

1. Məlumat toplama;
2. Etibar qazanma;
3. Manipulyasiya;
4. Məqsədə nail olma;
5. İzlərin silinməsi.

1. Məlumat Toplama

Məlumat toplama, sosial mühəndislik prosesinin ilk və ən vacib mərhələsidir. Bu mərhələdə hücum edən şəxs, hədəfi haqqında mümkün qədər çox məlumat əldə etməyə çalışır. Toplanan məlumatlar, hücumun sonrakı mərhələlərində qurbanın manipulyasiya edilməsində və hücum edən şəxsin məqsədlərinə çatmasında istifadə olunur. Hücumun effektivliyi və uğuru, məlumat toplama mərhələsinin nə qədər dəqiq və genişmiqyaslı həyata keçirilməsindən asılıdır. Bu səbəbdən, hücum edən şəxslər bu mərhələyə xüsusi diqqət yetirirlər[33].

Bu mərhələdə toplanan məlumatlar çox müxtəlif ola bilər. Bunlara qurbanın fərdi məlumatları, iş yeri və vəzifəsi, maraqları və sosial media fəaliyyətləri daxildir. Hücum edən şəxslər, həmçinin texnoloji zəifliklər, istifadə olunan cihazları və təhlükəsizlik tədbirlərini öyrənməyə çalışırlar. Bu məlumatlar, hücum edən şəxs qurbanın zəif

[32] The social-engineer framework - www.social-engineer.org/framework/general-discussion
[33] Social engineering: the art of human hacking - Christopher Hadnagy

tərəflərini müəyyən etməsinə və manipulyasiya texnikalarını daha təsirli şəkildə tətbiq etməsinə imkan yaradır.

Məlumat toplama prosesi bir neçə üsulla həyata keçirilir. Açıq mənbə kəşfiyyatı, məlumat toplamanın əsas vasitələrindən biridir. Hücum edən şəxslər, sosial media platformaları, onlayn forumlar, şirkət veb-saytları və digər açıq mənbələrdən məlumat toplayaraq qurban haqqında geniş bilik əldə edirlər. Məsələn, qurbanın "LinkedIn" profilindəki məlumatları onun iş yeri və vəzifəsi barədə dəyərli məlumatlar təqdim edə bilər. "Facebook" və "Instagram" kimi platformalar isə qurbanın şəxsi maraqları və gündəlik fəaliyyəti barədə ipucları verə bilər.

Hücum edən şəxslər, həmçinin saxta sorğular və ya zənglər vasitəsilə məlumat əldə etməyə çalışırlar. Məsələn, bir sorğu və ya müsahibə adı ilə qurbanın həssas məlumatları tələb edilə bilər. Bu metodlar, qurbanın şübhələrini azaltmaq və məlumat paylaşmasını asanlaşdırmaq üçün istifadə edilir. Hücum edən şəxslər, bu üsullarla qurbanın etibarını qazanır və daha çox məlumat əldə etmək üçün imkan yaradırlar.

Texnoloji vasitələr də məlumat toplama prosesində geniş şəkildə istifadə olunur. Hücum edən şəxslər, "phishing" e-poçtları və ya zərərli proqramlar vasitəsilə qurbanın cihazına daxil olaraq onun məlumatlarını əldə edə bilərlər. Eyni zamanda, "Wi-Fi" şəbəkələrinin zəifliklərindən istifadə edərək internet trafiki üzərindən məlumatların izlənməsi də bu mərhələdə tətbiq olunan texnikalardandır.

Məlumat toplama mərhələsi, sosial mühəndislik prosesinin əsasını təşkil edir və hücumun sonrakı mərhələlərinin uğurla həyata keçirilməsi üçün zəmin yaradır. Bu səbəbdən, şəxslər və təşkilatlar, şəxsi və korporativ məlumatlarının qorunmasına diqqət yetirməli, sosial media fəaliyyətlərində ehtiyatlı olmalı və həssas məlumatları paylaşarkən diqqətli davranmalıdırlar. Bu mərhələdə hücumların qarşısını almaq üçün güclü məlumat mühafizə strategiyaları tətbiq edilməlidir.

2. Etibar qazanma

Etibar qazanma, sosial mühəndislik prosesinin əsas mərhələlərindən biridir və hücumun uğurla davam etdirilməsi üçün vacib rol oynayır. Bu mərhələdə hücum edən şəxs, qurbanın diqqətini və inamını qazanmaq üçün müəyyən taktikalardan istifadə edir. Hücum edən şəxsin məqsədi, qurbanla etibarlı bir əlaqə qurmaq və onu öz niyyətlərinə inandıraraq lazımi məlumatları könüllü şəkildə paylaşmağa yönəltməkdir[34].

Hücum edən şəxslər bu mərhələdə qurbanla birbaşa və ya dolayı yolla əlaqə qururlar. Birbaşa əlaqələr adətən telefon zəngləri, e-poçtlar və ya sosial media vasitəsilə həyata keçirilir. Məsələn, hücum edən şəxs özünü texniki dəstək işçisi, bank nümayəndəsi və ya tanınmış bir təşkilatın əməkdaşı kimi təqdim edərək qurbanın etibarını qazanmağa çalışır. Bu zaman hücum edən şəxs inandırıcı olmaq üçün peşəkar üslubda danışır, texniki terminlərdən istifadə edir və ya qurbanın diqqətini cəlb etmək üçün real problemlərə istinad edir.

[34] Veri güvenliği saldırıları: sosyal mühendislik ve korunma yöntemleri - www.garantibbva.com.tr/blog/sosyal-muhendislik-saldirilari

Dolayı əlaqələrdə isə hücum edən şəxs, qurbanın fərqinə varmadan onu manipulyasiya etməyə çalışır. Məsələn, bir e-poçt və ya mesaj vasitəsilə saxta bir təklif təqdim edilir, belə ki, qurbanın marağını oyadaraq onun məlumatlarını paylaşmağa təşviq edir. "Hesabınızda təhlükə aşkar edilib, problemi həll etmək üçün şifrənizi təsdiqləyin" kimi mesajlar bu taktikanın geniş yayılmış bir nümunəsidir.

Hücum edən şəxslər bu mərhələdə qurbanın şübhələrini azaltmaq üçün müxtəlif üsullardan istifadə edirlər. Məsələn, qurbanın tanıdığı və etibar etdiyi bir şəxs və ya qurumun adından çıxış edirlər. Sosial media və digər açıq mənbələrdən əldə edilən məlumatlar, hücum edən şəxsin qurbanla əlaqəni daha da inandırıcı etmək üçün istifadə etdiyi əsas vasitələrdən biridir.

Texniki biliklərdən istifadə etməklə yanaşı, hücum edən şəxslər psixoloji manipulyasiyaya da xüsusi önəm verirlər. Onlar qurbanın emosional zəifliklərini, qorxularını və ya təcili yardım ehtiyacını istismar edirlər. Məsələn, qurban "sistem problemləri" ilə bağlı bir təhdidlə qarşılaşdıqda, təcili qərarlar qəbul etməyə və məlumatlarını paylaşmağa daha meyilli olur.

Etibar qazanma mərhələsi, sosial mühəndislik hücumunun uğurlu olması üçün təməl yaradır. Hücum edən şəxsin bu mərhələdə istifadə etdiyi inandırıcı taktikalar, qurbanın manipulyasiya edilməsini asanlaşdırır və sonrakı mərhələlərin həyata keçirilməsi üçün zəmin yaradır. Bu səbəbdən, şəxslər və təşkilatlar potensial manipulyasiya cəhdlərini tanımaq və bu cür hallarda diqqətli davranmaq üçün maarifləndirilməlidir. Etibarın istismarı yolu ilə həyata keçirilən hücumlara qarşı mübarizə üçün təhlükəsizlik tədbirlərinin gücləndirilməsi vacibdir.

3. Manipulyasiya

Manipulyasiya, sosial mühəndislik prosesinin ən kritik mərhələlərindən biridir və hücumun əsas məqsədlərinin həyata keçirildiyi məqamdır. Hücum edən şəxs, bu mərhələdə qurbanın davranışlarını təsir altına almaq və onu istədiyi hərəkətləri etməyə məcbur etmək üçün müxtəlif psixoloji və emosional taktikalardan istifadə edir. Manipulyasiyanın uğurlu olması, hücum edən şəxsin qurbanın zəif tərəflərini düzgün müəyyən etməsinə və onları istismar etməkdəki peşəkarlığından asılıdır[35].

Bu mərhələdə qurbanın qorxu, maraq, təcili yardım ehtiyacı və ya digər emosional vəziyyətləri manipulyasiya üçün əsas vasitələr kimi istifadə olunur. Hücum edən şəxslər, qurbanı həyəcanlandırmaq, çaşdırmaq və ya tələsik qərar qəbul etməyə məcbur etmək üçün diqqətlə seçilmiş ifadələrdən və ya təhdidlərdən istifadə edirlər. Məsələn, "Hesabınız bloklanıb, dərhal şifrənizi yeniləməlisiniz" kimi mesajlar, qurbanın vəziyyəti qiymətləndirmək üçün vaxtı olmadığı bir anda hərəkət etməsinə səbəb olur.

Manipulyasiya mərhələsində hücum edən şəxslər, qurbanın diqqətini dağıtmaq və ya şübhələrini azaltmaq üçün real vəziyyətlərə istinad edə bilərlər. Məsələn, qurbanın tez-tez istifadə etdiyi bir bankın və ya xidmətin adından gələn bir mesaj, qurbanın manipulyasiya edilməsini asanlaşdırır. Hücum edən şəxs, bu cür realistik ssenarilər

[35] Sosial mühəndislik nədir? - İlqar Şabanov

vasitəsilə qurbanın özünə inamını zəiflədir və onun qərar qəbul etmə qabiliyyətinə təsir göstərir.

Hücum edən şəxslər, qurbanın davranışlarını manipulyasiya etmək üçün həm də texnoloji vasitələrdən istifadə edə bilərlər. Saxta veb-saytlar, phishing e-poçtları və ya zərərli proqram təminatı, qurbanı müəyyən hərəkətləri etməyə təşviq edən alətlərdir. Məsələn, qurbanın zərərli bir linkə klikləməsi və ya saxta bir formaya şəxsi məlumatlarını daxil etməsi, manipulyasiyanın texnoloji tərəfini təşkil edir.

Manipulyasiya mərhələsi, sosial mühəndislik hücumunun nəticəsini birbaşa müəyyən edən həlledici bir mərhələdir. Bu mərhələnin uğurla həyata keçirilməsi, qurbanın emosional və psixoloji zəifliklərinin nə dərəcədə təsirli istismar edilməsindən asılıdır. Manipulyasiyanın qarşısını almaq üçün fərdlər və təşkilatlar şübhəli davranışları tanımağı öyrənməli, məlumat paylaşarkən ehtiyatlı olmalı və emosional reaksiyalarla deyil, rasional qərarlar əsasında hərəkət etməlidirlər. Təhlükəsizlik tədbirlərinin gücləndirilməsi və manipulyasiya üsullarının tanınması bu mərhələdə hücumların qarşısını almaq üçün əsas şərtlərdir.

4. Məqsədə nail olma

Məqsədə nail olma, sosial mühəndislik prosesinin kulminasiya nöqtəsidir və əsas məqsədin həyata keçirdiyi mərhələdir. Bu mərhələyə qədər hücum edən şəxs, məlumat toplama, etibar qazanma və manipulyasiya mərhələlərini uğurla tamamlamış və qurbanın zəifliklərindən maksimum istifadə etmişdir. Bu mərhələdə hücum edən şəxs, əldə etdiyi məlumatları və girişləri istifadə edərək qurbanın maliyyə resurslarına, şəxsi məlumatlarına və ya texnoloji sistemlərinə icazəsiz çıxış əldə edir[36].

Hücum edən şəxslər bu mərhələdə müxtəlif konkret fəaliyyətlər həyata keçirirlər. Bunlara şəxsi məlumatların oğurlanması, maliyyə əməliyyatlarının qanunsuz şəkildə aparılması, texnoloji sistemlərin zədələnməsi və ya zərərli proqramların yayılması daxildir. Məsələn, hücum edən şəxs qurbanın bank hesab məlumatlarına çıxış əldə edərək qanunsuz maliyyə əməliyyatları həyata keçirə bilər. Eyni zamanda, qurbanın texnoloji cihazlarına zərərli proqram təminatı yüklənərək məlumatların şifrələnməsi və fidyə tələb olunması ilə nəticələnən hücumlar da bu mərhələdə baş verir.

Bu mərhələdə hücum edən şəxs əsas məqsədi əldə etdiyi nəzarəti qorumaq və mümkün qədər çox fayda əldə etməkdir. Hücumun təsiri, adətən, qurbanın şəxsi və ya korporativ təhlükəsizliyinin ciddi şəkildə pozulması ilə nəticələnir. Məsələn, təşkilatlara qarşı həyata keçirilən hücumlar zamanı məxfi sənədlərin sızdırılması, sistemlərin işinin dayandırılması və ya təşkilatın nüfuzuna zərər verilməsi geniş yayılmış nəticələrdəndir.

Məqsədə nail olma mərhələsi, yalnız bir fərdin deyil, həm də təşkilatların və hətta cəmiyyətlərin genişmiqyaslı zərərə məruz qalması ilə nəticələnə bilər. Hücum edən şəxslərin bu mərhələdəki fəaliyyətləri qurbanların maliyyə sabitliyini və şəxsi təhlükəsizliyini ciddi təhlükə altına sala bilər. Buna görə də, şəxslər və təşkilatlar bu cür

[36] Социальная инженерия в информационной и кибербезопасности - Олег Антипов

hücumlara qarşı daha diqqətli olmalı, məlumatların qorunması üçün qabaqlayıcı tədbirlər görməli və təhlükəsizlik protokollarını gücləndirməlidirlər.

Bu mərhələnin qarşısını almaq üçün effektiv təhlükəsizlik tədbirlərinə ehtiyac var. Güclü şifrə siyasətləri, çoxfaktorlu identifikasiya, şübhəli fəaliyyətlərin monitorinqi və zərərli proqramlardan qorunma sistemləri bu cür hücumların təsirini minimuma endirmək üçün mühüm rol oynayır. Məqsədə nail olma mərhələsində hücumların təsirini azaltmaq üçün fərdlər və təşkilatlar potensial zəiflikləri aradan qaldırmalı və təhlükəsizlik mədəniyyətini inkişaf etdirməlidirlər.

5. İzlərin silinməsi

İzlərin silinməsi, sosial mühəndislik prosesinin sonuncu və strateji əhəmiyyət daşıyan mərhələsidir. Bu mərhələdə hücum edən şəxslər, öz fəaliyyətlərinin izlərini gizlətmək və aşkarlanmasının qarşısını almaq üçün xüsusi texnikalardan istifadə edirlər. Hücumun uğurla həyata keçirilməsi qədər, onun aşkar edilməməsi də hücum edən şəxsin hədəflərinə çatması və nəticələrinin daha uzunmüddətli təsir yaratması üçün vacibdir[37].

Hücum edən şəxslər bu mərhələdə, adətən, hücum zamanı istifadə etdikləri saxta identifikasiyaları, əlaqələri və ya digər rəqəmsal izləri silirlər. Məsələn, hücum zamanı göndərilən "phishing" e-poçtları və ya saxta veb-saytlar tez bir zamanda deaktiv edilir və ya sistemlərdən silinir. Bu, hücumun mənbəyinin müəyyən edilməsini və potensial əks-hücum tədbirlərinin qarşısını almaq məqsədi daşıyır.

Daha mürəkkəb hücumlarda hücum edən şəxslər, mənbə izlənməsini çətinləşdirmək üçün xüsusi texnologiyalardan və taktikalardan istifadə edirlər. Məsələn, hücum edən şəxslər virtual özəl şəbəkələr (VPN), anonimləşdirmə alətləri və ya saxta "IP" ünvanları vasitəsilə öz fəaliyyətlərini gizlədə bilərlər[38]. Həmçinin, hücum edən şəxslər zərərli proqramların fəaliyyətini avtomatik olaraq dayandırmaq və ya silmək üçün xüsusi mexanizmlər quraşdırırlar ki, bu da onların fəaliyyəti aşkarlanarkən dərhal deaktiv edilməsinə imkan yaradır.

Bu mərhələdə həyata keçirilən tədbirlər yalnız rəqəmsal mühitlə məhdudlaşmır. Hücum edən şəxslər, həmçinin, fiziki izləri silmək üçün də addımlar ata bilərlər. Məsələn, bir təşkilatın ərazisinə qanunsuz daxil olduqda, hər hansı bir müşahidə kamerasının görüntülərini silmək və ya saxta sənədlərin istifadəsini gizlətmək kimi üsullara müraciət edə bilərlər.

İzlərin silinməsi, hücum edən şəxslərin məsuliyyətdən yayınmasını təmin etmək və onların fəaliyyətlərinin daha geniş təsir göstərməsinə şərait yaradır. Bu səbəbdən, izlərin silinməsinə qarşı mübarizə tədbirləri təşkilatlar və şəxslər üçün kritik əhəmiyyət daşıyır. Rəqəmsal izlərin izlənilməsi, logların müntəzəm monitorinqi və güclü kibertəhlükəsizlik sistemlərinin tətbiqi bu mərhələdə hücumların qarşısını almaq üçün effektiv vasitələrdir.

Hücum edən şəxslər izlərini silməyə çalışdığı bu mərhələ, sosial mühəndislik hücumlarının daha uzunmüddətli nəticələrə səbəb olmasını təmin edir. Buna görə də,

[37] Как работает социальная инженерия - Алексей Малахов
[38] Bridgeport, connecticut awarded close to half a million for port security - www.securitymagazine.com/articles/93254-bridgeport-connecticut-awarded-close-to-half-a-million-for-port-security

təhlükəsizlik tədbirlərinin yalnız hücumun qarşısını almağa deyil, eyni zamanda hücum sonrası analiz və aşkarlama proseslərinə də fokuslanması vacibdir. Bu yanaşma, hücumların mənbəyini müəyyən etməyə və gələcəkdə bənzər hücumların qarşısını almağa kömək edir.

Sosial mühəndislik prosesinin həyata keçirilməsi

Sosial mühəndislik, insan davranışlarındakı zəifliklər texnoloji və psixoloji yanaşmalarla birləşdirərək həyata keçirilən mürəkkəb bir prosesdir. Hücum edən şəxslər bu prosesdə həm texnoloji, həm də insani faktorları istismar edərək, hədəflərinə çatmaq üçün hər bir mərhələni diqqətlə planlaşdırır və icra edirlər. Sosial mühəndislik, şəxsləri və ya təşkilatları manipulyasiya etməklə onların məlumatlarını və ya resurslarını ələ keçirməyi hədəfləyir. Bu prosesin uğuru, adətən, istifadə olunan metodların uyğunluğu və hücum edən şəxsin planlaşdırma qabiliyyətindən asılıdır.

Sosial mühəndislik prosesinin həyata keçirilməsində müxtəlif metodlar tətbiq olunur ki, bunlar hücum edən şəxslərin məqsədlərinə çatmasını asanlaşdırır. Bu metodlar arasında texnoloji tətbiqlərdən istifadə, fiziki tədbirlərin həyata keçirilməsi, qurbanların psixoloji manipulyasiya vasitəsilə təsir altına alınması və açıq mənbələrdən məlumatların toplanması kimi yanaşmalar yer alır. Hər bir metod, hücumun növünə və hədəfin xüsusiyyətlərinə uyğun olaraq fərqli şəkildə tətbiq edilir.

Sosial mühəndislik, yalnız texnoloji zəifliklərə əsaslanmır, eyni zamanda insan faktorunu manipulyasiya etməyi də əsas götürür. Bu, hücumun daha təsirli və genişmiqyaslı nəticələr əldə etməsinə imkan yaradır. Prosesin müxtəlif metodlarla həyata keçirilməsi, fərqli səviyyələrdə müdafiə tədbirlərinə ehtiyac olduğunu göstərir. Hər bir metod özünəməxsus yanaşma tələb edir və bu yanaşmaların təsirli olması, hücumların qarşısını almaq üçün zəruri addımları müəyyən etməyə kömək edir.

Bu prosesin detallı mərhələlərini anlamaq, həm şəxslərin, həm də təşkilatların sosial mühəndislik hücumlarına qarşı effektiv müdafiə tədbirləri tətbiq etməsi üçün vacibdir. Sosial mühəndislik prosesinin müxtəlif aspektlərini təhlil edərək, təhlükəsizlik tədbirlərini gücləndirmək və bu cür təhdidlərə qarşı daha hazırlıqlı olmaq mümkündür.

Prosesin həyata keçirilməsində aşağıdakı əsas metodlardan istifadə edilir:

- **Texnoloji tətbiqlər:** Sosial mühəndislik prosesində texnoloji tətbiqlər, hücum edən şəxslərin hədəflərinə çatmaq üçün istifadə etdiyi əsas metodlardan biridir. Bu yanaşma, rəqəmsal mühitdə texnologiyanın zəifliklərindən və insanların texnoloji biliklərinin kifayət qədər olmamasından faydalanaraq həyata keçirilir. Hücum edən şəxslər, texnoloji vasitələrlə qurbanların məlumatlarını ələ keçirmək, maliyyə resurslarına çıxış əldə etmək və ya sistemlərə zərər vermək üçün müxtəlif üsullardan istifadə edirlər.

Texnoloji tətbiqlərin ən geniş yayılmış forması “phishing” hücumlarıdır. Hücum edən şəxslər, saxta e-poçtlar və ya mesajlar vasitəsilə qurbanları manipulyasiya edərək onlardan həssas məlumatlar əldə etməyə çalışırlar. Bu e-poçtlar adətən, etibarlı bir qurumun adından göndərilir və təcili tədbir görməyi tələb edən məzmun daşıyır. Məsələn,

"Bank hesabınızda problem var, bu linkə klikləyərək şifrənizi yeniləyin" kimi mesajlar qurbanların diqqətini çəkir və onların məlumatlarını təqdim etməsinə səbəb olur.

Bundan əlavə, hücum edən şəxslər saxta veb-saytlar yaradırlar. Bu veb-saytlar real saytların dəqiq surətləri kimi təqdim olunur və qurbanları həssas məlumatlarını daxil etməyə məcbur edir. Məsələn, bank və ya sosial media platformalarının saxta səhifələri vasitəsilə qurbanların giriş məlumatları toplanır. Bu cür veb-saytlar, qurbanın diqqətsizliyindən və texnoloji detallara kifayət qədər diqqət yetirməməsindən istifadə edir.

Texnoloji tətbiqlərin digər bir forması zərərli proqramların yayılmasıdır. Hücum edən şəxslər, qurbanların cihazlarına viruslar, "trojanlar" və ya "ransomware" (fidyə proqramları) yükləyərək onların məlumatlarını oğurlayır və ya cihazlara zərər verir. Məsələn, qurbanın bir fayl yükləməsi və ya bir linkə klikləməsi nəticəsində bu proqramlar qurbanın cihazında aktivləşir və məlumatları hücum edən şəxsin nəzarətinə keçirir.

Texnoloji tətbiqlər, sosial mühəndislik hücumlarının təsirini artıran mühüm vasitələrdən biridir. Bu səbəbdən, şəxslər və təşkilatlar texnoloji təhlükəsizlik tədbirlərini gücləndirməli, phishing cəhdlərini tanımaq üçün təlimlərdə iştirak etməli və cihazlarında güclü antivirus proqramlarından istifadə etməlidirlər. Eyni zamanda, şübhəli e-poçt və linklərə qarşı diqqətli olmaq, texnoloji tətbiqlərlə həyata keçirilən sosial mühəndislik hücumlarının qarşısını almaq üçün vacibdir.

- **Fiziki tədbirlər:** Sosial mühəndislik prosesində fiziki tədbirlər, hücum edən şəxslərin qurbanın məlumatlarına və resurslarına birbaşa fiziki müdaxilə yolu ilə çıxış əldə etmək məqsədilə həyata keçirilən metodlardır. Bu yanaşma, texnoloji manipulyasiyadan fərqli olaraq, qurbanın fiziki mühitinə daxil olmağı və onun avadanlıqlarına və ya məlumat daşıyıcılarına təsir göstərməyi nəzərdə tutur. Fiziki tədbirlər, adətən, korporativ mühitlərdə və ya məxfi məlumatların saxlandığı yerlərdə tətbiq olunur.

Hücum edən şəxslər, qurbanın ərazisinə fiziki olaraq daxil olmaq üçün müxtəlif üsullardan istifadə edirlər. Məsələn, özlərini texniki xidmət əməkdaşı, işçi və ya ziyarətçi kimi göstərərək təhlükəsizlik baryerlərini aşa bilərlər. Təşkilat daxilində icazəsiz giriş əldə etdikdən sonra, hücum edən şəxslər xüsusi cihazlar yerləşdirmək və ya məlumat oğurlamaq üçün hərəkətə keçirlər.

Fiziki tədbirlərin geniş yayılmış formalarından biri, zərərli cihazların yerləşdirilməsidir. Hücum edən şəxslər, təşkilatın şəbəkəsinə qoşulmaq üçün gizli şəkildə "USB" cihazları, simsiz routerlər və ya zərərli proqramlarla təchiz edilmiş digər avadanlıqlar yerləşdirə bilərlər. Məsələn, işçilər tərəfindən diqqətsizlik nəticəsində istifadə edilən "USB" cihazları, qurbanın məlumatlarının oğurlanması və ya sistemlərinin kompromitasiya olunması ilə nəticələnə bilər.

Başqa bir fiziki tədbir isə məxfi sənədlərin və ya məlumatların oğurlanmasıdır. Hücum edən şəxslər, zibil qutularını araşdırmaq ("dumpster" "diving"), ofislərdə açıq qalmış sənədləri toplamaq və ya şəbəkə avadanlıqlarını manipulyasiya etmək kimi

üsullarla qurbanın məlumatlarını əldə edirlər. Bu cür fiziki tədbirlər, adətən, təşkilatın təhlükəsizlik qaydalarına riayət etməməsindən və ya zəif nəzarətdən istifadə edilir.

Fiziki tədbirlər, həm də müşahidə kameralarının və ya təhlükəsizlik sistemlərinin manipulyasiya edilməsini əhatə edə bilər. Hücum edən şəxslər, bu sistemləri təsirsiz hala gətirərək öz hərəkətlərini gizlədə bilər və ya təşkilatın fiziki təhlükəsizlik tədbirlərini aşmaq üçün digər üsullara müraciət edə bilərlər.

Bu cür hücumların qarşısını almaq üçün təşkilatlar fiziki təhlükəsizlik tədbirlərini gücləndirməlidirlər. Məsələn, giriş-çıxışların biometrik identifikasiya sistemləri ilə məhdudlaşdırılması, işçilərə təhlükəsizlik qaydalarının öyrədilməsi və zibil qutularının məxfi sənədlərdən təmizlənməsi kimi tədbirlər tətbiq edilməlidir. Fiziki tədbirlərin də sosial mühəndislik hücumlarının bir hissəsi ola biləcəyini nəzərə almaq və bu sahədə diqqətli olmaq təhlükəsizliyin təmin edilməsi üçün vacibdir.

- **Psixoloji manipulyasiya:** Psixoloji manipulyasiya, sosial mühəndislik hücumlarının ən güclü və təsirli metodlarından biridir. Bu yanaşma, qurbanın emosional zəifliklərini və insan psixologiyasının təbii xüsusiyyətlərini istismar edərək onun davranışlarına təsir göstərməyi hədəfləyir. Hücum edən şəxslər, qurbanın emosional vəziyyətlərindən və qərar qəbul etmə prosesindəki qısa yollardan istifadə edərək onu istənilən hərəkətləri etməyə məcbur edirlər.

Psixoloji manipulyasiya zamanı hücum edən şəxslər, qorxu, təcili yardım ehtiyacı, maraq və ya etibar kimi emosional faktorları təsir vasitəsi kimi istifadə edirlər. Məsələn, qurbanı təcili tədbir görməyə məcbur edən bir e-poçt və ya zəng göndərərək, "Hesabınız bloklanıb, dərhal məlumatlarınızı təsdiqləyin" kimi təhdidlər qurbanın soyuqqanlı davranmaq qabiliyyətini zəiflədir və tələsik qərar qəbul etməsinə səbəb olur.

Manipulyasiya prosesində inandırıcılığı artırmaq üçün hücum edən şəxslər özlərini etibarlı şəxslər və ya qurumlar kimi təqdim edə bilərlər. Məsələn, texniki dəstək işçisi, hüquq-mühafizə orqanı nümayəndəsi və ya bank işçisi rolunda çıxış edərək, qurbanın onlara inanmasını təmin etməyə çalışırlar. Qurban, bu "etibarlı" mənbəyə güvənərək şəxsi məlumatlarını könüllü şəkildə təqdim edə bilər.

Psixoloji manipulyasiyanın digər bir üsulu isə maraq oyatmaq və ya cəlbedici təkliflər təqdim etməkdir. Məsələn, "Pulsuz hədiyyə qazanın" və ya "Sizin üçün eksklüziv təklifimiz var" kimi mesajlarla qurbanın diqqəti çəkilir və onu zərərli linklərə klikləməyə və ya məlumatlarını paylaşmağa təşviq edir.

Hücum edən şəxslər həm də qurbanın etibarını qazanmaq üçün əlaqələrin gücündən istifadə edirlər. Qurbanın ailə üzvü, dostu və ya həmkarı kimi davranaraq, onun emosional bağlarını manipulyasiya edə bilərlər. Məsələn, "Mən sizin iş yoldaşınızam, sizin şifrənizə təcili ehtiyacım var" kimi bir müraciət, qurbanın şübhələrini azalda və onu məlumat paylaşmağa sövq edə bilər.

Psixoloji manipulyasiya, insan davranışlarının mürəkkəbliyindən və qurbanın ani emosional reaksiyalarından faydalanaraq həyata keçirilir. Bu cür manipulyasiyalara qarşı mübarizə aparmaq üçün fərdlər emosional reaksiyalara əsaslanaraq qərar qəbul etməkdən çəkinməli, hər bir müraciəti şübhə ilə qarşılamalı və məlumat paylaşmadan əvvəl onun mənbəyini dəqiq yoxlamalıdırlar.

- **Açıq mənbə kəşfiyyatı (OSINT-open source intelligence),** sosial mühəndislik prosesində hücum edən şəxslərin qurbanlar haqqında məlumat toplamaq üçün geniş istifadə etdiyi bir metoddur. Bu yanaşma, qanuni olaraq mövcud olan və açıq mənbələrdə yayımlanan məlumatların toplanmasına və təhlil edilməsinə əsaslanır. OSINT, qurbanın şəxsi və peşəkar məlumatlarını, maraqlarını, texnoloji istifadə vərdişlərini və digər zəifliklərini müəyyən etmək üçün effektiv bir vasitədir[39].

Hücum edən şəxslər, OSINT vasitəsilə müxtəlif onlayn platformalardan və mənbələrdən məlumat toplayırlar. Bu mənbələrə sosial media platformaları, şəxsi və ya şirkət veb-saytları, xəbər mənbələri, açıq bazalar, onlayn forumlar və hətta dövlətin ictimai məlumat resursları daxildir. Məsələn, LinkedIn profili vasitəsilə bir işçinin vəzifəsi və çalışdığı şirkət haqqında məlumat əldə edilə bilər, bu da hücum edən şəxslərin şirkətin strukturunu və potensial zəifliklərini müəyyən etməkdə kömək edir.

OSINT vasitəsilə toplanan məlumatlar qurbanın texnoloji və ya psixoloji zəifliklərini hədəfə almaq üçün hücumun digər mərhələlərində istifadə edilir. Hücum edən şəxslər, qurbanın sosial media paylaşımlarını təhlil edərək onun maraqlarını, gündəlik fəaliyyətlərini və şəxsi əlaqələrini öyrənə bilərlər. Bu məlumatlar, saxta e-poçtlar, hədəflənmiş phishing hücumları və ya qurbanın etibarını qazanmağa yönəlmiş strategiyalar hazırlamaq üçün istifadə olunur.

Məsələn, bir qurbanın tez-tez paylaşdığı maraqları və ya son iş səyahəti haqqında məlumatları öyrənən hücum edən şəxsi, bu məlumatlara əsaslanaraq inandırıcı və fərdiləşdirilmiş bir phishing mesajı hazırlaya bilər. Mesajın şəxsi görünməsi qurbanın şübhələrini azaldır və onun manipulyasiyaya məruz qalma ehtimalını artırır.

Hücum edən şəxslər, OSINT vasitəsilə təkcə şəxsləri deyil, həm də təşkilatları hədəf ala bilərlər. Məsələn, bir təşkilatın veb-saytında təqdim edilən işçi siyahıları, əlaqə məlumatları və ya fəaliyyət hesabatları hücum edən şəxslərə həmin təşkilatın daxili strukturunu anlamaqda və zəifliklər müəyyən etməkdə kömək edir. Bu məlumatlar, xüsusilə korporativ və ya dövlət qurumlarına qarşı həyata keçirilən sosial mühəndislik hücumlarında böyük əhəmiyyət kəsb edir.

Açıq mənbə araşdırmasına qarşı mübarizə üçün şəxslər və təşkilatlar öz məlumatlarının açıq mənbələrdə nə dərəcədə mövcud olduğunu mütəmadi olaraq təhlil etməli və həssas məlumatları paylaşarkən diqqətli olmalıdırlar. Sosial media məxfilik parametrlərinin düzgün tənzimlənməsi, işçi siyahılarının və digər korporativ məlumatların açıq paylaşılmaması, OSINT-ə qarşı əsas müdafiə tədbirləridir. Bundan əlavə, maarifləndirmə və təlimlər, fərdlərin və təşkilatların açıq mənbələrdəki məlumatlarının təhlükəsizliyini təmin etmək üçün vacibdir. OSINT hücumlarının qarşısını almaq, məlumatların qorunması üzrə mədəniyyətin inkişaf etdirilməsi ilə mümkündür.

[39] What is OSINT? - www.sentinelone.com/cybersecurity-101/threat-intelligence/open-source-intelligence-osint

Nəticə

Sosial mühəndislik, insan davranışlarındakı zəifliklərdən və texnoloji boşluqlardan istifadə edərək məlumatların oğurlanması, sistemlərə icazəsiz giriş təmin edilməsi və manipulyasiya yolu ilə müəyyən hədəflərə çatılması məqsədini daşıyan kompleks bir hücum növüdür. Bu metodlar, həm şəxslərin, həm də təşkilatların təhlükəsizlik tədbirlərini aşmaq üçün texnoloji, fiziki və psixoloji yanaşmaların birləşməsinə əsaslanır. Sosial mühəndislik, müasir dövrdə şəxslərin və təşkilatların təhlükəsizliyinə qarşı ən ciddi təhdidlərdən biri olaraq qəbul edilir.

Sosial mühəndisliyin uğuru, onun mərhələlərinin dəqiqliklə planlaşdırılması və icra edilməsindən asılıdır. Məlumat toplama mərhələsindən başlayan bu proses, etibar qazandıqdan sonra manipulyasiya və hücumun əsas məqsədinə nail olma ilə davam edir. Hücumun təsirini artırmaq və qurbanın manipulyasiyaya qarşı müqavimətini zəiflətmək üçün psixoloji və texnoloji vasitələrdən peşəkar şəkildə istifadə edilir. Nəticədə, qurbanın maliyyə resursları, şəxsi məlumatları və ya texnoloji sistemləri risk altında qalır.

Texnoloji tətbiqlər, fiziki tədbirlər, psixoloji manipulyasiya və açıq mənbə araşdırmaları sosial mühəndislik hücumlarının həyata keçirilməsi üçün əsas vasitələrdir. Hücum edən şəxslər, bu yanaşmalar vasitəsilə qurbanın zəifliklərindən faydalanaraq müxtəlif səviyyələrdə təhlükəsizlik tədbirlərini pozurlar. Xüsusilə texnoloji vasitələrdən istifadə edərək phishing e-poçtları, saxta veb-saytlar və zərərli proqramlar yaymaq, fiziki müdaxilə ilə məlumat daşıyıcı cihazları manipulyasiya etmək və qurbanın psixoloji zəifliklərini manipulyasiya etmək bu metodların əsas nümunələridir. Bu yanaşmalar, sosial mühəndislik hücumlarının yalnız fərdlərə deyil, təşkilatlara və hətta dövlətlərə qarşı tətbiq oluna biləcəyini göstərir.

Sosial mühəndislik hücumlarının təsiri geniş və çoxşaxəlidir. Bu hücumlar fşəxsi həyata, təşkilatların iş proseslərinə, dövlətlərin milli təhlükəsizliyinə və bütövlükdə cəmiyyətin sabitliyinə mənfi təsir göstərə bilər. Hücumların nəticələri maliyyə itkilərindən şəxsi məlumatların sızmasına, ictimai sabitliyin pozulmasından dövlətlərin reputasiya zərərlərinə qədər geniş bir spektri əhatə edir. Hücum edən şəxslərin izlərini silmə və məsuliyyətdən yayınma cəhdləri isə bu təsirlərin uzunmüddətli olmasına səbəb ola bilər.

Nəticədə, sosial mühəndislik hücumlarının qarşısını almaq üçün çoxsəviyyəli və sistemli yanaşma tətbiq olunmalıdır. İnsanların və təşkilatların məlumat təhlükəsizliyi haqqında maarifləndirilməsi, texnoloji təhlükəsizlik tədbirlərinin gücləndirilməsi və psixoloji manipulyasiyalara qarşı davamlılığın artırılması bu mübarizənin əsas elementləridir. Sosial mühəndislik hücumlarını anlamaq və onların mürəkkəb təbiətini təhlil etmək, bu təhdidlərə qarşı daha hazırlıqlı olmaq və təhlükəsizlik səviyyəsini artırmaq üçün vacibdir. Gələcəkdə daha təhlükəsiz və sabit bir cəmiyyət üçün sosial mühəndislik hücumlarına qarşı davamlı diqqət və mübarizə zəruridir.

§ 4. Sosial mühəndisliyin psixoloji aspektləri və psixoloji manipulyasiya texnikaları

Giriş

Sosial mühəndislik, insanların psixoloji xüsusiyyətlərini və davranışlarının təbii zəifliklərini manipulyasiya edərək məlumatların oğurlanması, sistemlərə icazəsiz girişin təmin edilməsi və ya müəyyən hədəflərə çatmaq üçün tətbiq olunan mürəkkəb texnikalar toplusudur. Bu metod, insan psixologiyasının qərar qəbul etmə prosesindəki qısa yollarına və emosional reaksiyalarına əsaslanır. Sosial mühəndisliyin uğuru yalnız texnoloji vasitələrin istifadəsi ilə deyil, həm də insan davranışlarının dərindən təhlil edilməsi və manipulyasiya üçün uyğun zəifliklərin tapılması ilə bağlıdır.

İnsanlar, təbii olaraq, müəyyən sosial normalara və emosional reaksiyalara sahibdirlər. Etibar etmək, kömək etmək, qorxulara və ya təhlükələrə reaksiya vermək kimi davranış nümunələri, sosial mühəndislik hücumlarında əsas istismar nöqtələri hesab edilir. Hücum edən şəxslər, qurbanların psixoloji vəziyyətlərini və fərdi xüsusiyyətlərini diqqətlə analiz edərək, onların zəifliklərini istismar etmək üçün spesifik taktikalardan istifadə edirlər. Bu yanaşma, sosial mühəndislik hücumlarının təsir gücünü artırır və qurbanların manipulyasiyaya məruz qalmasını asanlaşdırır.

Psixoloji manipulyasiya texnikaları, qurbanın emosional vəziyyətlərini oyanış nöqtəsinə çatdıraraq, onu daha sürətli, düşünülməmiş və diqqətsiz qərarlar qəbul etməyə məcbur edir. Hücum edən şəxslər, qorxu yaratmaq, təcili yardım ehtiyacı yaratmaq və ya qurbanın inamını qazanmaq kimi üsullardan istifadə edərək onu öz nəzarətləri altına alırlar. Məsələn, “Hesabınız bağlanmaq üzrədir, dərhal məlumatlarınızı təsdiqləyin” kimi mesajlarla qurban tələsik hərəkət etməyə məcbur edilir və qərar qəbul etmə prosesi pozulur.

Bu cür manipulyasiya metodları şəxslər və təşkilatlar üçün ciddi təhlükələr yaradır. İnsanların emosional zəifliklərindən və psixoloji reaksiyalarından istifadə edilərək həyata keçirilən hücumlar, təkcə şəxslərə deyil, həm də təşkilatlara və cəmiyyətə genişmiqyaslı təsir göstərə bilər. Hücum edən şəxslərin istifadə etdiyi psixoloji texnikalar, sosial mühəndislik hücumlarının texnoloji aspektlərinə əlavə olaraq, bu hücumları daha mürəkkəb və təhlükəli hala gətirir.

Psixoloji manipulyasiya, sosial mühəndisliyin əsasını təşkil edir və hücum edən şəxslərin hədəflərinə çatması üçün ən təsirli vasitələrdən biridir. Bu səbəbdən, fərdlər və təşkilatlar yalnız texnoloji təhlükəsizlik tədbirlərinə deyil, eyni zamanda psixoloji manipulyasiyalara qarşı müdafiə tədbirlərinə də diqqət yetirməlidirlər. Hücumların uğur qazanmasının əsas səbəbi insan davranışlarının zəifliklərindən istifadə edilməsidir. Buna görə də, bu zəiflikləri anlamaq və aradan qaldırmaq üçün davamlı maarifləndirmə və təlimlər vacibdir. Psixoloji manipulyasiyaya qarşı hazırlıqlı olmaq, sosial mühəndislik hücumlarının təsirini minimuma endirmək üçün ən mühüm addımlardan biridir.

Sosial mühəndisliyin psixoloji aspektləri

Sosial mühəndisliyin əsasını insan psixologiyasının zəif tərəflərindən istifadə təşkil edir. Bu yanaşma, insanların emosional reaksiyalarını və davranış nümunələrini manipulyasiya etməklə onların qərar qəbul etmə prosesinə təsir göstərməyə əsaslanır. Texnologiya nə qədər inkişaf etsə də, insanlar hələ də təhlükəsizlik sistemlərində ən zəif halqa hesab olunurlar. Sosial mühəndislikdə hücum edən şəxslər texniki vasitələrlə yanaşı, qurbanın psixoloji xüsusiyyətlərini də istismar edərək hədəflərinə çatırlar. Psixoloji aspektlər, bu prosesin ən incə və təsirli tərəflərindən biri olaraq qəbul edilir.

Sosial mühəndislik, insanın təbii ehtiyacları, zəiflikləri və qısa yolla qərar qəbul etməyə meyilləri kimi psixoloji xüsusiyyətlərdən faydalanır. Hücum edən şəxslər, qurbanın qorxu, maraq, inam və ya təcili yardım ehtiyacından istifadə edərək onu manipulyasiya edirlər. Bu yanaşma, qurbanın rasional düşünmə qabiliyyətini zəiflədir və onu düşünülməmiş qərarlar qəbul etməyə məcbur edir. Psixoloji aspektlərin anlaşıldığı və tətbiq edildiyi hallarda sosial mühəndislik hücumlarının təsir gücü əhəmiyyətli dərəcədə artır.

Sosial mühəndisliyin psixoloji aspektləri, qurbanın emosional vəziyyətini və psixoloji zəifliklərini manipulyasiya etməklə onun davranışlarını yönləndirməyə əsaslanır. Bu aspektlər, insan psixologiyasının təməl prinsipləri üzərində qurulub və qərar qəbul etmə prosesində qısa yolların istismar edilməsini nəzərdə tutur. Qorxu, təcili qərar tələbi, sosial qəbul olunma ehtiyacı və etibar kimi faktorlar, sosial mühəndisliyin psixoloji bazasını təşkil edir.

Məsələn, insanlar çox vaxt təhdidlərə reaksiya vermək üçün dərhal tədbir görməyə çalışır və ya etibarlı mənbədən gələn tələbləri şübhə altına almadan yerinə yetirirlər. Bu, Hücum edən şəxslərin qurbanları daha sürətli manipulyasiya etməsinə şərait yaradır. Sosial mühəndisliyin psixoloji aspektləri, yalnız şəxslərə deyil, eyni zamanda qruplara və təşkilatlara qarşı da tətbiq edilə bilər. İnsanların sosial normlara uyğun davranmaq və ya müəyyən bir situasiyada uyğunlaşmaq ehtiyacları, psixoloji manipulyasiya üçün əsas zəmin yaradır.

Müxtəlif mütəxəssislər və tədqiqatçılar sosial mühəndisliyin psixoloji aspektlərini analiz edərək bu sahənin əsas mexanizmlərini izah etmişlər. Onların fikirləri, sosial mühəndislik hücumlarının təbiətini və təsir mexanizmlərini anlamağa kömək edir. Aşağıda bu sahədə tanınmış mütəxəssislərin fikirləri və müvafiq istinadları təqdim olunur:

Kevin Mitnick: İnsan etimadının manipulyasiyası

Mitnick, sosial mühəndisliyi "insan etimadını manipulyasiya etmə sənəti" kimi təsvir edir. Onun fikrincə, hücumlar texnologiyadan daha çox insan zəifliklərinə əsaslanır. Mitnick qeyd edir ki, "hücumların əsasını qurbanın etimadını qazanmaq və bu etimadı istismar etmək təşkil edir".[40]

[40] The art of deception: controlling the human element of security - Kevin D. Mitnick, William L. Simon

Robert B. Cialdini: Sosial təsir prinsipləri

Cialdini, sosial mühəndislikdə manipulyasiya metodlarını sosial təsir prinsipləri ilə əlaqələndirir. Onun araşdırmalarına görə, sosial təsir prinsipləri - o cümlədən uyğunlaşma, təzyiq və sosial sübut - qurbanların davranışlarını manipulyasiya etmək üçün effektiv mexanizmlərdir[41].

Christopher Hadnagy: İnsan psixologiyasının istismarı

Hadnagy, sosial mühəndisliyin insan psixologiyasını manipulyasiya etməyə əsaslanan mürəkkəb bir proses olduğunu vurğulayır. O bildirir ki, "sosial mühəndislik, insan beyninin necə işlədiyini və onun emosional reaksiyalarını istismar etməyi anlamaqla əlaqəlidir".[42]

Daniel Kahneman: Emosional və intuitional düşüncə

Kahneman, insanların sürətli və düşünülməmiş qərar qəbul etmə meyillərinin sosial mühəndislik hücumlarında geniş istifadə edildiyini bildirir. O qeyd edir ki, "emosional və intuitional reaksiyalar çox vaxt rasional düşüncəni üstələyir, bu da manipulyasiya üçün şərait yaradır".[43]

Müxtəlif mütəxəssislərin analizləri, sosial mühəndislikdə istifadə olunan manipulyasiya texnikalarının yalnız fərdi zəifliklərdən deyil, insan davranışlarının universal prinsiplərindən qaynaqlandığını vurğulayır. İstinad olunan mənbələr bu sahəni dərindən öyrənmək və təhlükəsizlik strategiyalarını inkişaf etdirmək üçün əsaslı bilik mənbələridir.

