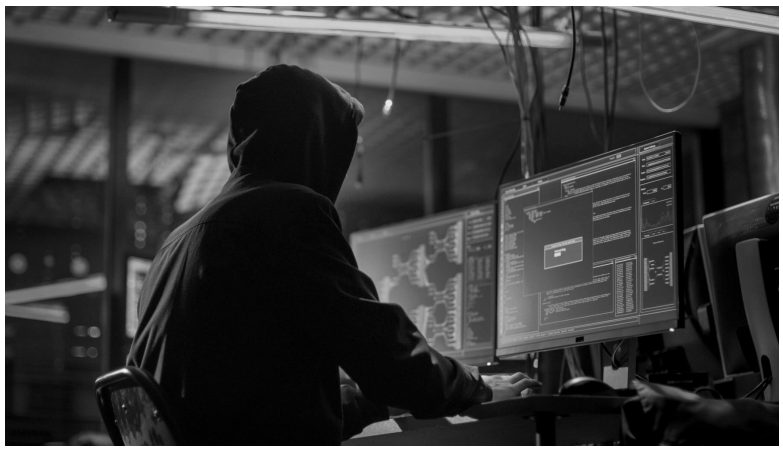
facebook QARABAĞ AZƏRBAYCANDIR! Ses Media Holding səs 16 sentyabr 2021-ci il

Kiber terrorizm - GÜNÜN PROBLEMİ

Yaşadığımız texnoloji çağ kiber riskləri və kiber təhdidləri ilə aktualdır. Pis niyyətli hakerlər olaraq bilinən qara şapka hakerləri və ya haker qrupları hökumətlər, qurumlar, xəstəxanalar və ya kafelər kimi bir çox quruma və ya təşkilata zərər verə bilər.



Viruslar, trojan və ya buna bənzər zərərli kodlarla həyata keçirilən və ümumiyyətlə planlaşdırılan bu zərərli davranışlara kiber hücumlar deyirik. Son illərdəki kiber hücumları araşdırdığımızda pul, şantaj və ya siyasi səbəblərdən oğurluq hadisələrinə qədər çox məqsədlə həyata keçirildiyini görə bilərik. Kiber hücumların bir məqsədi ola bilsə də, hücumların heç bir məqsəd olmadan təşkil olunduğunun da şahidi oluruq.

Bəs kiber-hücum nədir?

Kiber-hücum - kiber-insident yaratmaq üçün informasiya sistemlərinə qarşı kiber-silahın və ya kiber-silah kimi istifadə edilə bilən sistemin qəsdən istifadəsidir. Kompüterlərdə və kompüter şəbəkələrində hücum, aktivin icazəsiz istifadəsi, dəyişdirilməsi, aradan qaldırılması, məhv edilməsi, oğurlanması və ya əldə edilməsi üçün edilən hər hansı bir cəhddir. Dövlətlər arasında kiber hücumlar baş verdikdə, bu proses "Kiber müharibə" olaraq təyin edilir. Dövlətlərarası cəsusluq, gizli sənədlərin oğurlanması və casusluq kimi bir çox sahədə kiber hücumlar son illərdə artdı və dövlətlər üçün böyük maddi və mənəvi problemlərə səbəb oldu.

Kiber-hücumlarının növləri hansılardır?

- Hədəf sistemin təhlükəsizliyini keçərək məlumatları kopyalamaq
- Açıq mikrofon/kamera dinləmək
- "Network scanning" dediyimiz şəbəkə axtarışı ilə sistemə sızmaq
- Hədəf sistemdəki bütün istifadə edilə bilən servisləri sıradan çıxarmaq (Denial of Service)
- Hədəflənən şəbəkənin bütün internet servislərini məhv etmək
- Kripto hücumlar ilə şifrələri sındırmaq
- IP gizlətmə və başqa IP-ə keçmək (IP Masquerading)
- İki şəbəkə arasına sızaraq dinləmək və məlumat oğurlamaq (MITM)
- Aldatmaq-Yemləmək (Phishing)

