Kibertəhlükəsizlik:

Ətraf mühit analizi və önləyici mexanizmlər

Kibertəhlükəsizlik:

Ətraf mühit analizi və önləyici mexanizmlər

Müəlliflər: Davit Şavqulidze və Giorgi Qurgenidze

Gürcü dilindən Azərbaycan dilinə tərcümə və redaktə: Ramilia Əliyeva

2023 il

Dərslik haqqında

Qarşıda duran dərslik qeyri-sahibkar (qeyri-kommersiya) hüquqi şəxs «Gürcüstanın Strategiya və İnkişaf Mərkəzi»nin sifarişi ilə qeyri-sahibkar (qeyri-kommersiya) hüquqi şəxs «Gürcüstanın İnformasiya və Texnologiyaların Analiz Mərkəzi» (GITAC) tərəfindən hazırlanıb.

Layihə «Cəmiyyət üçün informasiyalı mövzular» – ABŞ səfirliyinin Demokratiya Komisiyasının kiçik qrantlar proqramının dəstəyi ilə həyata keçirilir. Proqramın məqsədi Gürcüstanda milli azlıqlar və məcburi köçkün olan şəxslərlin sıx məskunlaşdığı regionlarda (Sameqrelo, Samtsxe-Cavaxeti, Kvemo Kartli, Şida Kartli) yaşayan cəmiyyətin kiber və dezinformasiya tərkibli təhlükələrə qarşı dayanıqlığını gücləndirməkdir.

Dərsliyin hazırlanması zamanı ictimai şəkildə açıq olan, kommersiya tərkibli olmayan ədəbiyyatdan istifadə edilib. Dərsliyin əsas metodoloji bazasını təqdim edir:

- ABŞ-ın Kiber Təhlükəsizlik və Kritik İnfrastruktur Agentliyinin (US CISA) dərslikləri;
- ABŞ-ın Standartlar və Texnologiyalar Milli İnstitutunun (US NIST) dərslikləri;
- Böyük Britaniyanın Milli Kiber Təhlükəsizlik Mərkəzinin (UK NCSC) dərslikləri;
- Kanada Kiber Təhlüksəzilik Mərkəzinin (Canadian Centre for Cybersecurity) dərslikləri;
- Avropa Şurasının (CoE) dərslikləri;

Dərsliyin hazırlanması zamanı həmçinin Gürcüstanın informasiya və fərdi göstəricilərin müdafiəsi haqqında qüvvədə olan qanunvericilik istifadə edildi.

Dərslikdə verilən kiber təhlükəsizliyin nəzarəti və məsləhətlər kiber risklərin azalmasını və təhlükələrin idarəsini təmin edir. Vacibdir ki dərslik hər növ kiber hücumdan özünü müdafiə üçün zəmanət vermir, lakin aşağıda qeyd edilən addımlar təhlükə şansını əhəmiyyətli dərəcədə azaldacaq ki, siz, sizin biznesiniz və ya təşkilatınız kiber cinayətin qurbanı olmasın.

Gürcüstanın Strategiya və İnkişaf Mərkəzi (GCSD)

Gürcüstanın Strategiya və İnkişaf Mərkəzi (GCSD) qərəzsiz və neytral qeyri-hökümət təşkilatıdır. Təşkilatın dəyərlər bərabərlik, insanın azadlığı, ləyaqəti, hesabat cavabdehliyi və şəffaflıq prinsiplərinə əsaslanır. Mərkəzin əsas məqsədləri: Gürcüstanın milli təhlükəsizliyinin təmin edilməsinə dəstək; Ölkənin effektli və demokratik idarə prinsiplərinin möhkəmlənməsi; Ölkənin Avropa və Avro-Atlantik inteqrasiyasına dəstək və ölkənin dayanıqlı inkişaf şəraitinin yaradılması.

Detallı məlumat üçün baxa bilərsiniz:
https://www.gcsd.org.ge/ge

Mündəricat

Kibertəhlükəsizlik:
Ətraf mühit analizi və önləyici mexanizmlər

Terminlərin izah

Kiber təhlükəsizlik - İnformasiyanın məxfiliyi, vahidliyi və əlçatanlığının təminatı prosesi ilə özünü göstərən, şəbəkələrin, cihazların və göstəricilərin qanunsuz hərəkətlərdən, əlçatanlıqdan və ya kriminal istifadədən müdafiəsidir.

Məxfilik - Göstəricilərə yalnız bu məlumatın lazım olduğu şəxsin əlçatanlığını təmin edir. Məsələn, əgər siz internetdə informasiya yerləşdirsəniz o daim mövcud olacaq.

Vahidlik - Göstəciliərin dəqiqliyini və tamlığını təmin edir. Misal üçün, modifikasiya edilmiş / təhrif edilmiş göstəricilərin bu informasiyanın lazım olduğu şəxslər üçün dəyəri yoxdur.

Əlçatanlıq - İnformasiyanın istənilən zaman, bu informasiyanın lazım olduğu hər kəsə əlçatanlığını təmin edir. Məsələn, sürətli və güvənli əlaqə, kompüter sistemlərinin daha effektli işləməsinə yardım edir.

Sensitiv məlumat - İtirilməsi, sui-istifadəsi, modifikasiyası və ya avtorizə edilməmiş giriş, fərdin məxfiliyinə, rifahına, biznesin ticarət sirlərinə, yaxud milli təhlükəsizlik və beynəlxalq əlaqələrə mənfi təsir göstərə biləcək məlumat.

Fərdi göstəricilər - Şəxsin identifikasiyası mümkün olduğu hər növ məlumat. Məsələn: sizin adınız, soyadınız, şəxsi nömrəniz, fotonuz, video yazısı, elektron poçtun ünvanı, bank hesabı nomrəsi, sosial

şəbəkə hesabınız, şəxsi yazışma. Həmçinin sizin iş yeriniz, gəliriniz, ailə vəziyyətiniz və s. kimi informasiya da fərdi göstəricidir.

Xüsusi kateqoriyalı fərdi göstəricilər - Şəxsin irqi və ya etnik mənşəyi, siyasi baxışı, dini və ya fəlsəfi inamı, peşə ittifaqı üzvlüyü, sağlamlıq vəziyyəti, cinsi həyatı, məhkumluğu, inzibati məhkumluq, qarşısını alma tədbirinin tətbiq olunması, prosesual razılaşma, uzaqlaşdırılma, cinayət qurbanı kimi və ya zərərçəkmiş kimi tanınmaq ilə əlaqəli məlumatdır.

Biometrik və genetik göstəricilər - Biometrik və genetik əlamətlərlə fiziki şəxsin identifikasiya imkanını verən xüsusi kateqoriyalı fərdi göstəricilər.

Misinformation (yanlış məlumat) - Qəsdən zərər vermə niyyəti olmadan paylaşılan yanlış məlumat.

Disinformation (dezinformasiya) - Qəsdən zərər vermə niyyəti ilə paylaşılan yanlış məlumat.

Malinfromation (zərərli məlumat) - Qəsdən zərər vermə niyyəti ilə paylaşılan etibarlı məlumat.

Zərərli kod (Malware) - Casus proqram (Spyware), qəsbçi proqram (Ransomware), viruslar (Virus) və qurdlardan (Worm) ibarət olan zərərli proqram olaraq müəyyənləşdirilir.

Qəsbçi proqram (Ransomware) - Məbləğ ödənilməsinə qədər, kompüter sisteminə daxil olmanın bloklanması məqsədilə yaradılmış zərərli proqram təmin etmə növü.

Sosial mühəndislik - Hücumçunun kompüter sisteminə nəzarət əldə

etmək, şəxsi və ya maliyyə məlumatını oğurlamaq üçün qurbanın manipulasiyası, ona təsir etmə və aldatma taktikasıdır. Sosial mühəndislik psixoloji manipulasiyadan istifadə edir ki, hücumçu sensitiv məlumata giriş əldə etsin və ya qurbanı təhlükəsizlik qaydalarını / normalarını pozmasına məcbur etsin.

Fişinq - Etibarlı subyekt kimi görünmək məqsədilə elektron poçt, SMS yazılı mesjalar və ya telefonla sensitiv məlumatın - istifadəçi adlarının, parolların və kredit kartı detallarının əldə edilməsi prosesi fişinq adlanır.

Vişinq (Vishing) - Səsli kommunikasiyadan istifadə edən sosial mühəndislik növü.

Smişinq (Smishing) - SMS və ya yazılı mesajlardan istifadə edən sosial mühəndislik növü

Denial of Service, Distributed Denial of Service - Servisin söndürülməsi (Denial of Service) kiber hücumun sahələrindən biridir. Servisin söndürülməsi zamanı hücumçu çox saylı tələbi yaratmaq yolu ilə şəbəkəni və ya kompüter sistemini yükləyir, bununla kompüter legitim tələblərə cavab verə bilmir. Servisin bölüşdürülmüş söndürülməsi (Disturbed Denial of Service) də həmin məqsədə xidmət edir, lakin bu zaman hücumu bir deyil, (çox sayda müxtəlif kompüterlərin iştirakı ilə) kompüter şəbəkəsi həyata keçirir.

Man-in-the-middle - Hücum, haker tərəfindən iki subyekt arasındakı kominikasiyaya müdaxilə kimi tanınır. Bu hücumçuya (hakerə) tərəflər arasında mübadilə edilən məlumatı oxumağa və əldə etməyə imkan verir.

Kiber gigiyena - Sizə onlayn mühitdə müdafiəli olmanıza yardım edəcək təkrarlanmış və ümumi təcrübə.

Zəiflik - İnformasiya sistemində, sistemin təhlükəsizlik prosedurlarında daxili nəzarət və implementasiyada üçüncü tərəfin (threat source) yarada və ya istifadə edə biləcəyi zəiflik.

Proqram patçı (patch) - İnstalasiya zamanı, proqram təminatının digər komponentləri ilə, versiya nömrəsi və ya müvafiq proqram komponentinin buraxılış detallarının dəyişilməsi olmadan, faylları və ya cihazın parametrlərini birbaşa dəyişən, proqram təminatı komponenti.

Çoxfaktorlu autentifikasiya - İki və ya daha çox faktorun istifadəsi ilə autentifikasiya prosesi. Faktorlar ibarətdir: (I) Bildiyiniz (məs., şifrə/fərdi identifikasiya nömrəsi (PIN)); (II) Olanınız (məs., kriptoqrafik identifikasiya cihazı, token); Yaxud (III) insana aid olan nəsə (məs., biometrik göstəricilər)

Şifrələmə - Aşkar edilməsinin və ya istifadəsinin qarşısının alınması üçün göstəricilərin ilkin anlamını gizlədən, göstəricilərin kriptoqrafik transformasiyası, sözdə «adi mətndən», sözdə «şifrəli mətnə» transformaisyası. Əgər transformasiya geri çevrilə biləndirsə müvafiq çevrilmə prosesi «deşifrələmə» adlanır. Bu şifrələnmiş göstəriciləri ilkin vəziyyətdə bərpa edən transformasiyadır.

Ehtiyyat nüsxələri - Lazım olduğu halda bərpa etməni asanlaşdırmaq üçün yaradılan fayl və proqramların nüsxəsi.

Router - İki şəbəkə arasında göndərişləri ötürən komunikasiya cihazı.

1. Kiber təhlükəsizliyin ümumi prinsipləri

1.1. Kiber təhlükəsizlik nədir?

Kiber təhlükəsizlik şəbəkələrin, cihazların və göstəricilərin qanunsuz hərəkətlərdən, giriş imkanından və ya kriminal istifadədən müdafiəsini təqdim edir. Bu məlumatın məxfililiyinin, vahidlik və əlçatanlığının təminatı prosesi ilə biruzə olur. Sizin şəxsi məlumatınızın böyük hissəsi sizin kompüterinizdə, smartfon və ya planşetdə saxlanır. Sizin məlumatlarınızı necə müdafiə etməyinizi bilməniz tək fərdlər üçün deyil, həmçinin təşkilatlar üçün də vacibdir. Hər dəfə internetdən istifadə edərkən siz təhlükəsizliklə əlaqəli seçim qarşısında dururusunuz. Sizin və dövlətin təhlükəsizliyi onlayn mühitdə cavabdehli qərarlardan asılıdır. Təhlükəsiz internet üçün bizim hər birimizin öz kiber cavabdehliyimizi anlamamız mütləqdir.

İzahda qeyd olunduğu kimi kiber təhlükəsizliyin məqsədi məxfiliyin, vahidlik və əlçatanlığın təmin edilməsidir.

- **Məxfilik** – Göstəricilərin, yalnız bu informasiyaya gərəkliyi olanlara əlçatanlığını təmin edir. Məsələn, əgər siz internetdə məlumat

yerləşdirsəniz, o həmişə mövcud olacaq.

- ¬ **Vahidlik –** Göstəricilərin dəqiqlik və tamlığını təmin edir. Misal üçün, modifikasiyalaşdırılmış / təhrif edilmiş göstəricilərin, bu göstəricilərin lazım olduğu şəxslər üçün dəyəri yoxdur.
- ¬ **Əlçatanlıq –** İstənilən zaman lazım olduğu insanlara infromasiyanın əlçatanlığını təmin edir.

1.2. Təhlükələr

1.2.1. Zərərli kod

Casus proqram (Spyware), qəsbçi proqram (Ransomware), viruslar (Virus) və qurdlardan (Worm) ibarət olunan zərərli proqram olaraq müəyyənləşdirilir. Zərərli proqram istifadəçinin elektron poçtun zərərli əlavəsinə və ya linkinə basdığı zaman hərəktə düşə bilər. Bu da istifadəçinin kompüter sistemində proqram təminatının yüklənməsinə səbəb olur. Bəzi zərərli proqram bacara bilir:

- ¬ Ödəniş alma məqsədilə (ransomware) kompüter şəbəkəsinin kritik komponentlərinə girişi məhdudlaşdırsın.
- ¬ Yeni, əlavə zərərli proqram təminatını yükləsin.
- ¬ Sərt diskdən gizli olaraq informasiya oğurlasın (casus proqramı – spyware).
- ¬ Kompüter sisteminin ayrı-ayrı komponentlərini məhv və istifadəyə yararsız etsin.

1.2.2. Şəxsiyyət oğurluğu və saxtakarlıqlar

Şəxsiyyətin oğurlanması (identity theft) və saxtakarlıqlar cinayətdir. Onların qurbanı hətta kompüteri heç vaxt istifadə etməyən insan belə ola bilər. Bir çox yol mövcuddur ki, kriminallar sizin məlumatınıza giriş tapa, sizin elektron cüzdanınızı oğurlaya, sizin telefon danışmanızı dinləyə, sizin hesab nömrəsi olan atılan səndi götürə bilsin.

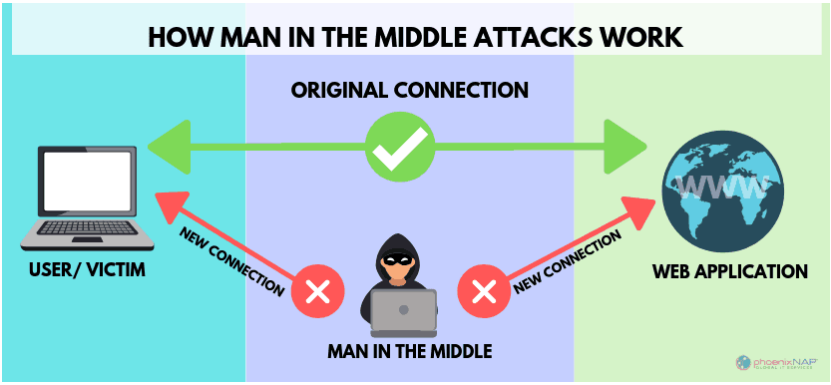
1.2.3. Denial of Service

Xidmətdən imtina (Denial of Service) kiber hücumun sahələrindən biridir. Bu zaman hücumçu çox saylı tələb yaratmaq yolu ilə şəbəkəni və ya kompüter sistemini həddindən artıq yükləyəcək, bununla o, legitim tələblərə cavab verə bilməyəcək. Paylanmış xidmətdən imtina (Disturbed Denial of Service – DDOS) də həmin məqsədə xidmət edir, lakin belə halda hücumu bir deyil, kompüter şəbəkəsi (çox sayda müxtəlif kompüterlərin iştirakı ilə) həyata keçirir. Oxşar hücumlar başqa məqsədə də xidmət edə bilər. Kiber hücumçu şəbəkənin nasaz olduğu müddəti effektli şəkildə istifadə edə və sonraki hücumları başlaya bilər.

Bununla yanaşı diqqət ediləsidir ki, DDOS hücumunun bir növü olan botnet mövcuddur. Bu vaxt hücumçular (hakerlər) milyonlarla haking olunmuş cihazdan istifadə edə bilərlər. Botnetləri çox vaxt hədəf sistemlərə hücm edən və onların imkanlarını ağırlaşdırmaq istəyən zombi sistemlər kimi də adlandırırlar. Botnet dünyanın müxtəif bucaqlarında yerləşə bilər, bu da ona nəzarət etməni çətinləşdirir.

1.2.4. Men-in-the-Middle

Hücum haker tərəfindən iki subyekt arasındakı kommunikasiyaya müdaxilə kimi tanınır. Bu hücumçuya (hakerə) tərəflər arasında mübadilə edilən məlumatı oxumağa və əldə etməyə imkan verir. Ziyarətçilər müdafiəsiz (şifrəsi olmayan) ictimai Wi-Fi şəbəkəsinə qoşulduqları zaman MITM hücumları daha çox olur.