Sosial mühəndisliyin əsas psixoloji aspektləri insan psixologiyasının müxtəlif zəifliklərinə əsaslanır və aşağıdakı əsas növlərə bölünür:

Etibarın istismarı

Etibarın istismarı, sosial mühəndislikdə ən geniş istifadə olunan psixoloji manipulyasiya texnikalarından biridir. İnsanların təbii olaraq etibarlı mənbələrə inanmaq, onlara güvənmək və təqdim edilən məlumatları şübhə altına almadan qəbul etmək meyilləri bu texnikanın əsasını təşkil edir. Hücum edən şəxslər, qurbanların bu xüsusiyyətindən istifadə edərək onları manipulyasiya edir və lazımi məlumatları əldə etməyə çalışırlar.

İnsanlar, adətən, tanınmış şəxslərə, qurumlara və ya real görünən mesajlara qarşı daha az şübhə göstərirlər. Bu, hücum edən şəxslərin özlərini etibarlı bir mənbə kimi təqdim edərək qurbanların inamını qazanmasını asanlaşdırır. Məsələn, hücum edən şəxs özünü bir bankın əməkdaşı, texniki dəstək mütəxəssisi və ya iş yoldaşı kimi təqdim edərək qurbanın şəxsi məlumatlarını və ya maliyyə resurslarına girişini əldə edə bilər.

Qorxu və təcili qərar tələbi

Qorxu və təcili qərar tələbi, sosial mühəndislikdə geniş istifadə olunan güclü psixoloji manipulyasiya üsullarından biridir. Bu texnika, qurbanın emosional reaksiyalarını istismar edərək, onu tələsik və düşünülməmiş qərarlar qəbul etməyə

[41] Influence: the psychology of persuasion - Cialdini, R. B

[42] Human hacking: win friends, influence people, and leave them better off for having met you - Christopher Hadnagy, Seth Schulman

[43] Thinking, fast and slow - Daniel Kahneman

məcbur etmək məqsədi daşıyır. Hücum edən şəxslər, qurbanın qorxu, təhdid və ya təhlükə hisslərini artıraraq, onun rasional düşünmə qabiliyyətini zəiflədir və sürətli qərar qəbul etməsini təmin edirlər.

Bu metod adətən "təcili" və ya "kritik" vəziyyətlər yaratmaqla həyata keçirilir. Məsələn, hücum edən şəxs bir e-poçt və ya zəng vasitəsilə qurbana "Hesabınızda şübhəli fəaliyyət aşkar edilib, dərhal məlumatlarınızı təsdiqləməsəniz, hesabınız bağlanacaq" kimi mesaj göndərir. Qurban, təhlükə hissinə qapılaraq, bu məlumatı dərhal paylaşmaqla manipulyasiyaya məruz qalır.

Uyğunlaşma və sosial təsir

Uyğunlaşma və sosial təsir, sosial mühəndislikdə qurbanın sosial davranış meyillərindən istifadə etməyə əsaslanan bir manipulyasiya texnikasıdır. İnsanlar, təbii olaraq, müəyyən sosial normalara uyğunlaşmağa və başqalarına kömək etməyə meyillidirlər. Hücum edən şəxslər, bu xüsusiyyətləri manipulyasiya edərək qurbanların müəyyən hərəkətlər etməsini və ya məlumatları paylaşmasını təmin edirlər.

İnsanların uyğunlaşma ehtiyacı, cəmiyyətin bir hissəsi olmaq və sosial qəbula nail olmaq istəyindən qaynaqlanır. Hücum edən şəxslər, bu ehtiyacı manipulyasiya edərək qurbanların qərar qəbul etmə prosesinə təsir göstərirlər. Məsələn, bir şəxs özünü tanıdığınız və ya hörmət etdiyiniz bir qrupun üzvü kimi təqdim etdikdə, siz onun tələblərinə daha az şübhə ilə yanaşa bilərsiniz. Bu, qurbanın diqqətsiz davranmasına və təhlükəsizlik tədbirlərini pozmasına səbəb ola bilər.

Marağın oyandırılması

Marağın oyandırılması, sosial mühəndislikdə qurbanın diqqətini cəlb etmək və onu müəyyən hərəkətlərə yönləndirmək üçün istifadə olunan psixoloji manipulyasiya texnikasıdır. Bu texnikanın əsas məqsədi, qurbanın marağını və ya təşvişini artıraraq, onun təhlükəsizlik tədbirlərini unudub tələsik qərarlar qəbul etməsini təmin etməkdir. Hücum edən şəxslər, qurbanın təbii maraq hissindən, qazanmaq istəyindən və ya eksklüziv bir təklifə cavab vermək ehtiyacından faydalanırlar.

Bu texnika adətən cəlbedici təkliflər və ya qeyri-adi məlumatlarla qurbanın diqqətini çəkmək yolu ilə həyata keçirilir. Məsələn, "Pulsuz hədiyyə qazanın", "Bu eksklüziv təklifi qaçırmayın" və ya "Sizin haqqınızda şok edici məlumatlar aşkar edilib" kimi mesajlar qurbanı manipulyasiya etmək üçün geniş istifadə olunur.

Təzyiq və məcburiyyət

Təzyiq və məcburiyyət, sosial mühəndislikdə qurbanın sosial və ya emosional vəziyyətini manipulyasiya etmək üçün istifadə olunan texnikalardan biridir. Bu texnika, qurbanın üzərinə müəyyən bir məsuliyyət və ya məcburiyyət hissi yükləyərək, onu istənilən hərəkətləri etməyə məcbur etməyi hədəfləyir. Hücum edən şəxslər, bu texnikada sosial normlardan, qurbanın məcburiyyət hissindən və ya təzyiq altında düzgün qərar qəbul etmə qabiliyyətinin zəifliyindən istifadə edirlər.

Bu manipulyasiya texnikasında əsas məqsəd, qurbanın rasional düşüncə qabiliyyətini zəiflətmək və onu təzyiq altında tələsik hərəkət etməyə vadar etməkdir. Hücum edən şəxslər, sosial öhdəlik, nüfuz qorumaq istəyi və ya emosional zəifliklər kimi elementləri manipulyasiya edərək, qurbanın diqqətini əsas məqsəddən yayındırır.

Sosial mühəndislik prosesinin əsasını təşkil edən texnikalar - etibarın istismarı, qorxu və təcili qərar tələbi, uyğunlaşma və sosial təsir, marağın oyandırılması və təzyiq və məcburiyyət - insan davranışlarındakı təbii zəifliklərdən və emosional reaksiyalardan istifadə edir.

Bu texnikalar bir-birindən fərqli yanaşmalara malik olsa da, hamısı insan psixologiyasının zəifliklərini istismar etməyə əsaslanır. Sosial mühəndislik hücumlarının uğur qazanmasının əsas səbəbi, qurbanın emosional reaksiyalarının və qısa yolla qərar qəbul etmə meyillərinin manipulyasiya edilməsidir.

Bu texnikalara qarşı effektiv müdafiə, insanları maarifləndirmək, təlimlər keçirmək və təhlükəsizlik tədbirlərini gücləndirməkdən asılıdır. Emosional reaksiyalara nəzarət etmək, qərar qəbul etmədən əvvəl məlumatları və mənbələri yoxlamaq, həm şəxsi, həm də təşkilati səviyyədə təhlükəsizliyin təmin edilməsinə kömək edir. Sosial mühəndislik texnikalarını tanımaq və onlara qarşı tədbirlər görmək, müasir dünyada məlumat təhlükəsizliyini təmin etmək üçün vacibdir. Rasional düşüncə və ehtiyatlı yanaşma bu cür hücumların təsirini minimuma endirməyin əsas yollarıdır.

Psixoloji manipulyasiya texnikaları

Psixoloji manipulyasiya texnikaları, sosial mühəndislikdə insanların davranışlarını və qərarlarını manipulyasiya etmək üçün istifadə edilən strategiyalardır. Bu texnikalar insan psixologiyasının təbii zəifliklərini, emosional reaksiyalarını və qərar qəbul etmə prosesindəki qısa yollarını istismar etməyə əsaslanır. Manipulyasiya texnikaları şəxslərin qorxu, etibar, sosial təsir, maraq və ya təzyiq kimi emosional və davranış meyillərini hədəf alır. Texnikaların məqsədi qurbanın təhlükəsizlik qaydalarını pozaraq məlumat paylaşması və ya istənilən hərəkəti yerinə yetirməsidir.

Bu texnikalar yalnız fərdi səviyyədə deyil, həm də təşkilatlar və cəmiyyətlər üçün ciddi təhlükələr yaradır. Psixoloji manipulyasiya sosial mühəndislik hücumlarının uğurunda əsas rol oynayır, çünki hücum edən şəxslər qurbanın zəifliklərini maksimum dərəcədə istismar edirlər. Bu texnikaları başa düşmək və onlara qarşı effektiv tədbirlər görmək, təhlükəsizliyin təmin edilməsi və hücumların təsirinin azaldılması üçün vacibdir.

Sosial mühəndisliyin iki əsas elementi - hücum növləri və psixoloji manipulyasiya texnikaları - sosial mühəndisliyin uğurlu həyata keçirilməsi üçün bir-birini tamamlayan komponentlərdir. Hücum növləri, daha geniş bir çərçivədə sosial mühəndisliyin məqsədini və tətbiq sahəsini müəyyən edir, texnikalar isə bu məqsədə çatmaq üçün istifadə edilən konkret üsulları ifadə edir.

Hücum növləri şəxslər, təşkilatlar və dövlətlərə yönələ bilən geniş miqyaslı strategiyaları təsvir edir. Psixoloji manipulyasiya texnikaları isə bu strategiyaların icrasını təmin edən spesifik taktikalardır. Bu yanaşmaların hər biri sosial mühəndislikdə mühüm rol oynayır və onların oxşar və fərqli cəhətlərini araşdırmaq, bu hücumları daha yaxşı başa düşməyə və qarşısını almağa imkan verir.

Sosial mühəndislik hücumlarının növləri ilə psixoloji manipulyasiyanın oxşar və fərqli cəhətləri

Sosial mühəndislik hücumlarının növləri ilə psixoloji manipulyasiya texnikaları arasında əsas oxşar cəhət onların hər ikisinin insan davranışlarının zəifliklərini və psixoloji xüsusiyyətlərini manipulyasiya etməyə yönəlməsidir. Hər iki yanaşma qurbanın emosional reaksiyalarını, diqqətsizliyini və ya qərar qəbul etmə meyillərini hədəf alır. Bu yanaşmalar həm şəxsləri, həm də təşkilatları manipulyasiya etməyə xidmət edir və hücumun məqsədinə nail olmaq üçün texnologiya ilə birləşdirilə bilər. Qorxu yaratmaq, etibardan faydalanmaq, maraq oyatmaq və təcili qərar qəbul etdirmək kimi üsullar həm növlərdə, həm də texnikalarda əsas prinsiplərdir.

Həm hücum növləri, həm də psixoloji manipulyasiya texnikaları, qurbanı manipulyasiya etməklə məlumatların oğurlanmasına, təhlükəsizlik tədbirlərinin pozulmasına və ya sistemlərin komprometasiya olunmasına yönəlir. Eyni zamanda, hər iki yanaşmada hücumlar planlaşdırılmış mərhələlər üzrə həyata keçirilir və qurbanın reaksiyalarını proqnozlaşdırmaq üçün psixoloji analizdən istifadə olunur.

Sosial mühəndislik hücumlarının növləri daha geniş bir təsnifatdır və hücumun məqsədini və miqyasını ifadə edir. Məsələn, şəxsi hədəflərə, korporativ qurumlara və ya dövlət sistemlərinə yönəlmiş hücumlar növlər arasında fərqlənir. Növlər, əsasən hücumun tətbiq sahəsini və ümumi strategiyasını təsvir edir. Digər tərəfdən, psixoloji manipulyasiya texnikaları spesifik taktikalardır və qurbanın müəyyən bir davranışını istiqamətləndirmək üçün konkret metodlardan istifadə edir. Texnikalar, növlərin tərkib hissəsi olaraq, hücumun necə həyata keçirildiyini müəyyənləşdirir.

Hücum növləri daha çox hədəfin kimliyinə və məqsədə fokuslanarkən, psixoloji manipulyasiya texnikaları, bu hədəfə çatmaq üçün tətbiq edilən fərdi üsullardır. Məsələn, fərdi hədəfə yönəlmiş bir hücumda "Etibarın istismarı" və "Qorxu və təcili qərar tələbi" texnikaları birlikdə tətbiq oluna bilər. Hücum növləri, hücumun miqyasını və istiqamətini müəyyənləşdirərkən, texnikalar onun icrasını təfərrüatlandırır.

Cəmiyyətdə rast gəlinən əsas manipulyasiya texnikaları aşağıdakılardır:

1. “Quid pro quo”: məlumat əldə etmək üçün müəyyən bir xidmət və ya fayda təklifi.

2. “Pretexting”: qurbanla əlaqə qurmaq üçün yalançı bir ssenari qurma.

3. “Baiting”: maraqlı və ya cazibədar məzmun təqdim edərək qurbanın diqqətini cəlb etmə.

4. “Phishing”: saxta e-poçt və ya veb-saytlar vasitəsilə məlumat toplama.

5. “Spear Phishing”: daha spesifik və hədəflənmiş phishing hücumları.

6. “Tailgatingv: qurbanın ardınca icazəsiz fiziki məkanlara daxil olma.

7. “Shoulder surfing”: qurbanın şifrə və ya PIN məlumatlarını müşahidə yolu ilə əldə etmə.

8. “Watering hole attack”: qurbanın tez-tez daxil olduğu platformaları manipulyasiya etmə.

9. “Honey trap”: qurbanın emosional zəifliklərindən istifadə edərək məlumat toplama.

10. “Scareware”: qorxuducu proqramlarla qurbanın məlumatlarını manipulyasiya etmə.

11. “Dumpster diving”: məlumat toplamaq üçün atılmış sənədlərin araşdırılması.

12. “Social media hijacking”: sosial media hesablarının ələ keçirilməsi.

13. “Reverse social engineering”: hücum edən şəxs əvvəlcə problem yaradır, sonra onu həll etmək üçün "yardım" təklif edir.

“Quid pro quo”, sosial mühəndislikdə qurbanın məlumatlarını əldə etmək üçün müəyyən bir xidmət və ya fayda təklif edilməsi ilə həyata keçirilən texnikadır. Bu texnika "bir şey qarşılığında bir şey" prinsipi ilə işləyir. Hücum edən şəxs, qurbanın ehtiyaclarını və ya zəifliklərini istismar edərək ona bir fayda və ya xidmət təklif edir və bunun müqabilində həssas məlumatların açıqlanmasını təmin edir[44].

Hücum edən şəxs, texniki dəstək nümayəndəsi, həkim və ya başqa bir sahədə çalışan şəxs kimi özünü təqdim edərək qurbanın qarşısında dəyərli görünməyə çalışır. Təklif etdiyi xidmət qarşılığında qurbanın şifrə, fərdi məlumatlar və ya texniki resurslara giriş icazəsi verməsini tələb edir. Məsələn, bir şəxsə zəng edilərək, "Texniki dəstəkdən zəng edirik, sisteminizdəki problemi həll etmək üçün şifrənizi təqdim etməlisiniz" deyilir. Qurban, texniki dəstək nümayəndəsinin həqiqiliyini yoxlamadan tələb olunan məlumatı paylaşır və nəticədə təhlükəsizlik pozuntusuna yol açır.

“Pretexting”, sosial mühəndislikdə hücum edən şəxsin qurbanla əlaqə qurmaq üçün yalançı və inandırıcı bir ssenari qurduğu texnikadır. Hücum edən şəxs özünü etibarlı və ya tanınmış bir şəxs, qurum nümayəndəsi və ya başqa bir hüquqi mənbə kimi göstərərək qurbanın məlumatlarını əldə etməyə çalışır. Bu texnika, inandırıcılığı artırmaq üçün təfərrüatlara əsaslanır və qurbanın şübhəsini minimuma endirərək onun etibarını qazanmağa yönəlir[45].

“Pretexting” texnikası diqqətlə planlaşdırılmış bir ssenari üzərində qurulur. hücum edən şəxs əvvəlcə qurban və onun mühiti haqqında kifayət qədər məlumat toplayır. Daha sonra bu məlumatlardan istifadə edərək qurbanla əlaqə qurur və müəyyən bir mövzuda saxta iddialar irəli sürür. Məsələn:

- Hücum edən şəxs özünü bank nümayəndəsi kimi təqdim edir və qurbanın hesabında şübhəli əməliyyatların olduğunu bildirir, bu zaman qurbanın şifrə və ya şəxsi məlumatlarını tələb edir.
- Hücum edən şəxs, bir şirkət işçisi kimi davranaraq texniki dəstək adı altında qurbanın kompüterinə daxil olmaq üçün icazə istəyir.

Bir şəxsə telefonla zəng edilərək, "Mən bankdan zəng edirəm, hesabınızda şübhəli bir əməliyyat var. Xahiş edirəm, bu problemi həll etmək üçün kart nömrənizi və təsdiqləmə kodunuzu təqdim edin" deyilir. Qurban, bu mesajın həqiqiliyini təsdiqləmədən tələb olunan məlumatı paylaşır.

[44] What is quid pro quo discrimination? - www.pelagohealth.com/resources/hr-glossary/quid-pro-quo
[45] What is pretexting? definition, examples, and attacks - Josh Fruhlinger

“Baiting”, sosial mühəndislikdə qurbanın diqqətini maraqlı və ya cazibədar bir təkliflə cəlb edərək onu manipulyasiya etməyə əsaslanan texnikadır. Bu texnikada hücum edən şəxs, qurbanın marağını oyatmaq üçün cazibədar məzmun və ya "pulsuz" təkliflər təqdim edir. Məqsəd, qurbanın təqdim olunan linkə klikləməsi, zərərli faylı yükləməsi və ya şəxsi məlumatlarını paylaşmasıdır. “Baiting” həm texnoloji mühitdə, həm də fiziki səviyyədə həyata keçirilə bilər[46].

Hücum edən şəxslə, qurbanın diqqətini çəkəcək məzmunlar yaradır və bu məzmun vasitəsilə manipulyasiya edirlər. Bu məzmunlar:

- Rəqəmsal mühitdə: "Pulsuz hədiyyə qazanın", "Eksklüziv təklif", "Bu faylı yükləyərək gizli məlumat əldə edin" kimi mesajlar vasitəsilə zərərli proqram və ya məlumat toplama hücumları həyata keçirilir.
- Fiziki mühitdə: Hücum edən şəxs, zərərli proqram yüklənmiş bir USB cihazını qurbanın iş mühitində görəcəyi bir yerə buraxır. Qurban bu cihazı taparaq maraqla kompüterinə daxil edir və nəticədə cihazın təhlükəsizliyinə zərər verən proqram yüklənir.

Bir e-poçt mesajında "Bu linkə klikləyərək 50% endirim kuponu qazanın!" ifadəsi yazılır. Qurban linkə kliklədikdə, ya zərərli bir veb-sayta yönləndirilir, ya da məlumatlarını paylaşmağa məcbur olur. Hücum edən şəxs, "Pulsuz musiqi yükləmə proqramı" adı altında zərərli bir fayl təqdim edir. Qurban bu faylı yükləyərək cihazını təhlükəyə atır.

“Phishing”, sosial mühəndislikdə saxta e-poçtlar, mesajlar və ya veb-saytlar vasitəsilə məlumat toplamaq məqsədi daşıyan ən geniş yayılmış texnikalardan biridir. Bu texnika, hücum edən şəxslərin qurbanın fərdi, maliyyə və ya digər həssas məlumatlarını əldə etmək üçün etibarlı mənbə adı altında manipulyasiya etməsinə əsaslanır. Phishing hücumlarında məqsəd qurbanı inandıraraq zərərli bir linkə klikləməyə, məlumatlarını təqdim etməyə və ya zərərli proqramı yükləməyə vadar etməkdir[47].

“Phishing” hücumları əsasən aşağıdakı üsullarla həyata keçirilir:

- E-poçt vasitəsilə: qurbana etibarlı bir qurumun adından saxta e-poçt göndərilir. Mesajda təcili bir vəziyyət vurğulanır və qurban linkə klikləyərək hesab məlumatlarını təqdim etməyə çağırılır.
- Saxta veb-saytlar: etibarlı bir qurumun veb-saytına bənzər saxta bir sayt yaradılır. Qurban linkə daxil olduqda, məlumatlarını təqdim edir və bu məlumatlar hücum edən şəxsin əlinə keçir.
- SMS və ya sosial media mesajları: qurban, mobil mesaj və ya sosial media vasitəsilə saxta təkliflərə və ya təhdidlərə məruz qalır.

Hücum edən şəxs, "Bank hesabınız bloklanıb, dərhal məlumatlarınızı yeniləyin!" mövzulu bir e-poçt göndərir. Mesajda qurbanın məlumatlarını daxil edəcəyi saxta bir link təqdim olunur. Saxta bir veb-sayt, tanınmış bir sosial media platformasına bənzədilir və qurbana "Hesabınıza giriş təsdiqi lazımdır" mesajı göndərilir. Qurban, həmin linkdə şifrəsini daxil edərək məlumatlarını itirir.

[46] What is baiting in cyber security? - www.terranovasecurity.com/blog/what-is-baiting
[47] Fişinq-kiberdələduzluq texnikası - www.cert.az/news/2017/fisinq-kiberdeleduzluq-texnikasi

“Spear phishing”, phishing-in daha spesifik və hədəflənmiş formasıdır. Bu texnika, qurban haqqında əvvəlcədən məlumat toplayaraq onun ehtiyaclarına, maraqlarına və ya zəifliklərinə uyğunlaşdırılmış saxta mesajların göndərilməsinə əsaslanır. Hücum edən şəxslər fərdiləşdirilmiş məzmun yaratmaq üçün qurbanın sosial media hesabları, iş mühiti, ictimai məlumat bazaları və digər mənbələrdən istifadə edirlər. Məqsəd, qurbanın etibarını qazanaraq onun həssas məlumatlarını ələ keçirməkdir[48].

“Spear phishing” hücumları ümumiyyətlə aşağıdakı üsullarla həyata keçirilir:

- Fərdiləşdirilmiş e-poçtlar: Hücum edən şəxslər, qurbanın maraqlarına və ya iş mühitinə uyğun saxta e-poçtlar hazırlayır. E-poçtda qurbanın adı, işlədiyi şirkətin adı və digər şəxsi məlumatlar yer alır.
- Spesifik hədəfləmə: mesajlar qurbanın yalnız özünü maraqlandıran bir məsələ ilə əlaqəli olur. Məsələn, "Komandanız üçün vacib bir sənəd əlavə etdim" kimi ifadələr təqdim edilir.
- Saxta sənədlər və ya linklər: mesajlara saxta linklər və ya zərərli sənədlər əlavə edilir. Qurban bu sənədləri açdıqda və ya linkə kliklədikdə, məlumatları hücum edən şəxslərin əlinə keçir.

Hücum edən şəxs, qurbanın sosial media hesabından əldə etdiyi məlumat əsasında saxta bir e-poçt hazırlayır. E-poçtda yazılır: "Hörmətli [Ad], iş yerinizdə ötən həftə müzakirə etdiyimiz layihənin sənədlərini əlavə edirəm. Xahiş edirəm, nəzərdən keçirib mənə bildirin." Qurban sənədi açdıqda, cihazına zərərli proqram yüklənir və ya məlumatları oğurlanır. Bir təşkilatın rəhbərinə göndərilən e-poçtda yazılır: "Təhlükəsizlik hesabatında problem var. Dərhal bu sənədi yükləyin və təcili tədbir alın." Mesaj rəhbərin diqqətini çəkərək onu linkə daxil olmağa məcbur edir.

“Tailgating”, sosial mühəndislikdə hücum edən şəxsin qurbanın ardınca təhlükəsizlik tədbirlərindən keçərək icazəsiz fiziki məkanlara daxil olmasına əsaslanan texnikadır. Bu texnika, hücum edən şəxsin özünü işçi, ziyarətçi və ya təsadüfi bir şəxs kimi göstərərək qurbanın etibarından və diqqətsizliyindən istifadə etməsinə yönəlir. Əsas məqsəd, məxfi məlumatlara, avadanlıqlara və ya resurslara birbaşa çıxış əldə etməkdir[49].

“Tailgating” hücumları müxtəlif üsullarla həyata keçirilə bilər:

- Fiziki yaxınlıq yaratmaq: hücum edən şəxs qapının açılmasını gözləyir və qurbanın ardınca qapıdan keçir. Məsələn, qurban qapını təhlükəsizlik kartı ilə açdıqda o sürətli bir hərəkətlə arxasınca keçir.
- Sosial təsir: hücum edən şəxs qurbanın empatiyasını manipulyasiya edərək giriş əldə edir. Məsələn, "Təcili işim var, təhlükəsizlik kartımı unutmuşam" kimi bəhanələr istifadə edir.
- İşçi kimi davranma: hücum edən şəxs, təşkilatın işçisi kimi davranaraq təhlükəsizlik tədbirlərindən yan keçmək üçün qurbanı aldadır.

Bir iş yerində hücum edən şəxs, qapını açmaq üçün təhlükəsizlik kartını istifadə edən işçinin arxasınca qapıdan keçir və həmin məkanda məxfi sənədləri və ya

[48] What is spear phishing? - Matthew Kosinski
[49] What is tailgating? - Isabel Leckie

məlumatları əldə edir. Hücum edən şəxs, "Mən buranın texniki dəstək işçisiyəm, amma kartım itdi" deyərək qurbanın qapını açmasını təmin edir və təhlükəsiz məkanlara daxil olur.

"Shoulder surfing" texnikası qurbanın şifrə, PIN və ya digər həssas məlumatlarını birbaşa müşahidə yolu ilə əldə etməyə əsaslanır. Bu texnika, əsasən ictimai yerlərdə, məsələn, bankomatlar və ya kompüterlərin qarşısında həyata keçirilir[50].

"Watering hole" texnikasında hücum edən şəxs, qurbanın tez-tez daxil olduğu veb-saytları və ya platformaları manipulyasiya edir. Bu texnika ilə hücum edən şəxs, həmin platformalara zərərli məzmun əlavə edir və qurbanın cihazına zərərli proqram yükləməsini təmin edir[51].

"Honey trap" texnikası, qurbanın emosional zəifliklərindən istifadə edərək məlumatların əldə edilməsi ilə həyata keçirilir. Hücum edən şəxs, adətən saxta romantik və ya dostluq əlaqələri yaradaraq qurbanın etimadını qazanır və onun məlumatlarını ələ keçirir[52].

"Scareware" texnikasında hücum edən şəxs, qurbanın cihazında virus və ya təhlükə olduğu ilə bağlı saxta xəbərdarlıqlar göndərir. Qurban, bu xəbərdarlığı həll etmək üçün zərərli proqram yükləməyə və ya məlumatlarını paylaşmağa məcbur edilir[53].

"Dumpster diving" texnikasında hücum edən şəxslər, qurbanın atılmış sənədlərindən məlumat toplayır. Bu texnika ilə hücum edən şəxs bank sənədləri, parollar və ya digər həssas məlumatlar əldə edə bilər[54].

"Social media hijacking" texnikasında hücum edən şəxs, qurbanın sosial media hesablarını ələ keçirir və bu hesablar vasitəsilə onun məlumatlarını toplayır və ya tanışlarını manipulyasiya edir. Bu texnika, saxta mesajlar göndərməklə qurbanın etibarını zədələyə bilər[55].

"Reverse social engineering" texnikasında hücum edən şəxs əvvəlcə bir problem yaradır və daha sonra həmin problemi həll etmək üçün "yardım" təklif edir. Məsələn, hücum edən şəxs bir sistemə zərər verə bilər və qurbanın həmin problemi həll etmək üçün ona müraciət etməsini gözləyir[56].

Bu texnikalar, sosial mühəndislik hücumlarının müxtəlif formalarını əks etdirir və insanların psixoloji və texnoloji zəifliklərini istismar etməyə əsaslanır. Onların mahiyyətini və icrasını başa düşmək, bu cür hücumlara qarşı effektiv müdafiə tədbirləri görmək üçün vacibdir.

[50] Shoulder surfing (computer security) - en.wikipedia.org/wiki/Shoulder_surfing_%28computer_security%29
[51] "Watering hole" hücumu nədir? - www.cybersign.az/xeber/watering-hole-hucumu-nedir
[52] Honey trapping - en.wikipedia.org/wiki/Honey_trapping
[53] Scareware - en.wikipedia.org/wiki/Scareware
[54] What is dumpster diving? - Gavin Wright
[55] What you need to know about social media hijacking - www.vcnbfamily.bank/Why-VCNB/VCNB-Blog/what-you-need-to-know-about-social-media-hijacking
[56] What is reverse social engineering? and how does it work? - aware.eccouncil.org/what-is-reverse-social-engineering.html

Sosial mühəndisliyə qarşı psixoloji müdafiə

Sosial mühəndislik hücumlarına qarşı effektiv mübarizə təkcə texnoloji tədbirlərlə deyil, həm də insanların psixoloji müdafiə qabiliyyətlərinin gücləndirilməsi ilə mümkündür. Psixoloji müdafiə, insanların manipulyasiya texnikalarını tanımaq, emosional reaksiyalarını idarə etmək və tənqidi düşüncə bacarıqlarını inkişaf etdirmək qabiliyyətlərini artırmağa yönəlmiş sistemli yanaşmadır. Bu, yalnız şəxslərin deyil, həm də təşkilatların təhlükəsizlik səviyyəsinin artırılmasına kömək edir.

Psixoloji müdafiə tədbirləri qurbanların şübhəli davranışları və manipulyasiya cəhdlərini tanıya bilmə qabiliyyətlərini inkişaf etdirməyi hədəfləyir. Bu yanaşma, şəxslərin emosional vəziyyətlərdə daha rasional və soyuqqanlı qərarlar qəbul etməsini təmin etmək üçün sistemli təlimlərə əsaslanır. İnsanların qorxu, maraq, təzyiq və etibar manipulyasiyalarına qarşı daha müqavimətli olması, onların sosial mühəndislik hücumlarından qorunmasında əsaslı rol oynayır.

Bu müdafiə tədbirləri, yalnız şəxslərin öz təhlükəsizliklərinə diqqət etməsini deyil, həm də təşkilatların təhlükəsizlik mədəniyyətini gücləndirməsini tələb edir. Təşkilatlar müntəzəm təlim proqramları təşkil etməli, real nümunələr və simulyasiya edilmiş hücumlar vasitəsilə işçilərin diqqətini və bilik səviyyəsini artırmalıdır. Belə yanaşmalar həm şəxslərin öz təhlükəsizliklərini təmin etməsinə, həm də təşkilatın ümumi təhlükəsizlik strategiyasına töhfə verir.

Sosial mühəndisliyə qarşı mübarizədə əsas aspektlərdən biri də insanların texnoloji və psixoloji cəhətdən maarifləndirilməsi və şübhə ilə yanaşma mədəniyyətinin formalaşdırılmasıdır. Qurbanların hər bir şübhəli mesaj və ya tələbə qarşı dərhal reaksiya vermək əvəzinə, bu tələbləri dəyərləndirə biləcək analitik düşüncə qabiliyyətlərinə malik olması vacibdir. Emosional reaksiyalara nəzarət və mənbələrin təsdiqlənməsi, sosial mühəndislik hücumlarına qarşı ən təsirli müdafiə vasitələrindən biridir.

Nəticə

Sosial mühəndislik, insan psixologiyasının zəifliklərini manipulyasiya etməklə məlumatı oğurlamaq qanunsuz ələ keçirmək, təhlükəsizlik tədbirlərini pozmaq və şəxslərin və ya təşkilatların davranışlarını idarə etmək məqsədini güdən mürəkkəb bir yanaşmadır. Psixoloji aspektlər və manipulyasiya texnikaları bu prosesin əsasını təşkil edir və hücum edən şəxslərin məqsədlərinə nail olmaq üçün istifadə etdiyi ən təsirli vasitələrdir. Hücum edən şəxslər qorxu, təcili qərar tələbi, etibarın istismarı, sosial təsir və maraq oyatmaq kimi psixoloji mexanizmlərdən istifadə edərək qurbanın diqqətini yayındırır və onu təhlükəli qərarlar qəbul etməyə məcbur edir.

Psixoloji manipulyasiyaların mahiyyətini və onların tətbiq üsullarını anlamaq, fərdlərə və təşkilatlara bu texnikalara qarşı hazırlıqlı olmağa və onların təsirlərini minimuma endirməyə imkan verir. Sosial mühəndislik hücumlarının kompleksliyini nəzərə alaraq, hər bir şəxs və təşkilat təhlükəsizlik sahəsində həm texnoloji, həm də psixoloji müdafiəni gücləndirmək üçün davamlı olaraq çalışmalıdır.

§ 5. Sosial mühəndislik və kibertəhlükəsizlik

Giriş

Sosial mühəndislik və kibertəhlükəsizlik arasında sıx və ayrılmaz bir əlaqə mövcuddur. Sosial mühəndislik, insan psixologiyasının zəifliklərini manipulyasiya edərək kibermühitdə təhlükəsizlik tədbirlərini pozmağa yönəlmiş texnikalar toplusudur. Hücum edən şəxslər, texnoloji sistemlərin müdafiəsini keçmək əvəzinə, birbaşa insanların emosional reaksiyalarını və davranışlarını hədəf alırlar. Bu yanaşma, insan zəifliklərini istismar etməklə həm şəxslərin, həm də təşkilatların təhlükəsizlik sistemlərini təsirsiz hala gətirir. Nəticədə, sosial mühəndislik, ən müasir texnoloji tədbirlərlə qorunan sistemlər üçün belə ciddi təhlükə yaradır.

Kibertəhlükəsizlik isə sosial mühəndislik hücumlarının təsirini azaltmaq və sistemləri qorumaq üçün həm texnoloji, həm də insani səviyyədə müdafiə tədbirlərinin həyata keçirilməsini nəzərdə tutur. Texnoloji cəhətdən güclü təhlükəsizlik tədbirləri, məsələn, “firewall”, antivirus proqramları və şifrələmə texnologiyaları, sistemlərin qorunmasında mühüm rol oynayır. Lakin bu tədbirlər kifayət etmir, çünki Hücum edən şəxslər insan zəifliklərini manipulyasiya edərək texnoloji müdafiəni təsirsiz edə bilirlər. Burada insan faktoru ön plana çıxır: şəxslərin təhlükəsizlik biliklərinin artırılması və manipulyasiya texnikalarına qarşı müqavimət göstərməsi ümumi təhlükəsizlik səviyyəsini artırır.

Sosial mühəndislik, texnoloji zəifliklərdən daha çox insan zəifliklərinə fokuslanır. Hücum edən şəxslər, qurbanların qorxu, etibar, təcili qərar tələbi və maraq kimi emosional reaksiyalarını manipulyasiya etməklə məlumat oğurlamaq və ya təhlükəsizlik qaydalarını pozmaq üçün hərəkətə keçirlər. Bu hücumlar “phishing”, “baiting”, “pretexting” kimi texnikalar vasitəsilə həyata keçirilir və qurbanın diqqətsizliyindən maksimum istifadə edir. Təəssüf ki, bu cür hücumlar günümüzdə getdikcə daha da mürəkkəbləşir və qlobal səviyyədə böyük təhlükəsizlik riskləri yaradır.

Bu mövzu, sosial mühəndisliyin kibertəhlükəsizliyə necə təsir etdiyini, hücum texnikalarının əsas xüsusiyyətlərini və bu hücumlara qarşı hansı müdafiə tədbirlərinin effektiv olduğunu izah etməyi hədəfləyir. İnsanların şəxsi məlumatlarının, maliyyə sistemlərinin və texnoloji resurslarının qorunması üçün sosial mühəndislik texnikalarının dərinliklə öyrənilməsi və onların tətbiqinə qarşı tədbirlərin gücləndirilməsi vacibdir. Həm fərdi, həm də təşkilati səviyyədə sosial mühəndislik hücumlarının artan mürəkkəbliyi, kibertəhlükəsizlik sahəsində insan faktorunun əhəmiyyətini daha da artırır. Təhlükəsizlik sistemlərinin davamlı olaraq təkmilləşdirilməsi və insanların bu sistemləri daha yaxşı başa düşməsi, sosial mühəndislik hücumlarının təsirini minimuma endirmək üçün vacib şərtlərdir.

Sosial mühəndislik və onun kibertəhlükəsizlikdə rolu

Sosial mühəndislik kibertəhlükəsizliyə müxtəlif yollarla təsir edir. Hücum edən şəxs, insan davranışlarını və zəifliklərini manipulyasiya edərək kibermühitdə yerləşən kritik məlumatları ələ keçirmək və təhlükəsizlik sistemlərini aşmaq üçün sosial mühəndislik texnikalarından geniş istifadə edirlər. Bu yanaşma, texnoloji müdafiə tədbirlərini aşmağın ən asan yollarından biri kimi qəbul edilir, çünki insan zəifliklərı, texnoloji maneələrlə müqayisədə daha asan istismar olunur. Qurbanların diqqətsizliyi, emosional reaksiyaları və sosial təsirlərə olan həssaslığı bu hücumların uğurlu olmasını təmin edir.

Sosial mühəndislik hücumları fərqli məqsədlərlə həyata keçirilir. Hücum edən şəxs şəxsi məlumatları, maliyyə məlumatlarını və ya sistemlərə giriş üçün istifadə olunan kritik məlumatları ələ keçirmək üçün fərqli manipulyasiya üsullarından istifadə edirlər. Məsələn, "phishing" hücumları vasitəsilə qurbanlar saxta e-poçtlarla manipulyasiya edilərək məlumatlarını paylaşmağa sövq edilir. Eyni zamanda, texnoloji zəifliklərdən yan keçmək üçün pretexting və baiting kimi texnikalar tətbiq olunur ki, burada qurbanın etibarı manipulyasiya edilir.

Sosial mühəndislik kibertəhlükəsizliyə yalnız fərdi səviyyədə deyil, həm də təşkilati və hətta dövlət səviyyəsində ciddi təsirlər göstərir. Təşkilatlar daxilində məlumatların sızdırılması, texniki sistemlərin pozulması və ya xidmətlərin dayandırılması kimi hallar sosial mühəndislik texnikaları vasitəsilə həyata keçirilir. Hücum edən şəxs yalnız texnoloji sistemlərdən deyil, həm də insan zəifliklərindən faydalanaraq daha geniş miqyasda təhlükəsizlik pozuntularına səbəb ola bilirlər. Bu da sosial mühəndisliyin kibertəhlükəsizlikdə yaratdığı təhlükələrin kompleksliyini və genişliyini vurğulayır.

Məlumatların oğurlanması, həm şəxslər, həm də təşkilatlar üçün ciddi nəticələrə səbəb ola bilən təhlükəli bir prosesdir. Bu cür hücumların fərdi səviyyədə təsirləri çox vaxt şəxsi həyatı və maliyyə vəziyyətini pozur, təşkilati səviyyədə isə biznes əməliyyatlarının dayandırılmasına və geniş miqyaslı təhlükəsizlik pozuntularına gətirib çıxarır. Bu hücumlar aşağıdakı əsas sahələrdə təsir göstərir:

- **Şəxslərə təsiri.** Məlumat oğurluğu fərdlərin şəxsiyyətləri və maliyyə məlumatları ilə bağlı ciddi təhlükələr yaradır. Fərdi məlumatların qanunsuz ələ keçirilməsi, hücum edən şəxslər qurbanın adından qanunsuz əməliyyatlar həyata keçirməsinə şərait yaradır. Məsələn, qurbanın adından saxta kreditlər götürülə bilər və ya maliyyə hesabları boşaldıla bilər. Bu isə şəxsin uzunmüddətli maliyyə problemləri ilə üzləşməsinə səbəb olur[57].

Maliyyə fırıldaqları isə şəxslərin bank hesablarından icazəsiz əməliyyatların aparılması və ya kredit kartı məlumatlarının istifadə edilməsi formasında həyata keçirilir. hücum edən şəxslər, şəxsi məlumatlardan istifadə edərək onlara böyük maliyyə ziyanı vura bilərlər. Bundan əlavə, şəxsi məlumatların sızdırılması, qurbanın özəl həyatı ilə bağlı həssas məlumatların ictimailəşməsinə və sosial təsirlərə səbəb ola bilər. Belə hallar

[57] Sosial mühəndislik haqda nələri bilirik ?! - cert.gov.az/az/news/sosial-muhendislik-haqda-neleri-bilirik?

qurbanların nüfuzuna zərbə vurmaqla yanaşı, emosional və psixoloji travmalar da yaradır.

- **Təşkilatlara təsiri.** Təşkilatlar üçün məlumat oğurluğu daha geniş miqyasda ciddi nəticələrə gətirib çıxarır. Kritik sistemlərə giriş, hücum edən şəxslər şirkətlərin daxili məlumatlarını manipulyasiya etməsinə, məxfi sənədləri oğurlamasına və ya fəaliyyətləri dayandırmasına şərait yaradır. Bu, təşkilatın əməliyyatlarının dayanmasına, maliyyə itkilərinə və hətta hüquqi məsuliyyətlərə səbəb ola bilər[58].

Məxfi məlumatların sızdırılması, şirkətin müştəriləri və tərəfdaşları ilə etibar əlaqəsini sarsıdır. Məsələn, müştəri məlumatlarının sızdırılması təşkilatın reputasiyasına ciddi zərbə vura bilər və hüquqi problemlərlə nəticələnə bilər. Bundan əlavə, biznes fəaliyyətlərinin pozulması, istehsalatın dayanmasına, işçi heyətinin məhsuldarlığının azalmasına və maliyyə itkilərinə səbəb olur. Bu kimi hallar uzunmüddətli iqtisadi problemlər yaradır və təşkilatın bazar mövqeyini zəiflədir.

Bu səbəblərdən məlumat oğurluğunun təsirlərini azaltmaq üçün həm şəxslər, həm də təşkilatlar təhlükəsizlik tədbirlərini gücləndirməli, texnoloji vasitələrdən effektiv istifadə etməli və sosial mühəndislik hücumlarına qarşı maarifləndirmə tədbirlərini genişləndirməlidirlər. Təhlükəsizliyin təmin edilməsi, yalnız texnoloji səviyyədə deyil, həm də şəxslərin və təşkilatların diqqətli davranışları ilə mümkündür.

Sosial mühəndislik və kibertəhlükəsizliyin qarşılıqlı əlaqəsi

Sosial mühəndislik və kibertəhlükəsizlik arasında qarşılıqlı əlaqə, insan faktorunun təhlükəsizlikdə oynadığı əhəmiyyətli rolu bir daha göstərir. Sosial mühəndislik hücumları texnoloji sistemlərin gücündən daha çox, insanların zəifliklərini və psixoloji davranışlarını manipulyasiya etməyə əsaslanır. Bu da kibertəhlükəsizliyi yalnız texnoloji tədbirlərlə deyil, eyni zamanda insanların davranışları və bilikləri ilə gücləndirməyi zəruri edir.

Texnoloji sistemlər nə qədər inkişaf etmiş olsa da, insan zəifliklərı bu sistemlərin ümumi təhlükəsizliyini risk altına sala bilər. Məsələn, müasir şifrələmə texnologiyaları və firewall sistemləri ilə qorunan bir şəbəkə belə, bir işçinin phishing e-poçtuna aldanaraq şifrələrini paylaşması nəticəsində təhlükəyə düşə bilər. Hücum edən şəxslər əsas məqsədi bu cür zəifliklərı aşkar edərək, təhlükəsizlik sistemlərinin yaratdığı texnoloji maneələri insani səviyyədə aradan qaldırmaqdır. Beləliklə, sosial mühəndislik, texnoloji tədbirlərin təsirini azaldan güclü bir vasitə kimi çıxış edir.

Kibertəhlükəsizlik, bu cür hücumların qarşısını almaq üçün iki əsas istiqamətdə fəaliyyət göstərir:

- texnoloji müdafiə tədbirlərinin tətbiqi;
- insanların məlumatlandırılması[59].

Texnoloji tədbirlər arasında antivirus proqramları, spam filtrləri, şifrələmə sistemləri və ikimərhələli autentifikasiya texnologiyaları yer alsa da, bu tədbirlər yalnız

[58] Sosial mühəndislik hücum texnikası nədir?! - cert.az/news/2019/sosial-muhendislik-texnikasi-nedir?
[59] "İnformasiya təhlükəsizliyinin müasir problemləri və həlli metodlarının qiymətləndirilməsi" - Amin Şıxəlizadə

texniki səviyyədə qoruma təmin edir. Ən güclü texnoloji müdafiə belə, insan diqqətsizliyinə və ya manipulyasiya edilən davranışlara qarşı təsirsiz qala bilər. Burada insan faktorunun rolu xüsusi əhəmiyyət qazanır.

İnsanların kibertəhlükəsizlikdəki bilik və davranışları sistemin ümumi müdafiə səviyyəsinə birbaşa təsir edir. Maarifləndirmə və təlim proqramları, şəxslərin və təşkilatların sosial mühəndislik texnikalarını tanımasını və onlara qarşı müqavimət göstərməsini təmin edir. İnsanlara "phishing" e-poçtlarını tanımaq, şübhəli linklərdən uzaq durmaq və emosional manipulyasiyalara məruz qalmamaq üçün müvafiq bacarıqlar öyrədilməlidir. Bu biliklər, həm fərdi, həm də təşkilati səviyyədə təhlükəsizlik tədbirlərini gücləndirir.

Güclü təhlükəsizlik mədəniyyətinin formalaşdırılması da bu qarşılıqlı əlaqənin əsasını təşkil edir. Təşkilatlar daxilində hər bir işçinin təhlükəsizliyə dair məsuliyyət daşıması, təhlükəsizlik qaydalarına riayət etməsi və şübhəli fəaliyyətləri vaxtında bildirməsi ümumi təhlükəsizlik səviyyəsini artırır. Məsələn, təşkilatlar, işçilərə mütəmadi olaraq sosial mühəndislik hücumlarının nümunələrini göstərərək onların şüurluluğunu artırmalı və real hücumlarla necə mübarizə aparmağı öyrətməlidir. Həmçinin, rəhbərlik tərəfindən təhlükəsizliyin prioritet məsələlərdən biri olaraq tanınması, işçilər arasında təhlükəsizlik qaydalarına ciddi yanaşma mədəniyyəti yaradır.