Kiber təhlükəsizlik mütəxəssisləri tərəfindən aparılan araşdırmalara görə, kiber təcavüzkarların ələ keçirdikləri sistemlərdə ortalama 200 gün müddətində aşkar edilmədikləri ortaya çıxdı. Bir sözlə, lazımi təhlükəsizlik tədbirlərini görməmisinizsə, hücuma məruz qalmış ola bilərsiniz. Qurumların və şirkətlərin şəbəkə və sistem infrastrukturları araşdırıldıqda, əksəriyyətinin lazımi qoruma sisteminə sahib olmadığını asanlıqla deyə bilərik. Təhlükəsizliyə gəldikdə investisiya əvvəlcə ağla gəldiyindən təəssüf ki, bir çox qurum və şirkət kiber hücumlardan xəbərdar deyil və təhlükəsizlik tədbirləri görmədikləri üçün bu cür kiber hücumlara məruz qala bilərlər.

Ölkəmiz kiber hücumların ən çox edildiyi ölkələr arasındadır. Dünya ortalamalarına baxdığımızda, kiber hücumlara məruz qalan və ya kiber təhdidlərə ev sahibliyi edən ölkələr arasındadır. Ən çox məruz qaldığımız kiber hücumları aşağıdakı kimi sadalamaq olar.

Şantaj edənlər: Şantaj və ya hədə-qorxu üsulu ilə hücumlar ümumiyyətlə qurumlara və ya şirkətlərə qarşı həyata keçirilir. Burada məqsəd hədəf sistemin zəif tərəflərindən istifadə etmək və içindəki məlumatları ələ keçirmək və şifrələyərək oxunmaz hala gətirməkdir. Hədəflərinə çatan kiber təcavüzkarlar hücum etdikləri qurumla əlaqə qurur və oxunmayan göstərdikləri məlumatların kilidini açmaq üçün pul tələb edirlər. Adətən saxta e-poçtla istifadəçilərə göndərilən bu tip hücumda, istifadəçiyə saxta faktura şəklində çatdırılır.

"Phishing" hücumları; Kimlik ovu adlanan "phishing" hücumları, qarşı tərəfin tamamilə aldatmasına əsaslanan bir üsul olaraq qarşılaşır. Bu hücumun məqsədi hədəf alan şəxsin parollarını və istifadəçi hesablarını tutmaqdır. Kiber-hücum uğurlu olduqda, qarşı tərəfin parolları tutula bilər, bank hesabları boşaldılır və korporativ şəbəkəyə lazımi giriş əldə edilə bilər. Kiber təcavüzkarlar ümumiyyətlə istifadəçiləri bu bankların adlarını bir bankdan və ya bir qurumdan göndərilmiş kimi hazırladıqları saxta e-poçtlarla istifadə edərək hazırlanan saxta saytlara yönləndirirlər. Bu tip hücumlarda, istifadəçiləri ümumiyyətlə istedadlı olduqları və tələyə yönəldikləri tələlər cəlb edir. Hazırlanan saxta saytlar ümumiyyətlə orijinal sayta çox oxşayan bir istifadəçi interfeysi ilə gəlir. Təbii olaraq, istifadəçilər fərqi anlamırlar və sonunda bir hədiyyə olduğunu düşünürlər və tələyə düşürlər.

Dünyada ən çox baş verən kiber-hücum növləri

İnternet rabitə dizaynındakı zəifliklər, idarəetmə çatışmazlığı, internetin işləməsini təmin edən açıq və şifrələnməmiş sistemlər, zərərli proqram təminatlarının paylanması qabiliyyəti və proqramdakı səhvlər və s. kimi problemlər üzündən fərqli kiber hücumlara məruz qala bilərik. Əlbətdə ki, kiber hakerlərin təzahürləri və ya siyasi hücumları bütün dünyaya olduğu kimi bir çox quruma təsir edi. Keçən ilin hücumlarını nəzərdən keçirdiyimiz zaman "GitHub"-un internet tarixindəki ən böyük kiber-hücumuna məruz qaldığını görürük. "GitHub" hücum zamanı saniyədə 1.35 terabit məlumatla qarşılaşdı və xidmət ümumilikdə 10 dəqiqə ərzində əlçatmaz hala gətirildi. Bənzər bir hücum 2017-ci ildə ABŞ-ı hədəf almış və kütləvi bir kiber-hücum həyata keçirilmiş və ABŞ-a təxminən 7 milyard dollar zərər vermişdi. "Spotify", "Netflix", "WhatsApp", "Amazon", "PlayStation Network", "The Verge"və "The New York Times" kimi məşhur veb saytları da daxil olmaqla bir çox qlobal şirkət bu hücumdan zərər gördü. Dünyaya baxdığımızda şifrələmə viruslarının, kiber-hücumlarının ön plana çıxdığını görürük.