1.2.5. Phishing

Etibarlı subyekt kimi görünmək məqsədilə elektron poçt, SMS mesjalar və ya telefonla sensitiv məlumatın – istifadəçi adlarının, parolların və kredit kartı detallarının əldə edilməsi prosesi fişinq adlanır. Fişinq hücumu zamanı, hücum edən təcililik maraq və ya qorxu hissini yaradır. Fişinq mesaj qurbanı sensitiv məlumat verməyə, zərərli veb-səhifələrin linklərinə basmağa və ya zərərli proqramlardan ibarət olan əlavələri açmağa sürükləyir.

1.2.6. Şifrənin qırılması (Password Cracking)

Kiber hücumçu istifadəçinin şifrəsini ələ keçirsə çox saylı məlumatı asanlıqla əldə etmə imkanı qazana bilər. Şifrənin qırılmsının müxtəlif növləri mövcuddur.

- **Seçmək (brute force attack) –** Haker sadəcə olaraq istifadəçinin şifrəsini ipuçlar əsasında tapa bilir (məsələn, doğum tarixi, itin adı və s.). Lakin seçim hücumu daha mükəmməl və çətin ola bilər. Məsələn, bir çox insan müxtəlif sistemlər üçün eyni şifrədən istifadə edir. Bəzi şifrə onlayn qırılmış (sızmış) saytlar bazasında əlçatan ola bilər və müvafiq olaraq haker sizin sızmış parolunuzu digər sistemləri qırmaq üçün istifadə edə bilər.
- **Lüğət hücumu (Dictionary attack) –** Lüğət hücumu, seçim hücumunun biraz daha mükəmməlləşmiş misalıdır. O, avtomatlaşdırlmış prosesdən istifadə edir. Nə zaman ki, hücumçu sizin şifrənizi istifadə olunmuş şifrələr və ifadələr siyahısı əsasında (məsələn, bir çox istifadəçi sonrakı şifrələrdən istifadə edir: 123456, qwerty, password və s.) tapmağa çalışır. Lüğətlərin əksəriyyəti ən çox yayılan şifrələr və sözlər birləşmələrindən ibarətdir. İnsanlar çox zaman şifrə kimi bir qayda olaraq sözlər şəklində olan, yadda qalan ifadələri istifadə edirlər. Sistemlərin insanlardan çox simvollu şifrələri istifadə etməyə çağırmasının əsas səbəbi də elə budur.

1.3. Müdafiə mexanizmləri – Kiber Gigiyena

1.3.1. Kiber gigiyenanı rutininizin hissəsi edin.

Sizin kiber təhlükəsizliyinin nizamlı monitorinqi kiber təhlükələrinin baş verməsi riskini azaldır. Hər bir vərdişdə olduğu kimi kiber gigiyenada rutin və təkrarlanmanı tələb edir. Kiber gigiyena prosesini «xatırlatmanı» (Reminder) qurmaq və ya təqvimdə tarixləri qeyd etməklə başlayın ki, sizi cihazınızla əlaqəli bir sıra məsələləri həll edəsiniz – anti-virus proqram təminatı ilə virusları skan etmək, sizin bütün cihazlarınızın operativ sistemini yeniləmək, təhlükəsizlik patçlarını yoxlamaq, sərt diski silmək və sizin şifrələrinizi dəyişmək.

1.3.2. Kiber gigiyena üçün əsas addımlar

Kiber gigiyena sizə onlayn mühitdə müdafiəli olmanıza yardım edəcək ümumi təcrübədir. Qarşıda duran sənəddə dörd əsas addımdan ibarət olan kiber gigiyenanın ən yaxşı təcrübə misalları müzakirə edilir.

Addım 1: Etibarlı anti-virus proqram təminatını yükləyin (install edin).

İlk və ola bilsin ki, ən əsas addım anti-virus proqramının install edilməsidir. Nə üçün yaradılıb? Anti-virus proqramnı kompüter viruslarını və ya zərərli proqramları skan edən və tapan proqram və ya proqramlar vahidliyidir. Məhz, anti-virus proqramı təmin edir:

- Tərkibində zərərli kod (proqram) olan faylları tapmanı.

- ¬ Avtomatik skan etmə planlaşdırmasını və yerinə yetirməni.
- ¬ Sizin konkret gərəkliyinizdən irəli gələrək, bir konkret faylı, bütün kompüterinizi, yaxud fleş drayvın skan edilməsini.
- ¬ Zərərli kodları və proqram təminatlarının silinməsini.

Addım 2: Şəbəkənin firewall-unu (qoruyucu divar) istifadə edin.

Şəbəkənin firewall-unu istifadə etmək kiber gigiyenanı qoruyub-saxlamaq üçün daha bir əsas addımdır. Firewall şəbəkə təhlükəsizliyində müdafiənin birinci xəttidir. Autorizə edilməmiş istifadəçilərin sizin veb-səhifələrinizə el-poçtunuzun serverlərinə və girişi internetdən mümkün olan digər məlumat mənbələrinə əlçatanlıqlarına maneə olur.

Addım 3: Müntəzəm olaraq proqram təminatını yeniləyin.

Müntəzəm olaraq sizin aplikasiyalarınızı, veb-brauzerlərinizi və operativ sistemlərinizi yeniləyin ki, təhlükəsizlik xətaları (zəifliklər) aradan qaldırlan və ya düzəldilən yeni proqramlarla işləmənizdə əmin olasınız. Bu yenilənmələr xüsusilə vacibdir, çünki onlarda çox vaxt proqram təminatı patçları (patch) var. Proqram təminatı developerləri (aplikasiya yaradan şirkətlər), hücumçu hakerlərin sistemlərə daxil olmaq üçün istifadə etdikləri proqram təminatı xətalarını aşkar etdikləri zaman, təhlükəsizlik patçlarını buraxırlar / dərc edirlər.

Addım 4: Güclü şifrələrdən istifadə edin.

Güclü şifrələrin istifadə edilməsi sizin bütün cihazlarınız üçün mütləqdir. Sizin şifrəniz unikal və çətin olmalıdır. Rəqəmlərdən, simvollardan, böyük və eləcə də, kiçik hərflərlə bərabər ən azı 12 simvoldan ibarət olmalıdır. Şifrənizi müntəzəm olaraq dəyişməniz (paylaşama və ya yenidən istifadəsi deyil) sizi hakerlərdən qoruyur.

Addım 5: Çoxfaktorlu autentifikasiya istifadə edin.

İkifaktorlu və ya çoxfaktorlu autentifikasiya sizə müdafiənin əlavə imkanını verən ən yaxşı təcrübədir. İkifaktorlu autenifikasiya bir qayda olaraq sizin şifrə və istifadəçi adınızın mobil telefonunuza göndərilən unikal kodla bərabər təqdim edilməsini tələb edir. Çoxfaktorlu autentifikasiya biometriyanın istifadəsi ilə təhlükəsizliyin, üzü və ya barmaq izini tanımaq kimi əlavə laylarını artırır ki, hakerlər üçün sizin cihazınıza və şəxsi məlumatınıza hücumu çətinləşdirsin.

Addım 6: Cihaz şifrələnməsini tətbiq edin.

Əksər şirkətlərin avtomatik olaraq məlumatların şifrələnmə funksiyası olduğuna baxmayaraq, həmçinin, sizə, daxilində sensitiv məlumatlarınız olan cihazlarınızın – leptopların, tabletlərin, smartfonların, disklərin, ehtiyyat fayllarının, bulud hovuzunun (cloud) və digər medya daşıyıcılarınızın (məsələn, USB flash drive) şifrələnməsi lazım ola bilər. Çox vaxt, bir çox cihaz smartfonlarda saxlanılan məlumatlar üçün standart

xüsusiyyət kimi şifrələməni istifadə edir. Bəzi aplikasiya tam şifrələməni istifadə edir, başqa xidmətlər isə sizin cihazlarınızda mövcud olan məlumatları şfirələyir və buludda (cloud-da) onların ehtiyyat nüsxələrini yaradır. Sizin sensitiv göstəricilərinizi müdafiə etmək üçün, əlavə variant olaraq şifrələnmiş USB yaddaş diskinin istifadə edilməsidir.

Addım 7: Müntəzəm olaraq ehtiyyat nüsxələrini yaradın

Sizin üçün dəyərli olan faylların ehtiyyat nüsxələrini oflayn, xarici sabit diskdə və ya buludda yaratmanız vacibdir. Qeyd edilən sizə, mühüm fayllarınızı müxtəlif növ məlumat itkisi risklərindən qorumağa kömək edəcək, xüsusən də hakerlərin sizin cihazlarınzdan birinə daxil olma imkanını əldə etdiyi zaman.

Addım 8: Sərt diski təmizləyin

Əgər siz öz leptopunuzu, tabletinizi və ya smartfonunuzu satırsınızsa təhlükəsizlik qaydalarına təmin etməniz vacibdir ki, alıcının əlinə sizin haqqınızda fərdi və ya sensitiv məlumat düşməsin. Əgər sizin cihazınızı qırsalar (daxil olsalar) təmiz sərt disk hücumçularda daha az informasiyanın olması deməkdir. Lakin təkcə faylların və ya göstəricilərin silinməsi yetərli olmaya bilər. Yaxşı kiber gigiyena üçün diskin formatlaşdırılması və sonra diskin təmizlənməsi (wipe out) mütləqdir. Məsələn, onlayn bank üçün istifadə etdiyiniz kompüteri satmaq istəyirsinizsə diskin təmizlənməsi haqqında düşünməlisiniz ki, sizin sərt diskinizdən proqram təminatları və göstəricilər silinsin.

Addım 9: Sizin routerinizi müdafiə edin

Sizin kabelsiz şəbəkənizi müdafiə etməyi unutmayın. Bunun üçün istehsalçıdan qalan ad və şifrəni dəyişməlisiniz. Həmçinin onun quraşdırılmasından sonra distant idarə funksiyasını söndürməniz mütləqdir. Əlavə olaraq əmin olun ki, sizin routeriniz şəbəkə vasitəsilə göndərilən məlumatın məxfiliyinin ən yuksək səviyyəsini qoruyub saxlaması üçün WPA2 və ya WPA3 şifrələməsini təklif edir.

1.4. Kiçik və orta təşkilatlar üçün kibertəhlükəsilik

Qarşıda duran dərslikdə vaxtınıza, pulunuza qənaət etməyə, təşkilatınızın imicini müdafiə etmək üçün sürətli və asan beş addım təqdim edilib. Dərslik hər növ kiber hücumdan özünü müdafiə etmək zəmanəti vermir. Lakin aşağıda göstərilən addımlar təhlükə şansını vacib dərəcədə azaldacaq ki, sizin biznesiniz / təşkilatınız kiber cinayətin qurbanı olmasın.

1.4.1. Addım 1 – Sizin göstəricilərinizin ehtiyyat nüsxəsinin yaradılması

Sizin təşkilatınızın istifadəçinin / vətəndaşların məlumatı, təklifləri, sifarişləri və ödəmə detallar kimi göstəricilərdən nə dərəcədə asılı olduğu haqqında düşünün. İndi isə bu göstəricilər olmadan nə qədər vaxt işləyəcəyinizi təsəvvür edin.

Hər bir biznes və ya təşkilat böyüklüyündən asılı olmayaraq müntəzəm olaraq vacib məlumatın ehtiyyat nüsxələrini hazırlamalıdır və əmin olmalıdır ki, bu ehtiyyat nüsxələri sondur

(up-to-date) və gərək olduğu zaman onların bərpası mümkündür. Bununla siz əmin olacaqsınız ki, təşkilatınız daşqın, yanğın, fiziki ziyan və ya oğruluq hadisələrindən sonra belə işləməyə davam edə biləcək. Bundan başqa sizdə tezliklə bərpa edə biləcəyiniz göstəricilərin ehtiyyat nüsxələri olduğu zaman təşkilatınız qəsbçi hücumlarına (ransomware attacks) qarşı daha az zəif olacaq.

Qarşıda duran başlıqlarda, sizin göstəricilərinizin ehtiyyat nüsxələrini yaratdığınız zaman nəzərə almalı olduğunuz 5 məsləhət verilib.

Məsləhət 1: Sizə hansı göstəricilərin ehtiyyat nüsxələrinin lazım olduğunu müəyyənləşdirin.

İlk addım sizin üçün çox vacib göstəricilərin identifikasiyasıdır. Yəni sizin biznesinizin onlar olmadan işləyə bilməyəcəyi məlumat. Adi olaraq bu sənədləri, fotoları, elektron poçtu, müqavilələr və təqvimləri əhatə edir. Onların əksəriyyəti sizin kompüterinizin, telefonunuzun, tabletinizin və ya şəbəkənin bir neçə adi qovluğunda saxlanılır.

Məsləhət 2: Ehtiyyat nüsxələrini kompüterdən ayırı saxlayın.

Bu istər USB daşıyıcısı, ayrıca disk və ya ayrı kompüter ola bilər. Göstəricilərin ehtiyyat nüsxələrinə giriş elə məhdud olmalıdır ki, onlar:

- Personal üçün əlçatan deyil

- ¬ Mütəmadi olaraq orijinal nüsxəsi olan cihazla əlaqələnmiş (fiziki və ya lokal şəbəkədə) deyil
- ¬ Ransomware (və digər zərərli proqram) çox vaxt avtomatik olaraq birləşmiş olan hovuza keçə bilər. Bu o deməkdir ki, istənilən belə ehtiyyat nüxəsi həmçinin infeksiyaya tutula bilər və bərpa ediləcək ehtiyyat nüsxəsi qalmaya bilər. Daha çox güclülük üçün siz öz ehtiyyat nüsxələrinizin başqa yedə saxlanması haqqında düşünməlisiniz. Belə yanğın və ya oğurluq hər iki nüsxənin itməsinə gətirib çıxarmayacaq. Buna nail olmaq üçün bulud saxlanması qərarları (aşağıda bax.) ekonomik və effektli yoldur.

Məsləhət 3: Bulud hovuzunu müzakirə edin

Siz yəqin artıq gündəlik iş və şəxsi həyatınızda bulud hovuzundan (cloud) istifadə edirsiniz və bunun haqqında heç bilmirsiniz belə. Bir qayda olaraq sizin öz elektron poçt serveriniz yoxdur. Sizin el-poçtanız artıq «buludda» saxlanılır.

Bulud hovuzunun istifadəsi (xidmət provayderi öz infrastrukturunda sizin göstəricilərinizi saxlayır) onu nəzərdə tutur ki, sizin göstəriciləriniz fiziki olaraq sizin yerləştiyiniz yerdən ayrıdır. Belə halda siz eləcə də əlçatanlığın yüksək keyfiyyətindən istifadə edəcəksiniz. Xidmət provayderləri sizin təşkilatınıza göstəricilər və veb xidmətləri elə verə bilərlər ki, sizə bahalı cihazlara evvəlcədən sərmayə qoymaq lazım olmasın. Provayderlərin əksəriyyəti saxlanma mühitinin məhdud miqdarını sizə pulsuz (məsələn, Google Drive 15GB-yadək saxlama yerini pulsuz təklif edir) və daha böyük hovuz həcmini

kiçik biznes üçün minimal xərclərlə təklif edir.

Məsləhət 4: Bulud təhlükəsizliyi təlimatını oxuyun.

Hər xidmət provayderi eyni deyil. Lakin bazar yetərincə yetişib və provayderlərin əksəriyyətinin quraşdırılmış təhlükəsizliyin yaxşı təcrubəsi var. Sizin IT xidmətlərinizin vacib hissələrinin xidmət provayderi üçün verilməsi ilə siz, çox vaxt kiçik və orta böyüklükdə olan təşkilatlar üçün əlçatan olmayan mütəxəssisləşmiş təcrübədən istifadə edəcəksiniz. Lakin xidmət provayderləri ilə əlaqə qurmamışdan əvvəl məsləhət görürük ki, bulutlu təhlükəsizliyin beynəlxalq təcrübəsi ilə tanış olasınız.

Məsləhət 5: Ehtiyyat nüsxəsini yaratmağı sizin gündəlik biznesinizin bir hissəsi edin

Təşkilatlar üçün ehtiyyat nüsxəsini yaratmaq bir elə də maraqlı proses deyil (və həmişə sizin düşüncənizə görə vacib məsələlər var və onlar prioritetli olmalıdır). Lakin şəbəkə və ya buludlu hovuzun qərarlarının əksəriyyəti hazırda imkan verir ki, avtomatik olaraq ehtiyyat nüsxləri yaradasınız. Məsələn, müəyyən növ yeni fayllar qeyd olunan qovluqlarda saxlanıldığı zaman. Avtomatik ehtiyyat nüsxələrinin istifadəsi bir tək vaxtınıza qənaət etməyəcək, həmçinin lazım olduğu təqdirdə sizin faylların ən yeni versiyalarının mövcudluğunu təmin edəcək.

Bir çox ehtiyyat qərarı (back-up solution) asandır və biznes üçün kəskin təhlükəsizlik nəzarətini nəzərə almaqla əlçatandır. Qərarı (proqram təminatını) seçərkən, həmçinin ehtiyyat nüsxəsini yaratmaq üçün nə qədər göstərici lazım olduğunu və istənilən hadisədən sonra göstəricilərə nə dərəcədə sürətlə əlçatanlığınızı nəzərə almalısınız.