Sosial mühəndislik və kibertəhlükəsizlik arasındakı bu əlaqə, texnologiya ilə insan faktoru arasında balansın qorunmasının vacibliyini vurğulayır. Hər bir təhlükəsizlik sistemi, texnoloji və insani tədbirlərin inteqrasiyasını tələb edir. Texnologiya hücumların qarşısını almaq üçün müdafiə təmin etsə də, insanların şüurlu davranışları bu müdafiəni daha da gücləndirir. Bu yanaşma, sosial mühəndislik hücumlarının təsirini minimuma endirmək və ümumi təhlükəsizliyi təmin etmək üçün ən effektiv üsullardan biridir. Beləliklə, kibertəhlükəsizlikdə insan və texnologiyanın harmonik şəkildə işləməsi müasir təhlükəsizlik sistemlərinin əsasını təşkil edir.

Kibertəhlükəsizlik mütəxəssisinin sosial mühəndisliklə bağlı bilik və bacarıqlarının formalaşdırılmasının əhəmiyyəti

Müasir dövrdə kibertəhlükəsizlik sahəsində effektiv mübarizə aparmaq üçün mütəxəssislərin yalnız texnoloji biliklərə deyil, həm də sosial mühəndislik texnikaları haqqında dərin məlumatlara malik olması vacibdir. Sosial mühəndislik, insan zəifliklərini manipulyasiya etməyə əsaslanan bir yanaşma olduğu üçün bu sahədə çalışan mütəxəssislərin insan davranışlarını, emosional reaksiyaları və qərar qəbul etmə proseslərini başa düşməsi kritik əhəmiyyət daşıyır.

Texnologiya ilə insan faktoru arasındakı qarşılıqlı əlaqəni anlamaq və manipulyasiya cəhdlərini erkən mərhələdə aşkar edə bilmək, təhlükəsizlik sistemlərinin effektivliyini artırır. Kibertəhlükəsizlik mütəxəssisləri, sosial mühəndislik texnikalarını tanımaq və onların təsirini minimuma endirmək üçün zəruri biliklərə sahib olmalıdırlar. Bu biliklərə phishing, spear phishing, pretexting, baiting və scareware kimi texnikaların mahiyyəti, həyata keçirilmə üsulları və onlara qarşı müdafiə tədbirləri daxildir.

Mütəxəssislər, bu texnikaların necə tətbiq edildiyini və qurbanların manipulyasiya edilməsi üçün hansı metodlardan istifadə olunduğunu anlamaqla, təhlükəsizlik sistemlərini bu cür hücumlara qarşı daha davamlı şəkildə hazırlaya bilərlər. Məsələn, hücumların təsirini minimuma endirmək üçün real vaxtda təhlükəsizlik monitorinqi, risklərin təhlili və maarifləndirmə tədbirlərinin tətbiqi mütəxəssislərin əsas bacarıqları sırasında olmalıdır. Bu bilik və bacarıqların formalaşdırılması, mütəxəssislərə yalnız mövcud təhlükəsizlik tədbirlərini gücləndirmək deyil, həm də potensial təhlükələri qabaqcadan proqnozlaşdırmaq və onların qarşısını almaq imkanı verir.

Sosial mühəndislik hücumları çox vaxt sistem daxilində və ya işçilərin diqqətsizliyindən qaynaqlandığı üçün mütəxəssislər, təşkilatlar daxilində təhlükəsizlik mədəniyyətini formalaşdırmaq üçün də əsas rol oynayırlar. Onların bilikləri, işçilərə sosial mühəndislik texnikalarını tanımağı öyrətmək, təhlükəsizlik siyasətləri hazırlamaq və şübhəli hallarda adekvat cavab tədbirləri həyata keçirmək üçün istifadə edilir. Daha geniş miqyasda, sosial mühəndislik bilikləri mütəxəssislərə hücumların psixoloji və davranış aspektlərini analiz etmək imkanı verir ki, bu da hücumların strukturunu daha yaxşı başa düşərək müdafiə mexanizmlərinin təkmilləşdirilməsinə töhfə verir. Bu biliklərin olmaması yalnız fərdi hücumların uğur şansını artırmaqla yanaşı, ümumi kibertəhlükəsizlik strategiyasını da zəiflədir. Buna görə də, sosial mühəndisliklə bağlı bilik və bacarıqların kibertəhlükəsizlik mütəxəssislərinin tədris proqramlarına daxil edilməsi və davamlı şəkildə inkişaf etdirilməsi müasir təhlükəsizlik ehtiyaclarına cavab vermək baxımından vacibdir.

Kibertəhlükəsizlik mütəxəssisinin sosial mühəndisliklə mübarizə sahəsində uğurlu olması üçün bir sıra əsas biliklərə və bacarıqlara malik olması vacibdir. Bu bilik və bacarıqlar müasir təhlükəsizlik mühitində sosial mühəndislik texnikalarının təsirini dərk etmək, hücumların mahiyyətini təhlil etmək, təhlükəsizlik sistemlərini təkmilləşdirmək və qurbanları manipulyasiya texnikalarına qarşı maarifləndirmək üçün əsas şərtdir.

Sosial mühəndislik, insan psixologiyasının zəifliklərini istismar edən mürəkkəb bir hücum yanaşmasıdır və bu səbəbdən onunla effektiv mübarizə yalnız texnoloji biliklərlə deyil, eyni zamanda psixoloji anlayışlarla da mümkündür. Hər bir texnika fərqli üsullarla həyata keçirildiyi üçün, bu texnikaların xüsusi əlamətlərini müəyyən etmək və vaxtında müdaxilə etmək üçün analitik bacarıqlar zəruridir. Hücum texnikalarının təhlili, mütəxəssisə yalnız mövcud hücumların təsirlərini azaltmağa deyil, həm də gələcəkdə baş verə biləcək təhlükələri proqnozlaşdırmağa imkan verir. Bundan əlavə, kibertəhlükəsizlik mütəxəssisinin sosial mühəndisliklə bağlı bilikləri, təhlükəsizlik sistemlərinin zəifliklərini dərk etməyə və bu zəifliklərin qarşısını almaq üçün effektiv strategiyalar hazırlamağa şərait yaradır. Məsələn, şifrələmə siyasətlərinin təkmilləşdirilməsi, ikimərhələli autentifikasiya sistemlərinin tətbiqi və açıq mənbə kəşfiyyatı vasitəsilə təhlükəsizlik tədbirlərinin gücləndirilməsi, sosial mühəndislik hücumlarına qarşı müdafiənin əsas komponentləridir.

Mütəxəssis həmçinin təşkilatlarda təhlükəsizlik mədəniyyətini formalaşdırmaq, işçilərin təhlükəsizlik qaydalarına riayət etməsini təşviq etmək və maarifləndirmə təlimləri keçməklə ümumi təhlükəsizliyə töhfə verməlidir. Bu yanaşmaların effektivliyi,

yalnız texnologiya ilə deyil, həm də insanların davranışlarını dəyişdirməklə bağlıdır. Sosial mühəndislik hücumlarının çoxu insanın emosional reaksiyalarından qaynaqlandığı üçün mütəxəssis, manipulyasiya texnikalarının psixoloji əsaslarını anlamağı və qurbanları bu texnikaları tanımaq üçün təlimləndirməyi bacarmalıdır. Hücumların qarşısını almaq üçün, şəxslərə təcili qərar tələbi, qorxu yaradan mesajlar və etibar manipulyasiyalarını aşkar etmək üçün praktik bacarıqlar öyrədilməlidir. Beləliklə, kibertəhlükəsizlik mütəxəssisinin sosial mühəndislik sahəsində bilik və bacarıqlarını inkişaf etdirməsi, həm fərdi, həm də təşkilati səviyyədə təhlükəsizlik sistemlərini gücləndirmək üçün vacibdir. Bu biliklər yalnız texnoloji müdafiəni gücləndirmək üçün deyil, həm də insan faktorunun manipulyasiyasına qarşı dayanıqlı mühit yaratmaq üçün zəruridir.

Təhlükəsizliyin təmin edilməsi yalnız texnologiya ilə məhdudlaşmamalı, insanların bu sistemlərdəki rolu nəzərə alınaraq hərtərəfli yanaşma tətbiq edilməlidir.

1. Sosial mühəndislik texnikalarının anlaşılması

Kibertəhlükəsizlik mütəxəssisi sosial mühəndislik texnikalarının mahiyyətini və onların həyata keçirilmə metodlarını dərindən başa düşməlidir. Bu biliklər mütəxəssisə sosial mühəndislik hücumlarını vaxtında müəyyən etmək, onların təsirini azaltmaq və qurbanların təhlükəsizlik biliklərini artırmaq üçün effektiv strategiyalar hazırlamağa imkan verir. Sosial mühəndislik texnikalarının müxtəlif növləri, onların tətbiq üsulları və müdafiə yolları ilə bağlı müfəssəl anlayış, mütəxəssisin bu sahədə uğurlu olmasının əsas şərtlərindəndir.

2. Psixoloji manipulyasiya texnikalarının tanınması

Sosial mühəndislik hücumlarının əsas hissəsi insan psixologiyasının zəif tərəflərinin manipulyasiyasına əsaslanır. Hücum edən şəxslər, insan davranışlarını yönləndirmək və emosional reaksiyalarını istismar etmək üçün müxtəlif psixoloji manipulyasiya texnikalarından istifadə edirlər. Bu texnikalar qurbanın qorxularına, inamına və sosial təsirlərə həssaslığını hədəf alır. Kibertəhlükəsizlik mütəxəssisinin bu texnikaları tanıması, onların tətbiq üsullarını başa düşməsi və onlara qarşı müdafiə strategiyaları hazırlaya bilməsi vacibdir[60]. Mütəxəssis aşağıdakıları başa düşməlidir:

- Təzyiq yaradan mesajları müəyyən etmək: Hücum edən şəxslərin istifadə etdiyi dil və emosional təsir yaradan ifadələri tanımaq.
- Qurbanın davranışını təhlil etmək: insanların qorxu və təcili qərar tələbi altında necə reaksiya verdiyini anlamalı.
- Müdafiə tədbirləri: şəxslərə qorxu yaradan mesajlara dərhal reaksiya verməkdən çəkinməyi və mənbənin etibarlılığını yoxlamağı öyrətmək.

Mütəxəssis aşağıdakı biliklərə malik olmalıdır:

- Etibarlılıq illüziyasını tanımaq: saxta e-poçtların və ya mesajların necə yaradıldığını və onların həqiqi mənbədən fərqlərini başa düşmək.
- Mənbənin doğruluğunu yoxlama strategiyaları: şəxsi məlumatlar tələb edən hər bir müraciətin rəsmi kanallar vasitəsilə təsdiqlənməsini təşviq etmək.

[60] Social engineering - www.imperva.com/learn/application-security/social-engineering-attack/

- Maarifləndirmə tədbirləri: insanlara etibar manipulyasiyasını tanımaq üçün nümunələr göstərmək və bu cür texnikalara qarşı dayanıqlı davranışlar öyrətmək.

Mütəxəssis aşağıdakıları öyrənməlidir:

- Sosial təsirin mexanizmləri: insanların uyğunlaşma davranışlarını və sosial rolları necə qəbul etdiyini başa düşmək.
- Manipulyasiyanın əlamətləri: sosial təsir vasitəsilə edilən müraciətlərin necə fərqləndiyini və hansı şərtlərdə şübhəli olduğunu müəyyən etmək.
- Müdafiə tədbirləri: insanlara sosial təzyiq altında müstəqil qərarlar qəbul etməyi öyrətmək və bu cür hallarda məlumatların mənbəyini yoxlamaq vərdişi aşılamaq.

Psixoloji manipulyasiya texnikalarının tanınması, kibertəhlükəsizlik mütəxəssisinin hücumların təsirini minimuma endirmək üçün istifadə edə biləcəyi ən güclü vasitələrdən biridir. Bu texnikaları başa düşmək, yalnız hücumların qarşısını almaq üçün deyil, həm də şəxsləri bu cür manipulyasiyalara qarşı daha davamlı etmək üçün əsaslı maarifləndirmə proqramlarının tərtibi və həyata keçirilməsi üçün də vacibdir. Təhlükəsizlik yalnız texnoloji tədbirlərlə deyil, insanların manipulyasiya cəhdlərini tanımaq və onlara qarşı müdafiə olunmaq bacarığı ilə də gücləndirilir.

Hücumların aşkarlanması və təhlili

Sosial mühəndislik hücumlarının effektiv şəkildə aşkarlanması və təhlil edilməsi kibertəhlükəsizliyin vacib tərkib hissəsidir. Mütəxəssis, bu cür hücumların əlamətlərini vaxtında müəyyən etmək, onların hansı texnikalarla həyata keçirildiyini təhlil etmək və təhlükəsizlik sistemlərinə yaratdığı təsirləri minimuma endirmək üçün zəruri bilik və bacarıqlara malik olmalıdır. Hücumların aşkarlanması real vaxtda baş verən proses olduğu üçün həm texnoloji alətlərdən istifadə etmək, həm də insan davranışlarının monitorinqi önəmli yer tutur. Hücumların təhlili isə onların təkrarlanmasının qarşısını almaq və müdafiə sistemlərini təkmilləşdirmək üçün əsaslı bir mərhələdir.

Spam filtrlərinin optimallaşdırılması

Spam filtrləri, sosial mühəndislik hücumlarının əsas giriş nöqtələrindən biri olan saxta e-poçt və mesajların qarşısını almaq üçün ən önəmli vasitələrdən biridir[61]. Mütəxəssis spam filtrlərini optimallaşdırmaq üçün aşağıdakıları təmin etməlidir:

- Şübhəli məzmunların tanınması: e-poçtlarda istifadə olunan dildə təcili qərar tələbləri, təhlükəli linklər və ya saxta göndərən məlumatlarını təhlil edərək bu cür mesajları erkən mərhələdə bloklamaq.
- Zərərli linklərin və əlavələrin qarşısını almaq: Hücum edən şəxslərin zərərli faylları qurbanlara göndərməsinin qarşısını alan avtomatik skanerlərin tətbiqi.
- Spam filtrlərinin yenilənməsi: yeni sosial mühəndislik texnikalarına uyğun olaraq spam filtrlərinin mütəmadi olaraq yenilənməsi və inkişaf etdirilməsi.

Spam filtrlərinin effektiv işləməsi yalnız texnoloji alətlərin istifadəsi ilə məhdudlaşmır, həm də mütəxəssisin bu sistemlərin işini davamlı monitorinq etməsi və

[61] How to avoid spam filters: 15 proven ways - Bernard Meyer

aşkarlanmış təhlükələri təhlil etməsi ilə əlaqəlidir. Məsələn, bir spam e-poçtu bloklandıqda, mütəxəssis onun məzmununu təhlil edərək hansı texnikanın istifadə olunduğunu və bu texnikaya qarşı əlavə tədbirlərin zəruriliyini müəyyən edə bilər.

Məlumat sızmasının monitorinqi

Sosial mühəndislik hücumlarının əsas məqsədlərindən biri həssas məlumatların ələ keçirilməsidir. Bu məlumatların yayılmasının qarşısını almaq və onların təsirini minimuma endirmək üçün məlumat sızmasının monitorinqi xüsusi əhəmiyyət daşıyır[62]. Mütəxəssis məlumat sızmasının aşkarlanması və idarə olunması üçün aşağıdakıları etməlidir:

- Daxili məlumatların izlənməsi: sistem daxilində məlumatlara kimin giriş etdiyini və bu məlumatların hansı məqsədlə istifadə edildiyini izləyən alətlərin tətbiqi.
- Sızma izlərinin müəyyən edilməsi: hücum nəticəsində əldə edilmiş məlumatların xarici resurslara sızıb-sızmadığını təhlil etmək üçün monitorinq sistemlərinin tətbiqi.
- Real vaxtda xəbərdarlıq: məlumat sızmasının aşkar edildiyi andan etibarən sistemlərdən real vaxt xəbərdarlıqların alınması və zərərli fəaliyyətlərin dərhal dayandırılması. Məsələn, mütəxəssis hücum nəticəsində sızdırılan məlumatları darknet bazarlarında və ya digər qeyri-qanuni platformalarda axtarış edən OSINT alətlərindən istifadə etməlidir.

Bu cür məlumatların yayılmasının erkən mərhələdə qarşısının alınması təşkilatın nüfuzunu qorumaq və hücumun təsirini minimuma endirmək üçün vacibdir.

Hücumların davranışsal təhlili

Hücumların davranış əsaslı təhlili sosial mühəndislik hücumlarının daha yaxşı başa düşülməsini və onların növbəti mərhələlərdə qarşısının alınmasını təmin edir[63]. Mütəxəssis aşağıdakıları həyata keçirməlidir:

- Qurban davranışlarının təhlili: hücumun hansı şərtlərdə uğurlu olduğunu və qurbanın hansı nöqtədə manipulyasiya edildiyini müəyyən etmək.
- Hücum edən şəxsin strategiyasının öyrənilməsi: Hücum edən şəxslərin istifadə etdiyi manipulyasiya texnikalarını və onların tətbiq üsullarını təhlil etmək.
- Təhlildən əldə olunan məlumatlara əsaslanan təkmilləşdirmə: təhlil nəticəsində əldə olunan məlumatları istifadə edərək təşkilatın təhlükəsizlik siyasətlərini gücləndirmək və yeni müdafiə strategiyaları hazırlamaq.

Sosial mühəndislik hücumlarının effektiv şəkildə aşkarlanması və təhlili kibertəhlükəsizlik strategiyalarının ayrılmaz hissəsidir. Hücumların qarşısını almaq üçün mütəxəssislər spam filtrlərinin optimallaşdırılması, məlumat sızmalarının monitorinqi və davranış əsaslı təhlil kimi üsullardan istifadə etməlidirlər. Bu yanaşma sayəsində zərərli mesajlar erkən mərhələdə bloklanır, həssas məlumatların sızmasının qarşısı alınır və hücum edən şəxslərin manipulyasiya strategiyaları müəyyən edilərək yeni müdafiə

[62] Məlumat itkisinin qarşısının alınması üzrə ən yaxşı vərdişlər - www.pitsdatarecovery.az/ways-to-prevent-data-loss/
[63] ATT&CK matrix for enterprise - attack.mitre.org/

tədbirləri hazırlanır. Təhlükəsizliyin gücləndirilməsi üçün bu mexanizmlərin davamlı olaraq təkmilləşdirilməsi və mütəmadi monitorinqi vacibdir.

Maarifləndirmə və təlim bacarıqları

Sosial mühəndislik hücumlarının qarşısını almağın ən effektiv yollarından biri şəxslərin və təşkilat işçilərinin təhlükəsizlik biliklərini artırmaqdır. Kibertəhlükəsizlik mütəxəssisi, istifadəçiləri sosial mühəndislik texnikalarına qarşı hazırlamaq və onları müdafiə tədbirləri haqqında məlumatlandırmaq üçün effektiv təlimlər təşkil etməyi bacarmalıdır.

Maarifləndirmə və təlim proqramları, şəxslərin şübhəli fəaliyyətləri tanımaq və dərhal reaksiya vermək bacarıqlarını gücləndirir. Bu, həm fərdi istifadəçiləri, həm də təşkilat işçilərini sosial mühəndislik hücumlarının təsirlərindən qorumaq üçün fundamental əhəmiyyət daşıyır. Effektiv təlim proqramları yalnız nəzəri bilikləri deyil, həm də praktiki yanaşmaları əhatə etməlidir. Simulyasiya edilmiş hücumlar, real nümunələr və interaktiv tapşırıqlar şəxslərin təhlükəsizlik təhdidlərini daha yaxşı dərk etməsinə kömək edir. Aşağıda kibertəhlükəsizlik mütəxəssisinin təşkil etməli olduğu əsas maarifləndirmə və təlim istiqamətləri izah olunmuşdur.

Saxta e-poçt və mesajların tanınması yolları

Sosial mühəndislik hücumlarının böyük bir hissəsi “phishing” və “spear phishing” texnikalarına əsaslanır[64]. Bu səbəbdən, mütəxəssis istifadəçilərə aşağıdakı mövzularda təlim keçməlidir:

- “Phishing” e-poçtlarının əsas əlamətləri: təlim iştirakçılarına saxta e-poçtların tipik xüsusiyyətləri (qrammatik səhvlər, şübhəli göndərənlər, təcili çağırışlar) izah edilməlidir.
- Həqiqi və saxta mənbələri ayırd etmə bacarıqları: saxta domen adlarının (məsələn, "paypa1.com" və ya "bank-secure-login.com") və real domen adlarının fərqləndirilməsi yolları öyrədilməlidir.
- Spam filtrlərinin və təhlükəsizlik alətlərinin istifadəsi: təhlükəli mesajların avtomatik aşkarlanması üçün hansı e-poçt təhlükəsizlik sistemlərinin mövcud olduğu və onların necə tətbiq ediləcəyi izah olunmalıdır.
- Real nümunələr üzərində təlimlər: keçmişdə baş vermiş phishing hücumlarının nümunələri göstərilməli və iştirakçılara saxta e-poçtları tanımaq üçün praktiki məşqlər verilməlidir.

Şəxsi məlumatların qorunması üçün davranış qaydaları

Sosial mühəndislik hücumları çox vaxt qurbanların şəxsi məlumatlarını manipulyasiya etməklə həyata keçirilir[65]. Bunun qarşısını almaq üçün mütəxəssis istifadəçilərə aşağıdakı əsas qaydaları izah etməlidir:

- Məlumat paylaşma qaydaları: fərdi və korporativ məlumatların kiminlə və hansı şəraitdə paylaşılmasının təhlükəsiz olduğu barədə konkret göstərişlər təqdim edilməlidir.

[64] Saxta e-poçtu necə tanımaq olar: sizə kömək edəcək 7 məsləhət - Pavel Jelic
[65] Data protection - commission.europa.eu/law/law-topic/data-protection_en

- Həssas məlumatların qorunması: şifrələrin, bank məlumatlarının, işgüzar sənədlərin və digər kritik informasiyanın qorunması üçün hansı tədbirlərin görülməsinin vacibliyi izah olunmalıdır.
- İctimai "Wi-Fi" şəbəkələrindən istifadə zamanı ehtiyat tədbirləri: şəxsi məlumatların açıq şəbəkələr vasitəsilə oğurlanmasının qarşısını almaq üçün VPN və şifrələmə metodlarının istifadəsi tövsiyə edilməlidir.
- Açıq mənbə kəşfiyyatına (OSINT) qarşı fərdi təhlükəsizlik: insanların öz şəxsi məlumatlarını sosial media platformalarında necə qoruyacağı və hücum edən şəxslərin bu məlumatları necə əldə edə biləcəyi barədə maarifləndirmə aparılmalıdır.

Şübhəli fəaliyyətlər barədə məlumat vermə mədəniyyətinin təşviqi

Təşkilatlar daxilində təhlükəsizlik mədəniyyətinin formalaşdırılması, sosial mühəndislik hücumlarının erkən aşkarlanması və qarşısının alınması üçün vacibdir. Bu səbəbdən, kibertəhlükəsizlik mütəxəssisi işçiləri aşağıdakı qaydalar barədə maarifləndirməlidir:

- Şübhəli fəaliyyətlərin dərhal bildirilməsi: işçilər şübhəli zənglər, e-poçtlar və ya digər manipulyasiya cəhdləri barədə dərhal rəhbərliyə və ya təhlükəsizlik şöbəsinə məlumat verməlidir.
- Məlumat sızmalarının aşkarlanması və cavab tədbirləri: işçilərə potensial məlumat sızmalarını necə müəyyən etməli və bu barədə kimə məlumat verməli olduqları izah edilməlidir.
- Təhlükəsizlik insidentlərinin sənədləşdirilməsi: bütün şübhəli fəaliyyətlər və insidentlər qeydə alınmalı və bu informasiyalar əsasında təşkilatın təhlükəsizlik siyasəti təkmilləşdirilməlidir.

Effektiv maarifləndirmə və təlim yanaşmaları

Təlim və maarifləndirmə proqramları mümkün qədər interaktiv və praktiki olmalıdır. Kibertəhlükəsizlik mütəxəssisi aşağıdakı üsullardan istifadə edərək təlimlərin effektivliyini artırmalıdır:

- Simulyasiya edilmiş hücumlar: real həyatda baş verə biləcək sosial mühəndislik hücumlarının işçilər üzərində test edilməsi və nəticələrin təhlili.
- İnteraktiv seminarlar: təhlükəsizlik üzrə mütəxəssislərin və işçilərin birgə müzakirələr aparmasına imkan yaradan təlimlər.
- Qısa və konkret maarifləndirmə materialları: işçilərin mütəmadi olaraq təhlükəsizlik qaydalarını yenidən nəzərdən keçirməsi üçün vizual və asan başa düşülən bələdçilərin hazırlanması.
- Mütəmadi yoxlama və testlər: işçilərin təhlükəsizlik biliklərinin artırılması üçün mütəmadi testlərin keçirilməsi və nəticələr əsasında yeni təlim modullarının hazırlanması.

Sosial mühəndislik hücumlarına qarşı effektiv mübarizə aparmaq üçün fərdlərin və işçilərin maarifləndirilməsi əsas prioritetlərdən biri olmalıdır. Kibertəhlükəsizlik mütəxəssisi, təhlükəsizlik biliklərini artırmaq və sosial mühəndislik hücumlarının təsirlərini azaltmaq üçün sistemli və davamlı təlimlər təşkil etməlidir. Təlimlər nə qədər praktiki və real nümunələr əsasında aparılarsa, istifadəçilər bir o qədər təhlükəsizlik

tədbirlərinə əməl edəcək və kibertəhlükəsizlik səviyyəsini yüksəldəcəklər. Təşkilat daxilində güclü təhlükəsizlik mədəniyyəti yaratmaq, sosial mühəndislik hücumlarının uğur şansını əhəmiyyətli dərəcədə azaldacaq.

Nəticə

Sosial mühəndislik, kibertəhlükəsizliyə qarşı yönəlmiş ən təhlükəli və mürəkkəb hücum metodlarından biri kimi, texnoloji müdafiə sistemlərini keçmək üçün insan zəifliklərini manipulyasiya edir. Hücum edən şəxslərin ən müasir təhlükəsizlik protokollarını aşmaq əvəzinə, insan psixologiyasından istifadə edərək şəxsləri və təşkilatları hədəf alırlar. Bu səbəbdən, sosial mühəndislik texnikaları yalnız texniki həllərlə qarşısı alına bilməz - insan faktorunun gücləndirilməsi və fərdi təhlükəsizlik biliklərinin artırılması bu mübarizənin əsasını təşkil edir.

Kibertəhlükəsizlik strategiyalarının effektiv olması üçün həm texnoloji, həm də insan yönümlü müdafiə tədbirlərinin paralel şəkildə tətbiq olunması vacibdir. “Firewal”lar, antivirus sistemləri və şifrələmə texnologiyaları sistemləri qorumaq üçün güclü vasitələr olsa da, sosial mühəndislik hücumları bu texnoloji baryerləri təsirsiz hala gətirə bilər. İnsanların diqqətsizliyi, etibarın istismarı, qorxu və təcili qərar tələbi kimi psixoloji manipulyasiya üsulları, ən güclü təhlükəsizlik sistemlərinin belə uğursuzluğa uğramasına səbəb ola bilər. Sosial mühəndislik hücumlarının qarşısını almaq üçün fərdlərin və təşkilatların təhlükəsizlik mədəniyyətini formalaşdırması və davamlı maarifləndirmə tədbirləri həyata keçirməsi vacibdir. İşçilər, şübhəli e-poçt və mesajları tanımaq, şəxsi və korporativ məlumatların qorunması üçün qaydalara riayət etmək və şübhəli fəaliyyətləri vaxtında bildirmək kimi əsas bacarıqlara sahib olmalıdırlar. Təhlükəsizlik mütəxəssisləri bu bilikləri inkişaf etdirmək və aktual təhlükələrə qarşı proaktiv tədbirlər görmək üçün mütəmadi təlimlər təşkil etməlidirlər.

Təşkilatlar və şəxslər, sosial mühəndislik hücumlarına qarşı dayanıqlı olmaq üçün təhlükəsizlik protokollarını daim yeniləməli, kibertəhlükəsizlik siyasətlərini gücləndirməli və fərdi bilikləri artırmalıdırlar. Hücumların mürəkkəbliyi və inkişaf edən texnologiyalar kibertəhlükəsizlik sahəsində adaptiv və hərtərəfli yanaşmanı tələb edir. Sonda qeyd etmək lazımdır ki, sosial mühəndislik və kibertəhlükəsizlik bir-biri ilə sıx bağlı olan anlayışlardır və təhlükəsizliyə hərtərəfli yanaşmanı tələb edirlər.

§ 6. Sosial mühəndisliyə qarşı mübarizənin təşkili və müdafiə üsulları

Giriş

Sosial mühəndisliyə qarşı effektiv mübarizə, yalnız texnoloji tədbirlərin tətbiqi ilə məhdudlaşmır. Bu mübarizə, həm təhlükəsizlik şüurunu artırmaq, insan faktorunu gücləndirmək və hücumların qarşısını almaq üçün sistemli yanaşmanı tələb edir. Sosial mühəndislik hücumları əsasən insan zəifliklərindən istifadə etdiyinə görə, bu hücumlarla mübarizə aparmaq üçün yalnız kibertəhlükəsizlik alətlərinə etibar etmək kifayət deyil. Hücum edən şəxslər manipulyasiya texnikalarına qarşı dayanıqlılığın artırılması üçün psixoloji, davranış və təşkilati müdafiə mexanizmləri inkişaf etdirilməlidir.

Sosial mühəndislik hücumlarına qarşı kompleks mübarizə üçün üç əsas istiqamət nəzərə alınmalıdır:

1. ***İnsan faktoru və maarifləndirmə[66]:***

- İstifadəçilərin təhlükəsizlik şüurunu artırmaq.
- Hücum texnikalarının izah edilməsi və onların psixoloji təsirlərinin izah olunması.
- Praktiki təlimlər və simulyasiya edilmiş hücumlar vasitəsilə şəxslərin və təşkilatların hazırlıq səviyyəsinin artırılması.

2. ***Texnoloji təhlükəsizlik tədbirləri[67]:***

- Hücumların erkən aşkarlanması və qarşısının alınması üçün kibertəhlükəsizlik sistemlərinin tətbiqi.
- Spam filtrləri, phishing hücumlarına qarşı qorunma sistemləri və iki faktorlu autentifikasiyanın aktiv edilməsi.
- Monitorinq və təhlükəsizlik tədbirlərinin avtomatlaşdırılması ilə hücumların təsirinin azaldılması.

3. ***Təşkilati təhlükəsizlik strategiyaları:***

- Korporativ təhlükəsizlik siyasətləri və daxili nəzarət sistemlərinin gücləndirilməsi.
- Hücum cəhdlərinə qarşı çevik reaksiya mexanizmlərinin inkişaf etdirilməsi.
- Sosial mühəndislik hücumlarının təşkilat daxilində test edilməsi və real təhlükə ssenarilərinin yaradılması.

Bu mühazirədə sosial mühəndislik hücumlarının qarşısının alınması üçün nəzəri yanaşmalar, texnoloji tədbirlər, təşkilati prosedurlar və fərdi müdafiə strategiyaları ətraflı izah ediləcək. Xüsusilə, real situasiyalar və praktiki müdafiə üsulları üzərində fokuslanaraq, hücumların aşkarlanması və qarşısının alınması üçün effektiv metodlar təqdim olunacaq. Şəxslər və təşkilatlar üçün sosial mühəndislik hücumlarına qarşı gündəlik həyatda tətbiq edilə biləcək konkret müdafiə tədbirləri və qabaqlayıcı strategiyalar müzakirə ediləcək.

---

[66] Is there a yelp for ransomware? - Matt Freeman

[67] Avoiding social engineering and phishing attacks - www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks

Sosial mühəndisliyə qarşı mübarizə strategiyaları

Sosial mühəndislik hücumlarının qarşısını almaq üçün effektiv strategiyalar təkcə texnoloji tədbirlərlə məhdudlaşmamalıdır. Hücumların əsas hədəfi insan faktoru olduğuna görə, bu mübarizədə maarifləndirmə, simulyasiyalar, psixoloji davamlılıq və təşkilati təhlükəsizlik siyasətləri əsas rol oynayır. Hücum edən şəxslər insan psixologiyasının zəifliklərindən istifadə edərək, qurbanları manipulyasiya yolu ilə gizli məlumatları açıqlamağa və ya təhlükəsizlik qaydalarını pozmağa sövq edirlər. Buna görə də, şəxslərin və təşkilatların bu texnikaları vaxtında tanıya bilməsi və uyğun cavab verməsi vacibdir.

Sosial mühəndisliyə qarşı mübarizənin uğurlu olması üçün real həyat təcrübələrinə əsaslanan praktik yanaşmalar tətbiq olunmalıdır. İşçilər və şəxslər sosial mühəndislik texnikalarının necə işlədiyini bilməklə yanaşı, hücumlara real vaxtda necə reaksiya verəcəklərini də öyrənməlidirlər. Məhz bu səbəbdən, təlimlər və simulyasiya edilmiş hücumlar təhlükəsizlik strategiyalarının əsasını təşkil etməlidir.

Aşağıda sosial mühəndisliyə qarşı effektiv mübarizə üçün tətbiq edilə bilən əsas strategiyalar və onların praktiki tətbiqi təqdim olunur:

1. Maarifləndirmə və təlimlər

Sosial mühəndislik hücumlarını tanıma qabiliyyətini artırmaq üçün mütəmadi maarifləndirmə və təlimlər təşkil olunmalıdır. Şəxslər və işçilər hücumların əsas xüsusiyyətlərini və real həyatda onları necə tanıya biləcəklərini bilməlidirlər.

Praktik Tədbirlər:

Simulyasiya edilmiş phishing hücumları: İşçilərə və şəxslərə qarşı real "phishing" e-poçtları göndərilərək onların reaksiyaları ölçülməli və nəticələr təhlil olunmalıdır. Aşağıda işçilərin və şəxslərin təhlükəsizlik biliklərini yoxlamaq və onların diqqətliliyini artırmaq üçün istifadə edilə bilən phishing hücum ssenariləri təqdim olunur. Hər bir ssenari, hücumun məqsədini, icra metodunu və gözlənilən reaksiyanı əks etdirir.

1. **"Təcili şifrə yenilənməsi" (Corporate IT phishing)**

- **Hücum məqsədi:** İşçilərdən şirkət hesablarının giriş məlumatlarını əldə etmək.
- **İcra metodu:** Saxta IT xidməti e-poçtu göndərilir.
- **Gözlənilən reaksiya:** İşçilərin bu tip saxta e-poçtları tanımasını və şifrə paylaşmaqdan imtina etməsini təmin etmək.

Simulyasiya mesajı:
Göndərən: *IT Dəstək* *security@company-support.com*
Mövzu: [TƏCİLİ] Şifrəniz bu gün yenilənməlidir - GİRİŞ LİNKİ
Məzmun:
Hörmətli işçi,

Şirkətimizin təhlükəsizlik qaydalarına əsasən, bütün işçilər bu gün son tarixinə qədər şifrələrini yeniləməlidirlər. Əks halda hesabınıza giriş məhdudlaşdırılacaq.

Zəhmət olmasa, aşağıdakı linkə daxil olaraq yeni şifrənizi yaradın: ***Şifrə Yeniləmə Portalı***

Diqqət! Əgər bu prosesi tamamlamazsınızsa, hesabınız avtomatik olaraq kilidlənəcək.

Təşəkkür edirik,
IT dəstək xidməti

2. "Bonus mükafat kampaniyası" (Financial scam phishing)

- **Hücum məqsədi:** İşçiləri və ya müştəriləri maliyyə fırıldağına aldatmaq.
- **İcra metodu:** "Şirkət bonusu qazandınız!" tipli saxta e-poçt göndərilir.
- **Gözlənilən reaksiya:** İşçilərin bu cür cəlbedici təkliflərə inanmaması və məlumat paylaşmaqdan çəkinməsi.

Simulyasiya Mesajı:
Göndərən: *HR Departamenti bonus@company-rewards.com*
Mövzu: TƏBRİKLƏR! 500 AZN Dəyərində Şirkət Bonusu qazandınız!
Məzmun:
Hörmətli əməkdaş,
2024-cü ilin performans dəyərləndirməsinə əsasən, siz şirkətimizin bonus proqramında qalib gəlmisiniz!
500 AZN dəyərində hədiyyə kartınızı aktivləşdirmək üçün aşağıdakı linkə daxil olun:
Mükafatınızı Daxil Edin
Diqqət! Bonusu təsdiqləmək üçün bank hesab məlumatlarınızı daxil etməyiniz tələb olunur.

Təbriklər!
HR departamenti

3. "COVID-19 təhlükəsizlik yeniləməsi" (Health alert phishing)

- **Hücum məqsədi:** İşçiləri qorxu və təcili qərar verməyə məcbur etmək.
- **İcra metodu:** Saxta "Təcili Tibbi Xəbərdarlıq" e-poçtu göndərilir.
- **Gözlənilən reaksiya:** İşçilərin panikaya düşməməsi və rəsmi mənbələrdən məlumat yoxlaması.

Simulyasiya mesajı:
Göndərən: *Sağlamlıq Departamenti health@company-medical.com*
Mövzu: Təcili COVID-19 xəbərdarlığı – Siz yoluxmuş şəxslə təmasda olmusunuz!

Məzmun:

Hörmətli işçi,

Son 24 saat ərzində sizinlə eyni iş mühitində COVID-19 pozitiv test nəticəsi olan bir şəxs qeydə alınıb. Siz dərhal aşağıdakı linkə daxil olaraq sağlamlıq yoxlamasından keçməli və test nəticənizi təsdiqləməlisiniz:

Test nəticənizi yoxlayın

Əks halda, iş yerinə girişiniz məhdudlaşdırılacaq.

Sağlam qalın!

Şirkət sağlamlıq departamenti

Hər bir phishing simulyasiyası bitdikdən sonra işçilərin reaksiyaları analiz edilməli və nəticələr təhlil olunmalıdır:

- Neçə nəfər saxta linkə klikləyib?
- Neçə nəfər giriş məlumatlarını daxil edib?
- Neçə nəfər phishing hücumunu tanıyıb və təhlükəsizlik komandası ilə əlaqə saxlayıb?
- İşçilərin hansı hissəsi ən çox riskə məruz qalıb? (yeni işçilər, yüksək vəzifəli şəxslər və s.)
- Əsas zəifliklərin nələr olduğu və gələcəkdə hansı sahələr üzrə təlimlərin aparılmalı olduğu müəyyən edilməlidir.

Bu testlərin nəticələri əsasında şirkət daxilində maarifləndirmə proqramları təkmilləşdirilməli, işçilərə fərdi qaydada geri bildirim verilməli və təhlükəsizlik təlimləri gücləndirilməlidir.

Bu simulyasiyalar real həyatda baş verən phishing hücumlarını imitasiya edərək işçiləri və fərdləri daha diqqətli və ehtiyatlı olmağa hazırlayır. Eyni zamanda, təşkilatın təhlükəsizlik siyasətinin effektivliyini qiymətləndirmək və təkmilləşdirmək üçün əhəmiyyətli bir vasitədir. Mütəmadi olaraq simulyasiya edilmiş phishing hücumları həyata keçirməklə, təşkilatlar sosial mühəndislik hücumlarına qarşı daha güclü müdafiə mexanizmləri qura bilərlər.

Canlı təlimlər və vebinarlar:

İştirakçılar üçün sosial mühəndislik texnikaları haqqında seminarlar təşkil olunmalı, real hadisələr üzərində təhlillər aparılmalıdır.

Canlı təlimlər və vebinarlar sosial mühəndislik hücumlarına qarşı şəxsləri və təşkilatları hazırlamaq üçün ən effektiv maarifləndirmə üsullarından biridir. Bu təlimlər real hadisələrin təhlili, praktiki məşqlər və iştirakçıların interaktiv iştirakına əsaslanmalıdır. Aşağıda real istifadə oluna bilən təlim və vebinar nümunəsi təqdim edilir:

1. **"Sosial mühəndislik: düşmənin silahını tanıyın" (əsas təhlükəsizlik maarifləndirmə təlimi)**

➢ **Təlimin məqsədi:** Şəxslərin və işçilərin sosial mühəndislik hücumlarının əsas texnikalarını tanımasını və onlara qarşı müqavimət göstərməsini təmin etmək.

➢ **Təlim formatı:** 90 dəqiqəlik canlı seminar + interaktiv testlər və qrup müzakirələri.

➢ **Təlim iştirakçıları:** Təşkilat işçiləri, IT mütəxəssisləri və fərdi istifadəçilər.

Təlimin əsas mövzuları:

- **Sosial mühəndislik nədir?** Hücum edən şəxsin istifadə etdiyi əsas metodlar.
- **Phishing, smishing və vishing hücumlarını necə tanımaq olar?**
- **Həqiqi hadisələr üzərindən təhlil:** Ən böyük sosial mühəndislik hücumlarının nümunələri.
- **Real vaxtda phishing testi:** İştirakçılara saxta phishing e-poçtları təqdim edilir və onların analiz etməsi tələb olunur.
- **Qorunma yolları:** Real həyatda tətbiq edilə biləcək effektiv təhlükəsizlik strategiyaları.

Təlimin praktiki icrası:

1. İştirakçılara iki phishing e-poçtu göstərilir və onlardan təhlükəli elementləri tanımaları istənilir.
2. **Canlı hücum ssenarisi oynanılır:** Təlimçi iştirakçılardan birinə saxta texniki dəstək zəngi edir və məlumatları əldə etməyə çalışır.
3. **Təhlükəsizlik davranış testi keçirilir:** İştirakçılar fərqli hücum ssenarilərinə necə cavab verəcəklərini bildirirlər.

Təlim nəticələri və qiymətləndirmə:

- Təlimin sonunda iştirakçılara real həyat senarilərinə əsaslanan testlər keçirilir.
- Fərdi və komanda performansları analiz edilir.
- Təhlükəsizlik biliklərində zəif olan iştirakçılar üçün əlavə təlimlər tövsiyə olunur.

2. "CEO fraud və iş e-poçtu kompromaası (BEC): necə müdafiə olunmalı?"

➢ **Təlimin məqsədi:** rəhbər şəxslərə və maliyyə şöbəsi işçilərinə yönəlik iş e-poçtu kompromaası (BEC) və CEO fraud hücumları haqqında məlumat vermək və müdafiə tədbirlərini izah etmək.

➢ **Təlim formatı:** 60 dəqiqəlik vebinar + canlı demo və sual-cavab sessiyası.

➢ **Təlim iştirakçıları:** maliyyə menecerləri, rəhbər şəxslər, IT təhlükəsizlik komandası.

Təlimin əsas mövzuları:

- **İş e-poçtu kompromaası (BEC) nədir?** Şirkətlərin ən çox üzləşdiyi hücum formaları.
- **CEO Fraud hücumlarının anatomiyası:** Rəhbərlik adından göndərilən saxta e-poçtların analizi.
- **Canlı hücum ssenarisi:** Real vaxtda bir BEC hücumunun necə işlədiyini göstərən praktiki nümunə.

Maliyyə fırıldaqlarına qarşı müdafiə strategiyaları:

- İki faktorlu autentifikasiyanın vacibliyi.
- Mühasibat sistemlərinə giriş qaydalarının gücləndirilməsi.
- Şübhəli e-poçtların yoxlanılması üçün "daxili təhlükəsizlik protokolları".

Təlimin praktiki icrası:

1. **Canlı simulyasiya:** təlimçi rəhbərlik adından saxta e-poçt göndərir və iştirakçılardan səhvləri tapmaları istənilir.
2. **Hücumun təsir mexanizmi izah olunur:** hücumun necə həyata keçirildiyi və uğurla nəticələndiyi nümunələr əsasında izah edilir.
3. **Təhlükəsizlik tədbirləri təqdim edilir:** hücumların qarşısını almaq üçün ən yaxşı təhlükəsizlik təcrübələri paylaşılır.

Təlim nəticələri və qiymətləndirmə:

- İştirakçılar arasında təhlükəsizlik biliklərinin ölçülməsi üçün sorğular keçirilir.
- Rəhbər şəxslərə və maliyyə şöbəsinə xüsusi təhlükəsizlik qaydaları təqdim edilir.
- Təlimdən sonra şirkət daxilində təhlükəsizlik siyasətləri gücləndirilir.

3. "Sosial mühəndisliklə fiziki hücumlar: ofisiniz nə qədər təhlükəsizdir?"

- **Təlimin məqsədi:** təşkilat işçilərinə və təhlükəsizlik komandalarına, sosial mühəndislik texnikaları ilə icazəsiz fiziki girişlərin necə mümkün olduğunu öyrətmək.
- **Təlim formatı:** 120 dəqiqəlik canlı seminar + ofis daxilində simulyasiya edilmiş "tailgating" və "pretexting" sınaqları.
- **Təlim iştirakçıları:** şirkət işçiləri, təhlükəsizlik heyəti, resepsiya və mühafizə xidməti əməkdaşları.

Təlimin əsas mövzuları:

- **Fiziki sosial mühəndislik hücumları:** Hücum edən şəxsin icazəsiz ərazilərə necə daxil ola bildiyinin izahı.
- **Tailgating və shoulder surfing:** İcazəsiz şəxslərin iş mühitinə giriş metodları.
- **Real hadisələrdən nümunələr:** Fiziki sosial mühəndislik hücumları nəticəsində təşkilatlara dəyən real itkilərin analizi.

İcazəsiz girişin qarşısını almaq üçün tədbirlər:

- İşçilərin təhlükəsizlik nişanlarından istifadə qaydaları.
- İcazəsiz şəxslərin identifikasiyası.
- Tailgating və shoulder surfing hallarında tətbiq ediləcək protokollar.

Təlimin Praktiki İcrası:

1. **Simulyasiya edilmiş tailgating hücumu:** Təlimçi, bir işçi ilə birlikdə ofisə giriş etməyə çalışır və işçilərin reaksiyası müşahidə edilir.

2. **Pretexting sınağı:** Təlimçi, özünü "IT mütəxəssisi" kimi təqdim edərək bir işçidən şəxsi giriş məlumatlarını tələb edir.

3. **Real təhlükəsizlik tədbirləri tətbiq edilir:**

- İşçilərə, ofisə icazəsiz girişlərin qarşısını almaq üçün hansı tədbirləri görməli olduqları göstərilir.
- Qapı təhlükəsizlik sistemlərinin gücləndirilməsi üçün tövsiyələr verilir.

Təlim nəticələri və qiymətləndirmə:

- İcazəsiz girişlərin qarşısını almaqda işçilərin davranışları analiz edilir.
- Hansı bölmələrin təhlükəsizlik qaydalarına daha yaxşı əməl etdiyi müəyyən edilir.
- Təhlükəsizlik zəiflikləri aşkar olunaraq tədbirlər planı hazırlanır.