SİA mövzu ilə bağlı **İKT üzrə ekspert Rəşad Cəfərovun fikirlərini öyrənib:** "İstər sosial şəbəkələr üzərindən kiber dələduzluq, istərsə də iş fəaliyyətimizdə kiber hücumlara son zamanlar daha tez-tez rast gəlirik. Düşünürəm ki, bu kimi hallar nəinki azalacaq, hətta günü-gündən daha da artacaq. Çıxış yolu bu kimi hallarla mübarizə aparmaq, önləyici tədbirlər görməkdir: "Artıq bir neçə ildir ki, ardıcıl olaraq ölkəmizdə kibertəhlükəsizliklə bağlı tədbirlər keçirilməkdədir. Əlbəttə ki, bu tədbirlər maarifləndirmə baxımından çox vacibdir. Ölkəmizdə kibertəhlükəsizliyə cavabdeh olan qurumlar mövcuddur. Qurumlar kiberhücumlara qarşı birgə fəaliyyət göstərməlidir. Hətta deyərdim ki, dövlətlər birgə mübarizə aparmalıdır. Kibertəhlükəsizliyin etibarlı təmin edilməsi üçün maraqlı tərəflərin - dövlətin, özəl sektorun və vətəndaşların tərəfdaşlığını və əməkdaşlığı vacibdir. Bu, tək dövlətin, tək özəl sektorun, ya da tək vətəndaşın bacaracağı məsələ deyil. Bütün ölkələr kibertəhlükəsizlik sahəsində beynəlxalq əməkdaşlığın vacibliyini etiraf etsələr də, çox təəssüf hələ ki, ciddi addımları görmək olmur".

Rəşad Cəfərov fikirlərinə davam edərək həmçinin qeyd edib ki, vətəndaşlar arasında maarifləndirməyə böyük ehtiyac var: "Hər bir vətəndaş kibertəhlükəsizliklə bağlı yetərincə məlumatlı olmalıdır. Bunu artıq zaman tələb edir. Hər kəs fərdi məlumatlarını necə qorumalıdır, kiber dələduzları necə müəyyən edə bilər və sair bu kimi məsələlərdə ayıq olmalıdır. Ən azından emalinə gələn məktubları analiz etmək, təhlükəli görünən fayllardan, saytlardan uzaq durmaq, antivirus proqramlarından istifadə etmək qismən sizin kibertəhlükəsizliyinizi təmin edə bilər. Ümumilikdə isə kibertəhlükəsizliklə vətəndaş, özəl qurumlar, dövlət, hətta dövlətlər birgə mübarizə aparmalıdır. Əks halda bu sahədə təhlükəsiz mühit yaratmaq mümkün olmayacaq. Kibertəhlükəsizliyin təmin edilməsi ümumi işdir".