1.4.2. Addım 2 – Sizin təşkilatınızın zərərli proqramlardan müdafiə olunması

Zərərli proqram təminatı (həmçinin «zərərli proqram» kimi tanınan) sizin təşkilatınıza zərər verə biləcək proqram təminatı və ya veb kontentdir. Zərərli proqramın ən tanınmış forması viruslar, özünü nüsxələməyi bacaran proqramlardır. Bunlar legitim proqram təminatlarını infeksiya yoluxdururlar.

Qarşıda duran başlıqlar beş təmənnasız və asan həyata keçirilə biləcək məsləhətdən ibarətdir. Bu məsləhətlər sizə yardım edəcək ki, zərərli proqramların təşkilatınıza ziyan verməsinin qarşısını alasınız.

Məsləhət 1: Anti-virus proqramını instal edin və ya qurun

Anti-virus proqramı – çox vaxt tanınmış operativ sistemlərin tərkibində pulsuz olur. Hər bir kompüter və leptopda istifadə olunmalıdır. Sizin ofis təchizatınız üçün «işə salmaya» basaraq bununla proqramı aktivləşdirə bilərsiniz.

Məsləhət 2: İşçilərinizə qadağan olunmuş aplikasiyaları yükləməyi məhdudlaşdırın.

Siz mobil telefonlar və tabletlər üçün aplikasiyaları yalnız istehsalçı tərəfindən təsdiq edilmiş, «marketpleyslərdən» (Google Play və ya Apple App Store kimi) yükləməlisiniz. Burada mövcud olan aplikasiyalar, zərərli proqramlardan müəyyən səviyyəli müdfiəni təmin etmək üçün yoxlanılıb. Siz işçiləriniz tərəfindən güvənli olmayan (üçüncü tərəfin) aplikasiyaları tanılmayan təchizatçılardan yükləməyi məhdudlaşdırın. Təşkilatın işçilərinin hesablarının onların rolunu yetirmək üçün yetərli olacaq əlçatanlığı olmalıdır. Əlavə icazələr (məs., adinistrator hüquqları) yalnız bunun lazım olduğu şəxslərdə olmalıdır. Administrativ hesablar (accounts) yaradılan zaman onlar yalnız bu konkret məqsəd üçün (inzibatlaşdırmaq) istifadə edilməlidir. Standart istifadəçi hesabları isə ümumi iş üçün istifadə edilməlidir.

Məsləhət 3: Sizin IT infrastrukturunuzu yeniləyin (patching)

Əmin olun ki, proqram təminatı sizin IT infrastrukturunuz üçün (məs., tabletlər, smartfonlar, leptoplar və kompüterlər) yaradıcıların, cihaz təhcizatçılarının və satıcıların ən yeni versiyaları ilə yenilənib. Təhlükəsizliyi yaxşılaşdırmaq üçün edə biləcəyiniz ən vacib olan, bu yenilənmələrin (patching kimi tanınan proses) istifadəsidir. Operativ sistemlər, proqramlar, telefonlar və aplikasiyalar «avtomatik yenilənmə» rejimində olmalıdırlar.

Diqqətə almaq lazımdır ki, hər hansısa bir zaman üçün yenilənmələr əlçatan olmayacaq (belə ki, hər bir məhsulun dəstək xidmətinin həyat dövrü var). Bu vaxt siz onun muasir alternativ ilə dəyişilməsini düşünməlisiniz.

Məsləhət 4: USB diskləri və yaddaş kartlarının istifadəsinə nəzarət edin

Təşkilatlar və insanlar arasında faylları bir yerdən digər yerə keçirmək üçün USB disklər və yaddaş kartlarının istifadəsinin nə dərəcədə cəlb edici olduğunu hamımız bilirik. Lakin bir istifadəçi tərəfindən infeksiyaya yoluxmuş USB fleş yaddaş kartının istifadəsi belə yetərlidir ki, bütün təşkilatın məlumatı məhv olsun.

Disklər və fleş yaddaş kartları açıq şəkildə paylaşılan zaman tərkibində nə olduğuna və ya kimin istifadə etdiyinə nəzarət etmək çətindir. Siz infeksiyaya yoluxma (viruslanma) ehtimalını sonrakı yollarla azalda bilərsiniz:

- İstifadəçilərin əksəriyyəti üçün fiziki portlara girişi bloklamaqla
- Anti-virus vasitələrindən istifadə etməklə
- Sadəcə təsdiq olunmuş disklər və kartların, başqa heç bir yerdədeyil, yalnız sizin təşkilatda istifadə olunması icazəsi ilə

Təşkilatınız üçün arzu olunmayan risklərin qarşısını almaq üçün bu göstərişləri sizin təşkilatınızın / şirkətinizin siyasətinin hissəsi edin. Həmçinin işçilərinizdən faylları bir yerdən digər yerə

keçirmələrini USB fleş yaddaş kartı ilə deyil, alternativ vasitələrin (elektron poçt və ya buludlu xidmətlər kimi) istifadəsi ilə etmələrini xahiş edə bilərsiniz.

Məsləhət 5: Sizin firewall-ınızı işə salın.

Firewall-lar sizin öz şəbəkəniz və xarici şəbəkələr (internet kimi) arasında «bufer zona» yaradır. Ən popular operativ sistemlərə artıq firewall daxildir.

1.4.3. Addım 3 – Sizin smartfonlar və tabletlərinizin təhlükəsizliyinin müdafiəsi.

Mobil texnoloqiya hazırda muasir təşkilatın / biznesin mövcud hissəsidir. Bizim göstəricilərin böyük hissəsi tabletlər və smartfonlarda saxlanılır. Daha artıq, bu cihazlar artıq ənənəvi kompüterlər kimi güclüdürlər. Onların çox zaman ofis və ev təhlükəsizliyini buraxdqları üçün onlara daha çox müdafiə lazımdır nə ki, «desktop» cihazlarına.

Bunu nəzərə alaraq qarşıda duran başlıqlarda beş məsləhət verilib. Bunlar sizin mobil cihazlarınız və onlarda saxlanılan məlumatın təhlükəsizliyini qoryub saxlamaqda yardımçı olacaq.

Məsləhət 1: Şifrə ilə müdafiə qurun

Müvafiq olaraq çətin PIN və ya şifrə (sizin sosial medya profillərinizdən öyrənilməsi və ya tapılması mümkün olanlar deyil) orta səviyyəli kriminala sizin telefonunuza giriş tapmaqda

maneə olacaq. Bu gün bir çox cihazın şifrəyə gərək olmadan cihazı bloklamaq üçün barmaq izi tanıma funksiyası var. Lakin bu funksiyalar çox vaxt aktivləşdirilməyib. Buna görə də, bu funksiyanın qurulu olub-olmadığını yoxlayın.

Məsləhət 2: Əmin olun ki, itən və ya oğurlanan cihazların harda olduğunu izləmək, bloklamaq və ya silmək mümkündür

Əməkdaşların tabletləri və ya telefonları itə və ya kimlərsə tərəfindən oğurlana bilər. Xoşbəxtlikdən cihazların əksəriyyətinin sizin cihazların itməsi halında çox dəyərli, əsasən də pulsuz veb alətləri var. Siz onlardan istifadə edə bilərsiniz ki:

- Cihazın olduğu yeri nəzarətdə saxlayasınız
- Cihaza girişi uzaqdan kilidləyəsiniz
- Cihazda saxlanılan məlumatları üzaqdan siləsiniz
- Cihazda saxlanılan məlumatların ehtiyyat nüsxəsini əldə edəsiniz

Təşkilatınızın bütün cihazlarına bu alətlərin qurulması başdan çətin gələ bilər. Lakin mobil cihazların idarəsi proqram təminatının istifadəsi ilə, sadəcə bir kliklə sizin cihazları standart konfiqurasiyaya sala bilərsiniz.

Məsləhət 3: Sizin cihazınızı yeniləyin

Təkilatınızın hansı telefon və ya tabletdən istifadə etməsi vacib deyil. Vacib olan odur ki, onlar həmişə yenilənmiş olsun. Hər bir istehsalçı (Windows, Android, iOS) müntəzəm olaraq, cihazı

müdafiə etmək üçün təhlükəsizliyin kritik funksiyalarından ibarət olan, yenilənmiş versiyaları anons edir. Proses yetərincə sürətli, asan və pulsuzdur. Bu vaxt yaxşı olardı ki, cihaz avtomatik yenilənmə rejimində olsun. Sizin əməkdaşlarınızın qeyd edilən yenilənmələrin nə dərəcədə vacib olduğunu bildiklərindən əmin olun və gərəklik olduğu halda cihaz necə yenilənməli olduğunu izah edin. Müəyyən zamandan sonra yenilənmələr əlçatan olmayacaq (belə ki, cihaz dəstəklənən həyat dövrünün son mərhələsinə çatacaq – end of life). Bu zaman köhnə cihazları müasir alternətivləri ilə dəyişdirməniz mütləqdir.

Məsləhət 4: Aplikasiyalarınızı yeniləyin

Sizin təşkilatınızın cihazlarında mövcud olan operativ sistemlər kimi install olunmuş bütün aplikasiyanı da həmçinin müntəzəm olaraq proqram təminatçı istehsalçısının patçları ilə yenilənməsini etməlisiniz. Bu yenilənmələr yeni funksiyalar əlavə etməklə yanaşı, həmçinin təhlükəsizliklə əlaqədar istənilən maneəni düzəldəcək. İşçilərin cihazları necə və nə vaxt yenilənməli olduqlarını bildiklərinən əmin olun.

Məsləhət 5: Yad Wi-Fi Hotspot-lara qoşulmayın

Açıq Wi-Fi-dan (məsələn, hotel və restoranlarda) istifadə etdiyiniz zaman internetə kimin nəzarət etdiyini araşdırmağın asan yolu mövcud deyil. Əgər siz şəbəkəyə qoşulsanız marağı olan tərəfin girişi ola bilər:

- Şəbəkə qoşulduğunuz zaman nədə işlədiyinizə,

- Sistemdə olduğunuz zaman bir çox aplikasiya və veb xidmətin saxladığı sizin istifadəçi ad və şifrənizə

Ən asan təhlükəsizlik ölçüsü internetdən yad Wi-Fi-a qoşulmaqla istifadə etməməkdir. Təhlükəsizliyin daxildə olduğu öz mobil telefonunuzun 3G və ya 4G mobil şəbəkəsindən istifadə edin. Bu həmçinin o deməkdir ki, siz «tethering» (harada ki, sizin digər cihazlarınız 3G/4G əlaqəsini paylaşırlar) və ya sizin mobil şəbəkənizlə təqdim edilən kabelsiz «dongle» istifadə edə bilərsiniz (məsələn, kabelsiz MiFi modem). Həmçinin virtual şəxsi şəbəkələrdən (VPN) istifadə edə bilərsiniz onlar internetə göndərilənədək sizin göstəricinizi şifrələyəcək. Əgər üçüncü tərəfin VPN-lərini istifadə edirsinizsə provayderin nə dərəcədə güvənli olduğunu yoxlamağınız və onu özünüz konfiqurasiya etməniz mütləqdir.

1.4.4. Addım 4 – Sizin göstəricilərinizi müdafiə etmək üçün şifrələrin istifadəsi

Leptoplar, kompüterlər, tabletlər və smartfonlarda sizin biznesiniz üçün vacib olan çox sayda göstərici var – müştərilərin fərdi məlumatı və sizin giriş hüququnuz olduğu onlayn hesablar haqqında detallar. Bu göstəricilərin sizin üçün əlçatan olması mütləqdir. Lakin autorizə edilməmiş istifadəçilər üçün əlçatan olamamalıdır.

Şifrələr, düzgün tətbiq olunduğu halda autorizə edilməmiş istifadəçilərin sizin cihazlarınıza giriş etmələrinin qarşısının alınmasının pulsuz, asan və effektli yoludur. Qarşıda duran

başlıqlarda şifrələrdən istifadə etdiyiniz zaman yadda saxlamalı olduğunuz beş məsləhət verilib.

Məsləhət 1: Şifrə ilə müdafiəni qurduğunuza əmin olun

Ekranın blok edilmə şifrəsini PIN və ya autentifikasiyanın digər metodunu (barmaq izi və ya üz tanıma ilə blokun açılması) tətbiq edin. Əgər əsasən barmaq izi və ya üz tanımadan istifadə edirsinizsə, şifrəni daha az daxil edəcəksiniz. Buna görə də tapılması çətin olacaq uzun şifrənin tətbiq edilməsi üzrə düşünün.

Şifrə ilə müdafiə təkcə smartfonlar və tabletlər üçün deyil. Sizin ofis təchizatının (həmçinin leptoplar və kompüterlər) güvənli platform modulu (TPM) istifadəsi və ya FileVault macOS-da şifrələmə alətlərini (Windows üçün Bitlocker kimi) istifadə etdiyindən əmin olun. Muasir cihazların əksəriyyətinin özlərində şifrələmə funksiyası var. Lakin şifrələmə üçün yenə də funksiyanın işə salınması və konfiqurasiyası lazım ola bilər.

Məsləhət 2: «Vacib» hesablar üçün iki addımlı təsdiqdən istifadə edin

Funksiynalı mövcud olduğu sizin istənilən hesabınız üçün iki addımlı təsdiqi (2 step verification – 2SV kimi tanınır) istifadə etməyiniz mütləqdir. Qeyd edilən əlavə güc sərf etmədən sizin təhlükəsizliyinizi vacib dərəcədə yaxşılaşdırır. 2SV sizin kimliyinizi «təsdiq etmək» üçün iki fərqli metod tələb edir müvafiq olaraq istədiyiniz sistemə daxil olanadək, bir qayda

olaraq şifrə və daha bir göstəricini daxil etməli olacaqsınız. Bu göstərici sizin smartfonunuza göndərilən kod (yaxud bank kartı oxuyucusu ilə generasiya olunmuş kod) ola bilər, onu şifrə ilə birgə daxil etməlisiniz.

Məsləhət 3: Proqnozlaşdırıla biləcək şifrələrin istifadəsindən boyun qaçırın

Əgər siz təşkilatınızın IT siyasətinə cavabdehsinizsə, şifrələr haqqında məlumatın işçilərə onlar üçün asan anlaşılacaq və başa düşüləcək formada çatdırıldığından əmin olun.

Şifrələr asan yadda saxlanılmalı, lakin başqaları üçün çətin tapıla biləcək olmalıdır. Bununla əlaqəli yaxşı qayda mövcuddur: «Sizi yaxşı tanıyan insanın, sizin şifrənizi 20 cəhddə də tapa bilməyəcəyindən əmin olun». İşçilər həmçinin ən çox yayılmış, kriminalların tapa biləcəyi şifrələri istifadə etməməlidirlər.

Yadınızda saxlayın ki, sizin IT sistemləriniz işi yerinə yetirmək üçün işçilərdən hesabların və ya şifrələrin paylaşılmasını tələb etməməlidir. Hər bir istifadəçinin əvvəlcədən müəyyən edilmiş sistemlərə giriş hüququ olduğundan və verilən giriş hüququnun onların işi yerinə yetirmələri üçün lazım olan səviyyədən ən aşağı (least privilege approach) olduğundan əmin olun. Sizin işçilərinizə lazım olmayan sistemlərə əlavə giriş hüququnu azaldın.

Məsləhət 4: İşçilərinizə «şifrə sıfırlaması» ilə baş gəlməkdə yardım edin

Əgər təşkilatda şifrələrin istifadəsinə cavabdehsinizsə, təşkilatın təhlükəsizliyini yaxşılaşdıracaq bir neçə çıxış yolu mövcuddur. Ən əsası sizin əməkdaşlarınınız, onlarla, işlədilməyən şifrəni yadlarında saxlamağa məcbur olmayacaqlar. İstifadəçinin istifadə etmədiyi xidmətlərdə şifrələrin müntəzəm dəyişilməsi vacib deyil. İstifadəçinin fəal şəkildə istifadə etdiyi sistemlərdə şifrələri dəyişin. Həmçinin nəzərə alın ki, şifrənin ələ keçirildiyinə dair şübhə olduğu zaman, şifrənin dəyişilməsi zərurdir.

Siz həmçinin şifrələr menecerini (şifrələr hovuzunu) tətbiq etməlisiniz ki, işçi vacib hesabların (elektron poçt və bank xidməti kimi) şifrələrini təhlükəsiz olaraq saxlaya bilsin. Bir qayda olaraq işçilər şifrələri tez-tez unudurlar. Buna görə də onların öz şifrələrini asanlıqla dəyişə biləcəklərindən əmin olun.

Məsləhət 5: Varsayılan bütün şifrələri dəyişin

Ən çox yayılan səhvlərdən biri istehsalçının varsayılan şifrələrini (default password) istifadə etməkdir. Smartfonlar, leptoplar və digər növ təchizatlar istehsalçı tərəfindən belə verilir. Cihazların işçilərə verilməsinədək bütün varsayılan parolları dəyişin. Siz həmçinin dəyişməyən varsayılan şifrələri aşkar etmək üçün müntəzəm olaraq cihazları (və proqram təminatını) yoxlamalısınız.

1.4.5. Addım 5 – Fişinq hücumlarının qarşısının alınması

Bir qayda olaraq fişinq hücumu zamanı saxtakarlar minlərlə insana, saxta məktublar göndərirlər və sensitiv məlumat (bank detalları kimi) veriləsini və ya zərərli linkə keçid etməni istəyirlər. Hücumçu sizi pul göndərilməsi və ya sizin hesablarınızın (accounts) detallarını əldə etmək məqsədilə sizi aldatmağa cəhd göstərə bilər. Həmçinin hücumçunun təşkilat haqqında məlumat almaq üçün siyasi və ya ideoloji motivi ola bilər.