Bu təlimlər və vebinarlar işçiləri real hücum ssenarilərinə hazırlamaq, təhlükəsizlik biliklərini artırmaq və sosial mühəndislik hücumlarına qarşı daha güclü qoruma tədbirləri formalaşdırmaq üçün nəzərdə tutulub. Təşkilatlar bu təlimlər vasitəsilə işçi heyətini daha yaxşı hazırlaya və ümumi kibertəhlükəsizlik səviyyəsini yüksəldə bilərlər.

"Red Team" məşqləri:

Təşkilatlar daxilində "hücum qrupları" yaradılaraq işçilərin təhlükəsizlik reaksiyaları yoxlanılmalıdır.

Red Team məşqləri, təşkilatların və işçilərin sosial mühəndislik hücumlarına necə reaksiya verdiyini yoxlamaq və onların təhlükəsizlik biliklərini artırmaq üçün real hücum ssenarilərinin canlandırılmasıdır. Bu məşqlər texnoloji, fiziki və psixoloji manipulyasiya metodlarını test edərək təşkilatın təhlükəsizlik strategiyalarını təkmilləşdirməyə kömək edir.

Aşağıda üç fərqli sosial mühəndislik hücumu üzrə Red Team məşqi nümunəsi təqdim olunur:

1. Pretexting (yalançı təqdimat): "sənəd təsdiqləmə hücumu"

Məqsəd: işçilərin şirkət daxili məxfi sənədlərin üçüncü şəxslərlə paylaşılmasına qarşı nə qədər diqqətli olduğunu test etmək.

İcra metodu: Red Team üzvü mühasibatlıq və ya hüquq departamenti adından işçilərə müraciət edərək sənəd təsdiqləmə və ya müqavilə yenilənməsi üçün məxfi məlumat tələb edir.

Məşqin əsas məqsədləri:

- İşçilərin yalançı ssenariləri nə dərəcədə tanıdığı yoxlanılır.
- Mühasibat və HR komandalarının məlumat paylaşma protokollarına riayət edib-etmədiyi test edilir.
- Şirkət daxilində məlumat paylaşımlarında nəzarət mexanizmlərinin effektivliyi qiymətləndirilir.

Məşqin simulyasiya ssenarisi:

- Red Team üzvü özünü hüquq departamentinin əməkdaşı kimi təqdim edərək mühasibatlıq və ya HR şöbəsinə müraciət edir.

- "Yeni iş müqavilələrində dəyişiklik edilib, bu sənədləri təsdiqləmək üçün HR bazasından işçilərin şəxsi məlumatlarını bizə göndərməlisiniz" kimi bir tələblə çıxış edir.

İşçilərin reaksiyası analiz edilir:

- Məlumatı dərhal paylaşdılar?
- Rəsmi təsdiqləmə tələb etdilər?
- Hüquq departamentinə və ya təhlükəsizlik şöbəsinə məlumat verdilər?

Nəticələr və təhlil:

- Məlumatları paylaşan işçilər müəyyən edilir və xüsusi təhlükəsizlik təlimlərinə cəlb olunur.
- Şirkət daxilində məxfi məlumat paylaşımı üçün rəsmi təsdiq prosedurları gücləndirilir.
- Məlumat istəklərinə cavab verməzdən əvvəl mənbənin yoxlanılması qaydaları tətbiq edilir.

2. Tailgating (icazəsiz fiziki giriş): “qapını açıq saxla” hücumu

Məqsəd: İşçilərin şirkət daxilində fiziki təhlükəsizlik qaydalarına əməl edib-etmədiyini test etmək.

İcra metodu: Red Team üzvü icazəsiz şəkildə şirkət binasına və ya məhdud giriş zonalarına daxil olmağa çalışır.

Məşqin əsas məqsədləri:

- İşçilərin qapı təhlükəsizlik qaydalarına nə qədər riayət etdiyini ölçmək.
- Təhlükəsizlik xidmətinin icazəsiz girişlərə reaksiyasını analiz etmək.
- Şirkət daxilində "tailgating" risklərini aşkar etmək və həll yolları inkişaf etdirmək.

Məşqin simulyasiya ssenarisi:

- Red Team üzvü şirkət işçisinin ardınca qapıdan keçməyə çalışır.
- "Əlimdə çoxlu sənəd var, mənə kömək edin qapını açın" və ya "Mən yeni işçiyəm, kartım hələ hazır deyil" kimi bəhanələrlə içəri keçməyə cəhd edir.

İşçilərin reaksiyası izlənilir:

- İşçilər icazəsiz şəxsin girişinə mane oldular?
- Şübhəli şəxs barədə təhlükəsizlik xidmətinə məlumat verdilər?
- Qapıları bağlı saxlama qaydalarına riayət etdilər?

Nəticələr və təhlil:

- İcazəsiz girişə icazə verən işçilər müəyyən edilir və xüsusi təhlükəsizlik təlimlərinə cəlb olunur.
- Qapı təhlükəsizlik sistemlərinin təkmilləşdirilməsi üçün tədbirlər görülür.
- Şirkət daxilində "Tailgating" qarşısının alınması üçün xəbərdaredici təlimat lövhələri yerləşdirilir.

3. Baiting (cəlbedici təkliflə manipulyasiya): "USB flash disk hücumu"

Məqsəd: İşçilərin xarici və naməlum texnoloji cihazları şirkət sistemlərinə qoşub-qoşmadığını test etmək.

İcra Metodu: Red Team üzvü şirkət daxilində və ya parkinq sahəsində "itirilmiş" USB flash disk yerləşdirir və işçilərin reaksiyasını izləyir.

Məşqin əsas məqsədləri:

- İşçilərin xarici cihazları tanımadan istifadə etmə meylini yoxlamaq.
- Şirkət daxilində məlumat təhlükəsizliyi qaydalarının nə dərəcədə effektiv olduğunu ölçmək.
- USB və xarici cihaz təhlükəsizliyi siyasətinin gücləndirilməsinə ehtiyac olub-olmadığını müəyyənləşdirmək.

Məşqin simulyasiya ssenarisi:

- Red Team üzvü şirkət binasının yaxınlığında və ya parkinq sahəsində üzərində "MÜHÜM MƏLUMATLAR", "ŞİRKƏT SİRRİ", "İŞÇİ MAAŞ CƏDVƏLİ" yazılmış bir USB flash disk yerləşdirir.

İşçilərin reaksiyası izlənilir:

- USB-ni kim tapır və nə edir?
- USB-nin məzmununu yoxlamaq üçün onu şirkət kompüterinə qoşurlar?
- İşçilər təhlükəsizlik şöbəsinə bu barədə məlumat verirlər?

Nəticələr və təhlil:

- USB-ni kompüterə qoşan işçilər müəyyən edilir və fərdi təhlükəsizlik təlimlərinə cəlb olunur.
- Şirkət daxilində xarici cihaz siyasəti gücləndirilir və USB istifadəsi məhdudlaşdırılır.
- İşçilərə tapılan xarici texniki avadanlıqları dərhal təhlükəsizlik şöbəsinə təhvil vermək qaydaları öyrədilir.

Bu "Red Team" məşqləri real sosial mühəndislik hücumlarını imitasiya edərək təşkilatların və işçilərin təhlükəsizlik tədbirlərinə necə riayət etdiyini yoxlamaq üçün istifadə edilir. Müntəzəm olaraq bu cür məşqlərin həyata keçirilməsi, işçilərin sosial mühəndislik hücumlarına qarşı müqavimətini artırır, təşkilatın zəif tərəflərini aşkar etməyə kömək edir və təhlükəsizlik siyasətlərinin effektivliyini ölçməyə və təkmilləşdirməyə imkan verir.

Bu məşqlər təşkilatın insan və texnoloji təhlükəsizlik tədbirlərinin gücləndirilməsində mühüm rol oynayır.

2. Texnoloji müdafiə tədbirləri

Sosial mühəndislik hücumlarına qarşı texnologiya əsaslı müdafiə tədbirləri kritik rol oynayır. Kibertəhlükəsizlik həlləri və avtomatlaşdırılmış sistemlər hücumların erkən aşkarlanması, qarşısının alınması və potensial risklərin azaldılması üçün mühüm vasitələrdir. Müasir kibertəhlükəsizlik yanaşmaları süni intellekt və maşın öyrənmə texnologiyalarından istifadə edərək şübhəli fəaliyyətləri real vaxt rejimində analiz etməyə

və potensial hücumları müəyyən etməyə imkan yaradır. Təhlükəsizlik məlumatlarının və hadisələrin idarə edilməsi sistemləri (SIEM) hücum indikatorlarını aşkar edərək təhlükəli prosesləri dərhal bloklayır. Bundan əlavə, çoxfaktorlu autentifikasiya (MFA) və sıfır etibar modeli (Zero Trust Architecture) sosial mühəndislik vasitəsilə icazəsiz girişlərin qarşısını almaq üçün effektiv həllər arasında yer alır. Aşağıda real praktik tədbirlər və sektora uyğun texnoloji həllər təqdim olunur:

Praktik texnoloji tədbirlər:

1. Spam filtrlərinin gücləndirilməsi

Spam filtrləri saxta e-poçtların və phishing hücumlarının avtomatik bloklanmasını təmin edən əsas sistemlərdən biridir. Hücum edən şəxslər tez-tez rəsmi qurumlar və ya tanınmış brendlərin adından e-poçtlar göndərərək qurbanları manipulyasiya etməyə çalışırlar. Gücləndirilmiş spam filtrləri bu cür hücumların qarşısını almağa kömək edir.

Nümunə:

- Google Workspace[68] və Microsoft 365 Advanced Threat Protection (ATP)[69] - Bu sistemlər e-poçtlarda phishing linklərini avtomatik aşkar edir, spam məzmunlu mesajları filtrləyir və təhlükəli əlavələri bloklayır.
- Barracuda email security gateway[70] - Phishing və spam e-poçtlarını real vaxtda analiz edərək potensial təhlükələri işarələyir.

Əlavə təhlükəsizlik tədbiri:

- E-poçt filtr sistemləri mütəmadi olaraq yenilənməli və təlim olunmalıdır. Məsələn, Google və Microsoft-un spam süzgəcləri məlumat bazalarına əsasən yeni phishing üsullarını öyrənir və adaptasiya olur.

2. DNS və URL filtrləri

Saxta veb-saytlara girişin qarşısını almaq üçün avtomatik bloklama sistemlərinin tətbiqi mütləqdir. Hücum edən şəxslər qurbanları saxta bank və ya şirkət səhifələrinə yönləndirərək onların məlumatlarını ələ keçirə bilərlər.

Nümunə:

- Cisco Umbrella[71] və Cloudflare Gateway DNS filtrləri[72] - Saxta domenlərin və phishing saytlarının aşkarlanması üçün istifadə olunur. Bu sistemlər istifadəçinin fırıldaqçı linklərə daxil olmasını avtomatik bloklayır.
- "Google Safe Browsing"[73] və "Microsoft SmartScreen"[74] - Zərərli vebsaytlara qarşı xəbərdarlıqlar göstərir və təhlükəli səhifələrə girişin qarşısını alır.

Əlavə təhlükəsizlik tədbiri:

- Şirkətlər və fərdi istifadəçilər "DNS" filtrlərini aktiv etməli və internet trafiklərini qorumaq üçün təhlükəsizlik firewall-larından istifadə etməlidirlər.

[68] workspace.google.com/
[69] support.microsoft.com/sr-latn-rs/office/microsoft-365-advanced-protection-82e72640-39be-4dc7-8efd-740fb289123a
[70] www.barracuda.com/products/email-protection/secure-email-gateway
[71] umbrella.cisco.com/
[72] developers.cloudflare.com/cloudflare-one/policies/gateway/initial-setup/dns/
[73] safebrowsing.google.com/
[74] learn.microsoft.com/en-us/windows/security/operating-system-security/virus-and-threat-protection/microsoft-defender-smartscreen/

3. İki faktorlu autentifikasiya (2FA)

Şəxsi və korporativ hesabların qorunmasını artırmaq üçün iki faktorlu autentifikasiya (2FA) istifadə olunmalıdır. Bu metod şifrə oğurlandıqda belə, ikinci doğrulama tələb etdiyi üçün hesabın ələ keçirilməsini çətinləşdirir.

Nümunə:

- Google Authenticator[75] və Microsoft Authenticator[76] - istifadəçilər hər giriş zamanı mobil cihazları vasitəsilə ikinci doğrulama kodu alırlar.
- YubiKey[77] və Titan Security Key[78] - fiziki təhlükəsizlik açarları (hardware token) vasitəsilə giriş zamanı əlavə təhlükəsizlik tədbiri təqdim edir.

Əlavə təhlükəsizlik tədbiri:

- Bütün həssas xidmətlərdə (e-poçt, bank hesabları, şirkət daxili platformalar) 2FA aktiv edilməlidir.
- Təşkilatlar işçilərinə yalnız SMS kodu ilə 2FA deyil, daha etibarlı autentifikasiya üsullarından (biometrik giriş, hardware token) istifadə etməyi tövsiyə etməlidir.

4. Sistemlərin mütəmadi yenilənməsi

Antivirus və təhlükəsizlik proqramları daim yenilənməlidir. Çünki hücum edən şəxslər yeni zəifliklər aşkar etdikcə, onları istismar etmək üçün zərərli proqramlar və hücum texnikaları hazırlayırlar.

Nümunə:

- Windows və macOS yeniləmələri - Microsoft və Apple hər ay təhlükəsizlik yamaları təqdim edərək sistemlərin yeni zəifliklərdən qorunmasını təmin edir.
- Patch Management Tools (IBM BigFix, Qualys) - Şirkətlərdə istifadə olunan bütün sistemlərin avtomatik yenilənməsi üçün tətbiq edilir.

Əlavə təhlükəsizlik tədbiri:

- Şirkətlərdə sistem yeniləmələri məcburi edilməli və avtomatik yeniləmə siyasəti tətbiq olunmalıdır.
- Hər hansı proqram təminatı quraşdırılmadan öncə onun rəsmi mənbədən endirildiyinə əmin olunmalıdır.

Sahələr üzrə texnoloji tədbirlər:

1. E-poçt təhlükəsizliyi sistemləri

Şirkətlər və fərdi istifadəçilər üçün phishing hücumlarının qarşısını almaq üçün xüsusi e-poçt təhlükəsizlik sistemlərindən istifadə olunmalıdır.

Nümunə:

- Proofpoint email security[79] - İşçilərin phishing hücumlarına qarşı simulyasiya testləri ilə onların təhlükəsizlik biliklərini artırır.

[75] apps.apple.com/us/app/google-authenticator/id388497605
[76] www.microsoft.com/ru-ru/security/mobile-authenticator-app
[77] www.yubico.com/
[78] store.google.com/regionpicker?hl=en-US
[79] www.proofpoint.com/us/products/email-security-and-protection/email-protection

- Mimecast email security[80] - Saxta göndərici adreslərini müəyyən edir və təhlükəli məzmunu avtomatik silir.

Əlavə təhlükəsizlik tədbiri:

- Şirkət daxilində işçilərə "sıfır etibar" (zero trust) prinsipi öyrədilməlidir - yəni heç bir e-poçt və ya link dərhal etibarlı hesab edilməməlidir.

2. Məlumat sızmalarının monitorinqi

Dark Web və sızdırılmış məlumat bazalarında təşkilatın və ya fərdi istifadəçilərin məlumatlarının yayılıb-yayılmadığını yoxlamaq üçün xüsusi alətlərdən istifadə olunmalıdır.

Nümunə:

- Have i been pwned?[81] - İstifadəçilərə e-poçt və şifrələrinin sızdırılıb-sızdırılmadığını göstərən pulsuz xidmət.
- SpyCloud[82] və CybelAngel[83] - Şirkətlərin həssas məlumatlarının dark web üzərində monitorinqini həyata keçirir.

Əlavə təhlükəsizlik tədbiri:

- Şifrələrin mütəmadi dəyişdirilməsi və eyni şifrənin bir neçə platformada istifadə edilməməsi vacibdir.
- Məlumat sızmalarının qarşısını almaq üçün şifrələrin avtomatik idarəedilməsi üçün "Password Manager" proqramları (1Password, Bitwarden, LastPass) istifadə edilməlidir.

3. Ağıllı autentifikasiya metodları

Biometrik autentifikasiya və hardware token-lərdən istifadə edərək təşkilatlar giriş təhlükəsizliyini artırmalıdır.

Nümunə:

- Apple Face ID[84] və Windows Hello[85] - İstifadəçilərin girişini biometrik tanıma vasitəsilə qoruyur.
- YubiKey və Titan Security Key - Şəxsi identifikasiya üçün hardware əsaslı autentifikasiya cihazları.

Əlavə təhlükəsizlik tədbiri:

- Təşkilatlar kritik sistemlərə giriş üçün yalnız paroldan istifadə etməməli, fiziki autentifikasiya vasitələrini tətbiq etməlidir.
- Biometrik autentifikasiya sistemləri istifadə edildikdə, məlumatların yerli səviyyədə saxlanılmasına diqqət edilməlidir.

Texnoloji müdafiə tədbirləri sosial mühəndislik hücumlarına qarşı əsaslı qorunma təmin edir. Spam filtrləri, DNS qoruma sistemləri, iki faktorlu autentifikasiya və məlumat sızmalarının monitorinqi kimi tədbirlər təşkilat və fərdlərin təhlükəsizlik səviyyəsini

[80] www.mimecast.com/products/email-security/
[81] haveibeenpwned.com/
[82] spycloud.com/
[83] cybelangel.com/
[84] support.apple.com/en-us/102381
[85] www.microsoft.com/en-us/windows/tips/windows-hello

əhəmiyyətli dərəcədə artırır. Bu tədbirlər tətbiq edilmədikdə isə sosial mühəndislik hücumlarına qarşı zəifliklər yaranır və ciddi təhlükəsizlik pozuntularına səbəb ola bilər.

3. İdarəetmə və təşkilati təhlükəsizlik siyasətləri

Müasir təşkilatlarda kibertəhlükəsizliyin gücləndirilməsi yalnız texnoloji həllərlə məhdudlaşmamalıdır. Effektiv idarəetmə strategiyaları və təşkilati təhlükəsizlik siyasətləri təhlükələrin qarşısını almaq, riskləri minimuma endirmək və işçilərin təhlükəsizlik qaydalarına riayət etməsini təmin etmək üçün əsas rol oynayır. Sosial mühəndislik hücumları təşkilatlar üçün ciddi təhlükə yaradır, çünki bu hücumlar texnoloji sistemlərdən daha çox insan faktorunu hədəfə alır. Buna görə də, təşkilat daxilində güclü təhlükəsizlik siyasətlərinin hazırlanması və tətbiqi bu hücumların qarşısını almaqda mühüm rol oynayır.

Bu bölmədə təşkilatların təhlükəsizlik siyasətlərini effektiv şəkildə formalaşdırması, işçilərin bu qaydalara riayət etməsini təmin etməsi və təşkilati təhlükəsizliyi artırmaq üçün həyata keçirilməsi vacib olan strategiyalar izah ediləcəkdir.

1. Təşkilati təhlükəsizlik strategiyalarının formalaşdırılması

Təhlükəsizlik strategiyalarının düzgün planlaşdırılması təşkilatların davamlılığını qorumaq və sosial mühəndislik hücumlarına qarşı müqavimət göstərmək üçün vacibdir. Bu strategiyalar informasiya təhlükəsizliyi, işçilərin maarifləndirilməsi və təşkilati idarəetmə prinsipləri ilə birləşdirilməlidir. Təhlükəsizlik siyasətlərinin effektiv işləməsi üçün texniki həllərlə yanaşı, işçi heyətinin də təhlükəsizlik qaydalarına ciddi riayət etməsi təmin edilməlidir. Bundan əlavə, təşkilatlar mütəmadi olaraq kibertəhlükəsizlik risklərini qiymətləndirməli, təhlükəsizlik insidentlərinə qarşı cavab tədbirlərini optimallaşdırmalı və qabaqlayıcı müdafiə mexanizmləri tətbiq etməlidir. Yalnız inteqrasiya olunmuş və davamlı yenilənən təhlükəsizlik yanaşmaları sosial mühəndislik hücumlarına qarşı real qoruma təmin edə bilər.

1.1. Təhlükəsizlik mədəniyyətinin formalaşdırılması

Təşkilat daxilində təhlükəsizlik mədəniyyətinin formalaşdırılması üçün aşağıdakı prinsiplər tətbiq olunmalıdır:

- **Şəffaflıq və hesabatlılıq:** İşçilər təhlükəsizlik qaydalarına riayət etməli və hər hansı şübhəli fəaliyyət müşahidə etdikdə bu barədə müvafiq şöbəyə məlumat verməlidir.
- **Təhlükəsizlik məsuliyyətinin bölüşdürülməsi:** Hər bir işçi öz fəaliyyət sahəsinə uyğun təhlükəsizlik məsuliyyətlərini anlamalıdır.
- **Rəhbərlik tərəfindən təhlükəsizlik dəstəyi:** Yuxarı menecment təhlükəsizlik siyasətlərini aktiv şəkildə dəstəkləməli və nümunəvi davranış sərgiləməlidir.

1.2. Təhlükəsizlik siyasətlərinin rəsmi qaydalarla tənzimlənməsi

Təşkilatlar rəsmi qaydalar hazırlayaraq təhlükəsizlik siyasətlərini tənzimləməlidir. Bu siyasətlər aşağıdakı istiqamətləri əhatə etməlidir:

- **İstifadəçi giriş siyasəti:** İşçilərin yalnız iş funksiyalarına uyğun məlumatlara çıxış hüququ olmalıdır.

- **Parol və kimlik doğrulama siyasəti:** Güclü parolların istifadəsi və çoxmərhələli autentifikasiya (MFA) sistemi tətbiq olunmalıdır.
- **Məlumatların saxlanması və paylaşımı siyasəti:** Məxfi məlumatların kimlər tərəfindən istifadə ediləcəyi və necə qorunacağı haqqında təlimatlar hazırlanmalıdır.

2. Sosial mühəndislik hücumlarına qarşı müdafiə siyasətləri

Sosial mühəndislik hücumları insan zəifliklərindən istifadə edərək təşkilatın informasiya təhlükəsizliyini pozmağa çalışır. Buna görə də, effektiv təhlükəsizlik siyasətləri ilə bu cür hücumların qarşısı alınmalıdır. Təşkilatlar təhlükəsizlik protokollarını təkcə texniki səviyyədə deyil, həm də insan resursları baxımından gücləndirməlidir. İşçilərin şübhəli sorğuları tanıma qabiliyyəti artırılmalı, onların kiberhücum ssenarilərinə qarşı hazırlıqlı olması üçün mütəmadi təlimlər keçirilməlidir. Bundan əlavə, hər bir əməkdaşın təhlükəsizlik siyasətlərinə əməl etməsini təmin etmək üçün yoxlamalar aparılmalı və uyğunluq səviyyəsi qiymətləndirilməlidir. Eyni zamanda, təhlükəsizlik insidentlərinin erkən aşkar olunması və tez bir zamanda cavab verilməsi üçün effektiv insident idarəetmə sistemləri tətbiq edilməlidir. Belə strategiyalar təşkilatın müdafiə səviyyəsini artıraraq sosial mühəndislik hücumlarının uğurlu olma ehtimalını əhəmiyyətli dərəcədə azaldır.

2.1. İşçilərin maarifləndirilməsi və təlim siyasəti

İşçilərin təhlükəsizlik qaydaları haqqında məlumatlandırılması təşkilatın müdafiə gücünü artıran əsas amillərdən biridir. Təhlükəsizlik təlimlərinin aşağıdakı aspektləri əhatə etməsi tövsiyə olunur:

- **Sosial mühəndislik hücumlarının tanınması:** Phishing, vishing və pretexting kimi texnikalar haqqında maarifləndirmə.
- **Təcili hallarda hərəkət planı:** Şübhəli zənglər, e-poçtlar və mesajlarla qarşılaşdıqda hansı tədbirlərin görüləcəyi barədə təlimatların verilməsi.
- **Rutin təhlükəsizlik yoxlamaları:** İşçilərin mütəmadi olaraq simulyasiya edilmiş sosial mühəndislik testlərindən keçirilməsi.

2.2. Giriş idarəetmə siyasəti

Təşkilatlar işçilərin sistemlərə girişini effektiv idarə etmək üçün aşağıdakı siyasətləri tətbiq etməlidir:

- **Minimal giriş prinsipi (principle of least privilege - PoLP[86]):** İşçilərə yalnız işləri üçün zəruri olan məlumatlara giriş hüququ verilməlidir.
- **Rollara əsaslanan giriş nəzarəti (role-based access control - RBAC[87]):** Hər bir işçi yalnız öz vəzifəsinə uyğun sistemlərə giriş imkanı əldə etməlidir.
- **Davamlı autentifikasiya və icazə yenilənməsi:** İşçi sistemlərə giriş hüququnu saxlaması üçün dövri yoxlamalar aparılmalıdır.

2.3. İnsidentlərə cavab siyasəti

Təşkilatlar kibertəhlükəsizlik insidentlərinin operativ aşkarlanması və cavablandırılması üçün aşağıdakı strategiyaları tətbiq etməlidir:

[86] en.wikipedia.org/wiki/Principle_of_least_privilege
[87] en.wikipedia.org/wiki/Role-based_access_control

- **İnsidentlərin dərhal bildirilməsi:** Hər hansı şübhəli fəaliyyət aşkar edildikdə işçilər bunu dərhal təhlükəsizlik şöbəsinə bildirməlidirlər.
- **İT təhlükəsizlik qrupu tərəfindən insidentlərin araşdırılması:** Hadisənin təsir dairəsi müəyyən edilməli və müvafiq tədbirlər görülməlidir.
- **Məlumat sızmasının qarşısını almaq üçün tədbirlər:** Hücum zamanı kritik məlumatların qorunması üçün qabaqlayıcı tədbirlər görülməlidir.

3. Təşkilati təhlükəsizlik infrastrukturunun gücləndirilməsi

Təşkilatlar təhlükəsizlik infrastrukturunu müasir texnologiyalarla gücləndirməli və risklərə qarşı çevik cavab mexanizmləri yaratmalıdır. Bu məqsədlə, məlumat təhlükəsizliyi sistemləri mütəmadi yenilənməli və qabaqcıl kibertəhlükəsizlik həlləri tətbiq edilməlidir. Şəbəkə təhlükəsizliyi gücləndirilməli, firewall və davranış analizi texnologiyalarından istifadə olunaraq potensial təhlükələr erkən mərhələdə aşkarlanmalıdır. Bundan əlavə, təşkilatlar vahid təhlükəsizlik informasiya və hadisə idarəetmə (SIEM) sistemlərini tətbiq edərək real vaxt rejimində hücum cəhdlərini izləyə bilməlidir. Həmçinin, daxili təhlükəsizlik nəzarəti artırılmalı və işçilər üçün təhlükəsizlik qaydalarına riayət etməyi təşviq edən monitorinq və audit mexanizmləri gücləndirilməlidir. Təşkilat daxilində təhlükəsizlik insidentlərinin aşkarlanması və dərhal cavab verilməsi üçün xüsusi komandalar (SOC - Security Operations Center[88]) qurulmalı və onların çevik reaksiyası təmin edilməlidir.

3.1. Avtomatlaşdırılmış təhlükəsizlik monitorinqi və nəzarət

Təşkilatlar təhlükəsizlik insidentlərini real vaxtda izləmək üçün aşağıdakı yanaşmalardan istifadə etməlidir:

- **SIEM sistemləri (security information and event management[89]):** Təhlükəsizlik hadisələrinin real vaxtda monitorinqi və analizi üçün istifadə olunur.
- **Süni intellektlə gücləndirilmiş anomaliya aşkarlanması:** Şəbəkədə şübhəli fəaliyyətlər aşkar edildikdə avtomatik xəbərdarlıq sistemi tətbiq edilməlidir.

3.2. Risk dəyərləndirmə və təhlükəsizlik strategiyalarının yenilənməsi

Təhlükəsizlik siyasətləri və strategiyalarının effektivliyini qorumaq üçün mütəmadi olaraq risk dəyərləndirməsi aparılmalıdır:

- **Hər il təhlükəsizlik risklərinin qiymətləndirilməsi:** Məlumat sızma riskləri və potensial zəifliklər müəyyən edilməlidir.
- **Daxili və xarici təhlükəsizlik auditlərinin aparılması:** Kiber təhlükəsizlik ekspertlərinin köməyi ilə təşkilatın müdafiə səviyyəsi təhlil edilməlidir.

İdarəetmə və təşkilati təhlükəsizlik siyasətləri kibertəhlükəsizliyi gücləndirmək və sosial mühəndislik hücumlarına qarşı effektiv mübarizə aparmaq üçün kritik rol oynayır. Effektiv təhlükəsizlik strategiyalarının tətbiqi təşkilatların informasiya təhlükəsizliyini təmin etməsinə, işçilərin təhlükəsizlik qaydalarına riayət etməsinə və mümkün hücum ssenarilərinə qarşı daha hazırlıqlı olmasına kömək edir.

Təşkilat daxilində giriş idarəetməsindən tutmuş işçi təlimlərinə, təhlükəsizlik insidentlərinin aşkarlanmasından risk qiymətləndirmə prosedurlarına qədər bir sıra

[88] en.wikipedia.org/wiki/Security_operations_center
[89] en.wikipedia.org/wiki/Security_information_and_event_management

tədbirlər sosial mühəndislik hücumlarının təsirini minimuma endirməyə xidmət edir. Hücum edən şəxslərin istifadə etdiyi manipulyasiya metodları və yeni texnologiyalar daim dəyişdiyi üçün təşkilatlar təhlükəsizlik siyasətlərini mütəmadi olaraq yeniləməli və yeni hücum metodlarına qarşı adaptasiya olmalıdırlar.

Bundan əlavə, müasir təhlükəsizlik texnologiyalarının tətbiqi, təşkilat daxilində mədəniyyət halına çevrilmiş təhlükəsizlik şüuru və davamlı təlimlər vasitəsilə insan faktorunun risklərini azaltmaq mümkündür. Hücumların erkən aşkarlanması və cavab sistemlərinin gücləndirilməsi təşkilatların sosial mühəndislik hücumlarına qarşı dayanıqlılığını artıracaqdır. Təhlükəsizlik yalnız texnologiya ilə məhdudlaşmamalı, həm də insan faktorunun önəmini nəzərə alan kompleks yanaşma ilə təmin edilməlidir.

4. Psixoloji müdafiə

Sosial mühəndislik hücumlarının uğur qazanmasının əsas səbəbi insan psixologiyasının manipulyasiyaya məruz qalmasıdır. Hücum edən şəxslər qurbanların qorxu, tələş, təcili qərar vermə ehtiyacı və sosial təsir kimi psixoloji zəifliklərindən istifadə edərək onları təhlükəsizlik qaydalarını pozmağa məcbur edirlər. Bu səbəbdən fərdlərin və işçilərin manipulyasiya üsullarına qarşı psixoloji dayanıqlılığını artırmaq üçün xüsusi psixoloji möhkəmlik proqramları tətbiq olunmalıdır.

Aşağıda praktiki tədbirlər və təlim mövzuları ilə bağlı real nümunələr təqdim olunur.

Praktik tədbirlər:

1. Təzyiq altında rasional qərarvermə təlimləri

Sosial mühəndislik hücumları adətən təcili və emosional reaksiya verməyə yönəldilmiş manipulyasiyalar üzərində qurulur. Buna görə şəxslər təzyiq altında rasional qərar vermə bacarıqlarını inkişaf etdirməlidirlər.

Nümunə:

Bank işçiləri üçün "Təcili transfer" simulyasiyası:

Ssenari: hücum edən şəxs özünü bankın yüksək vəzifəli rəhbəri kimi təqdim edərək işçidən təcili ödəniş etməsini tələb edir.

Təlim məqsədi: İşçilərə belə hallarda rəhbərliklə alternativ rabitə kanalları ilə (rəsmi telefon nömrəsi və ya e-poçt) təsdiq almaq öyrədilir.

Nəticə: İşçilər təcili tələbləri dərhal icra etmədən əvvəl yoxlama mexanizmlərini işə salmağı öyrənirlər.

Həkimlər və tibbi personal üçün "fövqəladə xəstə məlumatı tələbi" təlimi:

Ssenari: Hücum edən şəxs özünü polis və ya hüquq-mühafizə orqanının nümayəndəsi kimi təqdim edərək, xəstə məlumatlarını tələb edir.

Təlim məqsədi: Hüquqi təsdiq olmadan heç bir şəxsi məlumatın açıqlanmayacağı öyrədilir.

Nəticə: Tibbi personal təcili tələb olunan məlumatların rəsmi sənədlərlə təsdiqlənməsini tələb etməyi öyrənir.

2. Emosional manipulyasiya texnikalarının tanıdılması

İnsanlar qorxu, təşviş və təcili yardım tələb edən situasiyalarla üzləşdikdə tez-tez səhv qərarlar verirlər. Hücum edən şəxslər bu vəziyyətdən istifadə edərək qurbanı istənilən məlumatı verməyə və ya təhlükəsizliyi pozmağa məcbur edirlər. Bu cür manipulyasiya texnikalarının tanıdılması fərdlərin belə hallara qarşı müqavimətini artırır.

Nümunə:

"İT dəstək" ssenarisi:

Ssenari: Hücum edən şəxs özünü təşkilatın IT şöbəsinin əməkdaşı kimi təqdim edərək işçidən şifrəsini dəyişdirməsini və ya yeni şifrə göndərməsini tələb edir.

Təlim məqsədi: İşçilərə şəxsi hesab məlumatlarını heç bir halda üçüncü tərəflərlə paylaşmamaq və IT dəstəyi ilə yalnız rəsmi kanallar vasitəsilə əlaqə saxlamaq öyrədilir.

Nəticə: İşçilər belə hallarda rəsmi IT departamenti ilə əlaqə saxlayaraq tələbin həqiqiliyini yoxlamaq vərdişi qazanır.

"Hüquq-mühafizə və ya təcili yardım" hücumu təlimi:

Ssenari: Hücum edən şəxs özünü polis, təcili yardım və ya fövqəladə hallar xidmətinin nümayəndəsi kimi təqdim edərək qurbanın fərdi məlumatlarını tələb edir.

Təlim məqsədi: İnsanlara rəsmi sənəd və identifikasiya olmadan heç bir şəxsi məlumatın açıqlanmaması öyrədilir.

Nəticə: İşçilər rəsmi identifikasiya tələb etmədən heç bir məlumat paylaşmamağın əhəmiyyətini anlayırlar.

3. Sosial təsir və uyğunlaşma texnikalarına qarşı müqavimətin artırılması

İnsanlar sosial normlara uyğunlaşmağa və kollektiv təsirlərə həssaslıq göstərməyə meyillidirlər. Hücum edən şəxslərbu xüsusiyyətdən istifadə edərək insanları öz istədikləri qərarı verməyə yönləndirirlər.

Nümunə:

"Hər kəs bunu edir" hücumu:

Ssenari: Hücum edən şəxs qurbanı inandırmağa çalışır ki, digər işçilər artıq tələbi yerinə yetirib və onun da eyni şeyi etməsi lazımdır.

Təlim məqsədi: İşçilərə "əksəriyyət belə edir" arqumentinin etibarsız olduğu və hər bir hərəkətin fərdi təsdiq olunmasının vacibliyi öyrədilir.

Nəticə: İşçilər sosial təsir altında emosional qərar verməkdən çəkinməyi öyrənir.

"Yüksək rəhbərlikdən gələn tələb" hücumu:

Ssenari: Hücum edən şəxs özünü təşkilatın rəhbəri kimi təqdim edərək işçidən konfidensial sənədləri göndərməsini və ya icazəsiz əməliyyat aparmasını tələb edir.

Təlim məqsədi: İşçilərə belə hallarda rəhbərliklə birbaşa əlaqə saxlamaq və tələbin həqiqiliyini yoxlamaq öyrədilir.

Nəticə: İşçilər səlahiyyətli şəxslərdən gələn hər tələbin əvvəlcədən təsdiqlənməsinin vacibliyini anlayırlar.

Təlim mövzuları:

Müasir dövrdə sosial mühəndislik hücumları sürətlə yayılaraq şəxslərə, təşkilatlara və hətta dövlət qurumlarına ciddi təhdid yaradır. Bu hücumlar əsasən insanların emosional reaksiyalarına və davranışlarına təsir edərək onları manipulyasiya etmək məqsədi güdür. Qorxu, tələş, sosial təsir və təcili qərar tələbi kimi psixoloji mexanizmlər Hücum edən şəxslərin istifadə etdiyi əsas vasitələrdir. Sosial mühəndislik hücumlarına qarşı effektiv mübarizə aparmaq üçün texnoloji müdafiə tədbirləri kifayət etmir. İnsanların psixoloji manipulyasiya üsullarını tanıması və onlara müqavimət göstərmək bacarığını inkişaf etdirməsi vacibdir. Bu məqsədlə təşkil olunan təlimlər insanların şübhəli situasiyalara qarşı daha həssas olmasını təmin edərək onların təhlükəsizlik biliklərini artırmağa yönəldilib.

Aşağıda təqdim edilən təlimlər insan faktorunun sosial mühəndislik hücumlarında necə istifadə edildiyini izah etməklə yanaşı, bu cür hücumlara qarşı müqavimət strategiyalarını da əhatə edir. Təlimlər qorxu və təcili qərar tələblərindən başlayaraq sosial təsir mexanizmlərinə və şübhəli sorğuların analizinə qədər müxtəlif mövzuları əhatə edir. Məqsəd insanlara təhlükəsizlik risklərini tanımaq və bu hücumların qarşısını almaq üçün effektiv bacarıqlar qazandırmaqdır.

1. Qorxu və təcili qərar tələblərinə qarşı müqavimət təlimi

Sosial mühəndislik hücumları tez-tez insanların qorxu və tələş hisslərindən istifadə edərək onları ani qərar verməyə məcbur edir. Hücum edən şəxslər özlərini bank işçisi, hüquq-mühafizə orqanlarının nümayəndəsi və ya texniki dəstək xidməti kimi təqdim edərək qurbanları tələsik addım atmağa vadar edirlər. Məsələn, "Hesabınızdan şübhəli əməliyyat aşkar edilib, dərhal məlumatlarınızı təsdiqləyin" və ya "Sisteminizə virus düşüb, təhlükəni aradan qaldırmaq üçün bu linkə keçid edin" kimi mesajlar insanları qorxu içində qərar verməyə sövq edir.

Bu təlim zamanı iştirakçılara belə hallara soyuqqanlı yanaşmağı öyrətmək məqsədilə simulyasiya edilmiş situasiyalar təqdim olunur. Onlara real hücum nümunələri göstərilir və bu cür hallarda hansı addımları atmaları izah edilir. Təlimin əsas məqsədi insanları emosional manipulyasiya üsullarına qarşı həssaslıqdan qorumaq və rasionallığı qoruyaraq hər hansı bir informasiya təqdim etməzdən əvvəl təsdiqləmə mexanizmlərindən istifadə etməyə təşviq etməkdir.

2. Sosial təsir və uyğunlaşma təzyiqlərinə qarşı müqavimət təlimi

İnsanlar sosial mühitə uyğunlaşmağa və ətrafdakıların hərəkətlərinə əsasən qərar verməyə meyillidirlər. Sosial mühəndislik hücum edən şəxsləri bu zəiflikdən istifadə edərək qurbanları müəyyən davranışlara sövq edirlər. Məsələn, bir təşkilatda hücum edən şəxs özünü rəhbər şəxs kimi təqdim edərək işçidən maliyyə əməliyyatı həyata keçirməyi və ya konfidensial məlumat paylaşmağı tələb edə bilər. Belə hallarda qurban, rəhbərin göstərişinə əməl etmək məcburiyyəti hiss edə bilər.

Bu təlim iştirakçılara sosial təsir mexanizmlərini tanımağı və bu cür təzyiqlər qarşısında müstəqil düşünməyi öyrətməyə yönəldilib. Təlimdə müxtəlif təşkilati

fırıldaqçılıq nümunələri göstərilir, onların necə baş verdiyi və qarşısının necə alınmalı olduğu izah edilir. Həmçinin, insanlara istənilən qərarı verməzdən əvvəl rəsmi təsdiqləmə mexanizmlərindən istifadə etməyi vərdiş halına gətirmək öyrədilir.

3. Şübhəli sorğulara qarşı analiz və təsdiqləmə bacarığı təlimi

Sosial mühəndislik hücumları adətən qurbanlardan məlumat əldə etməyə və ya onları müəyyən hərəkətlərə sövq etməyə yönəlir. Hücum edən şəxslər özlərini bank işçisi, texniki dəstək nümayəndəsi və ya şirkət əməkdaşı kimi təqdim edərək, qurbanın məlumatlarını ələ keçirməyə çalışırlar. Məsələn, hücum edən şəxs birbaşa e-poçt vasitəsilə "Sizin hesabınızda təhlükəsizlik problemi aşkar edilib, sistemə yenidən giriş üçün bu linki izləyin" kimi mesajlar göndərə bilərlər.

Bu təlim insanlara şübhəli sorğuları analiz etməyi və onların həqiqiliyini yoxlamağı öyrətmək üçün nəzərdə tutulub. İştirakçılara real nümunələr təqdim olunur və onlardan sorğuların mənbələrini araşdırmaq, göndəricinin kimliyini təsdiqləmək və təhlükəsizlik siyasətlərinə uyğun olaraq hərəkət etmək tələb edilir. Təlimin məqsədi insanlara fərdi və təşkilati məlumatlarını qorumaq üçün analiz etmə bacarığını inkişaf etdirmək və impulsiv reaksiyaların qarşısını almaqdır.

Bu təlimlər işçilərin və şəxslərin sosial mühəndislik hücumlarına qarşı psixoloji dayanıqlığını artırmağa, qorxu və sosial təsir manipulyasiyalarını tanımağa və belə hallarda daha rasional qərar vermələrinə kömək edəcək.

Psixoloji müdafiə sosial mühəndislik hücumlarına qarşı ən güclü qorunma vasitələrindən biridir. Emosional manipulyasiya, sosial təsir və təcili qərar tələb edən hücum texnikalarına qarşı fərdlərin hazırlıqlı olması təşkilatın təhlükəsizliyini artırır. Bu cür təlimlər və real həyat ssenariləri işçilərin təhlükəsizlik biliklərini və müqavimət gücünü artırmağa kömək edir.

Nəticə

Sosial mühəndisliyə qarşı effektiv mübarizə, texnologiya, insan faktoru və təşkilati təhlükəsizlik siyasətlərinin birgə fəaliyyət göstərdiyi kompleks yanaşma tələb edir. hücum edən şəxslərin əsas hədəfi texnoloji sistemlərdən daha çox insan zəifliklərıdir. Buna görə də, sosial mühəndislik hücumlarına qarşı dayanıqlı müdafiə yalnız güclü texnoloji həllərlə deyil, psixoloji davamlılıq və təhlükəsizlik mədəniyyətinin formalaşdırılması ilə mümkündür. Sosial mühəndislik hücumlarına qarşı mübarizə təkcə təhlükəsizlik mütəxəssislərinin və ya IT şöbələrinin işi deyil. Hər bir işçi, fərdi istifadəçi və rəhbərlik üzvü bu təhlükələrin qarşısını almaqda öz rolunu anlamalı və tədbirlər görməlidir. Təhlükəsizlik mədəniyyətinin formalaşdırılması, davamlı təlimlər və real simulyasiyalar bu sahədə ən effektiv vasitələrdən biridir.

Unutmaq olmaz ki, ən müasir texnoloji təhlükəsizlik sistemləri belə, insan faktorunun zəifliyi nəticəsində aşılır. Bu səbəbdən, sosial mühəndislik hücumlarına qarşı insan və texnologiyanın birgə işlədiyi balanslı və davamlı müdafiə strategiyaları tətbiq edilməlidir. Təhlükəsizlik yalnız bir departamentin vəzifəsi deyil, bütün təşkilatın və cəmiyyətin kollektiv məsuliyyətidir.

§ 7. Sosial mühəndislik hücumlarının nümunələri

Giriş

Sosial mühəndislər insan zəifliklərindən istifadə edərək fərdi şəxslər, dövlət qurumları və korporasiyalar üçün ciddi təhlükə yaradırlar. Bu hücumlar müxtəlif formalar alır və müxtəlif ssenarilər üzrə həyata keçirilə bilər. Hücum edən şəxslər qurbanları manipulyasiya etmək üçün müxtəlif texnikalardan istifadə edirlər, bunlara emosional manipulyasiya, qorxu, inandırıcılıq, tələsiklik hissi yaratmaq, təzyiq göstərmək və sosial təsir üsulları tətbiq etmək daxildir. Məsələn, hücum edən şəxslər özlərini dövlət rəsmisi, texniki dəstək işçisi, bank əməkdaşı və ya işəgötürən kimi təqdim edərək qurbanı aldatmağa və ona təsir etməyə çalışırlar.

Sosial mühəndislik hücumlarının geniş yayılmış növlərinə phishing, spear phishing, tailgating, dumpster diving, quid pro quo, watering hole attack, honey trap, scareware, pretexting və digər texnikalar daxildir. Bu hücumlar e-poçt vasitəsilə saxta mesaj göndərmək, telefon zəngləri ilə insanları aldatmaq, sosial media hesablarını ələ keçirmək, təşkilatların fiziki təhlükəsizlik zəifliklərindən istifadə etmək və hətta insanların şəxsi münasibətlərindən və emosional zəifliklərindən faydalanmaq kimi müxtəlif yollarla həyata keçirilə bilər.

Bu hücumlar təkcə fərdi şəxsləri deyil, böyük şirkətləri, bankları, hökumət qurumlarını, hərbi strukturları, səhiyyə təşkilatlarını və hətta beynəlxalq təşkilatları da hədəf ala bilər. Sosial mühəndislik hücumları nəticəsində milyonlarla insanın şəxsi məlumatları oğurlanmış, təşkilatlara milyardlarla dollar dəyərində maddi ziyan vurulmuşdur.

Bundan əlavə, sosial mühəndislik hücumları kütləvi fırıldaqçılıq hallarında da istifadə olunur. COVID-19 pandemiyası dövründə bir çox insan saxta peyvənd kampaniyaları, tibbi yardım təklifləri və saxta yardım fondları vasitəsilə aldanaraq maddi ziyana uğramışdır. Hücum edən şəxslər insanların qorxu və çaşqınlığından istifadə edərək onların şəxsi və maliyyə məlumatlarını ələ keçirmişdir. Bəzi hallarda Hücum edən şəxs hətta saxta hökumət agentlikləri və ya səhiyyə təşkilatlarının adından çıxış edərək insanları daha inandırıcı şəkildə manipulyasiya etmişdirlər. Onlar rəsmi vebsaytlara bənzəyən fişinq səhifələri yaratmaqla qurbanların məlumatlarını asanlıqla toplaya bilmişlər.