Mövzu ilə bağlı **sosioloq Elçin Bayramlı fikirlərini bölüşüb:** "Ölkəmizdə kiber-hücumlar lap əvvəldən yayılıb. İnternetin, sosial şəbəkələrin inkişafı ilə bağlı bu işlərlə məşğul olan xarici xüsusi xidmət orqanları və yaxud da fırıldaqçı biznes xarakterli şirkətlər quruluşlar bundan istifadə etməyə çalışırlar. Burada iki amil var. Bəzi ölkələrin ictimai, siyasi, sosial əhəmiyyətli nüfuzlu şəxslərin ələ keçirmək, onları şantaj yolu ilə pul almaq məqsədi güdürlər. Təbii ki, bu bir mənəvi, psixoloji terrordur. İnsan hüquqlarına, informasiya gizliliyi məsələlərinə müdaxilədir. Bu məsələnin qarşısı alınmalıdır. Çünki insanın şəxsi əlaqələri, yazışmaları istənilən motivdə olursa olsun başqaları tərəfindən icazəsiz paylaşıla bilməz. Bununla bağlı təbii ki, müvafiq tədbirlər görülməlidir. Məhkəməyə müraciət edərək texnik üsullarla aşkar etmək mümkündür. Bu cür tələlərə düşənlər məlumatsızlıqdan qaynaqlanır. Onlar elə bilirlər ki, şəxsi danışıqlarını, yazışmalarını, videolarını başqa heç kim görə bilməz. Onların müasir informasiya texnologiyalarından, casus proqramlarından məlumatları yoxdur. Yaxşı olardı ki, ümumiyyətlə sosial şəbəkələrdə, messengerlərdə tanış olmayan insanlarla, xüsusilə də xarici ölkələrdən olan əcnəbilərlə münasibət saxlamaq lazım deyil.

Bundan əlavə günümüzdə maliyyə-bank fırıldaqları da baş verir. İnsanları müəyyən kampaniyalarda, sorğularda iştirak etməyə sövq etməklə onların lazımi məlumatlarını əldə edirlər. Həmin əldə olunan məlumatlardan müxtəlif şirkətlər özlərinə sərf etdiyi şəkildə istifadə edirlər. Ona görə də informasiya təhlükəsizliyi ilə bağlı cəmiyyətimizdə məlumat azdır. Bu barədə maarifləndirmə işləri aparılmalıdır".

Kiber-hücumlardan necə qorunmalıyıq?

1. Antivirus işlətmək.

Artıq bir çox antiviruslarda bank şifrələrinin qorunmasından təhlükəsizlik divarına qədər (Firewall) bir çox funksiyalar var. Bu səbəbdən komputerinizdə hətta mobil telefonuzda təhlükəsizliyi təmin etmək üçün ilk növbədə antiviruslardan istifadə etməlisiniz.

2. Əməliyyat sisteminin Təhlükəsizlik Divarini deaktiv etməyin (Windows Firewall)

Bir çox istifadəçi təhlükəsizlik divarını deaktiv edərək əməliyyat sistemini elə istifadə edir. Bu bir başa cihazınızı kiber təhlükələrə qarşı qorunmasız qoymaqdır. Bu təhlükəsizlik divarı arxa planda işləyən servisləri analiz edərək bilinməyən servislərin internetə çıxışını qadağan edir.

3. Modem və ya Router-inizin sistemini yeniləyin

Şəbəkə ilə əlaqə quran cihazların da sistemləri var və bu sistemlərin də müəyyən açıqları ola bilir. Məsələn "Tp-link" cihazlarda tapılan son açıq ilə şəbəkəyə qoşularaq komputerə müdaxilə etmək mümkün idi. Şirkət tərəfindən yayımlanan yeni sistemlə bu açıq bağlandı. Ona görə də modem və router aldığınızda rəsmi saytına giriş edərək ən sonuncu sistemi yükləyib quraşdırın. Bu sizin kiber təhlükəsizliyini müəyyən dərəcədə təmin edir.

4. Təhlükəli görünən saytlardan,tətbiqlərdən və fayllardan uzaq durun.

Əgər, yuxarıda dediyimiz variantları istifadə etmirsinizsə daha da diqqətli olmaq məcburiyyətindəsiniz. Saytlar vasitəsilə "adaware" tipli viruslar, fayllardan virus və troyanlar, tətbiqlərdən isə virus və soxulcanlar yoluxa bilər. Ona görə girdiyiniz saytlara daha diqqətli olmalısınız, həmçinin hər faylı da yükləmək olmaz.

5. Gələn E-mailləri diqqətli analiz edin.

Son illərdə yemləmə (Phishing) üsulundan ən çox e-maillərdə istifadə olunur. "Apple", "Microsoft" kimi şirkətlərin adından istifadə edərək kiber cinayətkarlar yalan məlumatların olduğu e-maillər ilə istifadəçiləri aldadırlar. Ona görə də e-mailləri cavablamadan öncə göndərən mail adresinə diqqətlə baxın.

Arzu Qurbanzadə