Fişinq tərkibli elektron poçtun aşkar edilməsi daha da çətinləşir. Sizin təşkilatınız / biznesiniz necə olursa olsun hansısa zaman, yenə də fişinq hücumu qurbanı olur. Qarşıda duran başlıq sizə ən çox yayaılan fişinq hücumlarını identifikasiya etmək üçün yardım edəcək.

Məsləhət 1: Başarılı hücumların təsirini azaltmaq üçün hesablar konfiqurasiya edin.

Siz «minimal üstünlük» prinsipini istifadə etməklə sizin işçilərin hesablarını əvvəlcədən konfiqurasiya edin. Bu o deməkdir ki, işçilərə onların işini yerinə yetirmək üçün yetərli olacaq istifadəçi hüquqlarının ən aşağı səviyyəsi verilməlidir. Müvafiq olaraq onların fişinq hücumunun qurbanı olduğu halda belə potensial ziyan azalır. Zərərli proqram və ya hesaba daxil olmaq detallarını itirməklə yaranan ziyanın sonradan azaldılması məqsədilə sizin əməkdaşlarınızın administrator hüquqları olan hesabdan internetdən istifadə etmədiklərindən və ya məktubları yoxlamadıqlarından əmin olun. Administrator

hesabı digər istifadəçilərə təsir göstərəcək dəyişiklikləri həyata keçirmək imkanı verən istifadəçi hesabıdır. Administratorlar təhlükəsizlik parametrlərini dəyişə bilərlər, proqram təminatı və cihazları install, eləcə də kompüterdə mövcud olan bütün fayllara giriş edə bilərlər. Beləliklə, administrator hesabına autorizə edilməmiş girişi olan hücumçu, standart istifadəçi hesabına giriş halından daha ziyanlı ola bilər.

Elektron poçt kimi vacib olan hesablarda ikifaktorlu autentifikasiyadan (2FA) istifadə edin. Bu metodu istifadə etdiyiniz zaman, hücumçunun sizin şifrənizi bildiyi halda belə hesaba giriş edə bilməyəcək.

Məsləhət 2: Necə işlədiyiniz haqqında düşünün

Kiminsə sizin təşkilatınızı necə hədəfə almasına dair düşünün. Əməkdşların çatışmamazlığı / anomal tələbləri fərq etmələri üçün daha yaxşı hazır olmaları üçün işləmənin normal yollarını (xüsusilə başqa təşkilatlarla münasibət zamanı) anlamalarından əmin olun.

Yayılan üsullara sizin istifadə etmədiyiniz xidmətin invoysunun göndərilməsini daxildir. Əlavə açılarkən zərərli proqram avtomatik olaraq sizin kompüterinizdə install olur. İkincisi, əməkdaşların, pul köçürülməsi və ya təşkilat haqqında məlumat almaq məqsədilə elektron poçt vasitəsilə aldadılmasıdır. Sizin adi iş təcrübəniz və yuxarda qeyd edilən yolları necə anlamaq mümkün olduğu haqqında düşünün. Məsələn,

- Əməkdaşlar el-poçta gələn qeyri-adi xahişlərə dair nə etmələrini və yardımı haradan almalarını bilirlər ya yox?

- Özünüzdən soruşun, elektron poçt ilə alınan tələbin təsdiq edilməsi üçün menecerin cəlb edilməsi lazımdırmı?
- Sizin müntəzəm iş əlaqələrinizi yaxşımı anlayırsınız? Saxtakarlar çox vaxt fişinq məktubları böyük təşkilatlardan (banklar kimi) göndərirlər, o ümidlə ki, elektron poçtu alanların bəzilərinin bu təşkilatla əlaqəsi olacaq. Əgər işgüzar münasibətiniz olmadığınız təşkilatdan elektron poçt alsanız mütləq kontrol edin.
- Sizin əməkdaşlarınızda şübhəli və ya qeyri adi tələblərə qarşı, onların vacib provayderlərdən (məsələn, şirkətin təsisçisi və ya təşkilatın rəhbəri) gəldiyi halda belə suallarının yaranmasını necə həvəsləndirilmək və əməkdaşlarınıza necə dəstək verəcəyiniz haqqında düşünün.

Məsləhət 3: Fişinqin aşkar əlamətlərini yoxlayın

Əməkdaşların bütün fişinq elektron məktublarını tanımaları və silmələri gözləntisi mümkün deyil və təşkilatın / biznesin məhsuldarlığına ciddi şəkildə mənfi təsir göstərəcək. Lakin fişinq cəhdi yenə də ənənəvi hücum formasına uyğun gəlir. Buna görə də sonrakı xəbərdarlıq əlamətlərini axtarın.

- Bir çox fişinq saxtakarlığı xaricdə yaranır və çox vaxt düzgün yazılış, qramatika və durğu işarələri səhv olur. Bəzən hücumçular loqo və qrafika da daxil olmaqla rəsmi şəkilli elektron məktublar yaratmağa çalışırlar. Buna görə də göndərilən məktubu dizayn və düzgün yazılış formalarının müvafiqliyini yaxşı yoxlayın.

- Əgər adınızla müraciət etmirlərsə və «əziz istifadəçi», «dost» və ya «kolleqa» kimi standart müraciətdən istifadə edirlərsə. Bu yollayanın real olaraq sizi tanımadığına əlamət ola bilər və bu fişinq saxtakarlığının bir hissəsini təşkil edir.
- Diqqətlə baxın elektron poçt sizin təcili hərəkət etmənizi tələb edən ifadələrdən ibarətdirmi. Fişinq zamanı çox vaxt bu ifadələr istifadə edilir - «bu detalları 24 saat ərzində göndərin» və ya «siz cinayyət qurbanı idiniz, təcili olaraq buraya basın».
- Göründüyü kimi sizin təşkilatınızın yüksək rütbəli şəxsidən gələn və ödəmənin konkret bank hesabına olduğu elektron poçta diqqət yetirin. Göndərənin adına baxın. Legitim səslənir yoxsa kimisə təqlid etməyə çalışır?
- Əgər məktub həddindən artıq yaxşı səslənirsə, məsələn, çox nadir ehtimaldır ki, kimsə sizə əsassız pul vermək istəsin.

Elektron poçt filtrasiya servisləri fişinq məktublarını spam qovluğuna yerləşdirməyə çalışırlar. Lakin filtrasiyanı müəyyənləşdirən qaydalar sizin təşkilatınızın gərəkliklərinə uyğun olmalıdır. Əgər qaydalar çox açıq və şübhəlidirsə, elektron poçt spam/lazımsız qovluqlara göndərilməyəcək. Belə halda istifadəçilər elektron poçta daxil olan çox saylı məktubları idarə etməli olacaqlar. Bu isə onlar tərəfindən müəyyən enerji tələb edir. Əgər qaydalar çox kəskindirsə, bəzi legitim elektron məktublar itə bilər. Buna görə də sizə müəyyən zaman ərzində

kompromisi təmin etmək üçün qaydaların dəyişilməsi lazım ola bilər.

Məsləhət 4: Hər hücum haqqında bildiriş edin

Sizin əməkdaşların potensial hücum haqqında struktur vahidi və ya cavabdeh olan şəxsə məlumat verməkdə həvəsləndirildiklərindən əmin olun. Belə zaman zərərli proqramların skan edilməsi və şifrələrin dəyişilməsi üçün mümkün olan dərəcədə tez ölçülərin götürülməsi vacibdi.

Əməkdaşlarınızı onların fişinq meili açdıqları halında cəzalandırmayın. Bu insanlara gələcəkdə report etməkdə maneə olacaq və bu onları o dərəcədə qorxuda bilər ki, hər elektron poçtun öyrənilməsinə yetərincə artıq vaxt və enerji sərf etsinlər. Bu iki şey sizin biznesinizə uzun müddətli prespektivdə daha çox ziyan verir

Məsləhət 5: Sizin rəqəmsal izinizi yoxlayın

Hücumçular sizin təşkilatınız və işçiləriniz haqında ictimai şəkildə əlçatan məlumatdan istifadə edirlər ki, fişinq mesajlarını daha da inandırıcı etsinlər. Onlar qeyd edilən məlumatı təşkilatın veb-səhifəsindən və sosial medya hesablarından götürürlər («rəqəmsal iz» kimi tanınan məlumat).

- Sizin təşkilatınızın veb-səhifəsində və sosial media səhifələrində paylaşılan məlumatın təsirini öyrənin. Sizin veb-səhifənizə baxış edənlər nəyi bilməlidirlər və hansı detallar lazımsızdır (lakin hücumçular üçün faydalı ola

bilər)?

- Sizin partnyorlarınızın, müqavilədə olduğunuz təşkilatlar və təchizatçıların, təşkilat haqqında onlayn olaraq, hansı məlumatları paylaşdıqlarını bilin.
- Sizin əməkdaşlarınıza şəxsi məlumatın paylaşılmasının onlara və sizin təşkilatınıza hansı təsirin olacağını anlamaqda yardım edin. Bu o demək deyildir ki, insanlar intenetdən özləri haqqında bütün izi silməlidirlər. İşçiləriniz özlərinin rəqəmsal izlərini idarə etdikləri, onlar və təşkilat üçün işləyəcək profil yaratdıqları zaman onları dəstəkləməniz vacibdir.

Mövzuya dair misallar

2.1. Fərdi göstəricilərin müdafiəsi – nəyi bilməliyik?

2.1.1. Mənim fərdi göstəricilərim nədir?

Fərdi göstəricilərin müdafiəsi haqqında Gürcüstan qanunu müəyyənləşdirir ki, fərdi göstəricilər şəxsin identifikasiyasının mümkün olduğu hər növ məlumatdır. Məsələn: Sizin adınız, soyadınız, şəxsi nömrəniz, fotonuz, video yazınız, elektron poçt ünvanınız, bank hesabı nomrəsi, sosial şəbəkə hesabı, şəxsi yazışma. Sizin işlədiyiniz yer, gəlirləriniz, ailə vəziyyətiniz və s. haqqında məlumat da fərdi göstəricidir.

Həmçinin xüsusi kateqoriyalı fərdi göstəricilər də mövcuddur. Qeyd edilən kateqoriyaya şəxsin irqi və ya etnik mənşəyi, siyasi baxışı, dini və ya fəlsəfi inamı, peşə ittifaqı üzvlüyü, sağlamlıq vəziyyəti, cinsi həyatı, məhkumluğu, inzibati məhkumluq, qarşısı alınma tədbirinin tətbiq olunması, prosesual razılaşma, uzaqlaşdırılma, cinayət qurbanı kimi və ya zərərçəkmiş kimi tanınmaq ilə əlaqəli məlumat aiddir. Əlavə olaraq xüsusi kateqoriyaya biometrik və genetik göstəricilər də daxildir. Onlar yuxarıda qeyd edilən əlamətlərlə fiziki şəxsin identifikasiya imkanını verir.

Gürcüstanda qüvvədə olan qanunvericilik xüsusi kateqoriyaya aid olan fərdi göstəricilərin daha yüksək standartını təyin edir və həmçinin qaydaların pozulması zamanı sanksiyalaşdırma mexanizmləri də standart fərdi göstəricilər halında olduğundan daha kəskindir.

2.1.2. Fərdi göstəricilərin qanunsuz işlənməsi nə deməkdir?

Fərdi göstəricilərin müdafiəsi haqqında Gürcüstan qanunu müəyyənləşdirir ki, göstəricilərin işlənməsi, fərdi göstəricilərə qarşı həyata keçirilən hər hansı bir hərəkətdir: toplamaq, yazmaq, saxlamaq, istifadə etmək, aşkara çıxarmaq, fotoya keçirmək, üçüncü şəxsə vermək, yaymaq, silmək, məhv etmək və s.

Vətəndaşın əlaqəsi olduğu, istənilən dövlət və ya özəl təşkilat, vətəndaşın fərdi məlumatının işlənməsini edə bilər. Məsələn:

- Supermarketlər şəbəkəsi, vətəndaş loyallıq kartını qeydiyyatdan keçirdiyi zaman, vətəndaşın fərdi göstəricilərinin işlənməsini edir.
- Klinika, diaqnostika, tədqiqatlar keçirdiyi, tibb tarixçəsi tərtib etdiyi zaman vətəndaşın fərdi göstəricilərinin işlənməsini edir.
- Vətəndaş (istifadəçi) öz fotosunu yerləşdirdikdə və ya qeydiyyat məqsədilə müvafiq qrafaya elektron poçt ünvanını və şifrəsini daxil etdikdə sosial şəbəkə, vətəndaşın (istifadəçinin) fərdi göstəricilərinin işlənməsini edir.
- Tələbə tədris kursuna yazılması üçün öz şəxsi nömrəsini, ad və soyadını göstərdikdə təhsil müəssisəsi, tələbənin fərdi göstəricilərinin işlənməsini edir.

Vətəndaşın şəxsi məlumatları ilə təmasda olan bütün təşkilatlar məlumat işləyicisi, vətəndaş isə məlumat subyektidir.

Fərdi göstəricilərin sensitivliyini nəzərə alaraq Gürcüstanın qüvvədə olan qanunvericiliyi göstəriciləri işləyib-hazırlayanın göstəriciləri işləyib-hazırladığı zaman mütləq əməl etməli olduğu qaydaları, prinsipləri və təhlükəsizlik ölçülərini təyin edir. Bu qaydaların pozulması ilə göstəricilərin toplanması, saxlanılması, istifadə edilməsi və yayılması qanun pozuntusudur.

2.1.3. Göstəricilərin işlənməsi əsasları

Göstəricilərin işlənməsi yol veriləndir, əgər:

- **Göstəricilər subyektinin razılığı mövcuddur –** Şəxsin onun fərdi göstəricilərinin işlənməsinə dair özünün istəyi olaraq, məlumatlandırılmış və kəskin ifadə edilmiş razılığı. Məsələn:
  - Saytda qeydiyyat zamanı və ya aplikasiya yükləyərkən – veb-səhifədə yerləşdirilən məxfilik siyasəti ilə razılaşmaq;
  - Tibbi anket və ya loyallıq kartı açan zaman – müqaviləni imzalamaq.
- **Göstəricilərin işlənməsi qanunla nəzərə alınıb –** Bir sıra hallarda müxtəlif qanunverici aktlar vətəndaş haqqında personal göstəricilərin işlənməsi gərəkliyini nəzərə alır.
- **Göstəricilərin işlənməsi, işləyici tərəfindən qanunla müəyyən edilmiş öhdəliklərin yerinə yetirilməsi üçün lazımdır –** Məsələn, vergi məqsədilə göstəricilərin müəyyən vaxt ərzində saxlanılması;

- **Göstəricilərin işlənməsi, göstəricilərin subyektinin həyat maraqlarını müdafiə etmək üçün lazımdır –** Məsələn, əgər fövqaladə vəziyyət zamanı insanın həyatı təhlükədədirsə və onu xilas etmək üçün yerinin təyin edilməsi mütləqdir.
- **Göstəricilərin işlənməsi, göstəriciləri işləyən və ya üçüncü şəxsin qanuni maraqlarını müdafiə etmək üçün mütləqdir.**

Yalnız o hallar istisna olmaqla, nə zaman ki, göstəricilər subyektinin hüquq və azadlığının müdafiəsinin çox yüksək marağı mövcuddur;

- **Göstəricilər ictimai şəkildə əlçatandır və ya göstəricilər subyekti onları əlçatan edib.** Məsələn:
  - Sosial şəbəkədə ictimai şəkildə yerləşdirilən foto;
  - Onlayn ticarət platformalarında ictimai şəkildə yerləşdirilən əlaqə məlumatı;
- **Göstəricilərin işlənməsi qanuna müvafiq olaraq vacib ictimai marağı müdafiə etmək üçün vacibdir –** Məsələn, cinayətin prevensiyası, sahibkarlıq və ya həddi-büluğa çatmamışların zərərli təsirdən müdafiəsi məqsədilə;
- **Göstəricilərin işlənməsi, göstəricilər subyektinin ərizəsinin müzakirəsi və ya onun üçün xidmət göstərmək üçün mütləqdir.**

Xüsusi kateqoriyalı göstəricilərin işlənməsi yol verilməndir yalnız göstəricilər subyektinin yazılı razılığı və ya o hallarda ki:

- Məhkumluluq və sağlamlıq vəziyyəti ilə əlaqədar olan göstəricilərin işlənməsi əmək öhdəlikləri və əlaqələr

xasiyyətlərindən irəli gələrək həmçinin işə alma haqqında qərar vermək üçün mütləqdir;

- Göstəricilərin işlənməsi, göstəricilər subyektinin və ya üçüncü şəxsin həyatı maraqlarını müdafiə etmək üçün və göstəricilər subyektinin fiziki yaxud hüquqi olaraq göstəricilərin işlənməsinə razılıq bəyan etməsinə dair qabiliyyəti yoxdursa vacibdir;
- Göstəricilər ictimai səhiyyənin müdafiəsi,sağlamlığın müdafiəsi və ya müəssisə (işçi) tərəfindən fiziki şəxsin sağlamlığının müdafiə olunması məqsədilə, həmçinin bunun sağlamlığın müdafiə sisteminin idarəsi və ya işləməsi üçün vacidirsə;
- Göstəricilər subyekti onun haqqında göstəriciləri onların istifadəsinin açıq qadağası olmadan ictimayətləşdirdi;
- Göstəricilər siyasi, fəlsəfi, dini və ya peşə birlikləri, yaxud qeyri hökümət təşkilatları tərəfindən legitim iş həyata keçirildiyi zaman işlənilir;
- Göstəricilənin işlənməsi müttəhimlərin/həbs edilənlərin şəxsi işlərinin və reestrlərinin hazırlanması, həbsdə olana qarşı onun tərəfindən cəza çəkməsinin individual planlanması və ya həbsdə olanın cəza çəkməsinin şərti vaxtından əvvəl azad olunması və onun üçün cəzanın çəkilməyən hissəsinin daha yüngül növlü cəzayla dəyişdirilməsi ilə əlaqəli olan məsələlərin müzakirəsi məqsədilə baş verir.
- Göstəricilər «həbs nəzərdə tutmayan cəzanın yerinə yetirilməsi qaydası və probasiya haqqında» Gürcüstan

qanununun ikinci maddəsi ilə nəzərdə tutulan hüquqi aktların həyata keçirilməsi məqsədilə.