Bu nümunələr sosial mühəndislik hücumlarının real və ciddi təhlükə olduğunu açıq şəkildə göstərir. Hücum edən şəxslərin əsas silahı insan etimadı və ehtiyatsızlığıdır. Buna görə də fərdi şəxslər və təşkilatlar yalnız texnoloji təhlükəsizlik tədbirləri görməklə kifayətlənməməli, həm də işçilərin və istifadəçilərin maarifləndirilməsinə və kibertəhlükəsizlik biliklərinin artırılmasına xüsusi diqqət yetirməlidirlər.

1. Quid pro quo

Quid pro quo hücumları, Hücum edən şəxslərin qurbanlara müəyyən bir xidmət, güzəşt və ya fayda təklif edərək onlardan məxfi məlumat əldə etdiyi sosial mühəndislik üsuludur. Hücum edən şəxslər adətən peşəkar və ya texniki dəstək kimi təqdim edilən saxta təkliflər vasitəsilə həyata keçirilir.

Aşağıda bu hücum növü ilə bağlı 3 nümunə təqdim olunur:

Nümunə 1: "Təhlükəsizlik xidməti təklifi" fırıldağı (2015)[90]

Hadisə:

2015-ci ildə ABŞ-da fəaliyyət göstərən bir neçə texnologiya şirkətinin işçiləri kibercinayətkarların hədəfinə çevrildi. Hücum edən şəxslər özlərini IT mütəxəssisləri və ya təhlükəsizlik analitikləri kimi təqdim edərək işçilərə e-poçt və telefon zəngləri vasitəsilə yaxınlaşdılar.

Onlar işçilərə şirkət daxilində kibertəhlükəsizlik zəifliklərini yoxlamaq və gücləndirmək üçün pulsuz xidmət təklif etdilər**.** "Xidmətdən" istifadə etmək istəyən işçilərdən şifrələrini paylaşmaq və ya xüsusi bir proqram quraşdırmaq tələb edildi.

Nəticə:

- Bir neçə böyük şirkətdə IT administratorlarının və mühəndislərinin hesablarına giriş əldə edildi**.**
- Hücum edən şəxslər bu hesablardan istifadə edərək maliyyə məlumatlarını oğurladı və həssas sənədləri sızdırdı**.**
- Hücum nəticəsində minlərlə müştəri məlumatı qara bazarda satışa çıxarıldı.

Nümunə 2: "COVID-19 peyvənd qeydiyyatı" fırıldağı (2021)[91]

Hadisə:

COVID-19 pandemiyası dövründə dünya miqyasında bir çox ölkələrdə peyvənd olunmaq istəyən vətəndaşlardan şəxsi və tibbi məlumatlar toplamaq üçün saxta qeydiyyat sistemləri yaradıldı**.**

Hücum edən şəxslər müxtəlif dövlət qurumları və ya səhiyyə təşkilatları adından e-poçtlar və SMS mesajları göndərərək vətəndaşlara "sürətli peyvənd qeydiyyatı" və "növbədənkənar vaksinasiya imkanı" təklif etdilər.

Məlumat əldə etmək üçün vətəndaşlardan şəxsiyyət vəsiqəsi məlumatları, bank kartı detalları və tibbi sığorta nömrələri tələb olundu**.**

Nəticə:

- On minlərlə insanın şəxsi və tibbi məlumatları oğurlandı və darknet bazarlarında satıldı**.**
- Bəzi hallarda hücum edən şəxslər peyvənd ödənişlərinin geri qaytarılması adı ilə insanların bank hesablarına daxil oldular**.**
- Hücumdan zərərçəkənlər müxtəlif maliyyə fırıldaqları və saxta kreditlər ilə qarşılaşdılar.

[90] www.ic3.gov/

[91] consumer.ftc.gov/consumer-alerts/2021/01/scammers-cash-covid-19-vaccination-confusion

Nümunə 3: "Sürətli wi-fi təminatı" hücumu (2022)

Hadisə:

2022-ci ildə Avropa və Asiyada beynəlxalq hava limanlarında və otellərdə müşahidə edilən bir hücum taktikası ortaya çıxdı.

Hücum edən şəxslər özlərini Wi-Fi texniki dəstəyi mütəxəssisi kimi təqdim edərək hava limanlarında, otellərdə və ictimai yerlərdə istifadəçilərə "sürətli və təhlükəsiz Wi-Fi xidməti" təklif etdilər.

Bunun üçün istifadəçilərdən Wi-Fi şəbəkəsinə qoşulmazdan əvvəl şifrələrini daxil etmələri, email ünvanlarını paylaşmaları və ya bir tətbiq yükləmələri tələb olundu. Əslində isə bu sistemlər hücum edən şəxslərin nəzarətində olan saxta Wi-Fi şəbəkələri idi**.**

Nəticə:

- Minlərlə istifadəçinin bank hesabları, sosial media giriş məlumatları və işgüzar e-poçtları oğurlandı**.**
- Hücum nəticəsində şirkətlərin daxili şəbəkələrinə icazəsiz giriş əldə edildi**.**
- Zərərçəkənlərdən bəziləri kredit kartları vasitəsilə böyük məbləğlərdə pul oğurlandığını bildirdi**.**

Quid pro quo hücumları insanların pulsuz xidmətlərə və ya xüsusi təkliflərə həddindən artıq güvənməsi üzərində qurulur. Bu səbəbdən şəxslər və təşkilatlar:

- İstənilən "pulsuz xidmət" təklifini araşdırmalıdır və yalnız rəsmi kanallardan təsdiq almalıdırlar**.**
- Şəxsi məlumatlarını və giriş şifrələrini heç vaxt telefon və ya e-poçt vasitəsilə paylaşmamalıdırlar**.**
- Hər hansı bir texniki dəstək və ya IT xidməti yalnız təşkilatın daxili rəsmi resursları vasitəsilə həyata keçirilməlidir**.**

Bu cür fırıldaqlar qarşısında ayıq olmaq kibertəhlükəsizlik mədəniyyətinin ayrılmaz hissəsi olmalıdır**.**

2. Pretexting

Pretexting**,** hücum edən şəxsin müəyyən bir yalançı ssenari yaradaraq qurbanı manipulyasiya etməsi və məxfi məlumatları ələ keçirməyə çalışmasıdır. Bu cür hücumlar əsasən rəsmi qurumların və ya nüfuzlu şəxslərin adından çıxış edərək həyata keçirilir.

Aşağıda Pretexting hücumu ilə bağlı 3 nümunə təqdim edilir:

Nümunə 1: "Apple support" telefon fırıldağı (2018)[92]

Hadisə:

2018-ci ildə ABŞ-da geniş yayılan bir telefon fırıldağı Apple müştəri xidməti adından həyata keçirildi. Hücum edən şəxslərin saxta telefon nömrələri yaradaraq Apple Support xidməti kimi çıxış etdilər və minlərlə insana zəng etdilər.

[92] support.apple.com/en-us/HT208165

Zəng zamanı hücum edən şəxslər istifadəçilərə bildirirdilər ki, onların Apple ID hesabları hakerlər tərəfindən təhlükə altındadır və bu problemi həll etmək üçün dərhal təsdiqləmə kodu və ya şifrə paylaşmaları lazımdır.

Nəticə:

- Minlərlə istifadəçinin Apple ID hesabları sındırıldı və onların iCloud məlumatları oğurlandı.
- Hücum edən şəxslər bəzi istifadəçilərin iPhone-larını uzaqdan kilidlədilər və "kilidi açmaq" üçün fidyə tələb etdilər.
- Fırıldaq nəticəsində bir çox insanın şəxsi şəkilləri və sənədləri sızdırıldı.

Nümunə 2: "CEO fraud" və iş e-poçtu kompromaası (2020)[93]

Hadisə:

2020-ci ildə Fransa və Almaniyada bir neçə böyük şirkət yüksək səviyyəli rəhbərlik adından həyata keçirilən pretexting hücumlarına məruz qaldı.

Hücum edən şəxslər, şirkətlərin maliyyə departamentlərinə e-poçt göndərərək özlərini şirkət CEO-su və ya maliyyə direktoru kimi təqdim etdilər. Onlar bildirirdilər ki, təcili bir beynəlxalq ödəniş edilməlidir və mühasibatlıq şöbəsi dərhal verilən bank hesabına pul köçürməlidir.

Bəzi hallarda hücum edən şəxslər rəhbərlərin səs nümunələrini süni intellekt vasitəsilə təqlid edərək (deepfake audio) maliyyə mütəxəssislərinə zəng etdilər və bu ödənişin "rəsmi" olduğunu bildirdilər.

Nəticə:

- Fransa və Almaniyada yerləşən iki şirkət hücum nəticəsində ümumilikdə 12 milyon avro itirdi**.**
- Hücum edən şəxslər şirkət rəhbərliyinin adından çıxış edərək çoxlu sayda saxta ödəniş həyata keçirdilər**.**
- Şirkətlər sonradan rəhbərləri ilə təsdiqləmə protokollarını gücləndirdilər və hər hansı böyük maliyyə əməliyyatından əvvəl ikiqat təsdiq tətbiq etməyə başladılar.

Nümunə 3: "İş təklifi" adından fırıldaq (2021)[94]

Hadisə:

2021-ci ildə LinkedIn və digər iş elan platformalarında yeni iş axtaran şəxslərə qarşı pretexting hücumu həyata keçirildi**.** Hücum edən şəxslər nüfuzlu şirkətlərin adından saxta iş təklifləri göndərərək qurbanları aldadırdılar.

Hücum zamanı saxta HR menecerləri qurbanlarla əlaqə saxlayaraq onların CV-lərini və şəxsi məlumatlarını istəyirdilər**.** Daha sonra "işə qəbul prosesi" üçün müəyyən bir sistemə daxil olmağı və orada şəxsi məlumatlarını və bank hesab detallarını daxil etməyi tələb edirdilər**.**

Bəzi hallarda, qurbanlara müəyyən bir proqram yüklətmək tələb olunurdu ki, bu da əslində zərərli proqram idi və qurbanın cihazından məlumatları oğurlayırdı.

[93] www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/business-email-compromise
[94] www.cognyte.com/blog/2021-linkedin-breach-cybercriminals-are-the-new-headhunters/

Nəticə:

- Minlərlə insanın şəxsi məlumatları oğurlandı və kimlik oğurluğu məqsədilə istifadə edildi.
- Bəzi qurbanlar "işə qəbul haqqı" ödənişi adı altında pul itirdilər.
- Hücum LinkedIn və digər platformalar tərəfindən araşdırıldı və onlarla saxta profil silindi.

Pretexting hücumları insanlara etibarlı mənbə kimi təqdim olunan saxta ssenarilər üzərində qurulur. Bu səbəbdən fərdlər və təşkilatlar:

- Hər hansı bir tələbi yerinə yetirmədən əvvəl mənbənin həqiqiliyini yoxlamalıdırlar.
- Rəhbərlikdən və ya IT xidmətlərindən gələn təcili maliyyə və ya təhlükəsizlik tələblərinə ehtiyatla yanaşmalıdırlar.
- İş təklifləri və digər sorğular yalnız rəsmi veb-saytlar və rəsmi kanallar vasitəsilə təsdiqlənməlidir.

Bu hücumlara qarşı hazırlıqlı olmaq təşkilatların və fərdlərin təhlükəsizlik biliklərini artırmaq və yoxlama mexanizmlərini gücləndirmək baxımından həyati əhəmiyyət daşıyır.

3. Baiting

Baiting hücumu qurbanı müəyyən bir hərəkətə yönləndirmək üçün cazibədar və ya maraqlı bir təklif təqdim etməklə manipulyasiya etməyə əsaslanır. Bu texnika hədiyyələr, pulsuz proqramlar, endirimlər və ya maraqlı məlumatlar təqdim etməklə qurbanı aldatmaq üçün istifadə olunur.

Aşağıda baiting hücumu ilə bağlı 3 nümunə təqdim edilir:

Nümunə 1: "Pulsuz USB Flash Disk" hücumu (2010, ABŞ)[95]

Hadisə:

2010-cu ildə ABŞ Müdafiə Nazirliyi (Pentagon) tərəfindən böyük bir kibertəhlükəsizlik insidenti araşdırıldı. Naməlum şəxslər Pentaqonun avtomobil dayanacağında bir neçə USB flash disk yerləşdirdilər. USB-lər üzərində "MÜHÜM FAYLLAR", "GİZLİ HESABAT" və ya "HƏDİYYƏ USB" kimi etiketlər yazılmışdı.

USB-ləri tapan bəzi işçilər USB-ləri kompüterlərinə qoşduqda, virus avtomatik aktivləşərək sistemlərə yoluxdu. Virus Müdafiə Nazirliyinin daxili şəbəkəsinə keçərək həssas məlumatları Hücum edən şəxslərə ötürməyə başladı.

Nəticə:

- Hücum nəticəsində yüzlərlə kompüter zərərli proqramla yoluxdu və kritik sistemlərə kiberhücum baş verdi.
- ABŞ ordusu təcili təhlükəsizlik tədbirləri gördü və xarici cihazların istifadəsini məhdudlaşdırdı.

[95] Worst cyber attack on US military came via flash drive - phys.org/news/2010-08-worst-cyber-military.html

- Sonradan bu hücum təşkilatlarda xarici USB cihazlarının istifadəsinin qadağan olunmasına səbəb oldu.

Nümunə 2: "Pulsuz film və musiqi yükləmə fırıldağı" (2016, qlobal)[96]

Hadisə:

2016-cı ildə milyonlarla internet istifadəçisi "pulsuz film və ya musiqi" yükləmək üçün zərərli saytlara yönləndirildi**.** Hücum edən şəxslər məşhur filmlərin, yeni çıxmış musiqilərin və ya premium proqram təminatının pulsuz versiyalarını təklif edən saytlar yaratdılar.

İstifadəçilər bu saytların təqdim etdiyi "pulsuz yükləmə" linklərinə daxil olduqda**,** sistemlərinə zərərli proqramlar (malware) yükləndi**.** Bəzi hallarda troyan virusları istifadəçilərin şəxsi məlumatlarını oğurladı**,** digərlərində isə fidyə proqramları qurbanların kompüterlərini kilidlədi və ödəniş tələb etdi.

Nəticə:

- Dünya üzrə milyonlarla insan kompüterlərinə virus yüklədi və fərdi məlumatlarını itirdi.
- Hücum nəticəsində bank hesab məlumatları oğurlanan istifadəçilər ciddi maliyyə itkiləri ilə üzləşdi**.**
- Təhlükəsizlik mütəxəssisləri internet istifadəçilərinə yalnız rəsmi mənbələrdən yükləmə etməyi tövsiyə etdilər**.**

Nümunə 3: "Sosial media baiting hücumu - saxta müsabiqələr" (2024, Facebook və Instagram)[97]

Hadisə:

2024-cü ildə Facebook və Instagram platformalarında "hədiyyə kampaniyası" adı altında minlərlə istifadəçi aldatıldı Hücum edən şəxslər böyük brendlərin (Apple, Samsung, Amazon) adından çıxış edərək "iPhone qazanın!", "1000$ hədiyyə kartı" kimi paylaşımlar etdilər.

İstifadəçilər bu müsabiqələrdə iştirak etmək üçün paylaşılan linkə daxil olub şəxsi məlumatlarını yazmalı idilər**,** bank kart məlumatlarını və ya sosial media giriş şifrələrini təqdim etməli idilər, müsabiqəni dostları ilə bölüşərək daha çox insanı tora salmalı idilər**.**

Ancaq müsabiqələr tamamilə saxta idi və məqsəd istifadəçilərin bank və sosial media hesablarını oğurlamaq idi**.**

Nəticə:

- Facebook və Instagram platformalarında 50 mindən çox istifadəçi bank məlumatlarını paylaşdığı üçün maliyyə fırıldaqlarına məruz qaldı.
- Hesabları ələ keçirilən istifadəçilərin sosial media profilləri vasitəsilə başqa insanları aldatmaq üçün istifadə olundu.

[96] Major sites including New York Times and BBC hit by 'ransomware' malvertising - www.theguardian.com/technology/2016/mar/16/major-sites-new-york-times-bbc-ransomware-malvertising

[97] How fraudsters are getting fake articles onto Facebook - Jane Wakefield

- Facebook və Instagram saxta reklam kampaniyalarına nəzarəti artırdı və bu tip hücumların qarşısını almaq üçün yeni filtrlər tətbiq etdi.

Baiting hücumları insanların maraqlarını və ya maddi istəklərini manipulyasiya etməyə əsaslanır. Təhlükədən qorunmaq üçün:

- Şübhəli pulsuz təkliflərə inanmamaq və həqiqiliyini yoxlamaq.
- USB və digər xarici cihazları heç vaxt təsdiqlənməmiş mənbələrdən istifadə etməmək.
- Sosial mediada yayılan "pulsuz hədiyyə kampaniyaları" və "lotereya qazancları" kimi vədlərə qarşı ehtiyatlı olmaq.

Bu hücum növünə qarşı maarifləndirmə və təhlükəsizlik tədbirləri fərdləri və təşkilatları maddi və informasiya itkisinə qarşı qoruyur.

4. Phishing

Phishing hücumu kiberfırıldaqçılar tərəfindən istifadəçiləri saxta e-poçtlar, veb-saytlar və ya mesajlar vasitəsilə manipulyasiya edərək həssas məlumatları açıqlamağa məcbur etmək üçün istifadə edilən ən geniş yayılmış sosial mühəndislik hücumlarından biridir. Bu hücumlar, adətən, bank hesabları, sosial media giriş məlumatları, şəxsi identifikasiya nömrələri və ya şirkət daxili şifrələri ələ keçirmək üçün həyata keçirilir.

Aşağıda phishing hücumu ilə bağlı 3 nümunə təqdim edilir:

Nümunə 1: "Google docs phishing hücumu" (2017, qlobal)[98]

Hadisə:

2017-ci ildə Google istifadəçilərinə göndərilən saxta e-poçtlar milyonlarla insanın hesablarını ələ keçirməyə səbəb oldu. Hücum edən şəxslər istifadəçilərə Google Docs-a dəvət mesajı kimi görünən bir phishing e-poçtu göndərdilər.

E-poçtda, "Bir sənədə baxmaq üçün aşağıdakı linkə klikləyin" deyə yazılmışdı. İstifadəçilər bu linkə daxil olduqda, Google-un orijinal giriş səhifəsinə bənzəyən saxta bir veb-sayta yönləndirilirdi. Bu səhifəyə giriş edənlər öz Google hesablarının giriş məlumatlarını birbaşa hücum edən şəxslərə təqdim etmiş olurdular.

Nəticə:

- Milyonlarla insanın Gmail və Google Drive hesabları təhlükə altına düşdü.
- Google hücumu araşdıraraq saxta tətbiqləri sistemdən sildi və təhlükəsizlik tədbirlərini gücləndirdi.
- Təşkilatlar və fərdi istifadəçilərə phishing e-poçtlarının tanınması və təsdiq edilməmiş linklərə klikləməmək tövsiyə edildi.

[98] Google docs phishing campaign - www.cisa.gov/news-events/alerts/2017/05/04/google-docs-phishing-campaign

Nümunə 2: "Sony pictures hack" (2014, ABŞ)[99]

Hadisə:

2014-cü ildə Sony Pictures şirkətinə qarşı böyük bir phishing hücumu həyata keçirildi. Hakerlər, şirkət əməkdaşlarına saxta e-poçtlar göndərərək onları zərərli linklərə klikləməyə məcbur etdilər.

Bu e-poçtlarda "Şifrənizi yeniləmək üçün aşağıdakı linkə daxil olun" kimi təcili mesajlar yer alırdı. Sony işçilərindən bir neçəsi bu linklərə klikləyərək şəxsi hesab giriş məlumatlarını təcavüzkarlara təqdim etdilər.

Bu məlumatları əldə edən hücum edən şəxslər, Sony Pictures-ın daxili şəbəkəsinə daxil olub, yeni filmlərin və ssenarilərin oğurlanmasına səbəb oldular, milyonlarla işçiyə və müştəriyə aid şəxsi məlumatları ifşa etdilər, təşkilat daxilində fəaliyyətləri məhdudlaşdırdılar və sistemlərə ciddi ziyan vurdular.

Nəticə:

- Sony Pictures 100 milyondan çox dollar itirdi və böyük nüfuz zədəsi aldı.
- Şirkət kibertəhlükəsizlik tədbirlərini gücləndirdi və phishing hücumlarına qarşı işçilərə maarifləndirmə proqramları keçdi.
- Hücum ABŞ və Şimali Koreya arasında kiber təhlükəsizlik böhranına səbəb oldu, çünki hücumu Şimali Koreya dəstəkləyən qrupların həyata keçirdiyi iddia edildi.

Nümunə 3: "PayPal phishing fırıldağı" (2020, qlobal)[100]

Hadisə:

2020-ci ildə milyonlarla PayPal istifadəçisinə phishing hücumları edildi. Hücum edən şəxslər istifadəçilərə PayPal-dan gəldiyi kimi görünən saxta e-poçtlar göndərdilər.

E-poçtda aşağıdakı kimi mesajlar yer alırdı:

"Hesabınız şübhəli fəaliyyət səbəbilə məhdudlaşdırılıb. Girişinizi bərpa etmək üçün aşağıdakı linkə klikləyərək hesabınızı təsdiqləyin."

İstifadəçilər bu linkə kliklədikdə, PayPal-ın rəsmi saytına bənzəyən saxta bir veb-sayta yönləndirilirdilər. Orada PayPal giriş məlumatlarını daxil etdikdə, bu məlumatlar birbaşa hücum edən şəxslərin serverlərinə göndərilirdi.

Nəticə:

- Minlərlə istifadəçinin PayPal hesabları oğurlandı və bank hesablarından pullar çıxarıldı.
- PayPal phishing hücumlarına qarşı istifadəçiləri maarifləndirmək üçün təhlükəsizlik xəbərdarlıqları yaydı.
- E-poçtlarda göndərilən linklərin həqiqiliyini yoxlamaq və yalnız rəsmi PayPal tətbiqindən giriş etmək tövsiyə edildi.

Phishing hücumları milyonlarla insanı aldadaraq bank hesablarını, sosial media profillərini və şirkət şəbəkələrini ələ keçirməyə yönəlmişdir.

Bu hücumlara qarşı müdafiə olunmaq üçün:

---

[99] 2014 Sony Pictures hack - en.wikipedia.org/wiki/2014_Sony_Pictures_hack

[100] PayPal account holders warned about phishing - www.actionfraud.police.uk/alert/paypal-account-holders-warned-about-phishing

- E-poçtlarda göndərilən linkləri diqqətlə yoxlamaq və şübhəli mesajlara klikləməmək.
- Rəsmi qurumların veb-saytlarını birbaşa brauzerə yazaraq daxil olmaq.
- İki faktorlu autentifikasiyadan (2FA) istifadə edərək hesabların təhlükəsizliyini artırmaq.
- Şübhəli e-poçtlar alındıqda, göndərənin həqiqiliyini yoxlamaq üçün rəsmi müştəri xidməti ilə əlaqə saxlamaq.

Bu tədbirlərə riayət etməklə həm fərdi, həm də təşkilati səviyyədə phishing hücumlarının qarşısını almaq mümkündür.

5. Spear phishing

Spear phishing, adi phishing hücumlarından fərqli olaraq fərdi və ya təşkilata qarşı xüsusi hazırlanmış, fərdiləşdirilmiş phishing hücumudur. Hücum edən şəxslər qurban haqqında əvvəlcədən məlumat toplayır və e-poçt, sosial media mesajları və ya digər ünsiyyət vasitələrindən istifadə edərək qurbanı manipulyasiya etməyə çalışırlar.

Aşağıda baş vermiş 3 spear phishing hücumunun nümunəsi təqdim olunur.

Nümunə 1: "John Podesta və ABŞ prezident seçkilərinə müdaxilə" (2016, ABŞ)[101]

Hadisə:

2016-cı ildə ABŞ prezident seçkiləri zamanı Hillary Clinton-un seçki qərargahının rəhbəri John Podesta bir spear phishing hücumunun qurbanı oldu.

Hücum edən şəxslər ona Google təhlükəsizlik komandası adından gələn saxta e-poçt göndərdilər. Mesajda aşağıdakı məzmun yer alırdı:

"Hesabınız sındırılıb! Şifrənizi dərhal yeniləməlisiniz!"

E-poçtda "Şifrəni yenilə" düyməsi var idi. Podesta bu linkə kliklədikdə, Google-un giriş səhifəsinə bənzəyən, lakin əslində rusiyalı hackerlərin idarə etdiyi saxta bir veb-sayta yönləndirildi. O, yeni şifrəni daxil etdikdə, bütün hesab məlumatları birbaşa hücum edən şəxslərə göndərildi.

Bu yolla hücum edən şəxslər John Podesta-nın e-poçt hesabına daxil oldu və seçki kampaniyası ilə bağlı minlərlə məxfi sənədi oğurladılar. Daha sonra bu məlumatlar Wikileaks-də yayımlandı və ABŞ siyasətinə böyük təsir göstərdi.

Nəticə:

- ABŞ Kəşfiyyat Xidməti bu hücumun Rusiya tərəfindən təşkil edildiyini açıqladı.
- ABŞ Prezidenti Donald Trump və Demokratlar arasında siyasi gərginlik yarandı.
- Google təhlükəsizlik sistemlərini gücləndirdi və istifadəçilərə phishing hücumlarına qarşı xəbərdarlıq etdi.

Nümunə 2: "Ubiquiti networks hücumu - 46 milyon dollar oğurluq"

[101] The phishing email that hacked the account of John Podesta - www.cbsnews.com/news/the-phishing-email-that-hacked-the-account-of-john-podesta/

(2015, ABŞ)[102]

Hadisə:

2015-ci ildə Ubiquiti Networks adlı ABŞ texnologiya şirkəti spear phishing hücumunun qurbanı oldu.

Hücum edən şəxslər, şirkət daxilində maliyyə şöbəsi işçilərinə CEO adından saxta e-poçt göndərərək 46 milyon dollar vəsaitin üçüncü şəxsin bank hesabına köçürülməsini tələb etdilər.

E-poçt tamamilə rəsmi bir maliyyə sorğusu kimi görünürdü, hətta şirkətin daxili sənədlərinə uyğun ifadələr və rəhbərlik tərzi istifadə olunmuşdu.

Maliyyə şöbəsində çalışan bir neçə işçi bu e-poçtları real zənn edərək, şirkətin bank hesablarından milyonlarla dollar vəsaiti hücum edən şəxslərin təqdim etdiyi bank hesabına köçürdü. Bu, rəhbərlik tərəfindən aşkarlanana qədər 46 milyon dollar oğurlandı.

Nəticə:

- Ubiquiti Networks şirkəti milyonlarla dollar itirdi və yalnız bir hissəsini geri qaytara bildi.
- Şirkət daxilində phishing hücumlarına qarşı ciddi kibertəhlükəsizlik siyasəti tətbiq edildi.
- CEO Fraud və Business Email Compromise (BEC) hücumlarına qarşı dünya miqyasında böyük xəbərdarlıqlar yayımlandı.

Nümunə 3: "Facebook və Google-dan 100 milyon dollarlıq fırıldaq" (2013-2015, ABŞ)[103]

Hadisə:

2013-2015-ci illərdə hakerlər Google və Facebook-un maliyyə şöbələrinə hədəflənmiş spear phishing hücumları təşkil etdilər.

Hücum edən şəxslər Tayvan əsilli elektronika təchizatçısı Quanta Computer-in adı ilə saxta e-poçtlar göndərdilər. E-poçtlarda, "Şirkətinizə göndərilən avadanlıq üçün ödəniş tələb edirik" yazılmışdı, həqiqi görünən fakturalar və sənədlər əlavə olunmuşdu, ödənişlərin hücum edən şəxslərin bank hesablarına köçürülməsi tələb edilirdi.

Facebook və Google-nin maliyyə şöbələri bu tələbləri real qəbul edərək, ümumilikdə 100 milyon dollarlıq ödənişi hakerlərin hesablarına köçürdü.

Nəticə:

- ABŞ Ədliyyə Nazirliyi hücumun arxasında Litva mənşəli Evaldas Rimasauskas adlı fırıldaqçının dayandığını aşkar etdi.
- 2017-ci ildə Rimasauskas həbs edildi və ABŞ-a ekstradisiya edildi.
- Facebook və Google hüquqi tədbirlər gördü və təhlükəsizlik prosedurlarını gücləndirdi.

[102] Tech firm Ubiquiti Suffers $46M cyberheist - krebsonsecurity.com/2015/08/tech-firm-ubiquiti-suffers-46m-cyberheist/
[103] Facebook and Google were conned out of $100m in phishing scheme - www.theguardian.com/technology/2017/apr/28/facebook-google-conned-100m-phishing-scheme

Spear Phishing hücumları adi phishing hücumlarından daha təhlükəlidir, çünki xüsusi bir şəxsi və ya təşkilatı hədəfə alır və yüksək səviyyəli fərdiləşdirilmiş məlumatlar əsasında həyata keçirilir**.**

Bu hücumlara qarşı qorunmaq üçün:

- Şübhəli e-poçtlardakı linklər və göndərici ünvanları diqqətlə yoxlanmalıdır**.**
- Daxili korporativ ödənişlər üçün həmişə ikiqat təsdiq tələb edilməlidir**.**
- İki faktorlu autentifikasiya (2FA) bütün işçi hesablarında aktiv edilməlidir**.**
- İşçilərə kibertəhlükəsizlik təlimləri keçirilməli və real spear phishing simulyasiyaları təşkil olunmalıdır**.**

Bütün təşkilatlar və fərdi istifadəçilər bu cür hücumlara qarşı ciddi tədbirlər görməzsə, Spear Phishing-in yaratdığı təhlükə daha da böyüyəcəkdir.

6. Tailgating

Tailgating hücumu, icazəsiz şəxsin fiziki təhlükəsizlik nəzarətindən yayınaraq qurbanın ardınca qapalı və məhdud giriş icazəsi olan bir məkana daxil olmasıdır**.** Bu hücum adətən ofislərdə, hökumət binalarında, laboratoriyalarda, hava limanlarında və digər yüksək təhlükəsizlik tələb edən obyektlərdə baş verir**.**

hücum edən şəxslər insan psixologiyasından istifadə edərək, qapını açan şəxsin onların da içəri keçməsinə icazə verəcəyini düşünürlər**.** Onlar bunu aşağıdakı üsullarla həyata keçirə bilərlər**:**

- Qapını saxlatmaq: "Bağışlayın, əlimdə sənədlər var, qapını tuta bilərsinizmi?"
- Rəhbərlik və ya işçi kimi davranmaq: "Mən yeni işçiyəm, kartım hələ verilmir, amma tələsirəm."
- Təcili vəziyyət yaratmaq: "Mən texniki işçiyəm, server otağına dərhal daxil olmalıyam, sistemdə problem var!"

Aşağıda baş vermiş 2 tailgating hücumu və onların nəticələri təqdim edilir.

Nümunə 1: "Google-un təhlükəsizlik testi - baş texniki direktorun (CTO) hücumu"[104]

Hadisə:

Google-un baş texniki direktoru (CTO) Jeff Dean, Tailgating-in nə qədər təhlükəli olduğunu test etmək üçün öz şirkətinin təhlükəsizlik sistemini yoxlamağa qərar verdi**.**

O, şirkət binasına daxil olmaq üçün işçilərdən birinin ardınca keçməyə cəhd etdi. O, "Bağışlayın, kartımı evdə unutmuşam, mən Google-da işləyirəm" deyərək qapını açan işçidən içəri keçmək üçün kömək istədi.

İşçi, onun həqiqətən də Google-da çalışıb-çalışmadığını yoxlamadan qapını saxladı və içəri keçməsinə icazə verdi**.**

Nəticə:

- Google təhlükəsizlik qaydalarını sərtləşdirdi və Tailgating hücumlarının qarşısını almaq üçün xüsusi təlimlər keçirdi**.**

[104] en.wikipedia.org/wiki/Jeff_Dean

- Google-un təhlükəsizlik protokolları gücləndirildi və işçilər bu cür hallara qarşı ciddi şəkildə maarifləndirildi.
- "Google Security Awareness Program" adlı yeni təhlükəsizlik proqramı istifadəyə verildi.

Nümunə 2: "Fransa müdafiə nazirliyində tailgating - casusluq hücumu" (2021, Fransa)

Hadisə:

2021-ci ildə Fransa müdafiə nazirliyinin əsas qərargahına icazəsiz şəkildə daxil olan şəxs, yüksək məxfi sənədlərə çıxış əldə etməyə çalışdı.

Hücum edən şəxslər özünü hökumət əməkdaşı kimi təqdim edərək, real işçilərdən biri ilə binaya daxil olmağa çalışdı. O, işçilərdən birinə yaxınlaşaraq dedi:

"Mən müdafiə nazirliyindənəm, kartımı maşında unutmuşam, zəhmət olmasa qapını saxlaya bilərsinizmi?"

İşçi, təhlükəsizlik prosedurlarını pozaraq hücum edən şəxslər binaya daxil olmasına icazə verdi. Hücum edən şəxslər nazirlik daxilində casusluq fəaliyyəti aparmağa başladı, ancaq təhlükəsizlik kameraları vasitəsilə dərhal müəyyən edilərək həbs edildi.

Nəticə:

- Fransa Müdafiə Nazirliyi bütün işçilər üçün ciddi təhlükəsizlik qaydaları tətbiq etdi.
- Tailgating hücumlarının qarşısını almaq üçün "Yalnız fərdi giriş" qaydası qüvvəyə mindi.
- Bina girişlərində mühafizəçilər üçün əlavə yoxlama və identifikasiya tələbləri tətbiq olundu.

Tailgating ən sadə, lakin ən təhlükəli sosial mühəndislik hücumlarından biridir. Fiziki məkanlara icazəsiz daxil olmaq, həm məxfi məlumatların oğurlanmasına, həm də təşkilatın sistemlərinə kiberhücumların həyata keçirilməsinə səbəb ola bilər.

Yuxarıdakı nümunələr göstərir ki, böyük şirkətlər, hökumət qurumları və maliyyə institutları belə Tailgating hücumlarından sığortalanmayıb. Buna görə həm fərdlər, həm də təşkilatlar ciddi fiziki təhlükəsizlik tədbirləri görməlidirlər.

Unutmayın: Bir qapını açaraq hücum edən şəxslər içəri buraxmaq, bütün təşkilat üçün bərpa olunmaz nəticələrə səbəb ola bilər!

7. Watering hole attack

Watering hole attack - Hücum edən şəxslərin müəyyən bir hədəf qrupu tərəfindən tez-tez istifadə olunan veb-saytlara və ya platformalara zərərli kod yerləşdirməsi üsuludur. Bu hücum xüsusilə dövlət qurumları, böyük şirkətlər və yüksək səviyyəli şəxslər üçün ciddi təhlükə yaradır. Hücum edən şəxslər istifadəçilərin etibar etdiyi və mütəmadi olaraq daxil olduğu veb-saytlara virus və ya zərərli kodlar yerləşdirərək onların sistemlərini ələ keçirməyə çalışırlar.

Bu texnika əsasən APT (advanced persistent threat) hücumları çərçivəsində həyata keçirilir və qurbanlar bəzən heç bir şübhəli aktivlik hiss etmədən yoluxmuş sistemlərdən istifadə etməyə davam edirlər.

Aşağıda baş vermiş 3 watering hole hücumu və onların nəticələri təqdim edilir.

Nümunə 1: "Operation Aurora" - Google və Microsoft-a qarşı kiberhücum (2009-2010)[105]

Hadisə:

2009-2010-cu illərdə Çin hökuməti ilə əlaqələndirilən hücum edən şəxslərin, "Operation Aurora" adlanan bir hücum həyata keçirdi. Hücum Google, Adobe, Microsoft və digər iri texnologiya şirkətlərini hədəf aldı.

Hücum edən şəxslər bu şirkətlərin əməkdaşlarının tez-tez ziyarət etdiyi veb-saytlara (məsələn, tədqiqat və texnologiya forumları) zərərli kod yerləşdirdilər. İşçilər bu saytlara daxil olduqda, onların kompüterlərinə "zero-day" (sıfır-gün) boşluğundan istifadə edən viruslar yükləndi.

Hücumun məqsədi:

- Şirkətlərin məxfi məlumatlarını oğurlamaq
- Google və Microsoft-un məxfi sistemlərinə giriş əldə etmək
- Çin hökumətinə kritik informasiya toplamaq

Nəticə:

- Google, Microsoft və Adobe kimi böyük şirkətlər təhlükəsizlik sistemlərini gücləndirdi.
- Google Çin bazarından çıxaraq fəaliyyətini məhdudlaşdırdı.
- Google, bu hücumların Çin hökuməti tərəfindən təşkil edildiyini iddia etdi.
- Dünyada texnoloji şirkətlər arasında təhlükəsizlik standartları yüksəldildi.

Nümunə 2: "US department of labor attack" - ABŞ hökumət saytına hücum (2013)[106]

Hadisə:

2013-cü ildə naməlum bir haker qrupu ABŞ Əmək Departamentinin (US Department of Labor) rəsmi saytına bir Watering Hole hücumu təşkil etdi. Sayt ziyarət edən istifadəçilər, heç bir xəbərdarlıq olmadan zərərli proqramlarla yoluxurdular.

Hücum edən şəxslər saytın koduna "IE8 Zero-Day Exploit" yerləşdirdilər və bu boşluq vasitəsilə istifadəçilərin kompüterlərinə zərərli proqram yükləndi.

Hədəf qruplar:

- ABŞ dövlət qurumlarının əməkdaşları
- Milli təhlükəsizlik və hərbi sektorun üzvləri
- Tədqiqatçılar və media nümayəndələri

Nəticə:

[105] Google hack attack was ultra sophisticated, new details show - www.wired.com/2010/01/operation-aurora/
[106] U.S. Department of labor website discovered hacked, spreading poisonIvy - Kelly Jackson Higgins

- ABŞ Əmək Departamenti saytı dərhal bağladı və təhlükəsizlik tədbirlərini gücləndirdi.
- Microsoft IE8 brauzerindəki boşluğu təcili olaraq düzəltmək üçün təhlükəsizlik yeniləməsi (patch) buraxdı.
- ABŞ hökuməti bu hücumun xarici dövlətlər tərəfindən həyata keçirildiyini iddia etdi.

Nümunə 3: "CCleaner watering hole attack" - antivirus proqramına hücum (2017)[107]

Hadisə:

2017-ci ildə Piriform şirkətinin məşhur sistem təmizləmə proqramı olan "CCleaner" bir Watering Hole hücumuna məruz qaldı.

Hücum edən şəxslər CCleaner proqramının rəsmi serverinə daxil olaraq, proqramın yeni versiyasına zərərli kod yerləşdirdilər. İstifadəçilər CCleaner proqramını rəsmi saytdan yüklədikdə, sistemlərinə zərərli proqram da yüklənirdi.

Bu hücum vasitəsilə sistemlərə casus proqram (spyware) quraşdırıldı və istifadəçilərin şifrə və digər həssas məlumatları oğurlandı.

Hədəf qruplar:

- Böyük texnologiya şirkətləri və onların əməkdaşları
- İT administratorları və təhlükəsizlik mütəxəssisləri
- CCleaner istifadə edən adi istifadəçilər

Nəticə:

- Cisco Talos kiber təhlükəsizlik qrupu hücumu aşkar etdi və dərhal Piriform şirkətini məlumatlandırdı.
- Piriform yeni təhlükəsizlik yamaları buraxdı və zərərli versiyanı bazardan çıxardı.
- Böyük şirkətlər Watering Hole hücumlarına qarşı əlavə qorunma tədbirləri tətbiq etdilər.

Watering hole attack - hədəflənmiş təşkilatları və fərdi şəxsləri yoluxdurmaq üçün çox güclü bir sosial mühəndislik texnikasıdır. Bu hücumun qurbanı olan şəxslər bəzən heç bir fərqində olmadan öz cihazlarını və korporativ şəbəkələrini yoluxdururlar.

Təhlükəsizlik yeniləmələrini vaxtında yerinə yetirmək, DNS filtrlərindən istifadə etmək və yalnız etibarlı mənbələrdən proqramlar yükləmək Watering Hole hücumlarına qarşı ən effektiv müdafiə üsullarındandır!

8. Honey trap

Honey Trap - sosial mühəndislik hücumlarının ən qədim, lakin ən təsirli üsullarından biridir. Bu texnika əsasən hədəfin emosional zəifliyindən istifadə edərək onu manipulyasiya etmək və məxfi məlumatları əldə etmək məqsədi daşıyır.

[107] CCleaner APT attack: a technical look inside - Priyanka Aash

Bu üsul romantik əlaqələr, dostluq və ya şəxsi inam yaradan digər münasibətlər üzərindən qurulur. Hücum edən şəxslər özünü cazibədar və etibarlı şəxs kimi təqdim edərək hədəfi informasiya paylaşmağa təşviq edir. Hədəf şəxs hiss etmədən dövlət sirrləri, korporativ məlumatlar və ya şəxsi bilgiləri paylaşa bilər.

Aşağıda baş vermiş 3 məşhur honey trap hücumu və onların nəticələri təqdim edilir.

Nümunə 1: "Mata Hari" - tarixin ən məşhur honey trap casusu[108]

Hadisə:

Mata Hari (1876-1917), Hollandiyalı rəqqasə və casus idi. O, I Dünya Müharibəsi zamanı Almaniya və Fransa arasında casusluq fəaliyyəti ilə məşğul olmuşdur.

Mata Hari Fransa, Almaniya və digər ölkələrin yüksək rütbəli zabitləri ilə romantik əlaqələr quraraq onlardan hərbi və siyasi məlumatlar topladı. O, bu şəxsləri öz gözəlliyi və cazibəsi ilə manipulyasiya edərək məxfi sənədləri əldə etməyə müvəffəq oldu.

Fransa təhlükəsizlik qüvvələri onun Almaniya üçün casusluq etdiyini aşkar etdikdən sonra onu həbs etdi və 1917-ci ildə edam etdi.

Nəticə:

- Mata Hari'nin fəaliyyəti nəticəsində bir çox məxfi məlumat düşmən əllərinə keçdi.
- Fransa hökuməti onun Almaniya üçün işlədiyini təsdiqlədikdən sonra onu edam etdi.
- Tarixdə Honey Trap üsulu ilə casusluğun ən məşhur nümunəsi kimi qaldı.

Nümunə 2: "Anna Chapman" - Rusiya kəşfiyyat agentinin honey trap əməliyyatı (2010)[109]

Hadisə:

Anna Chapman, Rusiya Federal Təhlükəsizlik Xidmətinin (FSB) agenti olaraq ABŞ-da casusluq fəaliyyəti ilə məşğul olub. O, Amerika siyasi dairələrində nüfuz qazanaraq ABŞ-ın məxfi məlumatlarını toplamağa çalışırdı.

Chapman bir neçə yüksək vəzifəli iş adamı və siyasətçi ilə tanış olaraq onları casus şəbəkəsinə məlumat ötürməyə təşviq edib. O, şəxsi cazibəsindən və xarizmatik davranışlarından istifadə edərək, insanları özünə güvənməyə məcbur edib və onlardan məxfi məlumatları əldə edib.

2010-cu ildə ABŞ Federal Təhqiqat Bürosu (FBI) "İlan Şəbəkəsi" (Operation Ghost Stories) adlı əməliyyat nəticəsində Anna Chapman və onun 9 casus yoldaşını həbs etdi.

Nəticə:

- Rusiya ilə ABŞ arasında casus böhranı yaşandı və Anna Chapman Rusiyaya deportasiya edildi.
- O, sonradan Rusiya televiziyasında və mediada məşhur simaya çevrildi.

[108] en.wikipedia.org/wiki/Mata_Hari

[109] Laptop from operation Ghost Stories - www.fbi.gov/history/artifacts/laptop-from-operation-ghost-storieswww.fbi.gov/history/artifacts/laptop-from-operation-ghost-stories

- Bu hadisə ABŞ kəşfiyyat sistemində Honey Trap hücumlarına qarşı ciddi tədbirlər görülməsinə səbəb oldu.

Nümunə 3: "Love Scam" - LinkedIn üzərindən honey trap hücumu (2018)[110]

Hadisə:

2018-ci ildə Çin kəşfiyyat xidmətləri LinkedIn platformasından istifadə edərək ABŞ və Avropadakı siyasi və hərbi şəxsləri hədəf aldı.

Hücum edən şəxslər özlərini cazibədar və nüfuzlu iş adamları, jurnalistlər və siyasətçilər kimi təqdim edərək hədəflərlə əlaqə qurdu. Onlar LinkedIn üzərindən romantik münasibət qurmağa və etibar qazanmağa çalışdılar.

Bu hücumda hədəflər əsasən ABŞ və Avropa hökumətində çalışan məmurlar və müdafiə sektorunda çalışan mütəxəssislər idi.

Nəticə:

- ABŞ kəşfiyyat xidməti bu hücumların Çinin dövlət dəstəyi ilə həyata keçirildiyini açıqladı.
- LinkedIn təhlükəsizlik siyasətlərini gücləndirdi və Honey Trap hücumlarına qarşı yeni müdafiə mexanizmləri yaratdı.
- Avropa və ABŞ hökumətləri rəsmiləri öz şəxsi məlumatlarını sosial şəbəkələrdə paylaşmamaq üçün daha sərt tədbirlər gördü.

Honey trap hücumları, əsasən yüksək vəzifəli şəxslərə, dövlət işçilərinə və hərbi sektor nümayəndələrinə qarşı istifadə olunur. Bu hücumlar emosional zəifliklərdən istifadə edərək hədəfi manipulyasiya etməyə və məxfi məlumatları əldə etməyə yönəlmişdir.

Təhlükəsizlik tədbirlərinin gücləndirilməsi və fərdi diqqətlilik, bu cür hücumların qarşısını almağın əsas yollarındandır. Şəxsi və iş həyatında emosional manipulyasiya riskini minimuma endirmək üçün honey trap texnikalarını tanımaq və onlara qarşı müvafiq müdafiə tədbirləri görmək vacibdir.

9. Scareware

Scareware - istifadəçiləri aldatmaq, panikaya salmaq və onları təhlükəsiz olmayan proqramları yükləməyə və ya şəxsi məlumatlarını açıqlamağa məcbur etmək üçün istifadə olunan bir sosial mühəndislik hücumudur. Adətən saxta antiviruslar, saxta sistem problemləri və ya təhlükəsizlik xəbərdarlıqları ilə təqdim olunur.

Hücum edən şəxslər qurbanları təhlükə altında olduqlarına inandıraraq onları fırıldaqçı proqramlar yükləməyə və ya şəxsi məlumatlarını paylaşmağa məcbur edirlər. Scareware hücumları maliyyə fırıldaqları, zərərli proqramların yayılması və şəxsi məlumatların oğurlanması üçün istifadə olunur.

Aşağıda 3 məşhur Scareware hücumu və onların nəticələri təqdim edilir.