- Göstəricilər «beynəlxalq müdafiə haqqında» Gürcüstan qanunu ilə birbaşa nəzərdə tutulan hallarda işlədilir.
- Göstəricilər, miqrasiya göstəricilərinin vahid analitik sisteminin funksionallığı üçün işlənilir.
- Göstəricilər xüsusi təhsil gərəkliyi olan şəxslərin təhsil hüququnu həyata keçirmək məqsədilə işlənilir.

2.1.4. Göstəricilərin işlənməsi prinsipləri

Fərdi göstəricilərin işlənməsi zamanı sonrakı prinsiplərin nəzərə alınması mütləqdir:

- **Ədalətlilik və qanunilik –** Fərdi göstəricilər ədalətli və qanuni şəkildə, şəxsin ləyaqətini zədələmədən işlənilməlidir.
- **Kəskin müəyyən edilmiş qanuni məqsədin mövcudluğu –** Göstəricilərin işlənməsinin nə üçün edildiyinə dair konkret məqsədin mövcudluğu mütləqdir. Başqa məqsədlərlə göstəricilərin işlənməsi yol verilməzdir.
- **Proporsionallıq və adekvatlıq –** Göstəricilər, göstəricilərin işlənməsinin konkret hədəfinə çatmaq üçün mütləq olan minimal həcmdə işlənilməlidir. Göstəricilərin özləri də bu məqsədə müvafiq olmalıdırlar.
- **Həqiqilik və dəqiqlik –** Göstəricilər həqiqi və dəqiq olmalıdır. Lazım olduğu halda yenilənməlidir. Həmçinin

məlumatın mənbəsinin etibarlılığı yoxlanmalıdır. Səhv və dəqiq olmayan göstəricilər düzəlməlidir.

- **Saxlama müddəti –** Fərdi göstəricilər qanunla müəyyən edilmiş və ya məqsədə çatmaq üçün mütləq olan zaman ərzində saxlanılmalıdır. Məqsədə çatdıqdan sonra onlar silinməli və ya şəxsin identifikasiya edilməsinin mümkün olmayacağı formada saxlanılmalıdır.

Əgər hesab etsəniz ki, təşkilatın sizin göstəricilərinizin işlənməsinə hüquqi əsası yoxdursa və ya qanunla müəyyən olunmuş hər hansı bir prinsipi pozursa, Fərdi Göstəricilərin Müdafiə Xidmətinə yaxud məhkəməyə müraciət edə bilərsiniz.

Pozuntunun təyin edilməsi halında «Fərdi göstəricilərin müdafiəsi haqqında» qanun xəbərdarlıq etmə və ya cərimə şəklində inzibati cavabdehlik müəyyənləşdirir.

2.1.5. Özüm haqqında məlumatı necə tələb edim?

- Fərdi göstəricilərin işlənməsi haqqında məlumatı şifahi, eləcə də yazılı şəkildə tələb edə bilərsiniz.
- Sizin ictimai müəssələrdə haqqınızda mövcud olan fərdi göstəricilərlə tanış olmağa və Gürcüstan qanunvericiliyi ilə, verilməsinə dair ödənişin nəzərdə tutulduğu göstəricilərdən başqa təmənnasız olaraq onların nüsxəsini almağa hüququnuz var.
- Bilməniz vacibdir ki, sizin yalnız özünüzə dair fərdi

göstəricilər haqqında məlumat almaq hüququnuz var. Başqa bir şəxsin göstəricilərinin işlənməsi haqqında məlumatın tələb edilməsi üçün, məsələn, valideyn tərəfindən övladının və ya vəkil tərəfindən müştərinin göstəriciləri haqqında məlumat tələb edildiyi hallarda xüsusi səlahiyyətin və ya nümayəndəliyin təsdiq edilməsi mütləqdir.

2.1.6. Fərdi göstəricilərin düzəldilməsi, silinməsi və ya yenilənməsi

Əgər subyektin fərdi göstəriciləri natamamdırsa, dəqiq deyilsə, yenilənməyibsə, yaxud onların toplanması və işlənməsi qanun tələblərinin pozulması ilə həyata keçirildiysə subyektin onların düzəldilməsini, yenilənməsini, əlavənin edilməsini, blok edilməsini (göstəricilərin işlənməsinin müvəqqəti dayandırılması), silinməsini və ya məhv edilməsini tələb etmək hüququ var.

Tələbin istənilən formasını subyektin özü seçir. Bunu həm şifahi, həm də yazılı şəkildə etmək olar. Göstəriciləri işlənən şəxs isə tələbi aldığı gündən 15 gün ərzində tələbi təmin etməli yaxud subyektə tələbinə dair rədd cavabı veriləmsini əsasını bildirməlidir.

2.1.7. Birbaşa marketinq məqsədi iilə göstəricilərin işlənməsi

Birbaşa marketinq istifadəçi üçün qısa mətn mesajlar, poçt göndərimlər, telefon zəng, elektron poçt və ya birbaşa komunikasiya vasitəsilə məhsulu, xidməti və ya işlə təmin etməni təklif etməkdir.

Birbaşa marketinq məqsədləri üçün göstəricilər işlənilə bilər, əgər:

- Vətəndaş yazılı şəkildə razılıq veribsə;
- Məlumat ictimai şəkildə əlçatadır və ya bu göstəricilərin təşkilatda olması qanunidir.

Çox vaxt istifadəçilər fərdi göstəriciləri, həmçinin əlaqə məlumatının istifadəsinə dair şirkətlərə özləri razılıq verirlər. Məsələn, toplama kartının doldurulması zamanı mağazaya bizə mesaj göndərmək icazəsi veririk. Mobil operatora bizim telefon nömrəmizi partnyor şirkətlərinin məqsədləri üçün istifadə etməyə icazə veririk, bankın müştərisi oluruq və onun bizə məlumat və reklam tərkibli bildirişlər göndərməyinə razılıq veririk.

Şirkətlər, əlaqə məlumatımız içtimai şəkildə açıq olduğu halda da birbaşa marketinq məqsədləri üçün bu məlumatdan istifadə edə bilərlər. Məsələn, əgər telefon nömrənizi alqı-satqı saytında açıq şəkildə yazıbsınızsa, Facebook səhifəsində elektron poçtunuzu açıq şəkildə göstərimisinizsə və s.

Lakin təşkilata bir başa marketinq məqsədləri üçün sizin

göstəricilərinizdən istifadə etmək hüququnu verib-vermədiyinizə baxmayaraq buna dair yox deməyə hüququnuz var – elə təklifin edildiyi formada yaxud digər əlçatan və adekvat vasitələrlə.

Məsələn, reklam mesajlarının mütləq onu rədd etmək mexanizmi və vətəndaşın reklam mesajını almağı dayandıra bilməsinə – SMS OFF dair kəskin göstəriş olmalıdır; Elektron poçt halında isə məktubda Unsubscribe mexanizmi olamalıdır.

Sizin göstəriciləri işləyəndən istədiyiniz zaman və istədiyiniz forma ilə (şifahi, yazılı) sizin göstəricilərinizin birbaşa marketinq məqsədləri üçün istifadə etməsini, dayandırılmasını, tələb edə bilərsiniz. Şirkət sizin tələbinizdən 10 iş günü müddətində sizin göstəricilərin birbaşa marketinq məqsədilə istifadəsini dayandırmaq öhdəliyi var.

Sizin haqqınızda hansı göstəricilərin işlənməsinə dair bilməyə və istənilən zaman onların düzəldilməsini, yenilənməsini, əlavə edilməsini, blok edilməsini, silinməsi və ya məhv edilməsini tələb etməyə haqqınız var. Həmçinin sizin hüququnuz var ki, marketinq işini həyata keçirənin kim olduğunu, sizin göstəricilərinizi hansı mənbədən və hansı əsasla əldə etdiyini biləsiniz

2.2. Fişinq və elektron poçt təhlükəsizliyi

2.2.1. Sosial mühəndislik nədir?

Sosial mühəndislik qurban üzərində manipulasiya, təsir və ya

aldatma taktikasıdır ki, hücum edən kompüter sisteminə nəzarəti əldə etsin, şəxsi və ya maliyyə məlumatını əldə etsin. Sosial mühəndislik sensitiv məlmatı əldə etmək və ya qurbanı təhlükəsizlik qaydalarını / normalarını pozmağa məcbur etmək üçün psixoloji manipulasiyadan istifadə edir.

Sosial mühəndislik bir və ya bir neçə mərhələdə baş verir. İlkin olaraq kiber kriminal ona potensial olaraq sistemə daxil olma yollarını və təhlükəsizlik zəifliklərini aşkar etmək üçün yardım edəcək, qurban haqqında ümumi məlumat toplayır. Sonrakı mərhələdə hücumçu qurbanın etibarını qazanmaq üçün təqlid etmə (impersonation) təcrübə formasını istifadə edir. Qeyd edilən etibar əsasında qurban sensitiv məlumatı və ya hücumçuya hədəfi olan sistemə giriş hüququ verir.

Sosial mühəndisliyin hücum növləri

Sosial münhəndisliyin, insanın olduğu hər yerdə həyata keçirilə biləcək hücumlarının çox sayda fərqli forması mövcuddur. Aşağıda sosial mühəndisliyin hücumunun formalar verilib.

Fişinq nədir?

Etibarlı subyekt kimi görünmə yolu ilə elektron poçt, SMS mesajalar və ya telefonla sensitiv məlumatın - istifadəçi adlarını, parollarını və kredit kartı detallarını əldə etməyə cəhd prosesi fişinq adlanır. Fişinq hücumu zamanı hücumçu təxirə salınmaz, maraq oyatma və ya qorxu hissini yaradır. Fişinq göndəri qurbanı sensitiv məlumat verməyə, zərərli veb-seəhifə linkinə

basmağa və ya zərərli proqramlardan ibarət olan əlavələri açmağa sövq edir.

Vişinq nədir?

Vishing sosial mühəndisliyin növüdür və səsli komunikasiyadan istifadə edir. Bu texnika, qurbanı müəyyən nömrəyə zəng etmələrinə və sensitiv məlumat vermələrinə məcbur edən sosial mühəndisliyin digər formaları ilə birləşə bilər. Vişinq hücumları tamlıqla səsli komunikasiya vasitəsilə Voice over Internet Protocol (VoIP) qərarları və yayım xidmətlərinin istifadəsi ilə həyata keçirilə bilər. VoIP asanlıqla abunənin identifikasiyasının (ID) saxtalaşdırılma vasitsəsini verir. Bundan hücumçu istifadə edə və cəmiyyətin etibar etdiyi müəssisələrin adlarını istifadə edə bilər. Məsələn, qurbanın telefonuna hər hansısa bir ictimai və ya özəl müəssisə kimi identifkasiya onunan zəng gələ bilər, həqiqətdə isə, bu hücumçu tərəsindən həyata keçirilən zəng ola bilər.

Smişinq nədir?

Smishing SMS və ya yazılı mesajlardan istifadə edən sosial mühəndislik növüdür. Yazılı mesajlar tərkibində veb-səhifələri, el-poçt ünvanları və ya telefon nömrələri ola bilər. Onlara basdıqda avtomatik olaraq brauzer pəncərəsi, elektron məktub və ya nömrə yığıla bilər. Elektron poçtun, səsin, yazılı mesajın və brauserin funkisonal inteqrasiyası istifadəçinin zərərli fəallıq qurbanı olma ehtimalını artırır.

Beytinq nədir (Baiting)?

Beytinq (yem) sosial mühəndisliyin hücum növüdür. Bu zaman saxtakar qurbanı tələyə salmaq üçün yalançı vədlərdən istifadə edir. Bu da sistemdə zərərli proqramın aldadılma ilə fəallaşması yolu ilə fərdi və ya maliyyə məlumatının sızmasına səbəb ola bilər. Bir qayda olaraq beytinq zamanı zərərli kodun yayılması üçün cəlb edici adı olan əlavə istifadə olunur.

Beytinqin ən yayılmış forması zərərli proqramları yaymaq üçün fiziki medya daşıyıcısını (məs., USB flash Drive) istifadə edir. Məsələn, hücumçu zərərli proqrama yoluxmuş fleş yaddaş kartını (yemi) görünən, qurbanın onu mütləq görə biləcək yerə yerləşdirir. Qurban fleş drayvı iş və ya ev kompüterində istifadə etdiyi zaman zərərli proqram avtomatik olaraq sistemdə install olacaq.

Təqib nədir (Tailgating)?

Təqib (tailgating, həmçinin "piggybacking" kimi tanınan) fiziki hücum növüdür. Bu hücum zamanı autorizə edilməmiş şəxs sosial mühəndislik vasitəsi ilə müdafiə olunan əraziyə (məs., bina girişi, ofis, müdafiə olunan otaq və s.) əraziyə giriş əldə edir. Misal üçün hücumçu özünü sürücü, kuriyer, ofis xidməti işçisi, xidmətçi, elektrik və s. kimi göstərə bilər. Hücumçu qapının yanında gözləyə bilər və əməkdaşın/sakinin qapını açan kimi hücumçu əməkdaşdan/sakindən qapını tutmasını xahiş edə bilər və bununla bina ərazisinə giriş əldə edər.

Qorxutmaq nədir (Scareware)?

Scareware sosial mühəndisliyin bir növüdür. Qurbanın saxta həyacan təbili və saxta hədə ilə qorxutmasından ibarətdir. Hücumçu qurbanı qorxudur ki, onun sisteminin zərərli proqramla infeksiyaya yoluxub və bunun üçün yeni proqram təminatını instal edilməsini təklif edir. Real olaraq bu proqramın instal edilməsi, kriminala qurbanın kompiuterinə distan olaraq giriş imkanı verir.

2.2.2. Fişinq haqqında nə bilməliyik?

Fişinq hücumları, xeyirxahlıq təşkilatları, geyim mağazaları, supermarketlər şəbəkəsi və s. kimi müxtəlif təşkilatlardan gələ bilər. Həmçinin çox vaxt, hücumçular cari hadisələr və ilin müəyyən dövrlərindən istifadə edirlər. Məsələn, fişinq hücumu sonrakıları nəzərdə tuta bilər:

- Təbii fəlakət (məs., Katrina fırtınası, İndoneziya sunamisi)
- Epidemiya və sağlamlıq təhlükələri (məs., H1N1, COVID-19)
- İqtisadi problemlər
- Əsas siyasi hadisələr (seçkilər)
- Bayramlar

2.2.3. Fişinqi necə tanımaq olar?

Göndərənin şüphəli ünvanı – göndərənin ünvanı legitim biznesin imitasiyası ola bilər. Kiber kriminallar çox vaxt,

reputasiyası olan şirkətin elektron poçt ünvanına çox bənzəyən, bir neçə simvol dəyişik, yaxud buraxılmış olan elektron poçt ünvanı istifadə edirlər (məsələn, www.microsoft.com əvəzinə www.microsofttt.com).

Ümumi salamlamalar və imza – fişinqin ən vacib indikatorlarından biri - «Əziz istifadəçi» və ya «Cənab/xanım» kimi ümumi salamlama və həmçinin imza blokunda məlumat əksikliyidir. Müqayisə üçün, etibarlı təşkilat sizə adi olarad adınızla müraciət edir və onlar haqqında əlaqə məlumatı təqdim edir.

Saxtalaşdırılmış hiper linklər və veb-səhifələr – Əgər kursoru elektron poçtun hər hansı bir linkinin üzərinə gətirəcəksinizsə, və linklər onun üzərinə gətirəndə görünən mətnə uyğun olmayacaqsa, link saxta ola bilər. Zərərli veb saytlar legitim saytlarla identik görünə bilər, lakin URL-da domenin başqa variyasiyaları istifadə edilə bilər (məs., .com əvəzinə .net). Diqqət yetirilməlidir ki, kiber kriminallar linkin həqiqi təyinatını gizləmək üçün URL qısaltma xidmətindən istifadə edə bilərlər.

Orfoqrafiya və cümlə strukturu – Pis qramatika və cümlə strukturu, orfoqrafiya səhvləri və sırasız formatlaşma fişinqin ehtimal cəhdinin indikatorlarından biridir. Müqayisə üçün reputasiyası olan institutlar istifadəçilərlə yazışmanı aparan yoxlayan və düzəldən işçilər ayırıb.