Nümunə 1: "Fake antivirus" hücumu (2010)[111]

[110] Beware the China honey traps of LinkedIn - Alistair Nicholas

[111] The rise of fake anti-virus - security.googleblog.com/2010/04/rise-of-fake-anti-virus.html

Hadisə:

2010-cu ildə FakeAV (Fake Antivirus) adlı Scareware kampaniyası milyonlarla insanı aldadaraq saxta antivirus proqramları yükləməyə məcbur etdi**.** Hücum saxta "Microsoft Security Essentials" və "McAfee Antivirus" yeniləmələri kimi təqdim edilirdi**.**

Bu hücumda istifadəçilərin kompüterlərinə saxta təhlükəsizlik xəbərdarlığı göndərilir və bildirilirdi ki, onların cihazı virusa yoluxub. Bildirişdə təhlükəni aradan qaldırmaq üçün xüsusi bir proqram yükləmək lazım olduğu qeyd edilirdi**.**

Lakin bu proqram əslində istifadəçilərin kompüterlərini infeksiyaya məruz qoyurdu, bütün şəxsi məlumatları oğurlayırdı, zərərli proqramın silinməsi üçün qurbanlardan pul tələb edilirdi.

Microsoft bu hücum barədə xəbərdarlıq yaydı və FakeAV hücumlarına qarşı yeni təhlükəsizlik tədbirləri tətbiq etdi.

Nəticə:

- Milyonlarla insan bu hücuma məruz qaldı və kredit kartı məlumatları oğurlandı.
- Hücum edən şəxslər təxminən 100 milyon dollar qazandı.
- ABŞ və Avropa İttifaqı hüquq-mühafizə orqanları FakeAV şəbəkəsinə qarşı əməliyyatlar keçirdi və bir neçə fırıldaqçını həbs etdi.

Nümunə 2: "Tech support scam" - saxta texniki dəstək hücumu (2016)[112]

Hadisə:

2016-cı ildə ABŞ-da geniş yayılan bir scareware hücumu zamanı fırıldaqçılar özlərini Microsoft, Apple və ya Google texniki dəstək xidməti kimi təqdim edərək minlərlə insanı aldatdı**.**

Hücum necə işləyirdi?

- İstifadəçilər internetdə gəzişərkən qəfil bir pop-up mesajı ilə qarşılaşırdılar.
- Mesajda "Kompüteriniz təhlükə altındadır! Dərhal texniki dəstəyə zəng edin: +1-800-XXX-XXXX" kimi bir xəbərdarlıq göstərilirdi.
- Qurban texniki dəstək nömrəsinə zəng etdikdə, saxta "dəstək mütəxəssisləri" ondan uzaqdan qoşulmaq üçün icazə istəyirdi.
- Fırıldaqçılar qurbanın kompüterinə daxil olaraq şəxsi məlumatlarını oğurlayır və ya "problemi həll etmək üçün" pul tələb edirdilər.

Bu texnika xüsusilə yaşlı insanları hədəf alırdı, çünki onların texnoloji bilikləri az olduğuna görə fırıldaqçılara daha tez inanırdılar**.**

ABŞ Federal Ticarət Komissiyası (FTC) bu fırıldaqçılığı aşkar etdi və 2018-ci ildə bəzi fırıldaqçılar həbs edildi.

Nəticə:

- Hücum nəticəsində ABŞ və Avropada 50 milyon dollardan çox itki baş verdi**.**
- Microsoft və Apple bu cür saxta texniki dəstək fırıldaqlarına qarşı xüsusi xəbərdarlıqlar yayımladı**.**

[112] FTC and florida charge tech support operation with tricking consumers into paying millions for bogus services - www.ftc.gov/news-events/news/press-releases/2016/07/ftc-florida-charge-tech-support-operation-tricking-consumers-paying-millions-bogus-services

- Bir neçə hindistanlı fırıldaqçı ABŞ hüquq-mühafizə orqanları tərəfindən həbs edildi.

Nümunə 3: "COVID-19 scareware" hücumu (2020)[113]

Hadisə:

2020-ci ildə koronavirus pandemiyası zamanı scareware hücumları kəskin şəkildə artdı. Hücum edən şəxslər insanların pandemiya ilə bağlı qorxularından istifadə edərək onları saxta proqramlar və məlumatlarla manipulyasiya etdilər.

Hücumun mexanizmi:

- Saxta COVID-19 xəritələri təqdim edən veb saytlar yaradıldı.
- İnsanlar bu saytlara daxil olduqda, onların kompüterlərinə zərərli proqramlar yüklənirdi.
- Bu zərərli proqramlar istifadəçilərin şəxsi və bank məlumatlarını oğurlayırdı.
- Bəzi scareware hücumlarında, saxta "COVID-19 Test Sonucu" e-poçtları göndərilərək insanlardan pullu testlər almaq tələb olunurdu.

Dünya Səhiyyə Təşkilatı (WHO) və FBI bu scareware hücumları barədə xəbərdarlıq etdi və istifadəçilərə yalnız rəsmi mənbələrdən məlumat əldə etməyi tövsiyə etdi.

Nəticə:

- Minlərlə insan şəxsi məlumatlarını və pullarını itirdi.
- WHO və FBI scareware hücumlarına qarşı tədbirlər gördü və bir neçə fırıldaqçını həbs etdi.
- Google və Microsoft COVID-19 scareware hücumlarını bloklamaq üçün yeni təhlükəsizlik mexanizmləri tətbiq etdi.

Scareware hücumları qurbanların qorxu və təşviş hisslərindən istifadə edərək onları manipulyasiya etməyə yönəlib. Bu hücumlar milyonlarla insanın şəxsi məlumatlarının oğurlanmasına və maliyyə fırıldaqlarına səbəb olub.

Təhlükəsizlik biliklərinin artırılması və doğru tədbirlərin görülməsi, scareware hücumlarının qarşısını almaq üçün vacibdir.

10. Dumpster diving

Dumpster diving, Hücum edən şəxslər atılmış sənədlər, qovluqlar, elektron cihazlar və digər fiziki materiallar üzərindən həssas məlumatları əldə etməyə çalışdığı bir sosial mühəndislik texnikasıdır. Bu texnika təkcə kağız üzərindəki məlumatlarla məhdudlaşmır, köhnə kompüterlər, sərt disklər, USB-lər və ya mobil telefonlarda saxlanılan məlumatlar da hücum edən şəxslər üçün dəyərli resurs ola bilər.

Hücum edən şəxslər təşkilatların və fərdlərin təhlükəsizliyə laqeyd yanaşmasından istifadə edərək, məxfi sənədlərin və elektron avadanlıqların düzgün şəkildə məhv edilməməsindən yararlanırlar. Dumpster diving vasitəsilə hücum edən şəxslər korporativ və fərdi məlumatları əldə edərək, daha genişmiqyaslı sosial mühəndislik hücumları həyata keçirə bilirlər.

[113] The Covid-19 hoax scareware - www.sonicwall.com/blog/the-covid-19-hoax-scareware

Aşağıda bir məşhur dumpster diving hücumu və onun nəticələri təqdim edilir.

Nümunə 1: "Amerikan Ekspress fırıldağı" (2007)[114]

Hadisə:

2007-ci ildə ABŞ-da bir fırıldaqçı qrup Amerikan Express (AmEx) şirkətinin atılmış sənədləri arasında bank müştərilərinə aid məxfi məlumatları əldə edərək genişmiqyaslı fırıldaqçılıq həyata keçirdi**.**

Hücum edən şəxslər şirkətin ofisinin yaxınlığında yerləşən zibil konteynerlərini araşdıraraq, orada bank kart nömrələri, müştəri müraciətləri və şəxsi məlumatları ehtiva edən sənədlər tapdılar**.** Bu məlumatlardan istifadə edərək saxta kredit kartları yaradan fırıldaqçılar, yüzlərlə insanın bank hesablarından pul çıxardılar və onlayn alış-verişlər etdilər**.**

Bu hadisədən sonra Amerikan Express təhlükəsizlik tədbirlərini gücləndirdi və bütün məxfi sənədlərin məhv edilməsini məcburi etdi**.**

Nəticə:

- Yüzlərlə müştərinin bank hesabları və şəxsi məlumatları oğurlandı.
- Fırıldaqçılar 1 milyon dollardan çox maliyyə ziyanına səbəb oldular.
- Şirkət məxfi sənədlərin təhlükəsiz şəkildə məhv edilməsini tələb edən yeni qaydalar tətbiq etdi.

Dumpster diving, sosial mühəndislik hücumlarının ən sadə, lakin ən təhlükəli formalarından biridir. Hücum edən şəxslərin həssas məlumatları əldə etməsi üçün yüksək texnoloji vasitələrə ehtiyacı yoxdur - sadəcə təşkilatların və fərdlərin sənədləri və elektron cihazları düzgün məhv etməməsi yetərlidir**.**

Şirkətlər və fərdi istifadəçilər bu cür hücumlara qarşı tədbir görməsə, məxfi məlumatların oğurlanması, maliyyə fırıldaqları və şəxsi məlumatların ifşası riski qaçılmaz olacaqdır.

11. Social media hijacking

Social Media Hijacking, hücum edən şəxslərin şəxsi və ya korporativ sosial media hesablarını ələ keçirərək məlumat oğurlaması, fırıldaqçılıq etməsi və ya reputasiya zədələyən paylaşımlar etməsi deməkdir. Bu hücumlar adətən zəif şifrələr, phishing hücumları, malware-infeksiyalar və ya açıq Wi-Fi şəbəkələrindən istifadə etməklə həyata keçirilir**.**

Bu cür hücumlar təkcə fərdi şəxslər üçün deyil, şirkətlər və dövlət qurumları üçün də ciddi təhlükə yaradır**.** Korporativ hesabların ələ keçirilməsi brendlərin nüfuzuna, maliyyə itkilərinə və hətta hüquqi problemlərə səbəb ola bilər**.**

Aşağıda baş vermiş üç məşhur sosial media hijacking hadisəsi, onların törədilməsi üsulları və nəticələri qeyd olunmuşdur.

[114] Recogniza the warning signs - www.americanexpress.com/us/security-center/phishing-scam-awareness/

Nümunə 1: "Associated press Twitter hücumu" (2013)[115]

Hadisə:

2013-cü ildə Associated Press (AP) xəbər agentliyinin Twitter hesabı hücum edən şəxslərin tərəfindən ələ keçirildi və səhv məlumat paylaşmaq üçün istifadə olundu.

Hücum edən şəxslərin hesabdan "Ağ Evdə partlayış oldu, prezident Obama yaralandı" mesajını paylaşdılar. Bu yalan xəbər ABŞ fond bazarında panikaya səbəb oldu və səhmlər 130 milyard dollar dəyər itirdi.

Məsələ araşdırıldıqdan sonra məlum oldu ki, hücum edən şəxslərin AP-nin jurnalistlərindən birini phishing hücumu ilə aldadaraq Twitter giriş məlumatlarını oğurlamışdılar.

Nəticə:

- Fond bazarında 130 milyard dollarlıq itki baş verdi.
- Twitter və digər sosial media platformaları iki faktorlu autentifikasiyanı (2FA) məcburi tətbiq etməyə başladılar.
- Jurnalistlər və media qurumları phishing hücumlarına qarşı daha ciddi təhlükəsizlik tədbirləri görməyə başladılar.

Nümunə 2: "Facebook-un CEO-su Mark Zukerberqin hesabının hack edilməsi" (2016)[116]

Hadisə:

2016-cı ildə Mark Zukerberqin Twitter, LinkedIn və Pinterest hesabları bir qrup haker tərəfindən ələ keçirildi. Hücum edən şəxslərin "OurMine" adlı qrup olduqlarını elan edərək Zukerberqin hesablarından mesajlar paylaşdılar.

Bu hücumun səbəbi LinkedIn-in 2012-ci ildə sızan istifadəçi məlumatları bazasında Mark Zukerberqin şifrəsinin ("dadada") yer alması idi. Çünki Zukerberq bütün sosial media hesablarında eyni şifrəni istifadə edirdi.

Nəticə:

- Zukerberqin sosial media təhlükəsizlik vərdişlərinin zəif olduğu üzə çıxdı.
- Şifrələrin bir neçə platformada eyni istifadə edilməsinin təhlükəli olduğu sübut olundu.
- Daha güclü şifrə siyasətləri və iki faktorlu autentifikasiya tətbiq edilməyə başlandı.

Nümunə 3: "Burger King twitter hesabının ələ keçirilməsi" (2013)[117]

Hadisə:

2013-cü ildə Burger King-in rəsmi Twitter hesabı hakerlər tərəfindən ələ keçirildi və hesab McDonald's brendinə aid kimi dəyişdirildi.

---

[115] Hackers compromise AP Twitter account - apnews.com/general-news-68a43f18c9aa4a87bfbf350a566404c9

[116] Mark Zuckerberg hacked on Twitter and Pinterest - www.theguardian.com/technology/2016/jun/06/mark-zuckerberg-hacked-on-twitter-and-pinterest

[117] Burger King Twitter account hacked to look like McDonald's - abcnews.go.com/blogs/technology/2013/02/burger-king-twitter-account-hacked-to-look-like-mcdonalds

Hücum edən şəxslərin Burger King-in profil şəklini, bioqrafiyasını və adını McDonald's-a uyğun şəkildə dəyişdilər və müxtəlif absurd və təhqiredici paylaşımlar etdilər**.**

Bu hadisədən sonra Twitter təhlükəsizlik tədbirlərini gücləndirdi və korporativ hesablar üçün daha sərt autentifikasiya qaydaları tətbiq etməyə başladı**.**

Nəticə:

- Burger King-in brend imicinə ciddi zərbə dəydi.
- Şirkət rəsmi açıqlama verməyə və yeni təhlükəsizlik tədbirləri görməyə məcbur oldu.
- Daha çox şirkət sosial media hesablarını qorumaq üçün güclü autentifikasiya metodları tətbiq etməyə başladı.

Sosial media hijacking, hücumları fərdi və korporativ təhlükəsizlik üçün ciddi risk yaradır**.** Şəxsi və şirkət hesablarının ələ keçirilməsi reputasiya itkilərinə, maliyyə fırıldaqlarına və şəxsi məlumatların oğurlanmasına səbəb ola bilər**.**

Bu tip hücumların qarşısını almaq üçün güclü şifrələr, iki faktorlu autentifikasiya və müntəzəm təhlükəsizlik yoxlamaları mütləq tətbiq olunmalıdır.

Nəticə

Sosial mühəndislik hücumları müasir kibertəhlükəsizlik üçün ən ciddi və mürəkkəb problemlərdən biridir. Hücum edən şəxslərin texnoloji zəifliklərdən daha çox insan psixologiyasından istifadə edərək fərdi şəxsləri və təşkilatları manipulyasiya edir, onların təhlükəsizlik sistemlərini aşaraq kritik məlumatlara çıxış əldə edirlər. Hədəflərin inamından, emosional zəifliklərindən və diqqətsizliklərindən istifadə edən sosial mühəndislər, bu üsulu müxtəlif formalarda tətbiq edərək maliyyə fırıldaqları, dövlət sirrlərinin ifşası, korporativ casusluq və hətta seçki müdaxiləsi kimi genişmiqyaslı hücumlar həyata keçirə bilirlər.

Bu hücumların sürətlə inkişaf etməsi və daha mürəkkəb formalar alması, fərdlərin və qurumların təhlükəsizlik tədbirlərini gücləndirməsini, daha mühafizəkar yanaşmalar tətbiq etməsini və daim yenilənən kibertəhlükəsizlik strategiyaları yaratmasını zəruri edir. Dövlətlər, böyük şirkətlər, banklar və hətta fərdi şəxslər bu hücumların qurbanına çevrilə bilər və nəticədə ciddi maliyyə itkiləri, reputasiya zədələnməsi və kritik məlumat sızmaları baş verə bilər. Xüsusilə böyük korporasiyalar və dövlət strukturlarında belə hücumların təsiri təkcə təşkilat üçün deyil, bütöv bir iqtisadiyyat və ictimai təhlükəsizlik üçün də fəlakətli ola bilər.

Bu mühazirədə fərdi və təşkilati səviyyədə baş verən sosial mühəndislik hücumlarına və onların müxtəlif formalarına – phishing, spear phishing, tailgating, dumpster diving, quid pro quo, watering hole attack, honey trap, scareware, social media hijacking və reverse social engineering kimi texnikalara və onların real həyatda törətdiyi fəsadlara geniş şəkildə toxunduq.

§ 8. Sosial mühəndislikdə hüquqi və etik məsələlər

Giriş

Sosial mühəndislik hücumlarının getdikcə inkişaf etməsi və müxtəlif formalarda tətbiq olunması onların hüquqi və etik aspektlərini də gündəmə gətirmişdir. Müasir dövrdə hüquq sistemləri yalnız texniki kibercinayətləri deyil, həm də insanlara qarşı psixoloji manipulyasiya yolu ilə həyata keçirilən kiberhücumları da tənzimləməyə çalışır. Hüquq sistemləri bu tip hücumları kibercinayətkarlıq, dələduzluq, məxfiliyin pozulması və şəxsiyyət oğurluğu kimi qiymətləndirir və onların qarşısını almaq üçün müxtəlif beynəlxalq və yerli qanunvericilik aktları mövcuddur. Bununla yanaşı, bəzi hallarda sosial mühəndislik cinayətkarlıqla mübarizə aparmaq üçün də istifadə edilir ki, bu da etik və hüquqi baxımdan müəyyən sərhədlərin müəyyən olunmasını zəruri edir.

Sosial mühəndislik hücumları fərdi şəxslərin və təşkilatların təhlükəsizliyini təhdid etməklə yanaşı, insan hüquqları və məxfilik kimi fundamental prinsiplərə də ciddi təsir göstərir. Qlobal miqyasda, Avropa İttifaqının Ümumi Məlumatların Qorunması Qaydası (GDPR), ABŞ-ın Kompüter Fırıldaqçılığı və Sui-istifadə Qanunu (CFAA) və digər beynəlxalq qanunlar sosial mühəndislik yolu ilə həyata keçirilən kibercinayətlərin qarşısının alınmasına yönəlmişdir. Bu qanunlar kibertəhlükəsizlik pozuntularının qarşısını almaq və şəxsi məlumatların qorunmasını təmin etmək məqsədini güdür. Lakin bəzi hallarda bu qanunlar hücum edən şəxslər**in** innovativ və texnoloji cəhətdən inkişaf etmiş metodları ilə ayaqlaşmaqda çətinlik çəkir.

Eyni zamanda, sosial mühəndislik təkcə cinayətkar məqsədlərlə deyil, həm də etik hakerlik, kibertəhlükəsizlik sahəsində təlimlər və hüquq-mühafizə fəaliyyəti üçün istifadə edilə bilər. Etik hakerlər və təhlükəsizlik mütəxəssisləri təşkilatların və şəxslərin məlumatlarını qorumaq üçün sosial mühəndislik üsullarını öyrənir və təhlükəsizlik zəifliklərini müəyyənləşdirirlər. Burada əsas məsələ sosial mühəndisliyin qanuni və etik sərhədlərinin aydın şəkildə müəyyənləşdirilməsidir. Məsələn, bir təşkilatın təhlükəsizliyini yoxlamaq məqsədilə etik hakerlər tərəfindən aparılan testlər qanuni və icazəli olduğu halda, eyni metodlardan kibercinayətkarlar tərəfindən istifadə edilməsi qanunsuz hesab edilir.

Bu mühazirədə sosial mühəndisliklə bağlı beynəlxalq və yerli hüquqi çərçivələr, etik prinsiplər, bu sahədə qəbul edilmiş qanunvericilik aktları, hüquq pozuntuları üzrə real dünya nümunələri, həmçinin hüquq-mühafizə orqanlarının sosial mühəndislik metodlarından istifadəsi geniş şəkildə araşdırılacaqdır. Beləliklə, bu mövzu sosial mühəndislik hücumlarının yalnız kibercinayətkarlıqla əlaqəli olmadığını, eyni zamanda etik və qanuni kontekstlərdə də müzakirə olunmalı olduğunu ortaya qoyur. Müasir dövrdə təşkilatlar, fərdi şəxslər və dövlətlər sosial mühəndislik hücumlarından qorunmaq üçün təkcə texniki tədbirlər deyil, həm də hüquqi və etik aspektləri nəzərə almalı və uyğun siyasətlər formalaşdırmalıdırlar.

Sosial mühəndisliyin hüquqi tənzimlənməsi

Sosial mühəndislik hücumları müxtəlif növ hüquq pozuntularına səbəb ola bilər. Bu pozuntuların əhatə dairəsi kiberdələduzluq, şəxsi məlumatların oğurlanması, kompüter sistemlərinə icazəsiz giriş, şəxsiyyət oğurluğu, maliyyə dələduzluğu, sosial media hesablarının qanunsuz ələ keçirilməsi və korporativ casusluq kimi geniş mövzuları əhatə edir. Hücum edən şəxslər təkcə şəxsləri deyil, həm də böyük təşkilatları və dövlət qurumlarını hədəfə almaqla mühüm məlumatları ələ keçirmək və onları müxtəlif məqsədlər üçün istifadə etmək niyyətində olurlar.

Bu hücumlar nəticəsində şəxslər, dövlət qurumları və özəl şirkətlər ciddi təhlükələrlə üzləşir. Kiberdələduzluq və şəxsiyyət oğurluğu vasitəsilə Hücum edən şəxslər qurbanların adından bank əməliyyatları həyata keçirə, saxta sənədlər yarada və maliyyə vəsaitlərinə çıxış əldə edə bilərlər. Kompüter sistemlərinə icazəsiz giriş və korporativ casusluq isə təkcə şəxslərə deyil, iri şirkətlərə və dövlət qurumlarına qarşı yönəldilərək məxfi məlumatların sızmasına və iqtisadi itkilərə səbəb ola bilər. Belə hallarda təşkilatlar reputasiya itkiləri ilə yanaşı, maddi zərərlərlə də üzləşirlər.

Bundan əlavə, sosial mühəndislik hücumları müxtəlif sahələrdə hüquqi məsuliyyətin yaranmasına səbəb olur. Məsələn, şəxsi məlumatların qanunsuz əldə edilməsi və yayılması, Ümumi Məlumatların Qorunması Qaydalarına (GDPR) və beynəlxalq kiber hüquq normalarına zidd hesab olunur. ABŞ-da Computer Fraud and Abuse Act (CFAA), Avropada isə ePrivacy Directive və digər qanunlar sosial mühəndislik yolu ilə həyata keçirilən kibercinayətlərin qarşısını almağa çalışır. Bəzi ölkələrdə sosial mühəndislik texnikalarından istifadə edərək cinayət törədən şəxslər maddi cərimələr, həbs və ya digər növ cəzalarla cəzalandırıla bilər.

Bu hüquq pozuntularının qarşısını almaq üçün daha sərt qanunvericilik, gücləndirilmiş kiber təhlükəsizlik protokolları və şəxslərin məlumatlılıq səviyyəsinin artırılması vacibdir. Dövlətlər və beynəlxalq təşkilatlar bu cür hücumların təsirini azaltmaq üçün müxtəlif tədbirlər görməkdədirlər. Bu tədbirlərə hüquq-mühafizə orqanlarının əməkdaşlığı, məlumat təhlükəsizliyi üzrə qanunvericiliyin gücləndirilməsi və fərdi maarifləndirmə proqramlarının tətbiqi daxildir. Interpol və Europol kimi beynəlxalq təşkilatlar bu cür cinayətlərin qarşısının alınması üçün qlobal miqyasda tədqiqatlar aparır və dövlətlər arasında əməkdaşlığı gücləndirirlər.

Bundan əlavə, təşkilatlar sosial mühəndislik hücumlarına qarşı ISO/IEC 27001 kimi beynəlxalq informasiya təhlükəsizliyi standartlarına uyğun olaraq təhlükəsizlik sistemlərini inkişaf etdirməli və işçiləri üçün müntəzəm maarifləndirmə proqramları təşkil etməlidirlər. Əgər təşkilatlar və şəxslər hüquqi və texnoloji müdafiə tədbirlərini gücləndirməsələr, kibercinayətkarların fəaliyyəti genişlənəcəkdir. Hüquqi çərçivələrin müasir dövrün tələblərinə uyğun inkişaf etdirilməsi sosial mühəndislik hücumlarının qarşısını almaqda vacib addımlardan biridir. Eyni zamanda, milli və beynəlxalq əməkdaşlığın gücləndirilməsi, kibercinayətkarlığa qarşı kollektiv müdafiə mexanizmlərinin yaradılması və qabaqcıl texnologiyaların hüquq-mühafizə orqanları tərəfindən aktiv istifadəsi bu sahədə uğurlu nəticələr əldə etməyə imkan verəcəkdir.

Beynəlxalq hüquqi çərçivə

Sosial mühəndislik hücumları qlobal bir təhlükə olaraq, şəxslərə, dövlət qurumlarına və özəl sektora ciddi zərər vura biləcək kiberhücumların əsasını təşkil edir. Bu səbəbdən, beynəlxalq hüquq sistemi bu hücumlarla mübarizə aparmaq üçün müxtəlif konvensiyalar, qanunlar və direktivlər qəbul etmişdir.

Beynəlxalq hüquqi çərçivə sosial mühəndislik yolu ilə həyata keçirilən kibercinayətlərə qarşı qlobal əməkdaşlığı gücləndirir və dövlətlərə hüquqi mexanizmlər təqdim edir. Bu çərçivələr kibertəhlükəsizlik sahəsində məlumat mübadiləsini artırmaq, hüquq-mühafizə orqanlarının fəaliyyətini əlaqələndirmək və cinayətkarların məsuliyyətə cəlb edilməsini asanlaşdırmaq məqsədi daşıyır.

Azərbaycan da bu sahədə beynəlxalq qanunvericilik aktlarını nəzərə alaraq milli hüquq sistemini təkmilləşdirmiş və bir sıra beynəlxalq sazişləri ratifikasiya etmişdir.

Budapeşt Konvensiyası[118] - Kibercinayətkarlığa qarşı ilk beynəlxalq müqavilə (rəsmi adı: "Kibercinayət Konvensiyası") Avropa Şurası tərəfindən qəbul edilən və kibercinayətkarlıqla mübarizəyə yönəlmiş ilk beynəlxalq müqavilədir. Bu konvensiya sosial mühəndislik hücumlarını da əhatə edən aşağıdakı cinayət növlərini tənzimləyir:

- Kompüter verilənləri və sistemlərinin məxfiliyi, tamlığı və istifadə imkanlarına qarşı cinayətlər
- Kompüter vasitələrindən istifadə ilə bağlı cinayətlər
- Məlumatların məzmunu ilə bağlı cinayətlər
- Müəllif hüquqlarının və əlaqəli hüquqların pozulması ilə bağlı cinayətlər

Azərbaycan 2009-cu ildə Budapeşt Konvensiyasını ratifikasiya etmişdir və buna əsasən, ölkədə kibercinayətkarlıqla mübarizədə bu konvensiyanın tələblərinə uyğun hüquqi tədbirlər görülür[119].

Ümumdünya insan hüquqları bəyannaməsi[120] - BMT-nin qəbul etdiyi bəyannamənin 12-ci maddəsinə əsasən, “heç kimin şəxsi və ailə həyatına özbaşınalıqla müdaxilə, evinin toxunulmazlığına, gizli məktublaşmalarına, şərəf və nüfuzuna özbaşınalıqla qəsd edilə bilməz. Hər bir insan bu cür müdaxilələrdən və ya belə qəsdlərdən qanunla müdafiə olunmaq hüququna malikdir”. Bu prinsip sosial mühəndislik hücumlarına qarşı mübarizənin hüquqi əsaslarından biridir. Xüsusilə, bu bəyannamə şəxsi məlumatların icazəsiz toplanmasını və yayılmasını qadağan edir.

Azərbaycan 1992-ci ildə BMT-yə üzv olduqdan sonra bəyənnamənin prinsiplərini tanıyıb və onlara uyğun milli qanunvericiliyi tənzimləyib. Yəni, Azərbaycan bəyənnaməni ayrıca ratifikasiya etməsə də, bu bəyannamənin prinsiplərini qəbul edib və insan hüquqlarına dair digər beynəlxalq konvensiyaları ratifikasiya edib.

Avropa ittifaqının ümumi məlumat qoruma qaydaları - (General Data Protection Regulation - GDPR) Avropa İttifaqı tərəfindən 2018-ci ildə qəbul edilən və

[118] “Kibercinayətkarlıq haqqında” 23 noyabr 2001-ci il tarixli Budapeşt Konvensiyası
[119] “Kibercinayətkarlıq haqqında” Konvensiyanın Təsdiq edilməsi barədə Azərbaycan Respublikasının 30 sentyabr 2009-cu il tarixli Qanunu
[120] BMT-nin “Ümumdünya insan hüquqları bəyannaməsi”. 10 dekabr 1948-ci il

şəxsi məlumatların qorunmasına dair ən sərt qanunlardan biridir. GDPR-in əsas prinsipləri aşağıdakılardır:

- Şəxsi məlumatlar yalnız müvafiq razılıq əsasında toplanmalı və işlənməlidir.
- Fırıldaqçılıq və sosial mühəndislik vasitəsilə əldə edilən şəxsi məlumatların istifadəsi ağır cinayət hesab edilir.
- Kibertəhlükəsizlik tədbirləri yetərli olmadığı təqdirdə, təşkilatlar hüquqi məsuliyyət daşıyır.
- GDPR pozuntularına görə şirkətlərə və şəxslərə 20 milyon avroya qədər cərimə və ya illik qlobal dövriyyəsinin 4%-i qədər cəza tətbiq edilə bilər.

Azərbaycan GDPR-i birbaşa qəbul etməsə də, "Fərdi məlumatlar haqqında" Azərbaycan Respublikasının Qanunu GDPR prinsiplərinə uyğun şəkildə tənzimlənməkdədir.

"Kompüter fırıldaqçılığı və zərərli aktlar" Qanunu (CFAA, 1986) - ABŞ-da qəbul edilən "Computer fraud and abuse act" kompüter sistemlərinə icazəsiz giriş, sosial mühəndislik fırıldaqçılığı və şəxsi məlumatların oğurlanması kimi cinayətləri cəzalandırmaq üçün hazırlanmışdır. CFAA aşağıdakı halları cinayət hesab edir:

- Kompüter sistemlərinə icazəsiz giriş və məlumat oğurluğu
- Dövlət və korporativ serverlərə hədəflənmiş hücumlar
- Şəxsi məlumatların və maliyyə hesablarının qanunsuz əldə edilməsi

ABŞ hökuməti CFAA çərçivəsində müxtəlif cinayətlərə qarşı ciddi tədbirlər görür və beynəlxalq hüquq əməkdaşlığı çərçivəsində digər dövlətlərlə birgə cinayətkarların izlənilməsinə dəstək verir.

Elektron fırıldaqçılıq haqqında direktivlər - Avropa İttifaqı tərəfindən qəbul edilən müxtəlif direktivlər sosial mühəndislik fırıldaqlarına qarşı hüquqi tədbirləri müəyyən edir. Bunlardan bəziləri:

- İnformasiya sistemlərinə qarşı hücumlar haqqında direktiv (2013/40/EU)[121] - Avropa ölkələrində kiberhücumlara və internet fırıldaqlarına qarşı tədbirləri müəyyən edir.
- Fərdi məlumatların emalı və bu cür məlumatların sərbəst hərəkəti ilə bağlı fiziki şəxslərin müdafiəsi direktivi (95/46/EC)[122] - Kiberhücumlar və sosial mühəndislik yolu ilə əldə edilən məlumatların icazəsiz istifadəsini qadağan edir.
- Elektron imza və elektron identifikasiya haqqında direktiv (eIDAS, 2014)[123] – dələduzluğa qarşı etibarlı elektron imza texnologiyalarının tətbiqini təşviq edir.

Azərbaycan Avropa İttifaqı ilə əməkdaşlıq çərçivəsində bu direktivlərin müəyyən elementlərini öz qanunvericiliyinə daxil etmişdir. Sosial mühəndislik hücumları qlobal təhlükə olduğundan, beynəlxalq hüquqi çərçivələr bu cinayətlərin qarşısını almaq üçün mühüm rol oynayır. Budapeşt Konvensiyası, GDPR, CFAA və digər beynəlxalq qanunlar şəxsi məlumatların qorunması və kibercinayətkarlıqla mübarizəyə yönəlib. Azərbaycan

[121] eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32013L0040&qid=1740071905447
[122] eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679&qid=1740071983553
[123] eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014R0910&qid=1740072041400

Budapeşt Konvensiyasını ratifikasiya edərək kibercinayətkarlığa qarşı mübarizədə beynəlxalq standartlara uyğun qanunvericilik tətbiq edir.

Azərbaycan Respublikası qanunvericiliyində kibercinayətkarlıqla mübarizə

Kibercinayətkarlıq və sosial mühəndislik hücumları qlobal təhlükə olmaqla yanaşı, Azərbaycan üçün də ciddi çağırış yaradır. Bu səbəbdən, ölkə daxilində kibertəhlükəsizliyin təmin edilməsi və şəxslərin rəqəmsal hüquqlarının qorunması məqsədilə müxtəlif qanunvericilik aktları qəbul edilmişdir. Azərbaycan həm milli qanunvericilik, həm də beynəlxalq sazişlər çərçivəsində kibercinayətkarlığa qarşı effektiv mübarizə aparır.

1. Azərbaycan Respublikasının Cinayət Məcəlləsi (maddə 271-273, 273-1/2)[124]

- Kompyuter sisteminə qanunsuz daxil olma, kompyuter məlumatlarını qanunsuz ələ keçirmə, kompyuter sisteminə və ya kompyuter məlumatlarına qanunsuz müdaxilə, kibercinayətlərin törədilməsi üçün hazırlanmış vasitələrin dövriyyəsi və kompyuter məlumatlarının saxtalaşdırılması kimi əməlləri cinayət məsuliyyəti yaradır.

2. "Fərdi məlumatlar haqqında" Qanun[125].

- Şəxsi məlumatların toplanması, işlənməsi və qorunmasına dair tənzimləmələri müəyyən edir və GDPR prinsiplərinə uyğunlaşdırılmaqdadır.

3. "Azərbaycan Respublikasının Rəqəmsal İnkişaf və Nəqliyyat Nazirliyi yanında Elektron Təhlükəsizlik Xidmətinin fəaliyyətinin təmin edilməsi haqqında" Azərbaycan Respublikası Prezidentinin Fərmanı[126].

- Kibertəhlükəsizlik sahəsində fəaliyyət göstərən əsas qurumlardan biri olan Elektron Təhlükəsizlik Mərkəzinin səlahiyyətlərini və funksiyalarını müəyyən edir.

4. "Elektron imza və elektron sənəd haqqında" Qanun[127].

- Rəqəmsal imzaların hüquqi qüvvəsini və elektron sənəd dövriyyəsinin təhlükəsizliyini təmin edir.

5. "İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında" Qanun[128].

- Dövlət, kommersiya və şəxsi məlumatların qorunmasına dair əsas qaydaları müəyyən edir.

- İnformasiya təhlükəsizliyinin qorunması və kritik infrastruktur obyektlərinin müdafiəsinə yönəlmiş qaydalar təqdim edir.

6. "Telekommunikasiya haqqında" Qanun[129].

- İnternet provayderlərinin, rabitə operatorlarının və informasiya texnologiyalarına dair hüquqi çərçivəni tənzimləyir.

---

[124] Azərbaycan Respublikasının Cinayət məcəlləsi. 30 dekabr 1999-cu il
[125] "Fərdi məlumatlar haqqında" 11 may 2010-cu il tarixli Azərbaycan Respublikasının Qanunu
[126] "Azərbaycan Respublikasının Rəqəmsal İnkişaf və Nəqliyyat Nazirliyi yanında Elektron Təhlükəsizlik Xidmətinin fəaliyyətinin təmin edilməsi haqqında" Azərbaycan Respublikası Prezidentinin 05 mart 2013-cü il tarixli Fərmanı
[127] "Elektron imza və elektron sənəd haqqında" 09 mart 2004-cü il tarixli Azərbaycan Respublikasının Qanunu
[128] "İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında" 03 aprel 1998-ci il tarixli Azərbaycan Respublikasının Qanunu
[129] "Telekommunikasiya haqqında" 14 iyun 2005-ci il tarixli Azərbaycan Respublikasının Qanunu

- İnternetə nəzarət və tənzimləmə mexanizmlərini müəyyən edir.

7. **“Dövlət sirri haqqında” Qanun[130].**

Xüsusi məxfi və dövlətə məxsus məlumatların yayılmasının qarşısını almaq üçün tənzimləyici mexanizmlər təqdim edir.

8. “Elektron ticarət haqqında” Qanun[131].

- Elektron ticarətdə şəffaflığı təmin etmək, fırıldaqçılığın qarşısını almaq və rəqəmsal kommersiya əməliyyatlarını qorumaq üçün normativ bazanı təqdim edir.

Azərbaycan Respublikasında kibercinayətkarlıqla mübarizə və rəqəmsal təhlükəsizliyin təmin edilməsi məqsədilə geniş və müasir hüquqi çərçivə formalaşdırılmışdır. Bu hüquqi baza, dövlət qurumları, özəl sektor və vətəndaşların rəqəmsal təhlükəsizliyini qorumaq üçün nəzərdə tutulmuş və beynəlxalq təcrübəyə əsaslanaraq daim təkmilləşdirilməkdədir. Xüsusilə, Cinayət Məcəlləsi çərçivəsində müəyyən edilmiş maddələr, fərdi məlumatların qorunmasına dair qanunvericilik və Elektron Təhlükəsizlik Xidmətinin fəaliyyəti kibercinayətkarlıqla mübarizədə mühüm rol oynayır.

Rəqəmsal dövrdə informasiya təhlükəsizliyinin təmin edilməsi təkcə texnoloji həllərə əsaslanmamalıdır. Hüquqi mexanizmlər və normativ tənzimləmələr bu sahədə əsas dayaqlardan birini təşkil edir. Azərbaycan Respublikasında qəbul edilən qanunvericilik aktları informasiya təhlükəsizliyi sahəsində bir neçə fundamental aspekti əhatə edir.

Bütün bu qanunvericilik tədbirləri Azərbaycan Respublikasının kibertəhlükəsizlik strategiyasının mühüm hissəsini təşkil edir. Rəqəmsal ekosistemin qorunması üçün hüquqi mexanizmlərlə yanaşı, beynəlxalq əməkdaşlıq da xüsusi əhəmiyyət kəsb edir. Azərbaycan, Budapeşt Konvensiyası (Kibercinayətkarlıq üzrə Avropa Şurasının Konvensiyası) və digər beynəlxalq hüquqi sənədlər çərçivəsində beynəlxalq tərəfdaşlarla əməkdaşlıq edərək kibertəhlükəsizlik sahəsində qabaqcıl təcrübələri tətbiq edir.

Bundan əlavə, dövlət və özəl sektorun əməkdaşlığı çərçivəsində kibertəhlükəsizlik üzrə maarifləndirmə və təlim proqramları həyata keçirilir. Bu tədbirlər ictimaiyyətin kibertəhlükələrə qarşı həssaslığını azaltmaq, dövlət və özəl qurumların kibertəhlükəsizlik biliklərini artırmaq və rəqəmsal sahədə təhlükəsizliyə dair biliklərin geniş yayılmasını təmin etmək məqsədi daşıyır.

Nəticə etibarilə, Azərbaycan Respublikasında kibercinayətkarlıqla mübarizə və rəqəmsal təhlükəsizliyin təmin edilməsi məqsədilə güclü və dinamik bir hüquqi çərçivə mövcuddur. Dövlət bu istiqamətdə qanunvericiliyi beynəlxalq standartlara uyğunlaşdıraraq inkişaf etdirməkdə davam edir. Bu tədbirlər, dövlət, biznes və vətəndaşlar üçün təhlükəsiz rəqəmsal mühitin yaradılmasına və kibertəhlükəsizliyin gücləndirilməsinə töhfə verir.

Bu yanaşmaların davamlı inkişafı və effektiv tətbiqi gələcəkdə daha güclü kibertəhlükəsizlik sisteminin qurulmasına, texnoloji innovasiyaların təhlükəsizliyinin təmin edilməsinə və vətəndaşların rəqəmsal hüquqlarının qorunmasına şərait

[130] “Dövlət sirri haqqında” 07 sentyabr 2004-cü il tarixli Azərbaycan Respublikasının Qanunu
[131] “Elektron ticarət haqqında” 10 may 2005-ci il tarixli Azərbaycan Respublikasının Qanunu

yaradacaqdır. Bununla yanaşı, kibertəhlükəsizlik sahəsində qanunvericiliyin təkmilləşdirilməsi və beynəlxalq əməkdaşlığın gücləndirilməsi, kibercinayətkarlığa qarşı daha effektiv mübarizə aparmağa imkan verəcəkdir. Həmçinin, ictimaiyyətin maarifləndirilməsi və təhlükəsizlik mədəniyyətinin formalaşdırılması bu istiqamətdə uzunmüddətli və dayanıqlı nəticələrin əldə olunmasına töhfə verəcəkdir.

Sosial mühəndisliyin etik tərəfləri

Sosial mühəndislik informasiya əldə etmək və manipulyasiya etmək məqsədilə insan psixologiyasının zəif cəhətlərindən istifadə edən bir yanaşmadır. Lakin bu yanaşma etik və hüquqi baxımdan iki fərqli aspektə malikdir. Bir tərəfdən, sosial mühəndislik kibercinayətkarlar tərəfindən insanları aldatmaq və şəxsi, korporativ, hətta dövlət məlumatlarını ələ keçirmək üçün istifadə olunur. Digər tərəfdən, etik sosial mühəndislik təşkilatların kibertəhlükəsizlik səviyyəsini qiymətləndirmək və inkişaf etdirmək üçün qanuni və icazəli şəkildə həyata keçirilə bilər.

Bu yanaşma informasiya təhlükəsizliyi sahəsində mühüm bir məsələ olaraq qiymətləndirilir, çünki sosial mühəndislik metodlarının istifadəsi müxtəlif hüquqi və etik dilemmlərə səbəb ola bilər. Məsələn, etik sosial mühəndislik hansı hallarda qəbul edilə bilər? Etik hakerlər bu metodlardan istifadə edərkən hansı sərhədləri gözləməlidirlər? Sosial mühəndislik texnikalarından istifadə edərək insanların şəxsi məlumatlarını əldə etmək həmişə etikdirmi, yoxsa müəyyən hallarda qəbul edilə bilər? Bu və digər suallar sosial mühəndisliyin etik və hüquqi aspektlərinin dərin araşdırılmasını tələb edir.

Bundan əlavə, sosial mühəndisliyin sərhədləri və icazə çərçivələri aydın şəkildə müəyyən edilmədikdə, bu metodlar şəxsi məxfiliyin pozulmasına, təşkilatların işçilərinin istismarına və hətta hüquqi mübahisələrə səbəb ola bilər. Məsələn, bir təşkilatın kibertəhlükəsizlik səviyyəsini yoxlamaq üçün sosial mühəndislik testi aparılırsa, işçilərin razılığı olmadan onların şəxsi məlumatlarının toplanması nə dərəcədə etik hesab edilə bilər?

Eyni zamanda, sosial mühəndisliyin etik aspektlərinin müəyyən olunması yalnız təşkilatlar və şəxslər üçün deyil, həm də hüquq-mühafizə orqanları və dövlət qurumları üçün də aktualdır. Hüquq-mühafizə orqanları cinayətkarların aşkar edilməsi və məxfi əməliyyatların keçirilməsi üçün sosial mühəndislik texnikalarından istifadə edə bilər. Lakin bu texnikaların istifadəsi hansı hallarda məqbul sayılır?

Daha geniş kontekstdə baxdıqda, sosial mühəndisliyin etik tərəfləri yalnız fərdi və təşkilati etik çərçivələrlə məhdudlaşmır. Bu texnikaların media, siyasət, reklam və sosial şəbəkələrdə manipulyasiya məqsədilə istifadəsi cəmiyyət üçün nə kimi təhlükələr yarada bilər? Sosial mühəndislik vasitəsilə dezinformasiya yayılması, ictimai rəyin yönləndirilməsi və kütləvi manipulyasiya halları da etik problemlər yaradır.

Bu səbəbdən, sosial mühəndisliyin etik sərhədlərinin düzgün müəyyən edilməsi, bu metodlardan istifadə edən şəxslərin etik qaydalara əməl etməsi və qanuni tənzimləmələrin dəqiq şəkildə işlənməsi kibertəhlükəsizlik və informasiya təhlükəsizliyi sahəsində vacib məsələlərdən biridir. Bununla yanaşı, etik sosial mühəndislik

metodlarının müəyyən çərçivələr daxilində tətbiqi və bu sahədə çalışan mütəxəssislərin məsuliyyətləri də etik prinsiplər çərçivəsində aydın şəkildə müəyyən olunmalıdır. Bu hissədə sosial mühəndisliyin etik aspektləri, etik hakerlik, şəxsi həyatın toxunulmazlığı və sosial mühəndislik hücumlarına qarşı hüquqi və etik müdafiə mexanizmləri geniş şəkildə araşdırılacaqdır.

Etik sosial mühəndislik kibertəhlükəsizlik sahəsində təşkilatların və şəxslərin müdafiə qabiliyyətini gücləndirmək məqsədilə həyata keçirilən qanuni və icazəli fəaliyyətlər toplusudur. Etik hakerlər kibertəhlükəsizlik üzrə mütəxəssislər olaraq sosial mühəndislik texnikalarından istifadə edərək, təşkilatların informasiya sistemlərindəki zəiflikləri aşkar edir və onların təhlükəsizlik strategiyalarını gücləndirmək üçün tövsiyələr verirlər. Bu fəaliyyətlər əsasən penetrasiya testləri, phishing simulyasiyaları, sosial mühəndislik hücumlarının modelləşdirilməsi və işçilərin kibertəhlükəsizlik biliklərinin artırılması kimi üsullarla həyata keçirilir.

Etik sosial mühəndislik, əsasən, real hücum ssenarilərini təqlid edərək təşkilatların mövcud təhlükəsizlik mexanizmlərini sınaqdan keçirmək üçün istifadə olunur. Bu yanaşma, işçilərin kibertəhlükəsizlik sahəsində maarifləndirilməsinə və onların sosial mühəndislik hücumlarına qarşı dayanıqlılığının artırılmasına xidmət edir. Eyni zamanda, etik hakerlər təşkilatlar üçün fərdi hazırlıq planları təqdim edir və potensial hücumların qarşısının alınması üçün yeni təhlükəsizlik protokolları formalaşdırırlar.