Şübhəli əlavələr – Zərərli proqramların yayılmasının ümumi mexanizmlərindən biridir. İstifadəçidən qoşma kimi əlavə edilmiş faylı yükləməyi və açmağı istəyən elektron poçtun istifadə edilməsidir. Hücumçu təcili vacibiyi olan illuziya / ssenari yarada bilər ki, istifadəçini əvvəlcədən yoxlanmamış əlavə şəklində birləşdirilən faylı yükləsin və ya açsın.

2.2.4. Fişinqdən necə qorunmaq olar?

- Sizdən müxtəlif sensitiv məlumatın verilməsini istəyən telefon zəngləri, SMS-lər və ya elektron poçt mesajlarına qarşı ehtiyyatlı olun. Əgər yad şəxs bildirir ki, legitim təşkilatın nümayəndəsidir, çalışın onun kimliyini birbaşa şirkətdən öyrənəsiniz. Şəxsiyyətin səlahiyyətindən və kimliyindən əmin olmadığınızda fərdi məlumat və ya sizin təşkilatınız, həmçinin onun strukturu və şəbəkələri haqqında məlumat verməyin.
- Şəxsi və ya maliyyə məlumatının elektron poçtda açıqlamayın və elə onun vasitəsilə bu məlumatın tələb edilməsinə cavab verməyin.
- Veb-səhifənin təhlükəsizliyini yoxlamadan internetlə sensitiv məlumat göndərməyin.
  - Veb-səhifənin Uniform Resource Locator-na (URL) diqqət yetirin. URL-lər “https” başlayırsa, bu saytın təhlükəsizlik əlamətidir, “http” isə deyil.
  - Örtülü qıfıl nişanəsini (icon) axtarın ki, sizin məlumatınız şəbəkədə ötürülən zaman şifrələnmiş olacaq.

- Əgər elektron poçtla alınan tələbin legitim olmasından əmin deyilsinizsə onu birbaşa şirkətlə əlaqə saxlamaq yolu ilə yoxlamağa çalışın. Lakin elektron poçt vasitəsilə aldığınız əlaqə məlumatından istifadə etməyin. Bunun əvəzinə şirkətin əlaqə məlumatını müxtəlif alternativ mənbələr yolu ilə (axtarış sistemləri, sosial medya postları, qruplar və s.) yoxlayın.
- Antivirus proqram təminatı, firewall və elektron poçt filtrlərini install və istifadə edin.
- Sizin elektron poçt proqramı və veb brauzerin təklif etdiyi fişinqə qarşı funksiyadan istifadə edin.
- Çox faktorlu autentifikasiyadan istifadə edin (MFA).
-

Əgər qurban olduğunuzu hesab edirsinizsə, nə edirsiniz?

- Əgər sizin təşkilatınız haqqında sensitiv məlumat deyəcəyinizi hesab edirsinizsə, mütləq təşkilatın müvafiq əməkdaşlarına (informasiya təhlükəsizlik departamenti, IT departament) meraciət edin.
- Əgər bank hesablarınızın qırıldığını düşünürsünüzsə təcili olaraq vaxt itirmədən sizin maliyyə institutunuz (bankla) əlaqə saxlayın və təhlükə altında olan hər bir hesabı bağlayın. Sizin hesabınızda hər hansı bir izahı olmayan tranzaksiyaya nəzarət edin.
- Təcili olaraq vaxt itirmədən hücumçu üçün bəlli ola biləcək şifrəni dəyişin. Əgər müxtəlif resurslar üçün eyni şifrədən istifadə edirdinizsə, hər bir hesab üçün şifrəni

dəyişdiyinizdən əmin olun və bu şifrədən gələcəkdə istifadə etməyin.

- Polislə əlaqə saxlayın və kiber hücum haqqında bildirin.

2.3. Onlayn mühitdə dezinformasiya: İdentifikasiya və nəzarətin prevensiya mexanizmləri

Avropa Şürasının izahına əsasən təbliğat, dezinformasiya və saxta xəbərlərin ictimai fikirin polarizasiyasına, zorakı ekstremizmə və nifrət nitqinə səbəb ola biləcək, nəticədə demokratiyaları sarsıtmaq və ona qarşı etibarı azaltmağa potensialı var.

«Propoqanda», «dezinformasiya» və «saxta xəbərlər» terminləri çox vaxt bir-biri ilə üst-üstə düşür. Onlar müxtəlif yolları qeyd etmək üçün istifadə olunur. Bununla məlumatın paylaşılması düşünülmüş və ya düşünülməmiş – adi olaraq konkret mənəvi və ya siyasi səbəbin yaxud baxışın dəstəklənməsi ilə əlaqədar ziyana səbəb olur.

MDM kateqoriyasına aid olan, məlumatın aşkar şəkildə fərqlənən istifadəsi üç yerə bölünə bilər.

- **Misinformation (yanlış məlumat) –** Zərər vermə niyyət olmadan paylaşılan yanlış məlumat.
- **Disinformation (dezinformasiya) –** Qəsdən zərər vermə niyyətiylə paylaşılan yanlış məlumat.
- **Malinfromation (zərərli məlumat) –** Qəsdən zərər vermə niyyətiylə paylaşılan etibarlı məlumat.

Baxmayaraq ki, bu fenomenlərdən heç biri qeyri-adi deyil, onlar son zamanlar infromasiya və kommunikasiya texnologiyalarının (ICT) mükəmməl formalarının geniş əlçatanlığı ilə yeni mühümlük əldə etdilər. Məsələn, mətnlərin, şəkillərin, videoların və ya linklərin onlayn paylaşılması informasiyanın bir neçə saat ərzində virus kimi yayılmasına imkan verir.

2.3.1. MDM-nı necə müəyyən edək?

İnformasiya landşaftını tənqidi olaraq dəyərləndirin və mənbələr və mesajları yoxlamağa vaxt ayırın. Məzmunu gördükdə istənilən formada özünüzə sonrakı sualları verin.

- ¬ Emosional reaksiya yaradırmı?
- ¬ Mübahisəli məsələyə cəsarətli bəyanat edir ya yox?
- ¬ Bu qeyri-adi iddiadır?
- ¬ Onda clickbait varmı?
- ¬ Kontekstə uyğun olan aktual informasiya varmı?
- ¬ Onun şişirdilmiş və ya çirkinləşdirilmiş kiçik məlumat istifadə edirmi ya yox?
- ¬ Onlar yoxlanılmamış və ya az yoxlanılmış platformalarda virus kimi yayıldımı?

Bu sizə MDM-nı müəyyən etmək üçün yardım edəcək bir neçə əsas sualdır. Suallardan biri mənbəyə istisna etsə belə, avtomatik şəkildə informasiyanın diskreditasiyasını etmir. Bu məsələyə etibar edənədək onu daha yaxşı araşdırmağa bir növ yardım etmə kimidir.

2.3.2. Təşkilatlar MDM-ya qarşı necə tədbir görə bilər?

Təşkilatlar MDM-nın təhlükəsindən özlərini sonrakı strateqiyalar və nəzarəti istifadə etməklə qoruya bilərlər:

- Sosial medya və veb monitorinq sistemi quraşdırın. Həmçinin sizin brend və təşkilatlarınızla əlaqədə olan saxta xəbərlərin identifikasiyası və nəzarət edilməsi üçün xəbərdarlıq sistemləri qurun. Bu xidmətlər çox vaxt sizə tək özünüzün sosial medya profillərinizi deyil, eləcə də ictimai postları, veb forumları, veb səhifələri, icmalları, xatırlatmaları və s. də nəzarət etməyə imkan verir.
- Şəffaf, yüksək keyfiyyətli kontentlə bərabər istənilən veb səhifədə axtarış sisteminin optimizasiyasından (SEO) istifadə edin. SEO sizin saytınız və sosial medyanızın axtarış sistemlərində (Google kimi) istifadə olunur və veb səhifənin pozisyasının göstərilməsini fərqləndirə bilər (sizin təşkilatınızı hədəf olaraq düşünən MDM ilə nisbətdə yuxarı və ya aşağı).
- Təşkilatınız haqqında yalan məlumat deyil, faktlar göstərmək, cavabları optimallaşdırmaq üçün Google Home, Amazon Alexa, Siri kimi səsli asistentlərə fokuslaşdırılmış Cavablar Mühərrikinin Optimizisiyasından (AEO) istifadə edin
- Gücləndirici şəbəkələrdən istifadə edin ki, sizin kontentin əlçatanlığını və görünməsini artırasınız, eləcə də yalan məlumatın yayılmasının qarşısını alasınız. Gücləndirici şəbəkələr «həqiqət səs ucaldıları» kimi hərəkət edir və

təşkilatın partnyorları, brend səfirləri və mövcud istifadəçiləri də əhatə edə bilər.

- Sizin müştərilərinizə və istifadəçilərinizə ilə iştirakı həvəsləndirin ki, etibarın yaranmasını və qorunub saxlanılmasını təmin edəsiniz. Məsələn, brendin etibarlılığının daha yaxşı dəyərləndirilməsi üçün axtarış sistemləri istifadəçiləri və onlar haqqında icmalı istifadə edirlər.
- Reaksiya verici qrup yaradın ki, məcazi mənada istənilən MDM kompaniyasına qarşı dursun və az bir müddətdə istifadəçilər üçün cavabların verilməsini təmin etsin.
- MDM ilə bir başa komunikasiyaya daxil olmayın. Cavablar passiv xasiyyətdə olmalıdır və MDM olan post altında yerləşdirilməməlidir. Bunun əvəzinə siz cavabı öz veb səhifənizdə yerləşdirə bilərsiniz. Əmin olun ki, MDM-ya cavab detallı, şəffaf, faktiki cavablardan ibarətdir. Cavab vermə yanaşması təşkilata görə fərqli ola bilər.

2.3.3. İstifadəçilər MDM-ya qarşı necə tədbir görə bilər?

İnformasiya istifadəçisi kimi məzmunu sonradan araşdırmaq və MDM-dan özünü qorumaq üçün sonrakıları həyata keçirə bilərisiniz:

- Yersiz dizayn elementlərini – qeyri-profesional loqolar, rənglər, interval və animasiya giflərini axtarıb tapın.
- Domen adlarını yoxlayın ki, onların təşkilata müvafiq

olduğundan əmin olasınz. Domen adında səhv ola bilər və ya– .net yaxud .org kimi ali səviyyə domen (TLD) istifadə oluna bilər.

- Təşkilatın əlaqə məlumatı, fiziki ünvanı və «bizim haqqımızda» səhifəsinin olmasını yoxlayın.
- Domenin axtarılmasını WHOIS sistemində edin ki, bu domenin kimə aid olduğunu görəsiniz və etibarlı təşkilata aid olub olmadığını təsdiqləyə biləsiniz. WHOIS domen adlarının göstəricilər bazasıdır və domenin sahibi, nə vaxt qeydiyyat olduğu və vaxtının nə zaman bitdiyi haqqında detalları var.
- Şəkil axtarışı (reverse image search) keçirin ki, şəkillərin legitim veb səhifələrdən və təşkilatlarda kopya edilmədiyindən əmin olasınız.
- Faktları yoxlayan saytdan istifadə edin ki, oxuduğunuz informasiyanın artıq təsdiq olunan yalan olmamasından əmin olasınız.
- Avtomatik olaraq düşünməyin ki, qəbul edilən məlumat düzgündür. Onun etibarlı mənbədən (dost və ya ailə üzvi kimi) alındığında belə.
- İnformasiyanın köhnəlmiş olmadığından əmin olun.

2.4. Təchizat zəncirinin kiber təhlükəsizliyi

2.4.1. Giriş – Təchizat zənciri nədir?

Avropa İttifaqının Kiber Təhlükəsizlik Agentliyinin (The European Union Agency for Cybersecurity – ENISA) izahına əsasən – «Təchizat zənciri, son qərarın verilməsi, yaxud məsulun yaranması və çatdırılmasında iştirak edən proseslərin, insanların, təşkilatların və distrubyutorların ekosistemidir. Kiber təhlükəsizlikdə təchizat zənciri resursların geniş spektrindən (texnika və proqram təminatı) ibarətdir – saxlanılma yeri (bulud və ya lokal), distrubusiya mexanizmləri (veb aplikasiyalar, onlayn mağazalar) və idarənin proqram təminatı».

ENISA təchizat zəncirinin dörd əsas elementini müəyyənləşdirir:

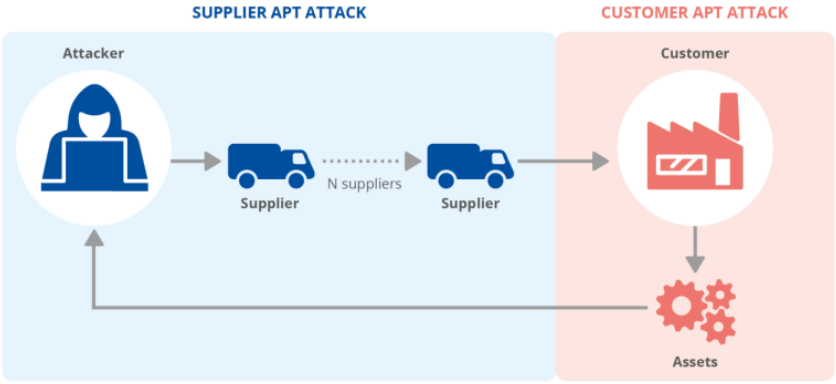
- **Çatdırıcı**: Digər subyektə məhsul və ya xidmət çatdıran vahid.
- **Çatdıranın aktivləri**: Çatdıranın məhsul və ya xidmət istehsal etmək üçün istifadə etdiyi dəyərli elementlər.
- **İstifadəçi**: Çatdıran tərəfindən isehsal edilən məhsul və ya xidməti istifadə edən subyekt.
- **İstifadəçilərin aktivləri**: Hədəfə aid olan dəyərli elementlər.

Vahid, individ, individlər qrupu və ya təşkilat ola bilər. Aktivlər kimi insanlar, proqram təminatı, sənədlər, maliyyə, cihazlar və s. hesab edilə bilər.

2.4.2. Hücumçular necə istifadə edirlər?

ENISA-nın izahına əsasən, təchizat zəncirinə hücum, ən azı iki hücumun konbinasiyasıdır. İlkin hücum təchizatçıya edilir, daha sonra aktivlərə giriş əldə etmək üçün hədəfə hücum üçün istifadə olunur. Hədəf sonuncu istifadəçi və ya digər çatdıran ola bilər. Buna görə də hücumun təchizat zəncirinə hücum kimi kvalifikasiya edilməsi üçün təchizatçı və istifadəçi hədəf olmalıdır.

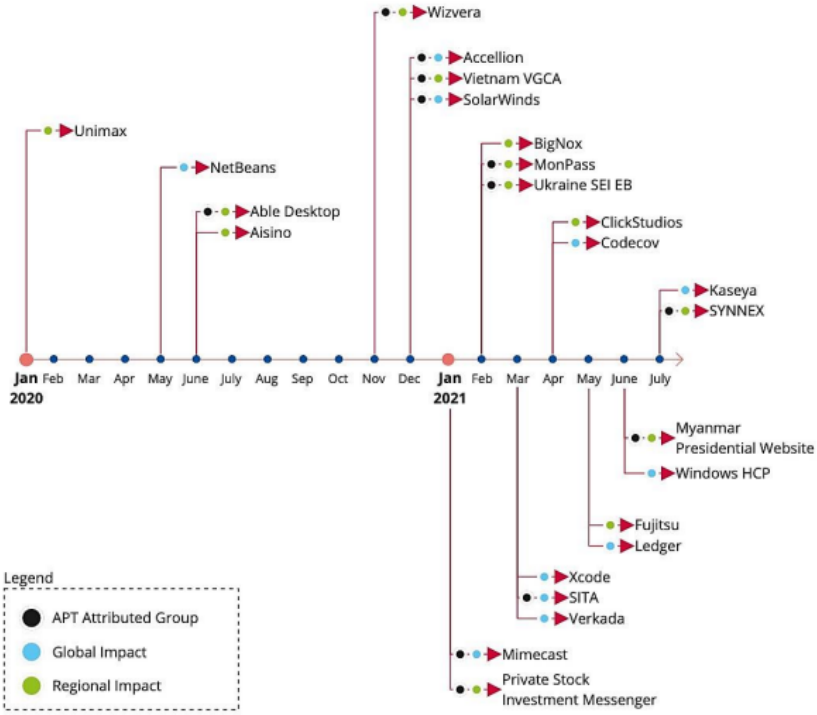
Diaqramda hakerlər qrupu tərəfindən (Advanced Persistent Threat – APT) təchizat zəncirinə hücumun necə edildiyinə dair «Asan mexanizm» göstərilib. İlik mərhələdə təchizatçının kompromatlaşdırılması baş verir, bu da sonradan istifadəçinin kopromatlaşdırılmasına səbəb olur.



Diaqram #1: ENISA THREAT LANDSCAPE FOR SUPPLY CHAIN ATTACKS

2.4.3. Nədən vacibdir?

2020-2021-ci illərdə müxtəlif ölkələrin dövlət və ya özəl strukturlarına bir neçə sayda təchizat zəncirinə hücum gördük. Diaqram #2-də verilmiş müxtəlif hücumlar haqqında məlumat arasında diqqət yetiriləsi fakt odur ki, hücumlar arxaında əsasən dövlətlər tərəfindən maliyyələşdirilən APT qrupları dayanır və bu hücumların regional, eləcə də qlobal təsiri vardı.