Bununla yanaşı, etik sosial mühəndislik kibertəhlükəsizlik sahəsində hüquqi və etik çərçivədə həyata keçirilməlidir. Təşkilatlar və şəxslər razılıq vermədikdə və ya etik prinsiplər pozulduqda, sosial mühəndislik hüquqi məsuliyyət yarada bilər. Bu səbəbdən, etik hakerlər və kibertəhlükəsizlik mütəxəssisləri yalnız icazəli testlər həyata keçirməli və təşkilatların kibermüdafiəsini gücləndirməyə yönəlmiş fəaliyyətlər göstərməlidirlər.

Etik sosial mühəndislik təşkilatların kibertəhlükəsizlik səviyyəsini qiymətləndirmək və onların sosial mühəndislik hücumlarına qarşı dayanıqlığını artırmaq məqsədi daşıyır. Bu proses çərçivəsində təhlükəsizlik zəiflikləri aşkar edilir, işçilərin kibermühitdə davranışları analiz olunur və potensial risklərə qarşı qabaqlayıcı tədbirlər görülür. Etik sosial mühəndislik texnikaları real hücum ssenarilərini simulyasiya edərək şirkətlərin təhlükəsizlik tədbirlərini təkmilləşdirməsinə kömək edir.

Etik sosial mühəndisliyin əsas məqsədləri aşağıdakılardır:

- **Kibertəhlükəsizlik biliklərinin artırılması -** İşçilərin sosial mühəndislik hücumlarına qarşı daha hazırlıqlı olması üçün maarifləndirmə aparılır.
- **Təşkilatın zəifliklərinin müəyyən edilməsi -** Kibertəhlükəsizlik üzrə mütəxəssislər simulyasiya edilmiş sosial mühəndislik hücumları təşkil edərək sistemlərin hansı hallarda risk altında olduğunu təyin edirlər.
- **Real hücumlara qarşı qorunma tədbirlərinin təkmilləşdirilməsi -** Etik sosial mühəndislik hücumları nəticəsində əldə edilən məlumatlar əsasında təşkilatların təhlükəsizlik tədbirləri yenilənir və gücləndirilir.

Lakin sosial mühəndislik etik çərçivədən çıxaraq şəxslərin razılığı olmadan həyata keçirildikdə hüquqi və etik problemlər yaradır. Bu baxımdan etik sosial mühəndislik

yalnız təşkilatın razılığı və hüquqi çərçivədə aparılmalıdır. Əks halda, bu cür fəaliyyətlər məlumatların icazəsiz əldə edilməsi, məxfiliyin pozulması və dələduzluq kimi hüquqi məsuliyyət yaradan hallara səbəb ola bilər. Bundan əlavə, etik qaydaların pozulması təşkilatın etibarına və nüfuzuna ciddi ziyan vura bilər. Buna görə də, etik sosial mühəndislik yalnız açıq, şəffaf və qanuni çərçivədə həyata keçirilməlidir.

Cinayətkarlığa mübarizədə sosial mühəndislik taktikalarından istifadə

Sosial mühəndislik yalnız kibercinayətkarlar tərəfindən tətbiq edilən bir metod kimi qəbul edilmir. Əksinə, bu texnika hüquq-mühafizə orqanları, kəşfiyyat xidmətləri və təhlükəsizlik agentlikləri tərəfindən cinayətkarlıqla mübarizə, istintaq aparma və hüquq pozuntularının qarşısını almaq üçün effektiv şəkildə istifadə edilir. Hüquq-mühafizə orqanları sosial mühəndislik texnikalarından cinayətkar qrupları ifşa etmək, dəlilləri toplamaq və əməliyyat-axtarış tədbirlərini həyata keçirmək üçün geniş istifadə edirlər.

Bu metodların hüquq-mühafizə sisteminə inteqrasiyası cinayətkarların psixoloji zəifliklərindən, davranış modellərindən və inandırıcılıq mexanizmlərindən istifadə etməklə onların qanunsuz fəaliyyətlərini aşkar etmək üçün mühüm alət rolunu oynayır. Həmçinin, hüquq-mühafizə orqanları sosial mühəndislik texnikalarından istifadə edərək şahidlərdən və şübhəlilərdən daha çox məlumat əldə edə bilər, onları istintaqa cəlb etmə prosesini asanlaşdıra bilər və cinayətkar şəbəkələrə qarşı strategiyalarını təkmilləşdirə bilərlər.

Bu bölmədə sosial mühəndisliyin hüquq-mühafizə sahəsində tətbiqini, onun müxtəlif cinayətlərlə mübarizədə oynadığı rolu və etik-hüquqi çərçivələr daxilində necə istifadə edildiyini ətraflı şəkildə araşdıracağıq.

1. Cinayətkar şəbəkələrin ifşası və məxfi əməliyyatlar

Sosial mühəndislik hüquq-mühafizə orqanlarına gizli əməliyyatlar aparmaq və cinayətkar şəbəkələrə daxil olmaq imkanı yaradır. Əməliyyat işçiləri cinayətkar qruplara sızmaq, onların fəaliyyətini müşahidə etmək və dəlillər toplamaq üçün sosial mühəndislik texnikalarından istifadə edirlər. Bu prosesin uğurlu olması üçün hüquq-mühafizə əməkdaşları cinayətkarların psixoloji zəifliklərini və davranışlarını diqqətlə araşdırır və onları manipulyasiya etmə yollarını təyin edirlər.

Praktik nümunələr:

- **Məxfi əməkdaşların (informatorların) istifadəsi:** Hüquq-mühafizə orqanları cinayətkar qruplara sızan məxfi əməkdaşlar vasitəsilə onların planlarını və əlaqələrini müəyyən edə bilirlər.
- **Saxta şəxsiyyətlər yaratmaq:** Cinayətkarların etibarını qazanmaq üçün saxta şəxsiyyətlərdən istifadə edilərək onların fəaliyyətləri izlənilir.
- **Daxili məlumatlara çıxış əldə etmək:** Cinayətkar şəbəkə üzvləri ilə inamlı əlaqələr quraraq, onların planlarını və əməliyyatlarını aşkar etmək mümkündür.

2. Dəlil toplama və manipulyasiya

Hüquq-mühafizə orqanları sosial mühəndislik texnikalarından istifadə edərək cinayətkarların özlərini ifşa etməsinə şərait yaradır. Bu taktika cinayətkarların müəyyən

situasiyalarda emosional reaksiyalarından və psixoloji təsirlərə məruz qalma meyillərindən istifadə edərək onları istintaqa açıq etmə məqsədi daşıyır.

Əsas yanaşmalar:

- **Cinayətkarların emosional zəifliklərini manipulyasiya etmək:** Hüquq-mühafizə əməkdaşları dindirilmə zamanı şübhəlilərin emosional reaksiyalarını təhlil edərək onların danışmasını təmin etmək üçün psixoloji təsir texnikalarından istifadə edirlər.

Süni məlumat sızdırılması: Cinayətkarlar bəzən müəyyən şərtlər altında özlərini ifşa edirlər. Hüquq-mühafizə orqanları bilərəkdən müəyyən məlumatları sızdıraraq, onların reaksiyalarını izləyə və əlavə sübutlar əldə edə bilərlər.

Daxili dəlillərin əldə edilməsi: Cinayətkarların etibarını qazanaraq, onların istifadə etdiyi cihazlar və ya sənədlər üzərində nəzarəti ələ keçirmək mümkündür.

3. Şübhəlilərin və şahidlərin dindirilməsi

Şübhəlilərin və şahidlərin verdiyi məlumatlar istintaqın gedişatında kritik rol oynayır. Sosial mühəndislik texnikaları hüquq-mühafizə orqanlarına şahidlərin və şübhəlilərin daha çox məlumat paylaşmasını təmin etmək üçün istifadə olunur.

Əsas üsullar:

- **Şübhəliyə inam yaratmaq:** Şübhəliyə dostcasına yanaşmaq və onu təhlükəsiz mühitdə hiss etdirmək, daha çox məlumat paylaşmasına səbəb ola bilər.
- **Alternativ həqiqət texnikası:** Hüquq-mühafizə əməkdaşları bəzən şübhəlilərə fərqli ssenarilər təqdim edərək onların real məlumatları açıq şəkildə bildirməsinə səbəb ola bilərlər.
- **Təcili qərar verməyə məcbur etmək:** Şübhəlilərin daha tez cavab verməsi üçün psixoloji texnikalardan istifadə edilir.

4. Kibercinayətkarlıqla mübarizə

Sosial mühəndislik kibercinayətkarların metodlarını aşkar etmək və onların fəaliyyətini ifşa etmək üçün hüquq-mühafizə orqanları tərəfindən istifadə edilir. Kiberdələduzluq, şəxsiyyət oğurluğu, fişinq hücumları və digər kiberhücumlarla mübarizədə sosial mühəndislik texnikaları effektiv bir üsul kimi tətbiq edilir.

Müasir kibertəhlükəsizlik tədbirləri:

- **Saxta fişinq hücumları:** Hüquq-mühafizə orqanları kiberhücumların mənbəyini müəyyən etmək üçün bəzən özləri saxta hücumlar təşkil edərək cinayətkarları izləyə bilirlər.
- **İnternet üzərindən əməliyyatlar:** Cinayətkarların istifadə etdiyi qaranlıq veb (dark web) platformalarını izləmək və sosial mühəndislik texnikaları ilə onların fəaliyyətlərini ifşa etmək mümkündür.
- **Haker qruplarına sızmaq:** Hüquq-mühafizə orqanları sosial mühəndislik texnikalarından istifadə edərək hücum edən şəxslərin istifadə etdiyi platformalara daxil ola bilər və onların planlarını ifşa edə bilər.

Sosial mühəndislik hüquq-mühafizə orqanları tərəfindən istifadə edildikdə etik və hüquqi çərçivələrin qorunması vacibdir. Hüquq pozuntularının qarşısını almaq və insan hüquq və azadlıqlarını təmin etmək üçün müəyyən prinsiplərə ciddi riayət edilməlidir.

İlk növbədə, hüquqi əsasların qorunması təmin edilməlidir. Sosial mühəndislik texnikaları yalnız qanunvericiliyin icazə verdiyi çərçivədə tətbiq edilməli və heç bir halda hüquq normalarını pozmamalıdır. Hüquq-mühafizə orqanları bu texnikalardan istifadə edərkən müvafiq məhkəmə qərarlarının və hüquqi prosedurların mövcudluğunu təmin etməlidir.

Bundan əlavə, şəxsi məxfiliyin qorunması əsas prinsiplərdən biri olmalıdır. İnsanların şəxsi məlumatlarına qanunsuz müdaxilə edilməsi, onların icazəsi olmadan şəxsi informasiyalarının toplanması və istifadəsi yolverilməzdir. Sosial mühəndislik texnikaları tətbiq edilərkən məxfiliyin qorunması üçün beynəlxalq və milli qanunvericilik normaları əsas götürülməlidir.

Eyni zamanda, etik davranış qaydalarına ciddi riayət olunmalıdır. Hüquq-mühafizə orqanları yalnız etik cəhətdən qəbul edilə bilən sosial mühəndislik metodlarından istifadə etməli, manipulyasiya və zorakılıq kimi qeyri-qanuni və qeyri-etik üsullara müraciət etməməlidirlər. Bu texnikaların tətbiqi zamanı şəxslərin hüquqlarının tapdanmamasına və onların istismar edilməməsinə diqqət yetirilməlidir.

Bütün bu prinsiplər hüquq-mühafizə orqanlarının sosial mühəndislik metodlarını yalnız qanuni və etik çərçivədə tətbiq etməsini təmin etmək üçün nəzərə alınmalıdır. Bu yanaşma həm hüquqi, həm də ictimai etimadın qorunmasına töhfə verəcək və hüquq-mühafizə orqanlarının fəaliyyətinin şəffaflığını artıracaqdır.

Sosial mühəndislik hüquq-mühafizə orqanları üçün cinayətkarlıqla mübarizədə mühüm alətə çevrilmişdir. Bu texnikalar cinayətkar qrupların ifşası, dəlil toplama, kibercinayətkarlıqla mübarizə və istintaq proseslərinin aparılmasında effektiv şəkildə tətbiq olunur. Hüquq-mühafizə orqanları sosial mühəndislik vasitəsilə cinayətkarların fəaliyyətini izləyə, onların planlarını aşkar edə və mütəşəkkil cinayətkar şəbəkələrə qarşı qabaqlayıcı tədbirlər görə bilərlər. Bununla yanaşı, sosial mühəndislik metodlarının istifadəsi hüquqi çərçivələrə uyğun həyata keçirilmədikdə, insan hüquqlarının pozulması və hüquq pozuntularının yaranması riski artır.

Hüquq-mühafizə orqanları sosial mühəndislikdən istifadə edərkən şəffaflığı təmin etməli, hüquqi icazələr əsasında fəaliyyət göstərməli və məqsədyönlü şəkildə qanuni metodlardan istifadə etməlidir. Hüquq sistemlərində sosial mühəndislik texnikalarının hansı hallarda qanuni olduğu açıq şəkildə müəyyən edilməli və bu sahədə çalışan mütəxəssislər etik davranış kodekslərinə riayət etməlidirlər. Əks halda, hüquq-mühafizə orqanlarının tətbiq etdiyi metodlar ictimai etimadı sarsıda və hüquqi mübahisələrə səbəb ola bilər.

Sosial mühəndislik texnikalarının hüquq-mühafizə sistemində tətbiqi üçün beynəlxalq və milli qanunvericilik bazasının təkmilləşdirilməsi də vacibdir. Dövlətlər bu texnikaların qanuni istifadəsi üçün xüsusi qaydalar və protokollar hazırlamalı, hüquq-mühafizə əməkdaşlarını bu sahədə mütəmadi təlimləndirməli və etik sərhədləri aydın şəkildə müəyyən etməlidirlər. Hüquq-mühafizə orqanları sosial mühəndislik texnikalarını daha effektiv və etik qaydalara uyğun istifadə etdikcə, cinayətkarlığa qarşı mübarizə güclənəcək və ictimai təhlükəsizlik səviyyəsi artacaqdır.

Etik və hüquqi qaydalara əməl etməklə, sosial mühəndislik hüquq-mühafizə sahəsində effektiv və qanuni bir vasitə olaraq davamlı inkişaf etdirilə bilər. Bu metodların qanuni çərçivədə tətbiqi, hüquq-mühafizə orqanlarının cinayətkarlıqla mübarizədə daha çevik və təsirli fəaliyyət göstərməsinə imkan yaradacaqdır. Hüquq-mühafizə sistemində sosial mühəndislik metodlarının balanslı və məsuliyyətli şəkildə tətbiqi həm təhlükəsizliyin gücləndirilməsinə töhfə verəcəkdir.

Sosial mühəndislik vasitəsilə cinayətkarlarla mübarizə üsullarının real nümunələri

Hüquq-mühafizə orqanları sosial mühəndislik texnikalarından istifadə edərək bir sıra irimiqyaslı cinayət əməliyyatlarını ifşa etmiş və kibercinayətkarlığa qarşı mübarizədə mühüm nailiyyətlər əldə etmişlər. Bu metodlar cinayətkar şəbəkələrə sızmaq, onların etibarını qazanmaq, hüquqazidd fəaliyyətlərin qarşısını almaq üçün tətbiq edilir.

Həyata keçirilmiş uğurlu əməliyyatlar göstərir ki, sosial mühəndislik hüquq-mühafizə orqanları üçün güclü bir istintaq aləti olmaqla, həm kibercinayətkarlığa, həm də digər transmilli cinayətlərə qarşı mübarizədə effektiv şəkildə istifadə edilə bilər. Aşağıda hüquq-mühafizə orqanlarının sosial mühəndislik taktikasından uğurla istifadə etdiyi bir neçə real nümunə təqdim edilir.

1. "Operation Firewall" (2004) - Kiberdələduzluq şəbəkəsinin ifşası

ABŞ-*ın gizli xidməti və digər beynəlxalq hüquq-mühafizə orqanları saxta kredit kartı fırıldaqları ilə məşğul olan Shadowcrew adlı haker şəbəkəsini ifşa etdilər.*

Metod: Hüquq-mühafizə orqanları cinayətkarlarla əlaqə qurmaq üçün saxta onlayn profillər yaratdılar və onların etibarını qazanaraq əsas hədəfləri müəyyən etdilər. Əldə edilən məlumatlar əsasında 28 haker həbs edildi[132].

2. "Dark Web Marketplace Takedown" (2017) - Qara bazar platformalarının bağlanması

FBI və Europol AlphaBay və Hansa Market kimi qara bazar platformalarını bağladı.

Metod: Hüquq-mühafizə orqanları sosial mühəndislik metodlarından istifadə edərək bazar administratorlarını manipulyasiya etdilər və onların etibarını qazandılar. Bu yolla, müştəri və satıcılar barədə geniş məlumat topladılar, 400 milyon dollarlıq qanunsuz narkotik və silah ticarətinin qarşısı alındı[133].

3. "Operation Trojan Shield" (2021) - Kriminal qrupların ifşası

ABŞ FBI və Avstraliya Federal Polisi birgə əməliyyat nəticəsində 800-dən çox cinayətkarı həbs etdi.

Metod: Hüquq-mühafizə orqanları xüsusi bir "təhlükəsiz mesajlaşma" tətbiqi yaratdılar və cinayətkar qruplara təqdim etdilər. Cinayətkarlar bu tətbiqdən istifadə etdikləri müddətcə onların danışıqları gizli şəkildə izlənildi[134].

---

[132] www.secretservice.gov/press/releases/2004/10/us-secret-services-operation-firewall-nets-28-arrests-international
[133] www.fbi.gov/news/stories/alphabay-takedown
[134] www.justice.gov/usao-sdca/pr/fbi-s-encrypted-phone-platform-infiltrated-hundreds-criminal-syndicates-result-massive

4. "Operation Bayonet" (2017) - AlphaBay və Hansa bazarlarının bağlanması

FBI və Europol birgə əməliyyatla AlphaBay və Hansa adlı qara bazar platformalarını bağladı.

Metod: Hüquq-mühafizə orqanları əvvəlcə AlphaBay-ı bağladı və istifadəçilərin Hansaya keçəcəyini gözləyərək Hansa-nı nəzarətə götürdü. Bu müddət ərzində istifadəçilərin məlumatları toplandı və nəticədə çox sayda həbs həyata keçirildi[135].

5. "Operation Pacifier" (2015) - Uşaq istismarı ilə bağlı qara bazarın ifşası

FBI Playpen adlı uşaq istismarı ilə bağlı qara bazar saytını ifşa etdi.

Metod: FBI saytı ələ keçirərək qısa müddət ərzində fəaliyyətini davam etdirdi və istifadəçilərin IP ünvanları və digər məlumatlarını topladı. Bu əməliyyat nəticəsində dünya üzrə yüzlərlə şəxs həbs edildi[136].

Hüquq-mühafizə orqanlarının sosial mühəndislik texnikalarından istifadə etməsi cinayətkarlıqla mübarizədə yeni və effektiv yanaşmalardan biridir. Yuxarıda təqdim edilən real nümunələr göstərir ki, bu metodlardan istifadə edərək transmilli cinayətkar qrupların ifşası, dəlil toplanması və kibercinayətkarlığın qarşısının alınması mümkün olur.

Bu yanaşmanın uğurlu tətbiqi bir neçə əsas amilə əsaslanır. İlk növbədə, hüquq-mühafizə orqanlarının cinayətkar şəbəkələrə sızmaq və etibar qazanmaq üçün yüksək səviyyəli istintaq texnikalarına və psixoloji manipulyasiya bacarıqlarına sahib olması tələb olunur. Bununla yanaşı, texnoloji vasitələrin effektiv istifadəsi sosial mühəndislik əməliyyatlarının uğurlu nəticələrini təmin edir. Xüsusilə, saxta platformalar və təhlükəsiz mesajlaşma tətbiqləri yaratmaq, qaranlıq veb bazarlarını nəzarətə götürmək və cinayətkarların rəqəmsal izlərini izləmək hüquq-mühafizə orqanlarının sosial mühəndislik vasitəsilə cinayətkarlığa qarşı mübarizədə tətbiq etdiyi qabaqcıl metodlardır.

Sosial mühəndislik hüquq-mühafizə sistemində təkcə kibercinayətkarlıqla mübarizə üçün deyil, həm də narkotik qaçaqmalçılığı, insan alveri, terrorçuluq və digər transmilli cinayətkarlıq növlərinə qarşı istifadə edilə bilər. Hüquq-mühafizə orqanları cinayətkarların psixoloji zəifliklərini və davranışlarını analiz edərək, onların fəaliyyətini istiqamətləndirə və hüquqi tədbirləri daha effektiv həyata keçirə bilərlər. Cinayətkar şəbəkələrə sızma, məxfi əməliyyatlar və saxta kimliklərdən istifadə etməklə, hüquq-mühafizə qurumları onların fəaliyyətini içəridən ifşa edə və uzunmüddətli cinayətkar planların qarşısını ala bilərlər.

Gələcəkdə sosial mühəndislik metodlarından istifadə daha da genişlənə bilər. Xüsusilə, süni intellekt, maşın öyrənməsi və avtomatlaşdırılmış analiz sistemləri hüquq-mühafizə orqanlarına daha effektiv əməliyyatlar həyata keçirməyə imkan verəcək. Cinayətkarların psixoloji davranışlarını analiz edən alqoritmlər, şübhəli fəaliyyətləri əvvəlcədən müəyyən edən sistemlər və sosial şəbəkələrdə riskli profilləri aşkarlayan

[135] www.europol.europa.eu/media-press/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation

[136] www.fbi.gov/news/stories/playpen-creator-sentenced-to-30-years

texnologiyalar hüquq-mühafizə sisteminə inteqrasiya edilə bilər. Bu yanaşmalar cinayətkarlıqla mübarizəni daha çevik və effektiv edəcək.

Ümumilikdə, sosial mühəndislik hüquq-mühafizə orqanları üçün mühüm istintaq alətidir və bu metodların qanuni çərçivədə istifadəsi cinayətkarlıqla mübarizədə böyük nailiyyətlər əldə etməyə imkan verir. Lakin etik və hüquqi sərhədlər gözlənilməli, şəxsi məlumatların qorunmasına xüsusi diqqət yetirilməli və hüquq-mühafizə orqanlarının tətbiq etdiyi sosial mühəndislik metodları cəmiyyətin təhlükəsizliyinə töhfə verəcək şəkildə həyata keçirilməlidir. Hüquq-mühafizə orqanlarının bu texnikaları effektiv və etik qaydalara uyğun tətbiq etməsi gələcəkdə daha təhlükəsiz və qanunçuluğa əsaslanan cəmiyyətin formalaşmasına xidmət edəcəkdir.

Nəticə

Sosial mühəndislik hüquq-mühafizə orqanları üçün cinayətkarlıqla mübarizədə strateji və innovativ bir alətə çevrilmişdir. Hüquq-mühafizə əməkdaşları sosial mühəndislik texnikalarından istifadə edərək cinayətkar şəbəkələrə sızmaq, dəlil toplamaq, kiberhücumları ifşa etmək və istintaq proseslərini sürətləndirmək imkanına malikdirlər. Bu metodlar transmilli cinayətkarlıqla mübarizədə, terrorizmə qarşı əməliyyatlarda, kiberdələduzluq və maliyyə fırıldaqları ilə mübarizədə hüquq-mühafizə orqanlarının effektivliyini artırmışdır.

Bununla yanaşı, sosial mühəndislik metodlarının istifadəsi zamanı hüquqi və etik çərçivələrə ciddi şəkildə riayət edilməlidir. Hüquq-mühafizə orqanları bu metodlardan istifadə edərkən qanunvericiliyə uyğun hərəkət etməli, şəxsi məxfiliyi qorumağa və insan hüquqlarına hörmət etməyə diqqət yetirməlidir. Əks halda, sosial mühəndislik texnikalarının qeyri-qanuni və ya sui-istifadə halları cəmiyyətin hüquq-mühafizə orqanlarına olan etimadını sarsıda bilər və hüquqi mübahisələrə səbəb ola bilər. Bu baxımdan, sosial mühəndislik hüquq-mühafizə sahəsində tətbiq edilərkən ciddi nəzarət mexanizmləri və etik prinsiplər əsas götürülməlidir.

Beynəlxalq əməkdaşlıq sosial mühəndislik vasitəsilə cinayətkarlığa qarşı mübarizədə mühüm rol oynayır. Müxtəlif ölkələrin hüquq-mühafizə orqanları arasında koordinasiyanın gücləndirilməsi, informasiya mübadiləsinin artırılması və transmilli əməliyyatların həyata keçirilməsi sosial mühəndislikdən istifadəni daha təsirli edir. Məsələn, "Operation Trojan Shield," "Operation Firewall" və "Dark Web Marketplace Takedown" kimi uğurlu əməliyyatlar göstərdi ki, qlobal səviyyədə əməkdaşlıq cinayətkar şəbəkələrin ifşası və zərərsizləşdirilməsi üçün mühüm əhəmiyyət kəsb edir.

Gələcəkdə sosial mühəndislik metodlarının hüquq-mühafizə sistemində daha da təkmilləşdirilməsi və texnoloji alətlərlə birləşdirilməsi gözlənilir. Süni intellekt, maşın öyrənməsi və davranış analizi texnologiyalarının tətbiqi hüquq-mühafizə orqanlarına daha effektiv əməliyyatlar həyata keçirməyə və cinayətkarlıqla mübarizədə daha güclü strategiyalar qurmağa imkan verəcəkdir. Bu texnologiyaların sosial mühəndislik metodları ilə birləşdirilməsi cinayətkarların davranışlarını daha əvvəlcədən proqnozlaşdırmağa və qabaqlayıcı tədbirlər görməyə şərait yaradacaq.

§ 9. Sosial mühəndislikdə - açıq mənbə kəşfiyyatı (OSİNT)

Giriş

Açıq mənbə kəşfiyyatı (OSINT - Open Source Intelligence[137]) ictimai mənbələrdən məlumat toplayaraq analiz etmə və bu məlumatları istifadə edərək qərarvermə prosesini dəstəkləmə metodudur. OSINT, informasiya təhlükəsizliyi, hüquq-mühafizə, kəşfiyyat və biznes analizləri kimi sahələrdə geniş tətbiq edildiyi kimi, sosial mühəndislik hücumlarında da kritik rol oynayır. OSINT vasitəsilə əldə edilən məlumatlar hüquqi və etik çərçivədə kiberhücumların qarşısını almaq üçün istifadə oluna bildiyi kimi, eyni zamanda kibercinayətkarlar tərəfindən hədəfə alınan şəxslərin və təşkilatların zəifliklərini aşkar etmək üçün də istifadə oluna bilər.

Bu metod kibercinayətkarlar tərəfindən şəxslərin və təşkilatların zəifliklərini aşkar etmək, potensial hədəflər seçmək və müxtəlif manipulyasiya strategiyaları qurmaq üçün istifadə edilir. Hücum edən şəxslər açıq mənbələrdən əldə etdikləri məlumatlar vasitəsilə qurbanların sosial həyatını, texniki biliklərini, gündəlik vərdişlərini və hətta emosional zəifliklərini analiz edərək maksimum təsir göstərə biləcək hədəfli hücumlar planlaşdırırlar. Eyni zamanda, OSINT hüquqi və etik çərçivədə kibertəhlükəsizlik mütəxəssisləri, jurnalistlər, hüquq-mühafizə orqanları və analitiklər tərəfindən də aktiv şəkildə istifadə edilir. Qanuni və etik çərçivədə istifadə edildikdə, OSINT təhlükəsizlik risklərinin aşkarlanmasına, cinayətkarlıqla mübarizəyə və korporativ təhlükəsizliyin gücləndirilməsinə kömək edir. Kibertəhlükəsizlik mütəxəssisləri OSINT vasitəsilə təşkilatların məlumat sızma risklərini müəyyən edərək qabaqlayıcı tədbirlər görə bilərlər. Hüquq-mühafizə orqanları cinayətkar fəaliyyətlərlə bağlı sübutlar toplamaq, terror qruplaşmalarını izləmək və potensial təhdidləri müəyyən etmək üçün bu metoddan geniş istifadə edirlər.

Bununla yanaşı, OSINT təkcə hüquq-mühafizə və kibertəhlükəsizlik sahəsində deyil, həm də korporativ sektor və biznes dünyasında mühüm bir alətə çevrilmişdir. Şirkətlər rəqiblərinin strategiyalarını analiz etmək, bazar tendensiyalarını araşdırmaq və müştəri davranışlarını anlamaq üçün OSINT-dən istifadə edirlər. Media və jurnalistika sahəsində çalışanlar isə ictimaiyyətə açıq olan məlumatları analiz edərək dərin araşdırmalar aparır, kəşfiyyat və siyasi analizlər həyata keçirirlər.

Bu mühazirədə OSINT-in sosial mühəndislikdə istifadəsi, əsas metodları, istifadə olunan alətlər və praktiki tətbiqləri geniş şəkildə araşdırılacaq. Eyni zamanda, OSINT-in etik və hüquqi aspektlərinə xüsusi diqqət yetiriləcəkdir. OSINT, həm kiberhücumlar, həm də təhlükəsizlik və istintaq məqsədləri üçün istifadə edilə bilər. Bu metod, şəxslər, dövlət qurumları, korporasiyalar və təşkilatlar haqqında geniş məlumat toplamaq üçün müxtəlif onlayn və oflayn mənbələrdən yararlanır. OSINT-in gücü, məlumatların böyük həcmini strukturlaşdıraraq, analiz etmək və praktik istifadəyə yararlı hala gətirmək qabiliyyətindədir.

[137] osintframework.com/

"OSINT analitik prosesləri və onun sosial mühəndislikdə rolu"

Müasir texnologiyalar və genişlənən rəqəmsal izlər açıq mənbə kəşfiyyatını sosial mühəndislik hücumları üçün güclü bir vasitəyə çevirib. Hücum edən şəxslər OSINT metodlarından istifadə edərək şəxslərin və təşkilatların onlayn fəaliyyətlərini təhlil edir, onların zəifliklərini müəyyənləşdirir və bu məlumatlardan manipulyasiya strategiyaları qurmaq üçün yararlanırlar. Eyni zamanda, bu texnikalar kibertəhlükəsizlik mütəxəssisləri və hüquq-mühafizə orqanları tərəfindən cinayətkarlıqla mübarizə, məlumat sızmalarının aşkarlanması və təhlükəsizlik risklərinin qiymətləndirilməsi məqsədilə tətbiq edilir. Açıq mənbələrdən əldə edilən informasiyalar analiz edilərək, həm hücum, həm də müdafiə strategiyalarının qurulmasına töhfə verir. OSINT-in effektivliyi, məlumatların düzgün toplanması, sistemləşdirilməsi və məqsədyönlü şəkildə istifadəsindən asılıdır. Bu proses ümumiyyətlə dörd əsas mərhələdən ibarətdir: məlumat toplama, təhlil və emal, profil çıxarma və istifadəyə hazırlıq.

1. Məlumat toplama

Bu mərhələdə açıq mənbələrdən hədəf haqqında maksimum məlumat toplanır. Mənbələr müxtəlif formatda ola bilər və bu proses passiv və aktiv OSINT metodlarını əhatə edir[138].

- **Passiv OSINT:** Bu metod hədəflə heç bir birbaşa qarşılıqlı əlaqəyə girmədən, açıq mənbələrdən məlumat toplanmasını əhatə edir. Buraya sosial media profillərinin, dövlət reyestrlərinin, xəbər saytlarının, forumların və sızdırılmış məlumat bazalarının analizi daxildir. Passiv OSINT hücum edən şəxslər və ya analitiklər üçün iz buraxmadan hədəflə bağlı geniş məlumat toplamaq imkanı yaradır, çünki bu proses üçüncü tərəf resurslardan istifadə etməklə həyata keçirilir.
- **Aktiv OSINT:** Bu metod isə hədəfin sistemləri və şəbəkələri ilə birbaşa əlaqəyə girməklə məlumat toplanmasını əhatə edir. Buraya DNS sorğuları göndərmək, serverlərin açıq portlarını skan etmək, e-poçt ünvanlarını yoxlamaq və müəyyən veb-saytların zəifliklərini araşdırmaq kimi texnikalar daxildir. Aktiv OSINT zamanı hədəf sistemin administratorları və ya təhlükəsizlik xidmətləri bu cəhdləri izləyə bilərlər, çünki bu proses müəyyən bir səviyyədə iz buraxır.

OSINT prosesində məlumatların effektiv şəkildə toplanması üçün müxtəlif açıq mənbələrdən istifadə edilir. Bu mənbələr şəxslər, şirkətlər və təşkilatlar haqqında geniş həcmdə məlumat təqdim edə bilər. Sosial media platformalarından tutmuş hökumət reyestrlərinə, forumlardan darknet bazalarına qədər geniş məlumat bazalarına giriş OSINT analitiklərinin və sosial mühəndislərin hədəflər haqqında ətraflı profil yaratmasına imkan verir.

Məlumat toplama üçün əsas mənbələr:

- Sosial media (Facebook, Twitter, Instagram, LinkedIn, TikTok və s.)

[138] ntrepidcorp.com/managed-attribution/defining-active-vs-passive-osint/

- Forumlar və müzakirə platformaları (Reddit, Quora, 4chan və s.)
- Xəbər saytları və bloqlar
- Şəxsi və korporativ veb-saytlar
- Hökumət və kommersiya məlumat bazaları
- WHOIS və DNS məlumat bazaları (domain və IP məlumatları üçün)
- Darknet forumları və bazarlar
- Google Dorking (xüsusi axtarış operatorları ilə məlumat əldə etmək)
- Məlumat sızmalarına dair verilənlər bazaları (pastebin, breach mənbələri)

Məlumat toplama OSINT prosesinin ən vacib mərhələlərindən biridir və toplanan məlumatların dəqiqliyi analiz və profil çıxarma proseslərinin effektivliyinə birbaşa təsir edir. Passiv və aktiv OSINT metodlarının düzgün tətbiqi analitiklərə və ya hücum edən şəxslərə hədəf haqqında ətraflı məlumat əldə etməyə imkan verir. Bununla belə, bu prosesdə əldə edilən məlumatların etibarlılığı və mənbələrinin dəqiqliyi daim yoxlanılmalıdır, çünki yanlış və manipulyasiya olunmuş məlumatlar səhv nəticələrə gətirib çıxara bilər. Eyni zamanda, OSINT-in etik və hüquqi çərçivədə həyata keçirilməsi bu texnikaların qanuni və təhlükəsizlik məqsədləri üçün istifadəsini təmin edir. Sonda, açıq mənbə kəşfiyyatının potensialı yalnız onun necə və hansı məqsədlə istifadə edilməsindən asılıdır.

2. Təhlil və emal

Bu mərhələdə toplanan məlumatlar sistemləşdirilir, dəyərləndirilir və uyğun analiz metodları tətbiq edilərək işlənilir. Bu prosesin əsas məqsədi xam məlumatı strukturlaşdırılmış və praktik istifadəyə yararlı bir formaya çevirməkdir. Təhlil və emal mərhələsində məlumatların doğruluğu, mənbələrin etibarlılığı və əlaqələndirilmiş analizlər əsas götürülür[139].

Təhlil üsulları aşağıdakı əsas komponentlərdən ibarətdir:

1. Məlumatların təsnifatı və kateqoriyalaşdırılması

- Toplanmış məlumatlar şəxsi, biznes, texniki və s. kateqoriyalara bölünərək daha sistemli analiz aparılır.
- Fərdi məlumatlar (ad, doğum tarixi, əlaqə vasitələri və sosial şəbəkə profilləri) ilə biznes məlumatları (şirkət adları, əlaqə məlumatları, maliyyə göstəriciləri) ayrılır.
- Texniki məlumatlar (IP ünvanları, domen adları, açıq portlar və server konfiqurasiyaları) xüsusi analiz metodları ilə işlənir.

2. Məlumatların süzgəcdən keçirilməsi

- Dəqiqliyin artırılması üçün məlumatların mənbələri təsdiqlənir və onların etibarlılığı yoxlanılır.
- Yanlış və ya manipulyasiya olunmuş informasiyaların çıxarılması məqsədilə müxtəlif mənbələrdən əldə edilən məlumatlar müqayisə edilir.
- Şübhəli və qeyri-dəqiq mənbələrdən gələn informasiyalara prioritet verilmədən əlavə araşdırma aparılır.

[139] What is OSINT (open source intelligence)? - www.sentinelone.com/cybersecurity-101/threat-intelligence/open-source-intelligence-osint/

3. Xronoloji analiz

- Hədəfin davranışlarını zaman xətti üzrə izləyərək hansı informasiyaların nə zaman yayımlandığını təyin etmək.
- Xronoloji cədvəllər vasitəsilə müəyyən hadisələrin və informasiyaların zamanla dəyişikliklərini araşdırmaq.
- Hədəfin əvvəlki fəaliyyətləri ilə cari fəaliyyətlərini müqayisə edərək mümkün tendensiyaları müəyyən etmək.

4. Görüntü və media analizləri

- Foto və video materialların EXIF məlumatlarını oxuyaraq cihaz modeli, çəkiliş tarixi və coğrafi koordinatlar kimi informasiyaların çıxarılması.
- Metadata analizləri apararaq şəkillərdə gizli məkan və vaxt məlumatlarının olub-olmadığını yoxlamaq.
- Dərin saxta (deepfake) analizləri edərək görüntü və media materiallarının manipulyasiya olunub-olunmadığını təyin etmək.
- Sosial media və xəbər portallarında yayımlanmış multimedia fayllarının mənbələrinin müəyyən edilməsi.

5. Dil və məzmun analizləri

- Məlumatların mənbə dilində təhlili, əsas məzmun və mesajların çıxarılması.
- Mənbə məqalələrin, sosial media paylaşımlarının və digər məzmunların semantik analizi.
- Avtomatik tərcümə və məzmun uyğunluğu yoxlamaları ilə dezinformasiyanın müəyyən edilməsi.

Təhlil və emal mərhələsində toplanmış məlumatlar strukturlaşdırılır, süzgəcdən keçirilir və müxtəlif analiz metodları tətbiq edilərək praktik istifadəyə yararlı hala gətirilir. Bu prosesdə məlumatların kateqoriyalaşdırılması, etibarlılığının yoxlanılması, zaman ardıcıllığının təhlili, görüntü və media analizləri, eləcə də məzmunun semantik qiymətləndirilməsi həyata keçirilir. Məqsəd, xam məlumatdan dəqiq və etibarlı informasiya əldə edərək effektiv qərarverməni təmin etməkdir.

3. Profiling (profil çıxarma)

Bu mərhələdə hədəf haqqında toplanmış məlumatlar birləşdirilir və konkret analizlər aparılır. Profiling, fərdin və ya təşkilatın zəifliklərini müəyyən etmək üçün aparılan sistemli bir prosesdir[140].

Profil çıxarma prosesi:

- Şəxsi və peşəkar məlumatlar - Hədəfin ad-soyadı, yaşadığı yer, təhsili, işlədiyi yerlər, əlaqələri və sosial çevrəsi.
- Onlayn aktivlik və davranış analizi - Şəxsin və ya təşkilatın sosial media paylaşımları, şərhləri və onlayn iştirakı.
- Texnoloji məlumatlar - İstifadə etdiyi cihazlar, proqram təminatı, IP ünvanları, email və digər texniki məlumatlar.

[140] OSINT & Psychology: profiling and behavioral analysis through open source intelligence - goldenowl.medium.com/osint-psychology-profiling-and-behavioral-analysis-through-open-source-intelligence

- Psixoloji və sosial zəifliklər - Hədəfin maraqları, qorxuları, inancları və ona təsir edə biləcək psixoloji manipulyasiya üsulları.

Profiling prosesi OSINT-in ən kritik mərhələlərindən biridir və toplanmış məlumatları analiz edərək hədəfin zəifliklərini və potensial risklərini aşkar etməyə imkan verir. Bu metod sosial mühəndislik hücumlarının hədəfli şəkildə aparılmasına, həmçinin kibertəhlükəsizlik və hüquq-mühafizə tədbirlərinin effektivliyinin artırılmasına xidmət edir. Profil çıxarma zamanı şəxsi, texnoloji və psixoloji amillərin nəzərə alınması, hücum edən şəxslərin manipulyasiya texnikalarını daha təsirli tətbiq etməsinə və ya təhlükəsizlik ekspertlərinin daha güclü müdafiə strategiyaları hazırlamasına imkan yaradır. Bununla belə, bu prosesin etik və hüquqi sərhədlər daxilində həyata keçirilməsi vacibdir, çünki icazəsiz məlumat toplanması və profil çıxarma şəxsi məxfiliyin pozulması kimi hüquqi problemlərə səbəb ola bilər.

4. İstifadə halları

Açıq mənbə kəşfiyyatı geniş istifadə sahəsinə malikdir və toplanmış məlumatların məqsədindən asılı olaraq həm təhlükəsizlik, həm də hücum yönümlü fəaliyyətlər üçün tətbiq oluna bilər. Bu metod sosial mühəndislik hücumları zamanı qurbanların zəifliklərini aşkar etmək, dələduzluq və manipulyasiya məqsədilə hədəfli kampaniyalar hazırlamaq üçün istifadə olunduğu kimi, kibertəhlükəsizlik və hüquq-mühafizə orqanlarının cinayətkarlıqla mübarizəsində də mühüm rol oynayır[141]. OSINT-in istifadəsi iki əsas istiqamətə bölünür:

Sosial mühəndislik və hücum məqsədilə istifadə

- Phishing və Spear Phishing hücumlarının hazırlanması
- Şəxslərin və şirkətlərin zəifliklərinin aşkar edilməsi
- Hədəf şəxslərə və təşkilatlara saxta məlumat ötürərək manipulyasiya edilməsi
- Dələduzluq və şəxsiyyət oğurluğu üçün fərdi məlumatların istifadəsi

Müdafiə və təhlükəsizlik məqsədilə istifadə

- Təşkilatların öz təhlükəsizlik risklərini təhlil etməsi
- Kibertəhlükəsizlik qruplarının potensial hücum vektorlarını müəyyən etməsi
- Hüquq-mühafizə orqanlarının cinayətkarların fəaliyyətini araşdırması
- Jurnalistlərin və tədqiqatçıların məlumat mənbələrini yoxlaması

OSINT alətləri və metodları fərdin və ya təşkilatın təhlükəsizlik strategiyasına uyğun şəkildə istifadə edilməlidir. Hər hansı bir OSINT əməliyyatı həyata keçirərkən, hüquqi və etik normalara ciddi şəkildə əməl edilməlidir.

OSINT-in effektiv tətbiqi informasiya mənbələrinin düzgün müəyyən edilməsi, məlumatların analitik işlənməsi və etik qaydalara riayət olunması ilə mümkündür. Məlumat toplama, təhlil, profiling və tətbiq mərhələləri OSINT prosesinin əsasını təşkil edir. Bu texnika sosial mühəndislik hücumları üçün kritik əhəmiyyət daşıdığı kimi, kibertəhlükəsizlik və istintaq fəaliyyətləri üçün də böyük rol oynayır. Hüquqi çərçivələrə

[141] www.carahsoft.com/learn/vertical/osint

uyğun olaraq istifadə edildikdə, OSINT texnologiyası informasiya təhlükəsizliyi və cinayətkarlıqla mübarizədə əvəzedilməz bir alət ola bilər.

OSINT məlumat mənbələri

Açıq mənbə kəşfiyyatı prosesində ən vacib amillərdən biri məlumatların əldə edildiyi mənbələrdir. OSINT məlumat mənbələri açıq və qanuni yollarla əldə edilə bilən ictimai resurslardan ibarətdir. Bu resurslar fərqli formatlarda ola bilər - internet üzərində açıq şəkildə yayımlanan məlumatlar, sənədlərin metadataları, texniki kəşfiyyat vasitəsilə aşkar edilən zəifliklər, hətta insanlarla birbaşa ünsiyyət nəticəsində əldə olunan bilgilər. OSINT-in effektivliyi, bu mənbələrdən alınan məlumatların dəqiq təhlili və uyğun strategiyalarla istifadəsinə əsaslanır.

Bu məlumatlar həm etik məqsədlər üçün kibertəhlükəsizlik mütəxəssisləri, hüquq-mühafizə orqanları və jurnalistlər tərəfindən istifadə edilə bilər, həm də pis niyyətli şəxslər tərəfindən sosial mühəndislik hücumlarında manipulyasiya vasitəsi kimi tətbiq oluna bilər.

OSINT məlumatları müxtəlif mənbələrdən əldə edilir və əsasən aşağıdakı kateqoriyalara bölünür:

1. İnternet resursları

İnternet resursları OSINT-in ən əsas və əlçatan məlumat mənbələrindən biridir. Sosial media platformaları, bloglar, forumlar, xəbər saytları və domen məlumat bazaları açıq şəkildə yayımlanan informasiyaların toplanmasına imkan verir. Bu resurslar xüsusi alətlər və axtarış texnikaları ilə analiz edildikdə, şəxslər və təşkilatlar haqqında dərin bilgilər əldə etmək mümkündür. Bu kateqoriya aşağıdakı əsas mənbələri əhatə edir:

- **Sosial media platformaları:** Facebook, Twitter, Instagram, LinkedIn, TikTok və Reddit kimi platformalar insanların həyatları, fəaliyyətləri, əlaqələri və maraqları barədə mühüm məlumatları açıq şəkildə təqdim edir.
- **Bloglar və forumlar:** Müzakirə platformaları (məsələn, Reddit, Quora, 4chan və Telegram qrupları) sosial mühəndislər və analitiklər üçün dəyərli bilgilər mənbəyidir.
- **Xəbər saytları və jurnalist məlumatları:** Media qurumları və xəbər portalları müxtəlif hadisələr və şəxslər haqqında məlumat təqdim edir.
- **WHOIS və DNS məlumat bazaları:** Domen adı qeydiyyatları və DNS məlumatları vasitəsilə veb-saytların sahibi, hostinq provayderi və digər texniki bilgilər əldə edilə bilər.
- **Google dorking:** Google və digər axtarış motorlarının xüsusi sorğularla optimallaşdırılmış istifadəsi ilə saytların gizli səhifələrinə, parol sənədlərinə və digər məxfi məlumatlara çıxış mümkündür.

Alətlər:

- Google Dorking[142] (xüsusi axtarış operatorları)
- Shodan.io[143] (şəbəkə cihazları və açıq portları aşkar etmək üçün)

[142] What is google hacking/dorking? - www.imperva.com/learn/application-security/google-dorking-hacking/
[143] www.shodan.io/

- Censys.io[144] (internetə açıq olan sistemlərin təhlili üçün)

2. Sənədlər və faylların təhlili

Sənədlər və fayllar OSINT məlumatlarının toplanmasında mühüm rol oynayır, çünki onların tərkibində gizli metadatalar və texniki detallar mövcud ola bilər. Müxtəlif formatlarda olan sənədlər (PDF, Word, Excel və s.) istifadəçi məlumatları, yaradılma tarixləri, redaktə qeydləri və hətta GPS koordinatları kimi vacib informasiyalar ehtiva edə bilər. Bu məlumatlar xüsusi analiz alətləri vasitəsilə çıxarılaraq dərin təhlil aparmaq və hədəf haqqında daha ətraflı bilik əldə etmək üçün istifadə olunur.