Diaqram #2: ENISA THREAT LANDSCAPE FOR SUPPLY CHAIN ATTACKS

Yuxarıda qeyd edilən hücumlarda ən çox səs-küy yaradan hücuma misal SolarWinds Orion-un hadisəsidir. Qeyd edilən hücum Rusiya Xarici Kəşfiyyatı (Russian Foreign Intelligence Service (SVR)) ilə əlaqəli olan APT 29 qruplaşmasına aid edildi.

2.4.4. Təchizat zəncirinin növləri

Təchizat zəncirinin təhlükəsizlik məsələsi mürəkkəbdir və məsələyə dair düzgün yanaşmanın seçilməsi vacibdir. Misal üçün, sonrakı kateqoriyalı təchizat zənciri elementlərini müzakirə edə bilərik.

2.4.5. Təhlükə tərkibli proqram təminatının alınması

ICT təchizat zənciri ilə əlaqəli risklərin ilk birinci misalı təhlükə tərkibli proqram təminatının alınması / istifadə edilməsidir. Klassik anlamda proqram təminatı:

1. Tərkibində istifadəçiyə zərər verən zərərli kod ola bilər.
2. İstifadəçi haqqında sensitiv məlumat toplaya bilər;

<u>Bir neçə təhlükə tərkibli proqram təminatını müzakirə edək:</u>

I. **Təhlükəsilik sistemi Kaspersky** – İllər ərzində Gürcüstanda ən yayılan təhlükəsilik sistemi Kaspersky antivirusu idi. Özəl, eləcə də ictimai strukturlar fəal olaraq «əfsanəvi» antivirusdan istifadə edirlər. Dediklərinə görə «rus viruslarını yaxşı tuturdu». ABŞ-nın Komunikasiyaların Federal Komissiyası (Federal Communications Commission) Kaspersky-nin məhsullarını milli təhlükəsizliyə təhlükə kimi hesab etdi və istifadə edilməsini qadağan etdi. Analoji olaraq Britaniya və Almaniya hökümətləri də istifadəçilərin yuxarıda qeyd edilən məhsullardan istifadədən çəkinməyə çağırdılar.

II. **Mail.Ru** – Rusyanın elektron poçt xidmətidir, post soviet məkanı ölkələrində fəal olaraq istifadə edilir. Vacibdir ki, istifadəçi oxşar xidməti istifadə edərkən istifadəçilərin fərdi göstəricilərinin, yazışmaları, maraqları və davranışları Rusiya xüsusi xidmətləri tərəfindən istifadə edilə bilər.

III. **1C ERP** – 1C Rusiya şirkətidir. Bu şirkətin 1C ERP məhsulu Gürcüstanda geniş yayılıb. Əlavə olaraq yerli bazarda bu sistemin developmentini və dəstəyini təmin edən bir çox konsultasiya şirkəti var. Qərar alınarkən şirkətin rəhbərlərinin anlaması lazımdır ki, təşkilatın biznes proseslərinin rəqəmsallaşdırılması zamanı istifadə edilən rus proqram təminatı sonrakı risklərdən ibarətdir: Təchizat zəncirinin hücumunun asanlığı və rus məhsulluğundan asılılıq (hansı ki, geosiyasi vəziyyət və sanksiyaları nəzərə almaqla əl çatmayan ola bilər.

IV. **Yandex Taxi** – Rusiya proqram təminatından istifadə edən və istifadəçi haqqında müxtəlif növ fərdi və bank – ad, soyad, ünvan, telefon nömrəsi, yerdəyişmə marşrutları, bank kartı məlumatları və s. kimi göstəriciləri toplayır. Müxtəlif məbələrə əsaslanaraq fəal olaraq Rusiya Federal Təhlükəsizlik Xidməti ilə əməkdaşlıq edir və istifadəçilər haqqında onlara məlumat verir. Bunu şirkətə Rusiya qanunvericiliyi həvalə edir. Fərdi baxımda hər hansı bir nəfər istifadəçi haqqında məlumat kritik olmaya bilər, lakin milli səviyyədə düşman əhval-ruhiyyəsində olan dövlət üçün böyük miqdarda fərdi göstəricilərin ötürülməsi dövlət üçün milli təhlükəsizliyin yeni çağırışılarını yaradır.

<u>Siyahı tam və hərtərəfli deyil</u>

2.4.6. Təhlükə tərkibli avadanlıqların alınması

Təhlükə tərkibli avadanlığın alınmasının ən çox yayılan misallarından biri çin istehsalı müşahidə sistemlərinin alınmasıdır. Ən yaxşı beynəlxalq təcrübə göstərir ki, təchizatçı zəncirə hücümlarda avadanlıq (hardware) da istifadə edilə bilər. Müvafiq olaraq, inkişaf etmiş dövlətlər təhlükə tərkibli avadanlığın istehsalçılarını aşkar və onları qadağan etmə üzərində işləyirlər. Misal üçün ABŞ hökümət strukturlarında istifadə üçün / alınması üçün çin istehsalı Huawei, Dahua, Hikvision avadanlığı qadağandır. (Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment, https://www.acquisition.gov/far/4.2101).

2.4.7. Dəstək xidmətləri ilə əlaqəli risklər

Proqram və avadanlıq təminatı təchizat zəncirinin risklərini müzakirə edərkən vacibdir ki, dəstək xidmətini edən tərəflə əlaqəli risklərdə düzgün dəyərləndirilsin. Məhz istənilən proqram yaxud avadanlıq təminatının alınması, zəmanət şərtlərini və müvafiq dəstək xidmətlərini nəzərdə tutur. Lahiyyənin ilkin mərhələsində gərəkliklikliərin müəyyən edilməsi, lisenziyaların həcmi yaxud avadalıq qərarının verilməsi, dəyərləndirmə və inteqrasiyası baş verir. Bundan sonra isə müxtəlif növ dəstək xidmətləri gəlir (məsələn, a) 5 biznes gün, 9 iş saatı; b) 7 gün, 24 saat və s.).

Dəstək xidmətini verən şirkətin regionunu nəzərə almağınız və dost niyyətli yaxud neytral dövlətin ofis nümayəndəliyi ilə əməkdaşlığı təmin etməniz vacibdir.

2.4.8. Konsultasiya xidmətlərinin göstərilməsi ilə əlaqəli olan risklər

Proqram təminatı və avadanlıq alınmasına bənzər olaraq **xidmət göstərmə zəncirinin təhlükələrini idarə etmək** də vacibdir. **Konsultasiya xidmətləri ilə əlaqəli risklərdir:**

Konsultantlar seçilən zaman onların mənşəyi və peşə bacarıqlarının nəzərə alınması vacibdir. Konsultasiya xidməti etdikləri zaman konsultantlar təşkilatın infrastrukturu haqqında məlumat toplayırlar, zəif və güclü tərəfləri öyrənirlər, əməkdaşların bacarıqlarına və kritik vəziyyətdə hərəkət etmə hazırlıqlarını müşahidə edirlər. Vacibdir ki, təşkilat yuxarıda qeyd edilən riskləri anlasın və təşkilat haqqında düşmən əhval-ruhiyyəli ölkələrin nümayəndələri üçün kritik məlumatın verilməsinin maksimal dərəcədə məhdudlaşdırılmasını təmin etsin. Belə konsulatsiya xidmətlərinə misaldır: Maliyyə auditi, müvafiqlik auditi, IT auditi, təşkilati audit, informasiya təhlükəsizlik auditi və konsultasiya xidməti, IT dəyərləndirmə, IT infrastruktur lahiyyələri və s.

2.4.9. İT kadrların miqrasiyası

Rusiya Federasiyasına qarşı tətbiq edilən sanksiyalara paralel olaraq bir çox rus İT mütəxəssisləri yaşamaq üçün Gürcüstana köçdü ki, sanksiyalardan yayınsınlar və Avropa və beynəlxalq lahiyyələr üzərində işləməyə davam edələr. Gürcüstanın proqram təminatı yaradıcıları və proqram təminatı istehsalçılarını cəlb etmək üçün (5%-dək vergi ödənişi) həddindən artıq yaxşı vergi qanunvericiliyi var.

Hazırki vəziyyətə əsasən yuxarda qeyd edilən miqrasiyanın potensial nəticələrini dəyərləndirmək mümkün deyil. Əlavə kvalifikasiyalı kadrların axını ictimai və özəl şirkətlərin rəqəmsal transformasiyasına yardımçı ola bilər. Belə ki, Gürcüstanın kvalifikasiyalı IT personal çatışmamazlığı var. Yerli şirkətlər həmçinin ölkənin kritik informasiya infrastrukturunun mövcud olan çatışmamazlığı bazarda yeni yaradılan kvalifikasiyalı miqrantlar və onların şirkətləri ilə doldurmaq imkanı var. Nə vaxt ki, təcrübədə risklərin kompensasiyası üçün çox az effektli nəzarət mexanizmi mövcuddur. İkinci tərəfdən sürətləndirilmiş rəqəmsal transformasiyanın dəyəri kompromatlaşdırılmış kritik informasiya infrastrukturu ola bilər. Rusiya ilə reqional münasibət kontekstini nəzərə almaqla Gürcüstanı təchizat zənciri və insayder təhlükələr (insider threat) ilə əlaqəli olan artmış təhlükələr hədələyir. Klassik izahatla desək, yuxarıda qeyd edilən, yeni yaradılmış şirkətlər təchizat zəncirinin hücumları izahatına uyğun gəlmirlər. Lakin Rusiya xüsusi

xidmətləri bir qayda olaraq Rusiya şirkətlərində, birbaşa və ya dolayı olaraq istifadəçilərin göstəricilərinə əlçatanlıq tələb edirlər. Bu da təchizat zəncirinə, eləcə də insayderə təhlükələr yaradır. Bundan başqa Gürcüstanın ictimai sektorunun, öz tenderlərində yerli olaraq qeydiyyatdan keçmiş IT şirkətləri filtrə etmək üçün hüquqi berketləri çox az və yaxud ümumiyyətlə olmayacaq.

2.5. Sosial şəbəkənin təhlükəsiz istifadəsi

Sosial şəbəkələr son 10 illik ərzində xüsusi populyarlıqdan istifadə edir. Bu dostlarla, ailə üzvləri ilə yaxud tam yad insanlarla mütəmadi əlaqəni yaratmaq üçün çox gözəl imkandır. Onun vasitəsi ilə müasir insan spesifik maraqları və tanışlar dairəsinə əsasən çox saylı məlumat alır. Milyonlarla insan gündəlik olaraq müxtəlif sosial şəbəkələrdən istifadə edir. Onların ümumi sayı isə bir neçə milyarda çatır. Onlar arasında xüsusi populyarlıqla bu kimi sosial şəbəkələr tanınır – Facebook, İnstagram, eCaht, Pinterest, Linkedin və s. Bir çox tanınmış şirkət və ya şəxsiyyət sosial şəbəkə hesabını yaradıb və onu geniş auditoriya ilə əlaqə qurmaq və komunikasiya vasitəsi kimi istifadə edir.

Sosial şəbəkələrdən təhlükəsiz istifadə etmək üçün 10 məsləhət təqdim edirik:

2.5.1. Parametrləri yoxlayın

Sosial şəbəkənin istifadəsi onda qeydiyyatdan keçməklə, yəni hesabın yaradılması ilə başlayır. Artıq bu mərhələdə qeydiyyat zamanı nəyin edilməsinin məqsədə uyğun olmasına dair addım-addım bildirişlər və məsləhətlərlə qarşılaşacaqsınız. Məsələn: asan yadda qalan şifrəni daxil etdiyiniz zaman sosial şəbəkə avtomatik olaraq çətin şifrə tətbiq etmənizi məsləhət gösəcək, bununla yanaşı variyantlardan biri kimi əlavə təhlükəsizlik ölçüləri – mobil telefona birdəfəlik kod almaqla autentifikasiyadan keçməni də təklif edəcək. Bu təkliflərdən yan keçməyin və təhlükəsizlik tələblərini ilkin mərhələlərdə də nəzərə alın.

Qeydiyyatdan keçikdən sonra menyuda yerləştirilən təhlükəsizlik və məxfilik bölmələrinə daxil olmanız yaxşı olar. Burada, düzənlənməsi ilə gələcəkdə baş verə biləcək insidentləri azalda biləcəyiniz vacib parametrlərlə qarşılaşacaqsınız:

- Sizin akauntunuzun qırılması/hacking edilməsi yəni ona icazəsiz giriş;
- Sizin tərəfinizdən idarə edilən səhifələrin itirilməsi;
- Sizin şəxsi yazışmalarınızın başqa ələ keçməsi, ictimailəşdirilməsi;
- Arzuolunmaz şəxslərdən gələn narahatedici məktublar və potensial təhlükə tərkibli linklərin alınması və s.

Yadda saxlayın ki, təhlükəsizlik parametrlərini quraşdırdığınız zaman itirdiyiniz bir neçə dəqiqə gələcəkdə zaman və

sinirlərinizə mühüm dərəcədə qənaət edəcək, böyük ehtimalla xoşa gəlməz hadisələrin qarşısını alacaq və kiber təhlükəsizlik risklərini azaldacaq.

2.5.2. Dost dairənizi tanıyın və idarə edin

Sosial şəbəkədə qeydiyyatdan keçdikdən sonra bir qayda olaraq ilk addım tanışlar, dostların və maraqlı şəxslərin «dostlar siyahısına» artırılması, onların səhifələrinə abunə olmaq/following və onlarla yazışmağa başlamaqdır. Diqqətli olun və dostlar dairəsinə kimi əlavə etdiyinizi yoxlayın. Kiber kriminallar çox vaxt saxta hesablar yaradırlar və bu yolla sizin fərdi göstəricilərinizə giriş tapmağa yaxud saxtakarlıq yolu ilə məbləğ qoparmağa çalışırlar.

Həmçinin yadınızdan çıxmasın ki, bu və ya digər şəxsi «dostlarınıza» əlavə etdiyinizdən sonra onu sizin ictimai şəkildə yerləştirmədiyiniz və yalnız dostlar dairəsinə aid olan foto, video və ya yazılı materialı görmək imkanı olacaq.

İkinci tərəfdən hansı səhifələri bəyənməyinizə və izləmənizə istər bu təşkilat, şirkət yaxud hər hansısa tanınmış şəxsiyyət olsun, diqqət yetirməniz vacibdir. Belə hallarda da saxta və oxşadılmış səhifələr yaradılır. Onlarda çox vaxt dezinformasiya və səhvə salan kontent (məzmun) yayırlar.

2.5.3. Bir dəfə post yerləşdirmək, daim post yerləşdirməkdir – nəyi paylaşırsınız?

İmicinizin qeydinə qalın. Bilin ki, sosial şəbəkədə bir dəfə yerləşdirilən, «post edilən» məlumat həmişəlik olaraq orada qala bilər, hətta əgər onu yerləşdirdiyinizdən iki dəqiqə sonra silsəniz belə. Hər hansısa bir çağırış etməzdən, foto və ya video material paylaşmazdan əvvəl yaxşı düşünün. Ola biləcək nəticələr haqqında düşünün, bunun nəticəsi nə ola bilər. Əksər hallarda insanlar eyni hadisələrə müxtəlif interpretasia verə bilərlər. Müvafiq olaraq zərərsiz şərh, fikir və ya fotonu/videonu insanların müxtəlif qrupu müxtəlif şəkildə anlaya bilər.

Sosial şəbəkələrin təsiri ilə əlaqəli bir neçə tədqiqat keçirildi. Bu tədqiqatlar göstərdi ki, məsələn, fikirləri soruşulan işverənlərin 70%-dən çoxu işə qəbul ediləcək namizədlərə onlar tərəfindən əvvəllər sosial şəbəkədə yerləşdirilən məlumata görə yox deyiblər. Həmçinin sosial şəbəkədə müəyyən zaman ərzində həyata keçirilən fəallıqlar üzündən çox vaxt xoş olmayan hadisələr, münaqişələr, aylar və ya illər sonra xoşa gəlməz vəziyyətlər çoxdur.

2.5.4. Diqqətli olun kimlərə paylaşırsınız?

Nəzərə alınmalıdır ki, yuxarıda sadalanan risklərin azaldırlması müəyyən hissədə sosial şəbəkələrin əksəriyyətində mövcud olan mexanizmlərlə mümkündür. Hədəf auditoriyasının məhdudlaşdırırlması, kimin icazəsi olduğunu sizin müəyyənləşdirə bilməyiniz nəzərdə tutulur, məhz:

- Sizin konkret postunuzu, fotonuzu və ya videonuzu görsün
- Ona şərhin edilməsi
- Sizin üçün daxili mesajların yazılması və s.

Həmçinin sizin postunuzu ictimai, yalnız dostlarınız, dostlarınızın kiçik dairəsi üçün yaxud yalnız yadda saxlamaq və gələcəkdə post etmək məqsədilə özünüz üçün saxlamağı müəyyənləşdirə bilərsiniz.

2.5.5. Xüsusi hallarda necə davranacağınızı bilin

Xüsusi hallarda necə hərəkət etmənizə dair əvvəlcədən təyin olmuş yollar mövcuddur. Məsələn, əgər kimsə sizə qarşı bullinq, alçaltma, şantaj və s. həyata keçirirsə, sosial şəbəkəyə müvafiq məktubla müraciət edə və report edə bilərsiniz. Yəni qeyd edilən hadisəni tədqiq etsin və konkret hesaba qarşı ölçülər götürsün.

Baxmayaraq ki, saxta hesablarla yuxarıda qeyd edilən hərəkətlərin həyata keçirilməsi tez-tez olur. Konkret sosial şəbəkənin qaydalarının tələb etdiyinə görə hərəkət etmənizə vacibdir. Ən asan halda isə, «hücumçü» hesabları sadəcə silin və ya blok edin.

Həmçinin sosial şəbəkəyə girişi itirilməsi halında nə edilməsinə dair yollar və hərəkətlərlə əvvəlcədən tanış olun. Sosial şəbəkələrin administrasiyası və ya hüquq mühafizəçilərinin sizdən tələb edəcək sənədləri və ya məlumat əvvəlcədən hazırlayın.

Sizin sosial şəbəkənizə icazəsiz giriş mümkünlüyünü hiss ediləcək dərəcədə azaldacaq bir neçə texniki məsləhət var. Müvafiq olaraq hakerlər və kiber kriminalların qurbanı olmanız riski azalır.

2.5.6. Mürəkkəb şifrələr istifadə edin

Mütləq mürəkkəb şifrələr istifadə edin. Müxtəlif saytlarda eyni şifrədən istifadə etməyin, çünki əgər başqa yerdə sizin hesabınızı qırsalar və sizin parolunuzu öyrənsələr, həmin şifrə ilə sizin sosial şəbəkənizə də giriş əldə edə biləcəklər. Çalışın hər sosial şəbəkənizdə unikal şifrəniz olsun.

2.5.7. Çoxfaktorlu autentifikasiya qurun

Şifrə ilə bir yerdə daha bir identifikasiya faktorunun daxil edilməsini nəzərə alan əlavə autentifikasiyanın qurulması xüsusilə vacibdir. Bu əsasən sizin mobil nömrənizə gələn bir dəfəlik kod yaxud ən yaxşı halda bir dəfəlik şifrələr generasiyası aplikasiyasıdır.

Ən yaxşı halda isə Hardware Token (məsələn, Yubico USB/NFC/Lightning) əldə edə bilərsiniz. Onların fiziki olaraq olması hər hansı bir sosial şəbəkənin yaxud digər xidmətə autentifikasiya keçmək üçün mütləqdir. Əgər kimsə sizin şifrənizi, həmçinin bir dəfəlik olaraq SMS kodu əldə etsə, yenə də sizin hesbınıza daxil ola bilməyəcək. Bu sonuncu metod bilik və bacarıqlar tələb edir. Bu bilik və bacarıqların əldə edilməsi

istehsalçının veb-səhifəsin də və müvafiq təlimatlarda mümkündür.

2.5.8. Tıklamadan əvvəl düşünün

Sosial şəbəkələrdə (Post, Tweet, Messages) mövcud olan linklər sizi çaşdırmaq və sensitiv məlumatı əldə etmək üçün kiber kriminallar üçün asan yoldur. Hər hansı bir linkə tıklayana və ona keçənədək diqqətli olun. Bu linklərdən nəyi isə yüklədiyiniz anda xüsusi ehtiyyat göstərin. Əgər linkə keçərkən daxil olduğunuz sosial şəbəkə hesabının adı və şifrəsi tələb edilsə bilin ki, böyük ehtimalla sizin akauntun qırılması üçün kiber kriminalların qurduğu tələdir.

2.5.9. Mənbələri yoxlayın

Sosial şəbəkələrdən alınan məlumat bizim gündəliyimizə və bəzi hallarda faktları alqılamağa da təsir edir. Son zamanlar onu fəal olaraq istifadə edirlər:

- İctimai fikrin formalaşdırılması üçün,
- Seçkilərə müdaxilə edən zaman əhval-ruhiyyəni öyrənmək yaxud formalaşdırmaq üçün,
- Marketinq fəallıqlarını planlaşdırmaq üçün,
- Xüsusi xidmətlərin məqsədlərini həyata keçirmək üçün və s.

Bu və digər məlumatı alarkən onunn mənbəsini yoxlamağı qayda və vədiş edin. Bacardığınız qədər müvafiq məlumatı kimin, nə vaxt, niyə və hansı formada yaydığını yoxlayın.

Nəticə çıxarana və məlumatı etibarlı sayanadək diqqətli olun!

2.5.10. Təhlükəsizlik və məxfilik tövsiyələri ilə tanış olun

Burada gətirilən ümumi məsləhətlərə baxmayaraq müxtəif sosial şəbəkələrə aid olan təhlükəsizlik və məxfililiyə dair konkret məsləhətlər mövcuddur. Əksər hallarda bütün bunlar elə həmin sosial platformada yerləşdirilib və asan anlanılacaq vizual məsləhət və izahat xasiyyətini daşıyır.

Təhlükəsizlik və məxfilik təlimatlarımızı oxuyun

Həmçinin sosial şəbəkənin təhlükəsiz istifadəsi ilə əlaqədar çox sayda video bələdçi, məqalə və bloq yaradılır.

Sosial şəbəkələr hər gün yenilənir, dəyişir və çox zaman yeni növ veb-səhifələr yaradılır. Onların təhlükəsiz istifadə edilməsi ilə əlaqəli məsləhət və tövsiyyələrdən geridə qalmayın. Kiber kriminallardan bir addım irəlidə olun.

2.6. Mobil cihazların təhlükələri və müdafiə yolları

Sizin smartfonunuz və ya tabletiniz şəxsən sizin, sizin aileniz, dostlar və əməkdaşlarınız haqqında dəyərli məlumat saxlayır.

Düşünmüsünüzmü, əgər sizin mobil cihazınızı başqa adam ələ keçirsə, o, hansı məlumatı ələ keçirəcək:

- ¬ Sizin şəxsi planlarınızı və yazılarınızı (notes)
- ¬ Sizin tanış-dostlarınız haqqında əlaqə məlumatı
- ¬ Sensitiv foto və videoları
- ¬ Nə vaxt və kimə zəng etdiyinizi, kimin zəng etdiyini, hansı

müddət ərzində

- İşə aid məxfi faylları
- İctimai olmayan və kompromatlaşdırıcı yazışmanı (messencerlər, sosial şəbəkələr)
- Müxtəlif saytlar və xidmətlər üçün şifrələri
- Hansı məzmunlu saytlara daxil olursunuz və nəyə baxırsınız
- Maliyyə və bank gəlirləri haqqında məlumatı
- Sizin əvvəlki olduğunuz yer haqqında bilgiləri (harda yaşayırsınız, işləyirsiniz və hansı yerlərdə qonaq olursunuz)
- Sizin sağlamlığınız haqqında məlumatı (xəstəlikləri, peyvəndləri, fitnesi, emosional və reproduktiv sağlamlığınız, qaçma marşrutları, allergiya, qəbul edilən dərmənlərin növü və intensivliyi)
- Və s.

Öz telefonlarını itirən, çarəsiz insanları yəqin görmüsünüz. Bu nigaran olmağın səbəbi isə, telefonda mövcud olan məlumatın yad bir insanın əlinə düşməsinin səbəb ola biləcək potensial ziyandır. Bu halda ziyan bu cihazın alınma dəyərindən xeyli çoxdur.

Mobil cihazların müvafiq kiber təhlükəsizlik risklərini azaltmaq, özünüzü, yaxınlarınızı və işinizi müdafiə etmək üçün aşağıda verilən məsləhətləri nəzərə alın.

2.6.1. PİN, şifrə, barmaq izi və üz

Sizin cihazınıza daxil olmaq üçün çətin pin-kodlar və şifrələr istifadə edin. Əgər cihaz imkan verirsə əlavə olaraq barmaq izi yaxud sifətin identifikasiyasını qurun. Bu yol sizin cihazı itirdiyiniz halda müdafiənin ilkin xəttidir.

Vacibdir ki, pin yaxud şifrə çətin olsun (1234 yaxud doğun tarixi, ləqəb olmasın). Onların bir neçə dəfə səhv daxil edilməsindən sonra isə mobil cihaz bloklansın yaxud sizə olduğu yer haqqında mesaja göndərilsin.

2.6.2. Yenilənmələr və bir daha yenilənmələr

Sizin mobil cihazınızın operativ sistemi və onda mövcud olan aplikasiyalar mütəmadi olaraq yenilənmiş olsun deyə avtomatik yenilənmə funksiyasını qurun. Hakerlər mütəmadi olaraq proqram təminatının yeni zəyifliklərinin axtarışındadırlar. İstehsalçılar isə öz tərəflərindən müvafiq yenilənmələri ona görə buraxırlar ki, qeyd edilən çağırışlarla baş edə bilsinlər. Mütəmadi yenilənən operativ sistemlər və aplikasiyalar sizin mobil cihazınızın hak edilməsini vacib dərəcədə çətinləşdirir.

Əgər aplikasiyaların yenilənməsi bir neçə saniyyədə başa çatırsa, bir qayda olaraq operativ sistemin (iOS, Android, Windows) yenilənmələri müəyyən vaxt (10-20 dəq.) tələb edir və bu vaxt mobil cihazı istifadə etmək müvəqqəti olaraq imkansız olur. Vacib yenilənmələri sonraya saxlamayın və onunla əlaqəli təhlükəsizlik parametrlərini dəyişməyin

2.6.3. İzləmək

Sizin mobil cihazınıza internetlə təqib etmək üçün xüsusi aplikasiya yükləyib install edin və ya işə salın. Bu yolla siz itirildiyi və ya oğurlandığı halda mobil cihazınızın yerini təyin edə bilərsiniz. Ən pis halda isə onda mövcud olan istənilən növ məlumatı silə biləcəksiniz.

2.6.4. Güvənli aplikasiyalar

Aplikasiyaları yalnız etibarlı və rəsmi platformalarda yükləyin:

- iPad və iPhone üçün aplikasiyaları rəsmi Apple App Store-dən yükləyin,
- Androidin aplikasiyaların Google Play-dən yükləyin,
- Amazon tabletləri üçün isə Amazon App Store,
- Və digər istehsalçı tərəfindən qeyd edilən etibarlı resurslardan.

Siz aplikasiyaları yad və daha az tanınan veb-səhifələrdən yüklədiyiniz zaman böyük ehtimalla onlar yoxlamanı keçmir və infeksiyalıdırlar.

Həmçinin aplikasiyanı yükləyənə qədər onun istifadəçilər tərəfindən müsbət dəyərləndirmələri və istehsalçı tərəfindən aktiv yenilənmələri olub olmadığını yoxlayın.

Az dəyərləndirilməsi və yenilənmə prosesini nadir hallarda keçən yad aplikasiyalardan çəkinin.

Və sonda, aplikasiyanı haradan yüklədiyinizə baxmayaraq, tövsiyyə edirik ki, lazım deyilsə və ya fəal olaraq istifadə

etmirsinizsə siləsiniz.

2.6.5. Məxfilik

Yeni aplikasiyanı instal etdiyiniz zaman onun məxfilik ayarlarını yoxlayın. Məsələn:

- Aplikasiyaya sizin bütün dostlarınızın əlaqə məlumatlarına əl çatması həqiqətən lazımdırmı?
- Eləcə də, tövsiyyə edirik ki, işləməsi üçün sizin olduğunuz məkanı müəyyənləşdirməsi lazım olmadığını hesab etdiyiniz bütün aplikasiyalarda məkan yerini təyin edən xidməti ləğv edin.
- Əgər sizi, aplikasiyanın cihazınıza dair müxtəlif icazələri qane etmirsə, sizin üçün uyğun olan digər analoqdan istifadə edin.
- Həmçinin, vaxtaşırı olaraq aplikasiyanın hansı funksiyalara icazəsi olduğunu yoxlayın və onların dəyişmədiyindən əmin olun.

Bilin ki, aplikasiyaların idare edilməsinin mənbələri sizin əlinizdədir və onlardan hansının sizin **fotolarınıza, yazışmalarınıza, video kameranıza, mikrafon və yerləşdiyiniz yerə əlçatanlığı olmasına qərar verə bilərsiniz.**

2.6.6 Ehtiyat nüsxələr / yedəkləmə

Həmişə sizin göstəricilərin ehtiyat nüsxələrini yaradın. Mobil cihazları halında isə ehtiyat nüsxələrinin leptop və personal cihazlara keçirmək, yani backup, yaxud daxildə quraşdırılmış onlayn rezervasiyanın (məsələn, icloud-un, yaxud google drive-ın) istifadə edilməsi. Bu halda sizin məlumatınız onun silinməsi, cihazınızın itməsi və ya fiziki zədələnməsi halında da silinməyəcək.

Avtomatik ehtiyat nüsxələrinin yaradılmasını həyata keçirmək nisbətən asandır, lakin ehtiyat nüsxələrinin yaradılmasının texniki qaydaları ilə yaxşı tanış olun.

Özünüzü sığorta etmək üçün, bir neçə dəfə ehtiyat nüsxələrini bərpa etməyə çalışın və onların sizin üçün məqbul olan qaydaya uyğun olaraq saxlandığına (ehtiyat olunduğuna) əmin olun:

- Dövrilik
- Həcm
- Tezlik
- Ehtiyat faylların məzmunu
- Saxlama sahəsi
- Saxlama forması
- və s.

2.6.7. İş və uzaqdan çalışmaq

İş yerində olan zaman xüsusi ehtiyyatla davranın ki, video və foto şəkil çəkdiyiniz zaman sensitiv məlumatı olan foto şəkil (löhvələrin, kompüter ekranlarının və s. göründüyü) çəkməyəsiniz.

Son zamanlar pandemiya və digər təhlükələr nəticəsində tez-tez dünyanın müxtəlif nöqtələrində – evdə, kafedə, otel və ya nəqliyyatda mobil cihazlarla işləməli oluruq. Bu halda sizin mobil cihazlarınıza hücum ehtimalı xüsusilə yüksək olur. Çünki kiber kriminallar sizin müdafiə səviyyənizin işdə (ofisdə) olduğunuz zaman korporativ-təşkilati səviyyədə həyata keçirilməndən daha zəif olacağını anlayırlar.

Əgər işlə təmin olunubsunuz və uzaqdan çalışırsınızsa sizin mobil cihazınızdan əldə edilən icazəsiz giriş, tək sizin fərdi göstəricilərinizə deyil, həmçinin işlədiyiniz təşkilatın sensitiv məlumatına da təhlükə yaratdığını unutmayın. Onun itirilməsi/sızması halında isə sizə qarşı intizam-inzibati tədbirlər də götürülə bilər və məsuliyyət daşıya bilərsiniz.

2.6.8. Hədiyyə etmək, satmaq, tullamaq

Əgər siz mobil cihazınızı dəyişmək qərarını versəniz köhnə cihazınızı başqasına verənədək yaxşı düşünün. Onda hansı məlumatın olduğu yadınızda olsun. Tam olaraq (və yalnız fotolar deyil) mobil cihazınızı silin, Factory Reset, Format funksiyalardan istifadə edin. Bu onda mövcud olan hər növ məlumatın silinməsini və zavod vəziyyətinə qayıtmasını təmin edəcək.

Belə halda yeni sahibin sizin köhnə fayllarınıza hər hansı bir növ giriş əldə etməsi ehtimalı çox azdır.

2.6.9. Wi-Fi internetdən istifadə etmək

Mobil cihazların üstünlüyü həqiqətən də onun mobil olmasıdır. Bu internet şəbəkəsində fiziki kabellər quraşdırılmadan istənilən yerdən işləməyi nəzərdə tutur. Belə hallarda kafelər yaxud ümumi məkanlarda mövcud olan pulsuz və açıq Wi-Fi şəbəkələrinin istifadəsi cəlbedicidir. Yadınızda saxlayın ki, belə şəbəkələr daha az müdafiəlidir və əksər hallarda onların istifadəsi ilə həyata keçirilən aktivlik riskli ola bilər. Əgər belə şəbəkələrin müdafiəli olduğundan əmin deyilsinizsə, sadalanan fəallıqlarla məşğul olmayın: vacib ünsiyyət, bank tranzaksiyalarının yerinə yetirilməsi, məxfi faylların başqası ilə paylaşılması və s.

2.6.10. Fors-major vəziyyətində davranış qaydası

Yadda saxlayın ki, sizin mobil cihazınızın unikal identifikatorları var (onlar arasında: IMEI nömrəsi, MAC ünvanı, seriya nömrəsi). Bu nömrələri qeyd edin və lazım olduğu halda müvafiq idarələrə bildirin. Bu nömrələrin, hüquq mühafizəcilər və mobil/internet provayderlərinin köməyi ilə sizin itən cihazınızı tapmaq mümkündür.

Müasir mobil cihazların fəlakətli vəziyyətlərdə avtomatik hərəkətlər etmək imkanı var: yəni əvvəlcədən seçilmiş hər hansı kombinasiyanı yazarkən:

- ¬ Avtomatik olaraq yerləşdiyiniz yeri təcili yardım xidmətinə göndərir,
- ¬ Əvvəlcədən müəyyən edilmiş nömrəyə lazımi SMS mesajı göndərir,
- ¬ Foto-video material çəkir və göstərilən ünvana göndərir,
- ¬ Daxili modul vasitəsilə sizin yıxılmanızı və ya hər hansı fiziki hadisəni qeyd edir;

Yuxarıda göstərilən qaydalarla tanış olun və yadda saxlayın ki, bəzən mobil cihaz sadəcə rəqəmsal ünsiyyət vasitəsi deyil.

Gürcüstanın Strategiya və İnkişaf Mərkəzi

www.gcsd.org.ge
gcsd@gcsd.org.ge
032 2 22 26 67
Mtsxeta küçəsi #48/50