Sənəd formatları və analiz metodları:

- PDF, Word və Excel sənədləri: Metadata analizləri nəticəsində müəllif, yaradılma tarixi və redaktə məlumatları əldə edilə bilər.
- Metadata analiz alətləri: ExifTool, FOCA, Metagoofil.

Alətlər:

- ExifTool – şəkillər və sənədlərin metadata analizini aparmaq üçün.
- FOCA – Microsoft Office sənədləri və PDF-lərin metadata analizini aparır.
- Metagoofil – Google vasitəsilə ictimai sənədləri tapmaq və analiz etmək üçün.

3. Şəkillər və videoların analizi

Şəkillər və videolar OSINT-də dəyərli məlumat mənbəyi kimi çıxış edir, çünki onlar vasitəsilə şəxslər, obyektlər, yerlər və hadisələr barədə ətraflı analiz aparmaq mümkündür. Exif metadata analizi sayəsində şəkillərin çəkilmə tarixi, istifadə olunan kamera modeli, GPS koordinatları və digər texniki detallar aşkar edilə bilər. Üz tanıma texnologiyaları və geolokasiya vasitələri isə vizual materialların məzmununu daha dərindən araşdıraraq, müəyyən şəxsləri və məkanları müəyyən etməyə kömək edir.

Şəkil və video analizi metodları:

- Exif metadata: Şəkilin çəkildiyi yer, vaxt, cihaz məlumatları.
- Geolokasiya: Şəkildə və ya videoda əks olunan obyektlər və landşaftlar əsasında məkan müəyyənləşdirmə.
- Üz tanıma texnologiyaları: Şəxslərin müəyyən edilməsi üçün.

Alətlər:

- Google Reverse Image Search – internetdəki şəkilləri araşdırmaq üçün.
- TinEye – şəkillərin mənbəsini tapmaq üçün.
- ExifTool – şəkil metadata analiz aləti.
- Yandex Reverse Image Search – şəkillərin internetdəki digər mənbələrini tapmaq üçün.

4. Məlumat bazarları və sızmış məlumatlar

Sızmış məlumat bazaları və darknet platformaları kiberhücumlar, məlumat sızmaları və digər qanunsuz fəaliyyətlər nəticəsində ortaya çıxan həssas informasiyaları ehtiva edir. Bu mənbələr sosial mühəndislər, kibercinayətkarlar və kibertəhlükəsizlik mütəxəssisləri

[144] censys.com/

tərəfindən istifadə edilərək fərdi və korporativ məlumatların kompрometasiya risklərini analiz etməyə imkan yaradır. Sızmış məlumatların təhlili təşkilatların və fərdi şəxslərin kibertəhlükəsizlik tədbirlərini gücləndirməsi üçün vacibdir.

Sızmış məlumat mənbələri:

- Darknet və hacker forumları: Cinayətkar qrupların istifadə etdiyi məxfi bazalar və platformalar.
- Pastebin və Breach bazaları: Sızdırılmış email, şifrə və digər şəxsi məlumatların yer aldığı verilənlər bazaları.

Alətlər:

- HaveIBeenPwned – email ünvanlarının məlumat sızıntılarında olub-olmadığını yoxlamaq üçün.
- DeHashed – sızdırılmış şifrələri tapmaq üçün.
- IntelX.io – müxtəlif mənbələrdən məxfi məlumatları analiz etmək üçün.

5. Texniki kəşfiyyat (TECHINT)

Texniki kəşfiyyat (TECHINT) OSINT-in bir hissəsi olaraq, açıq şəbəkələrdə mövcud olan texniki məlumatların toplanması və təhlilinə yönəlir. Buraya IP ünvanları, açıq portlar, server konfiqurasiyaları, şəbəkə trafik məlumatları və zəifliklərin müəyyən edilməsi daxildir. TECHINT kibertəhlükəsizlik mütəxəssisləri və tədqiqatçılar üçün sistemlərin müdafiəsini gücləndirmək və potensial hücum vektorlarını aşkar etmək üçün mühüm rol oynayır.

Əsas texniki kəşfiyyat metodları:

- Şəbəkə skanları və açıq portların yoxlanılması.
- Sistem və server versiyalarının aşkarlanması.
- Wi-Fi şəbəkələrinin və IoT cihazlarının analizi.

Alətlər:

- Shodan.io – açıq portlar və internetdəki cihazların aşkarlanması üçün.
- Censys.io – şəbəkə xidmətlərini təhlil etmək üçün.
- Nmap – şəbəkə təhlükəsizliyi yoxlamaları üçün.

6. İnsan kəşfiyyatı (HUMINT)

İnsan kəşfiyyatı (HUMINT) açıq mənbə kəşfiyyatının ən vacib və təsirli metodlarından biri hesab olunur. Bu yanaşma, sosial mühəndislik texnikalarından istifadə edərək birbaşa insanlardan məlumat əldə etməyə əsaslanır. Rəsmi müsahibələr, qeyri-rəsmi söhbətlər, sosial media əlaqələri və açıq diskussiyalar vasitəsilə toplanan bilgilər OSINT prosesində dərin analiz və profil yaratmaq üçün istifadə edilə bilər.

HUMINT metodları:

- Sosial şəbəkələr vasitəsilə əlaqə yaratmaq.
- Telefon və email üzərindən məlumat toplamaq.
- Canlı müşahidə və interaktiv sorğular aparmaq.

Alətlər:

- LinkedIn və Facebook kəşfiyyatı.

- Telefon və email analiz alətləri.
- Sosial mühəndislik hücumları üçün hazırlanan ssenarilər.

Açıq mənbə kəşfiyyatı müasir informasiya təhlükəsizliyi, hüquq-mühafizə fəaliyyəti, biznes analizləri və jurnalistika sahəsində mühüm bir alətə çevrilmişdir. OSINT metodları açıq və qanuni mənbələrdən məlumat toplayaraq təhlil etməyə və istifadə etməyə imkan verir. Bu, həm kibertəhlükəsizliyin gücləndirilməsi, həm də strateji qərarların daha effektiv şəkildə verilməsi üçün geniş imkanlar yaradır. Eyni zamanda, OSINT texnikalarından cinayətkarlar və sosial mühəndislər də istifadə edərək fərdləri və təşkilatları hədəfə ala bilərlər. Bu səbəbdən, bu metodların etik və hüquqi çərçivələr daxilində tətbiqi son dərəcə vacibdir.

OSINT məlumatları müxtəlif mənbələrdən toplanır və geniş spektrli analiz metodları ilə işlənilir. İnternet resursları, sənədlərin metadataları, şəkil və video analizləri, sızmış məlumat bazaları, texniki kəşfiyyat (TECHINT) və insan kəşfiyyatı (HUMINT) OSINT-in əsas komponentləridir. İnternetdə açıq şəkildə yayımlanan məlumatlar fərdlər və təşkilatlar haqqında dərin profillər yaratmağa imkan verir. Xüsusilə, sosial media platformaları və bloglar fərdlərin və təşkilatların onlayn davranışlarını analiz etmək üçün geniş imkanlar təqdim edir.

Sənədlər və faylların təhlili OSINT prosesində mühüm rol oynayır. PDF, Word, Excel kimi sənədlərin metadataları analiz edildikdə, onların yaradılma tarixi, müəllifləri və hətta coğrafi koordinatlar kimi məlumatlar aşkarlana bilər. Şəkil və video analizləri isə Exif metadata və geolokasiya texnologiyaları vasitəsilə məkan və obyektlərin müəyyənləşdirilməsinə kömək edir.

Sızmış məlumat bazaları və darknet forumları OSINT üçün xüsusi əhəmiyyət kəsb edir. Burada email, şifrə və digər şəxsi məlumatlar yer ala bilər. Bu məlumatlar hücum edən şəxslər üçün dəyərli bir resurs ola bilər, lakin kibertəhlükəsizlik mütəxəssisləri və hüquq-mühafizə orqanları da bu məlumatlardan istifadə edərək təşkilatların təhlükəsizlik səviyyəsini qiymətləndirə və hücum vektorlarını müəyyən edə bilərlər.

Texniki kəşfiyyat (TECHINT) sistemlərin və şəbəkələrin açıq portlarını, DNS məlumatlarını və digər texniki parametrləri araşdıraraq potensial zəiflikləri aşkar etməyə kömək edir. Shodan.io və Censys.io kimi OSINT alətləri bu məlumatları əldə edərək analiz etməyə imkan verir. İnsan kəşfiyyatı (HUMINT) isə sosial mühəndislik texnikalarından istifadə edərək birbaşa insanlardan məlumat əldə etmək strategiyasına əsaslanır.

Bütün bu OSINT metodları təşkilatların və fərdlərin təhlükəsizliyini qorumaq, potensial təhdidləri müəyyən etmək və hüquq-mühafizə fəaliyyətini gücləndirmək üçün böyük imkanlar yaradır. Lakin bu metodlardan etik və qanuni çərçivədə istifadə edilməlidir. Avropa İttifaqının GDPR qaydaları, ABŞ-ın CFAA qanunu və digər beynəlxalq hüquqi tənzimləmələr OSINT-in qanuni çərçivələr daxilində tətbiq edilməsini tələb edir.

Nəticə olaraq, OSINT məlumat mənbələri kiber təhlükəsizlik, hüquq-mühafizə, media və analitik araşdırmalar üçün əvəzolunmaz bir alət olsa da, onun etik və hüquqi prinsiplərə uyğun şəkildə istifadə olunması əsas şərtdir. OSINT metodlarının inkişafı ilə

yanaşı, bu sahədə çalışan mütəxəssislərin etik kodekslərə riayət etməsi və fərdi məxfiliyə hörmət etməsi də vacibdir.

OSINT və sosial mühəndislik

Açıq mənbə kəşfiyyatı sosial mühəndislik strategiyalarının əsasını təşkil edən ən güclü vasitələrdən biridir. Sosial mühəndislər OSINT metodlarından istifadə edərək qurbanlar haqqında geniş məlumat toplayır, onların davranışlarını analiz edir və zəif cəhətlərini müəyyən edirlər. Bu məlumatlar hədəfə uyğunlaşdırılmış manipulyasiya texnikalarının qurulmasına və daha effektiv hücum ssenarilərinin hazırlanmasına şərait yaradır. Eyni zamanda, OSINT hüquq-mühafizə orqanları, kibertəhlükəsizlik mütəxəssisləri və analitiklər üçün mühüm rol oynayır və təhlükəsizlik təhdidlərinin erkən aşkar edilməsinə imkan verir.

OSINT və sosial mühəndislik arasındakı əlaqə qarşılıqlı və güclü bir təsirə malikdir. Sosial mühəndislər OSINT vasitəsilə hədəf haqqında əldə etdikləri məlumatları manipulyasiya etmək üçün istifadə edirlər, bu isə onlara daha real və etibarlı görünən ssenarilər qurmağa imkan verir. Əldə edilən məlumatlar təkcə rəqəmsal hücumlar üçün deyil, fiziki giriş ssenarilərinin hazırlanması üçün də istifadə oluna bilər. Məsələn, açıq mənbələrdən əldə edilən təşkilati struktur, işçilərin adları və vərdişləri haqqında məlumatlar hücum edən şəxslərə bina daxilində hərəkət etməyə və təhlükəsizlik tədbirlərini aşmağa kömək edə bilər.

OSINT-in sosial mühəndislikdə istifadəsi həm fərdi, həm də təşkilati səviyyədə təhlükəsizlik risklərini artırır. Hücum edən şəxslər açıq mənbələrdən, sosial media profillərindən, şirkətlərin veb-saytlarından, forumlardan və məlumat bazalarından əldə etdikləri bilgiləri şəxsi və işgüzar manipulyasiya üçün istifadə edirlər. İşçilərin sosial media paylaşımlarından və onlayn fəaliyyətlərindən iş yerləri, gündəlik vərdişləri, maraqları və əlaqələri haqqında mühüm məlumatlar əldə edilə bilər. Bu cür informasiyalar, hədəf şəxsə etibarlı görünən mesajlar göndərməklə (məsələn, spear phishing hücumları ilə) onun şəxsi və ya iş hesablarına icazəsiz giriş əldə etməyə imkan yaradır.

Bununla yanaşı, OSINT metodlarından hüquq-mühafizə orqanları, kibertəhlükəsizlik mütəxəssisləri və risk analiz qrupları da istifadə edirlər. Hüquq-mühafizə orqanları cinayətkar qrupların fəaliyyətini izləmək, haker hücumlarını öncədən aşkar etmək və potensial təhdidləri müəyyənləşdirmək üçün OSINT metodlarından faydalanırlar. Təşkilatlar və fərdi şəxslər üçün isə OSINT öz təhlükəsizliklərini artırmaq və kibertəhlükələrə qarşı proaktiv tədbirlər görmək baxımından mühüm əhəmiyyət kəsb edir. Bunun üçün şəxsi və təşkilati məlumatların açıq mənbələrdəki görünürlüğünü azaltmaq, məxfiliyi qorumaq və kibertəhlükəsizlik biliklərini artırmaq vacibdir.

OSINT-in sosial mühəndislikdə rolu birmənalı deyil, çünki onun həm müsbət, həm də mənfi təsirləri mövcuddur. Müsbət tərəfdən, “OSINT” hüquq-mühafizə orqanlarına cinayətkarlıqla mübarizədə, kibertəhlükəsizlik mütəxəssislərinə isə şirkətlərin və fərdlərin kibermüdafiəsini gücləndirməkdə kömək edir. Şəffaf və açıq məlumatlardan

istifadə edərək təhlükəsizlik boşluqları öncədən aşkarlanır və uyğun müdafiə strategiyaları hazırlanır. Mənfi tərəfdən, OSINT metodları hücum edən şəxslər və sosial mühəndislər tərəfindən şəxsləri və təşkilatları hədəfə almaq üçün istifadə edilir. Qurbanların məlumatları manipulyasiya edilərək onların şəxsi və ya iş məlumatları əldə edilir və bundan zərərli məqsədlər üçün istifadə olunur.

Sosial mühəndislikdə "OSINT"-in istifadəsi getdikcə daha da mürəkkəbləşir və texnoloji inkişaflar bu prosesin effektivliyini artırır. Süni intellekt, maşın öyrənməsi və məlumat analiz alətləri hücum edən şəxslərə daha dəqiq və fərdiləşdirilmiş ssenarilər yaratmaq imkanı verir. Bu isə təşkilatların və fərdi şəxslərin öz rəqəmsal izlərini qorumaq üçün daha güclü təhlükəsizlik tədbirləri görməsini tələb edir.

Müdafiə məqsədilə təşkilatlar və fərdi şəxslər "OSINT" vasitəsilə özləri haqqında yayılan məlumatları izləməli və bu informasiyaların məxfiliyini təmin etməlidirlər. OSINT-in mənfi təsirlərindən qorunmaq üçün şəxsi və təşkilati təhlükəsizlik siyasətləri gücləndirilməli, işçilər maarifləndirilməli və açıq mənbələrdə paylaşılan həssas məlumatlar minimuma endirilməlidir. Bundan əlavə, hüquqi və etik qaydalara riayət olunaraq "OSINT" metodlarından düzgün istifadə edilməli və bu vasitələrin qanunsuz məqsədlər üçün istifadəsinin qarşısını almaq üçün hüquqi çərçivələr gücləndirilməlidir.

Nəticə olaraq, "OSINT" sosial mühəndislikdə əsas alətlərdən biri olaraq istifadə edilir və həm hücum, həm də müdafiə məqsədilə tətbiq oluna bilər. "OSINT" metodlarının inkişafı və tətbiqi hüquq-mühafizə, kibertəhlükəsizlik və təşkilati təhlükəsizlik sahələrində böyük imkanlar yaratsa da, eyni zamanda fərdi məxfiliyə və təşkilati təhlükəsizliyə ciddi təhdidlər də yaradır. Bu səbəbdən, OSINT və sosial mühəndislik metodlarının istifadəsi etik və hüquqi prinsiplərə əsaslanmalı, təşkilatlar və fərdi şəxslər isə öz rəqəmsal təhlükəsizliklərini gücləndirmək üçün davamlı tədbirlər görməlidirlər.

Praktiki OSINT alətləri və metodları

"OSINT" alətləri açıq mənbələrdən məlumat toplamaq, sistemləri analiz etmək və mümkün zəiflikləri aşkar etmək üçün istifadə olunur. Bu alətlər sosial mühəndislər, etik hakerlər, kibertəhlükəsizlik mütəxəssisləri və hüquq-mühafizə orqanları tərəfindən geniş tətbiq edilir. "OSINT" alətləri vasitəsilə internetdə yayımlanan məlumatların strukturlaşdırılması, təhlili və real təhlükəsizlik təhdidlərinin müəyyən edilməsi mümkündür. Bu texnologiyalar həm fərdi şəxslərin, həm də təşkilatların rəqəmsal məxfiliyini qorumaq, kibertəhlükəsizlik zəifliklərini aşkarlamaq və potensial hücum vektorlarını öncədən müəyyən etmək üçün vacibdir.

Bu alətlərdən düzgün istifadə edildikdə, məlumat təhlükəsizliyi risklərinin müəyyənləşdirilməsi və sosial mühəndislik hücumlarına qarşı müdafiənin gücləndirilməsi mümkündür. Eyni zamanda, "OSINT" alətləri kibertəhlükəsizlik strategiyalarının təkmilləşdirilməsi və təşkilatların risk idarəetmə proseslərini effektiv şəkildə həyata keçirməsinə kömək edir. İnformasiya təhlükəsizliyinin təmin olunması üçün OSINT metodları əsasən təhlükə kəşfiyyatı, rəqəmsal izlərin qorunması və məxfiliyin idarə

edilməsi məqsədilə tətbiq edilir. Lakin bu alətlərin qeyri-qanuni və etik prinsiplərə zidd istifadəsi hüquqi məsuliyyət yarada bilər və fərdi məxfiliyi təhlükəyə ata bilər.

Digər tərəfdən, kibertəhlükəsizlik mütəxəssisləri bu alətlərdən müdafiə məqsədilə istifadə edərək potensial hücum vektorlarını müəyyənləşdirir və qabaqlayıcı tədbirlər görürlər. Aşağıda "OSINT" sahəsində ən çox istifadə edilən alətlər və onların tətbiq sahələri haqqında ətraflı məlumat təqdim edilir.

Alət	İstifadə məqsədi	Link
Google dorking	Qabaqcıl Google axtarış operatorları ilə məxfi məlumatların tapılması	Google advanced search
Shodan.io	Şəbəkəyə açıq cihazların və açıq portların tapılması	Shodan.io
theHarvester	E-poçt, domen və IP məlumatlarını toplamaq	Github repository
Maltego	Qrafik əsaslı OSINT analiz aləti	Maltego
SpiderFoot	Avtomatlaşdırılmış OSINT analizləri	Spiderfoot
ExifTool	Şəkillərin metadata analiz edilməsi	Exiftool github
Have i been pwned?	E-poçt və şifrələrin sızıb-sızmadığını yoxlamaq	Have i been pwned

Google dorking[145]

Google dorking, Google axtarış operatorlarından istifadə edərək internetdə açıq qalmış həssas məlumatları tapmaq üçün istifadə olunan texnikadır. Bu metod vasitəsilə səhvən açıq qoyulmuş sənədlər, giriş panelləri, e-poçt ünvanları və digər məxfi məlumatlar aşkar edilə bilər.

Praktiki təcrübə: Google dorking ilə məlumat axtarışı

1. **Sayt daxili spesifik sənədlərin tapılması:**

- "filetype:pdf site:example.com" - example.com domenində açıq olan PDF sənədləri göstərir.
- "filetype:xls site:gov.az" - Azərbaycan hökumətinə aid açıq Excel sənədlərini tapmaq üçün istifadə edilə bilər.

2. **Admin panellərin aşkarlanması:**

- "intitle:'Admin Login' inurl:admin" - İdarəçi panelləri tapmaq üçün axtarış edir.
- "inurl:login site:edu.az" - edu.az domenində açıq giriş səhifələrini aşkar etmək üçün istifadə edilə bilər.

3. **Şifrələrin və konfiqurasiya fayllarının tapılması:**

- "ext:log | ext:cfg password" - Açıq qalmış loq və konfiqurasiya fayllarında şifrə axtarmaq üçün istifadə olunur.
- "ext:sql intext:'password'" - SQL fayllarında şifrə ehtiva edən məlumatları axtarmaq üçün istifadə edilə bilər.

[145] www.google.com/advanced_search

Shodan.io[146]

Shodan, internetə açıq olan cihazları (kameralar, serverlər, routerlər, IoT cihazları) analiz edən və onların zəifliklərini ortaya çıxaran axtarış sistemidir.

Praktiki təcrübə: Shodan ilə açıq cihazların tapılması

1. **Açıq IP və portları skan etmək:**

- "country:AZ" - Azərbaycanda açıq olan IP-ləri və xidmətləri tapır.
- "port:22" - Açıq SSH serverlərini aşkarlayır.
- "port:3389" - Açıq remote desktop protokolu (RDP) xidmətlərini göstərir.

2. **Zəifliklərin aşkarlanması:**

- "product:Apache version:2.4.49" - Apache serverinin zəif versiyalarını tapmaq üçün istifadə edilir.
- "vuln:CVE-2021-34527" - Məlum təhlükəsizlik boşluqlarını daşıyan sistemləri tapır.

3. **Açıq IP kameraların tapılması:**

- "inurl:/view/view.shtml" - Açıq IP kameraları göstərir.

theHarvester[147]

theHarvester açıq mənbələrdən (Google, Bing, LinkedIn, Shodan və s.) e-poçt ünvanları, subdomenlər və IP ünvanları toplamaq üçün istifadə edilir.

Praktiki təcrübə: Shodan ilə açıq cihazların tapılması

1. **Bir domenə aid açıq e-poçt ünvanlarını tapmaq:**

- theHarvester - d example.com - l 500 - b google - example.com domeninə aid açıq e-poçt ünvanlarını Google üzərindən toplamaq üçün istifadə edilir.

2. **Shodan və LinkedIn üzərindən məlumat toplamaq:**

- theHarvester - d example.com - b shodan - example.com domeninə aid IP ünvanlarını Shodan üzərindən əldə etmək üçün istifadə edilir.

3. **Subdomenlər və açıq serverlərin tapılması:**

- theHarvester - d example.com - b bing - example.com domeninə aid alt domenləri Bing üzərindən tapmaq üçün istifadə edilir.

Maltego[148]

Maltego qrafik analiz vasitəsidir və OSINT məlumatlarını vizual şəkildə təqdim etməyə kömək edir. Bu alət şəxslər, təşkilatlar, domenlər, IP ünvanları və sosial media məlumatlarını birləşdirərək kompleks əlaqələr yaradır.

Praktiki Təcrübə: Maltego ilə əlaqələrin xəritələnməsi

1. **Bir şəxsin sosial media fəaliyyətini analiz etmək:**

- Maltego interfeysində "Twitter Transform" modulunu aktivləşdirərək bir şəxsin Twitter fəaliyyəti analiz edilə bilər.

2. **Bir şirkətin subdomenlərini və DNS qeydlərini tapmaq:**

[146] www.shodan.io/
[147] GitHub Repository
[148] www.maltego.com/

- example.com domenini Maltego üzərində analiz edərək DNS qeydləri, subdomenlər və əlaqəli təşkilatlar vizuallaşdırıla bilər.

3. **Bir hədəfin e-poçt və telefon əlaqələrini təyin etmək:**

- Bir e-poçt ünvanı üzərində analiz aparılaraq həmin e-poçtla əlaqəli domenlər və sosial media profilləri tapıla bilər.

SpiderFoot[149]

SpiderFoot avtomatlaşdırılmış OSINT analiz vasitəsidir. Bu alət e-poçt ünvanları, IP ünvanları, subdomenlər, zəifliklər və digər məlumatları birləşdirərək təhlil etməyə imkan verir.

Praktiki Təcrübə: SpiderFoot ilə analiz aparmaq

1. **Bir domen haqqında məlumat toplamaq:**

- piderfoot - m sfp_dns,sfp_whois,sfp_shodan - t example.com - example.com domeni haqqında DNS, WHOIS və Shodan məlumatlarını toplayır.

2. **İP və açıq portları analiz etmək:**

- SpiderFoot interfeysi vasitəsilə bir təşkilatın şəbəkəsinə bağlı açıq portları və IP ünvanlarını analiz etmək mümkündür.

ExifTool[150]

ExifTool şəkillərin metadata məlumatlarını analiz etməyə imkan verir. Bu alət vasitəsilə bir şəkilin hansı cihazla çəkildiyi, GPS koordinatları və digər kritik məlumatlar əldə edilə bilər.

Praktiki Təcrübə: ExifTool ilə metadata analiz etmək

1. **Şəkil faylından metadata çıxarmaq:**

- exiftool image.jpg - image.jpg faylının metadatasını göstərir.

2. **GPS məlumatlarını aşkar etmək:**

- exiftool - gpslatitude - gpslongitude image.jpg - Şəkilin GPS koordinatlarını göstərir.

3. **Şəkil tarixini və cihaz modelini tapmaq:**

- exiftool - datetimeoriginal -model image.jpg - Şəkilin çəkilmə tarixini və istifadə olunan kameranı göstərir.

Have i been pwned?[151]

Bu alət e-poçt ünvanlarının və şifrələrin hansı sızmaların qurbanı olduğunu yoxlamaq üçün istifadə olunur.

Praktiki Təcrübə: E-poçt təhlükəsizliyini yoxlamaq

1. **E-poçt ünvanının sızıb-sızmadığını yoxlamaq:**

- Have i been pwned? saytına daxil olaraq e-poçt ünvanınızı yoxlaya bilərsiniz.

2. **Parolun təhlükəsizliyini yoxlamaq:**

[149] github.com/smicallef/spiderfoot
[150] exiftool.org/
[151] haveibeenpwned.com/

- "https://haveibeenpwned.com/Passwords" səhifəsində istifadə olunan parolun əvvəllər sızıb-sızmadığını öyrənmək mümkündür.

OSINT alətləri açıq mənbələrdən məlumat toplamaq və analiz etmək üçün geniş imkanlar yaradır. Google dorking, shodan, theharvester, maltego, spiderfoot, exiftool və have i been pwned? kimi vasitələr kiberkəşfiyyat, təhlükəsizlik auditi, hüquq-mühafizə və sosial mühəndislik hücumları üçün istifadə edilə bilər.

Bu alətlər arasında Google dorking internetdə açıq qalmış məlumatları tapmağa imkan verir, Shodan internetə qoşulmuş cihazların açıq portlarını və zəifliklərini aşkarlayır, theHarvester isə e-poçt ünvanları və subdomenlər üzrə məlumat toplamağa kömək edir. Maltego və SpiderFoot OSINT məlumatlarını strukturlaşdırılmış şəkildə təqdim edərək əlaqələri vizuallaşdırmağa imkan verir. ExifTool multimediaların metadata analizini aparır və Have I Been Pwned? vasitəsilə istifadəçilər parollarının sızıb-sızmadığını yoxlaya bilərlər.

Nəticə

Açıq mənbə kəşfiyyatı müasir dövrdə informasiya toplama və təhlil etmənin əsas vasitələrindən birinə çevrilmişdir. OSINT-in tətbiq dairəsi olduqca genişdir və bu metod hüquq-mühafizə orqanları, jurnalistlər, kibertəhlükəsizlik mütəxəssisləri, biznes analitikləri və tədqiqatçılar tərəfindən qanuni və etik çərçivədə istifadə olunduğu kimi, kibercinayətkarlar və sosial mühəndislər tərəfindən də müxtəlif məqsədlərlə istifadə edilə bilər.

Sosial mühəndislik hücumları OSINT məlumatlarına əsaslanaraq daha hədəflənmiş və effektiv olur. “Phishing”, “pretexting”, “tailgating”, “doxxing”, “watering” hole attack kimi hücum texnikaları açıq mənbələrdən toplanan bilgilər sayəsində daha inandırıcı və təhlükəli hala gətirilir. Məhz bu səbəbdən fərdi və korporativ təhlükəsizliyin qorunması üçün OSINT texnikalarının necə işlədiyini bilmək, onların qarşısını almaq üçün qabaqlayıcı tədbirlər görmək həyati əhəmiyyət daşıyır.

Bu mühazirədə OSINT metodlarının əsas mərhələləri - məlumat toplama, təhlil və emal, profil çıxarma və istifadəyə hazırlıq kimi fundamental aspektlər geniş şəkildə araşdırıldı. İnternet resursları, sənədlər və fayllar, şəkillər və videolar, məlumat bazarları, texniki kəşfiyyat və insan kəşfiyyatı kimi əsas məlumat mənbələri izah edildi və hər bir mənbənin OSINT prosesində oynadığı rol açıqlandı.

Bundan əlavə, “Google Dorking”, “Shodan”, “theHarvester”, “Maltego”, “SpiderFoot”, “ExifTool” və “Have I Been Pwned?” kimi OSINT alətləri praktiki nümunələrlə izah edildi. Bu alətlərin hər biri xüsusi məqsədlərə xidmət edir və məlumat toplama, zəiflik aşkarlama, kiberkəşfiyyat və sosial mühəndislik hücumlarının qarşısının alınması üçün istifadə edilə bilər.

OSINT yalnız hücum edən şəxslərin deyil, həm də müdafiə və təhlükəsizlik sahəsində çalışan mütəxəssislərin əlində güclü bir vasitədir. Hücum edən şəxslər OSINT vasitəsilə qurban haqqında kritik bilgiləri əldə edərək onları manipulyasiya etməyə çalışdıqları halda, kibertəhlükəsizlik mütəxəssisləri və hüquq-mühafizə orqanları bu

bilgilərdən potensial təhlükələri müəyyənləşdirmək və qorunma strategiyaları hazırlamaq üçün istifadə edirlər.

Buna görə də, fərdi şəxslər və təşkilatlar şəxsi və həssas məlumatlarını internetdə açıq şəkildə paylaşmaqdan çəkinməli, məlumat məxfiliyini qorumaq üçün qabaqlayıcı addımlar atmalı və OSINT metodları ilə özlərinə qarşı edilə biləcək hücumları əvvəlcədən təxmin etməlidirlər.

OSINT istifadə edilərkən hüquqi və etik çərçivələrə ciddi şəkildə riayət olunmalıdır. Hər hansı bir açıq mənbədən məlumat toplamaq qanuni olsa da, bu məlumatların hansı məqsədlə və necə istifadə edildiyi kritik əhəmiyyət daşıyır. Qanunsuz OSINT istifadəsi məxfilik pozuntularına, şəxsiyyət oğurluğuna və digər hüquqi məsuliyyətlərə səbəb ola bilər. Xüsusilə, GDPR (General Data Protection Regulation), Budapeşt Konvensiyası və yerli qanunvericilik aktları OSINT-in etik və qanuni istifadəsinə dair əsas qaydaları müəyyən edir.

Bu baxımdan, OSINT təkcə bir hücum aləti deyil, eyni zamanda müdafiə və təhlükəsizliyin təmin edilməsi üçün mühüm bir vasitədir. Bu biliklərdən düzgün istifadə edildikdə, fərdlər və təşkilatlar sosial mühəndislik hücumlarından qoruna bilər, riskləri qiymətləndirə bilər və kibertəhlükəsizlik strategiyalarını gücləndirə bilərlər.

OSINT bu gün və gələcəkdə informasiya təhlükəsizliyinin ən mühüm komponentlərindən biri olaraq qalacaqdır. Açıq mənbələrdən əldə edilən məlumatlar düzgün analiz edildikdə və effektiv şəkildə tətbiq edildikdə, OSINT kibertəhlükəsizlik, hüquq-mühafizə, istintaq və biznes analitikası sahələrində böyük imkanlar yaradır.

Buna görə də, OSINT metodlarını öyrənmək və onlardan həm fərdi, həm də təşkilati səviyyədə müdafiə məqsədilə istifadə etmək kibertəhlükəsizliyin və informasiya məxfiliyinin qorunması baxımından həyati əhəmiyyət daşıyır.

Tövsiyə olunan ədəbiyyatların siyahısı:

I.Normativ-hüquqi aktlar

1. Azərbaycan Respublikasının Konstitusiyası. 12 noyabr 1995-ci il
2. "Kibercinayətkarlıq haqqında" 23 noyabr 2001-ci il tarixli Budapeşt Konvensiyası
3. "Kibercinayətkarlıq haqqında" Konvensiyanın Təsdiq edilməsi barədə Azərbaycan Respublikasının 30 sentyabr 2009-cu il tarixli Qanunu.
4. BMT-nin "Ümumdünya insan hüquqları bəyannaməsi". 10 dekabr 1948-ci il.
5. eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32013L0040&qid=1740071905447
6. eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679&qid=1740071983553
7. eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014R0910&qid=1740072041400
8. Azərbaycan Respublikasının Cinayət məcəlləsi. 30 dekabr 1999-cu il. e-qanun.az/framework/46947
9. "Fərdi məlumatlar haqqında" 11 may 2010-cu il tarixli Azərbaycan Respublikasının Qanunu. e-qanun.az/framework/19675
10. "Azərbaycan Respublikasının Rəqəmsal İnkişaf və Nəqliyyat Nazirliyi yanında Elektron Təhlükəsizlik Xidmətinin fəaliyyətinin təmin edilməsi haqqında" Azərbaycan Respublikası Prezidentinin 05 mart 2013-cü il tarixli Fərmanı. e-qanun.az/framework/25375
11. "Elektron imza və elektron sənəd haqqında" 09 mart 2004-cü il tarixli Azərbaycan Respublikasının Qanunu. e-qanun.az/framework/5916
12. "İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında" 03 aprel 1998-ci il tarixli Azərbaycan Respublikasının Qanunu. e-qanun.az/framework/3525
13. Telekommunikasiya haqqında" 14 iyun 2005-ci il tarixli Azərbaycan Respublikasının Qanunu. e-qanun.az/framework/10663
14. "Dövlət sirri haqqında" 07 sentyabr 2004-cü il tarixli Azərbaycan Respublikasının Qanunu. e-qanun.az/framework/5526
15. "Elektron ticarət haqqında" 10 may 2005-ci il tarixli Azərbaycan Respublikasının Qanunu. e-qanun.az/framework/10406

II. Elmi məqalələr

1. Sosial mühədislik nədir? / Qlobal internetin təhlükəsizliyi - Emin Muhammadi
2. Hall of fame: Captain Crunch - Jochen Kressin
3. Top 10 best and most famous hackers in the world - Ellis Steward
4. Sosial şəbəkələrdə təhlükəsizlik problemlər - Şıxəliyev R.H.
5. Finance worker pays out $25 million after video call with deepfake 'chief financial officer' - Heather Chen, Kathleen Magramo
6. What is spear phishing? - Matthew Kosinski
7. Baiting in social engineering: how hackers trick you & staying safe - M.Salman Nadeem
8. What is a quid pro quo attack & how to avoid becoming a victim - Tyler Therpsiri
9. Sosial mühəndislik hücumları - Tacir Alıyev
10. Sosial mühəndislik hücumlarının psixoloji aspektləri: manipulyasiya üsullarının təhlili - Ranar Ramazanov
11. Sosial mühəndislik nədir? - İlqar Şabanov
12. Социальная инженерия в информационной и кибербезопасности - Олег Антипов
13. Как работает соци-альная инженерия - Алексей Малахов

14. What is pretexting? Definition, examples, and attacks - Josh Fruhlinger
15. What is spear phishing? - Matthew Kosinski
16. What is Tailgating? - Isabel Leckie
17. What is dumpster diving? - Gavin Wright
18. "İnformasiya təhlükəsizliyinin müasir problemləri və həlli metodlarının qiymətləndirilməsi" - Amin Şıxəlizadə
19. How to avoid spam filters: 15 proven ways - Bernard Meyer
20. Saxta e-poçtu necə tanımaq olar: sizə kömək edəcək 7 məsləhət - Pavel Jelic
21. Is there a yelp for ransomware? - Matt Freeman
22. How fraudsters are getting fake articles onto Facebook - Jane Wakefield
23. U.S. Department of labor website discovered hacked, spreading poisonIvy - Kelly Jackson
24. CCleaner APT Attack: a technical look inside - Priyanka Aash
25. Beware the China honey traps of LinkedIn - Alistair Nicholas

III. Tövsiyyə olunan xarici ədəbiyyatlar

1. The art of deception: controlling the human element of security - Kevin D. Mitnick, William L. Simon
2. Social engineering: understanding and auditing - Global information assurance certification paper - Chris Jones, 2003
3. Social engineering: the science of human hacking - Christopher Hadnagy
4. "Sosyal mühendislik ve oltalama saldırılarını anlamak: derinlemesine bir analiz" - Ceren Çubukçu Çerasi
5. Social engineering: The art of human hacking - Christopher Hadnagy
6. Influence: the psychology of persuasion - Cialdini, R. B
7. Human hacking: win friends, influence people, and leave them better off for having met you - Christopher Hadnagy, Seth Schulman
8. Thinking, fast and slow - Daniel Kahneman

IV. İstifadə olunan İnternet resursları

1. Sosial mühəndislik nədir? - cybersign.az/xeber/xeber_1
2. Holistic definition & meaning - www.merriam-webster.com/dictionary/holistic
3. Kevin Mitnick - https://en.wikipedia.org/wiki/Kevin_Mitnick
4. YouTube - The first internet worm (Morris Worm) - Computerphile
5. Advanced persistent threats (qabaqcıl davamlı təhdid qrupları) - cert.az/news/2024/etx-advanced-persistent-threats
6. Business email compromise (BEC) Nedir? BEC saldırıları nasıl engellenir? - uzmanposta.com/blog/bec/
7. Phishing (oltalama) nedir? Phishing saldırısı nasıl engellenir? - uzmanposta.com/blog/phishing-nedir/
8. Smishing nedir ve nasıl korunulur? - www.kaspersky.com.tr/resource-center/threats/what-is-smishing-and-how-to-defend-against-it
9. What is a watering hole attack? - www.fortinet.com/resources/cyberglossary/watering-hole-attack
10. Website and email spoofing - www.cloudflare.com/ru-ru/learning/ssl/what-is-domain-spoofing/
11. Man in the middle (MITM) attack - www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/

12. Credential stuffing vs. brute force attacks - www.cloudflare.com/ru-ru/learning/bots/what-is-credential-stuffing/
13. Pretexting definition - www.imperva.com/learn/application-security/pretexting/
14. Tailgating hücumu nədir? - cybersign.az/xeber/tailgating-hucumu-nedir
15. Dumpster diving - it.ufl.edu/security/learn-security/social-engineering/dumpster-diving/
16. Sosial mühəndislik hücum texnikası nədir?! - cert.az/news/2019/sosial-muhendislik-texnikasi-nedir
17. Sosial mühəndislik nüfuz testləri - allsafe.az/bizim-xidmetler/nufuzetme-sinaqlari/sosial-muhendislik-nufuz-testleri/
18. The social-engineer framework - www.social-engineer.org/framework/general-discussion
19. Veri güvenliği saldırıları: Sosyal mühendislik ve korunma yöntemleri - www.garantibbva.com.tr/blog/sosyal-muhendislik-saldirilari
20. Bridgeport, Connecticut awarded close to half a million for port security - www.securitymagazine.com/articles/93254-bridgeport-connecticut-awarded-close-to-half-a-million-for-port-security
21. What is OSINT? - www.sentinelone.com/cybersecurity-101/threat-intelligence/open-source-intelligence-osint
22. What is Quid Pro Quo discrimination? - www.pelagohealth.com/resources/hr-glossary/quid-pro-quo
23. What is Baiting in Cyber Security? - www.terranovasecurity.com/blog/what-is-baiting
24. Fişinq-kiberdələduzluq texnikası - www.cert.az/news/2017/fisinq-kiberdeleduzluq-texnikasi
25. Shoulder surfing (computer security) - en.wikipedia.org/wiki/Shoulder_surfing_%28computer
26. "Watering hole" hücumu nədir? - www.cybersign.az/xeber/watering-hole-hucumu-nedir
27. Honey trapping - en.wikipedia.org/wiki/Honey_trapping
28. Scareware - en.wikipedia.org/wiki/Scareware
29. What You Need To Know About Social Media Hijacking - www.vcnbfamily.bank/Why-VCNB/VCNB-Blog/what-you-need-to-know-about-social-media-hijacking
30. What Is Reverse Social Engineering? And How Does It Work? - https://aware.eccouncil.org/what-is-reverse-social-engineering.html
31. Sosial mühəndislik haqda nələri bilirik ?! - cert.gov.az/az/news/sosial-muhendislik-haqda-neleri-bilirik?
32. Sosial mühəndislik hücum texnikası nədir?! - cert.az/news/2019/sosial-muhendislik-texnikasi-nedir?
33. Social Engineering - www.imperva.com/learn/application-security/social-engineering-attack/
34. Məlumat itkisinin qarşısının alınması üzrə ən yaxşı vərdişlər - www.pitsdatarecovery.az/ways-to-prevent-data-loss/
35. ATT&CK matrix for enterprise - attack.mitre.org/
36. Data protection - commission.europa.eu/law/law-topic/data-protection_en
37. Avoiding social engineering and phishing attacks - www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks
38. workspace.google.com/
39. support.microsoft.com/sr-latn-rs/office/microsoft-365-advanced-protection-82e72640-39be-4dc7-8efd-740fb289123a
40. www.barracuda.com/products/email-protection/secure-email-gateway
41. umbrella.cisco.com/
42. developers.cloudflare.com/cloudflare-one/policies/gateway/initial-setup/dns/
43. safebrowsing.google.com/
44. learn.microsoft.com/en-us/windows/security/operating-system-security/virus-and-threat-protection/microsoft-defender-smartscreen/
45. apps.apple.com/us/app/google-authenticator/id388497605

46. www.microsoft.com/ru-ru/security/mobile-authenticator-app
47. www.yubico.com/
48. store.google.com/regionpicker?hl=en-US
49. www.proofpoint.com/us/products/email-security-and-protection/email-protection
50. www.mimecast.com/products/email-security/
51. haveibeenpwned.com/
52. spycloud.com/
53. cybelangel.com/
54. support.apple.com/en-us/102381
55. www.microsoft.com/en-us/windows/tips/windows-hello
56. en.wikipedia.org/wiki/Principle_of_least_privilege
57. en.wikipedia.org/wiki/Role-based_access_control
58. en.wikipedia.org/wiki/Security_operations_center
59. en.wikipedia.org/wiki/Security_information_and_event_management
60. www.ic3.gov/
61. consumer.ftc.gov/consumer-alerts/2021/01/scammers-cash-covid-19-vaccination-confusion
62. support.apple.com/en-us/HT208165
63. www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/business-email-compromise
64. www.cognyte.com/blog/2021-linkedin-breach-cybercriminals-are-the-new-headhunters/
65. Worst cyber attack on US military came via flash drive - phys.org/news/2010-08-worst-cyber-military.html
66. Major sites including New York Times and BBC hit by 'ransomware' malvertising - www.theguardian.com/technology/2016/mar/16/major-sites-new-york-times-bbc-ransomware-malvertising
67. Google docs phishing campaign - www.cisa.gov/news-events/alerts/2017/05/04/google-docs-phishing-campaign
68. 2014 Sony Pictures hack - en.wikipedia.org/wiki/2014_Sony_Pictures_hack
69. PayPal account holders warned about phishing - www.actionfraud.police.uk/alert/paypal-account-holders-warned-about-phishing
70. The phishing email that hacked the account of John Podesta - www.cbsnews.com/news/the-phishing-email-that-hacked-the-account-of-john-podesta/
71. Tech Firm Ubiquiti Suffers $46M Cyberheist - krebsonsecurity.com/2015/08/tech-firm-ubiquiti-suffers-46m-cyberheist/
72. Facebook and Google were conned out of $100m in phishing scheme - www.theguardian.com/technology/2017/apr/28/facebook-google-conned-100m-phishing-scheme
73. en.wikipedia.org/wiki/Jeff_Dean
74. Google hack attack was ultra sophisticated, new details show - www.wired.com/2010/01/operation-aurora/
75. en.wikipedia.org/wiki/Mata_Hari
76. Laptop from operation ghost stories - www.fbi.gov/history/artifacts/laptop-from-operation-ghost-storieswww.fbi.gov/history/artifacts/laptop-from-operation-ghost-stories
77. The rise of fake anti-virus - security.googleblog.com/2010/04/rise-of-fake-anti-virus.html
78. FTC and florida charge tech support operation with tricking consumers into paying millions for bogus services - www.ftc.gov/news-events/news/press-releases/2016/07/ftc-florida-charge-tech-support-operation-tricking-consumers-paying-millions-bogus-services
79. The Covid-19 hoax scareware - www.sonicwall.com/blog/the-covid-19-hoax-scareware
80. Recogniza the warning signs - www.americanexpress.com/us/security-center/phishing-scam-awareness/
81. Hackers compromise AP Twitter account - apnews.com/general-news-68a43f18c9aa4a87bfbf350a566404c9

82. Mark Zuckerberg hacked on Twitter and Pinterest - www.theguardian.com/technology/2016/jun/06/mark-zuckerberg-hacked-on-twitter-and-pinterest
83. Burger King Twitter account hacked to look like McDonald's - abcnews.go.com/blogs/technology/2013/02/burger-king-twitter-account-hacked-to-look-like-mcdonalds
84. www.secretservice.gov/press/releases/2004/10/us-secret-services-operation-firewall-nets-28-arrests-international
85. www.fbi.gov/news/stories/alphabay-takedown
86. www.justice.gov/usao-sdca/pr/fbi-s-encrypted-phone-platform-infiltrated-hundreds-criminal-syndicates-result-massive
87. www.europol.europa.eu/media-press/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation
88. www.fbi.gov/news/stories/playpen-creator-sentenced-to-30-years
89. osintframework.com/
90. ntrepidcorp.com/managed-attribution/defining-active-vs-passive-osint/
91. What is OSINT (Open Source Intelligence)? - www.sentinelone.com/cybersecurity-101/threat-intelligence/open-source-intelligence-osint/
92. OSINT & Psychology: profiling and behavioral analysis through open source intelligence - goldenowl.medium.com/osint-psychology-profiling-and-behavioral-analysis-through-open-source-intelligence
93. www.carahsoft.com/learn/vertical/osint
94. What is Google hacking/dorking? - www.imperva.com/learn/application-security/google-dorking-hacking/
95. www.shodan.io/
96. censys.com/
97. www.google.com/advanced_search
98. www.shodan.io/
99. GitHub repository
100. www.maltego.com/
101. github.com/smicallef/spiderfoot
102. exiftool.org/
103. haveibeenpwned.com/