AZƏRBAYCAN RESPUBLİKASI ELM VƏ TƏHSİL NAZİRLİYİ

AZƏRBAYCAN DÖVLƏT İQTİSAD UNİVERSİTETİ

UNEC BİZNES MƏKTƏBİ

"ŞİRKƏTDƏ KİBER TƏHLÜKƏSİZLİYİN VƏ KİBER RİSKLƏRİN TƏŞKİLİNİN QİYMƏTLƏNDİRİLMƏSİ"

mövzusunda

MAGİSTR DİSSERTASİYA İŞİ

ABBASOV HÜSEYN QURBAN

BAKI – 2023

AZƏRBAYCAN RESPUBLİKASI ELM VƏ TƏHSİL NAZİRLİYİ
AZƏRBAYCAN DÖVLƏT İQTİSAD UNİVERSİTETİ
UNEC BİZNES MƏKTƏBİ

UNEC Biznes Məktəbinin direktoru
i.e.n.,dos.Hacıyev Nazim Özbəy
"_____" (imza)
"___" _____ 2023-cü il

"ŞİRKƏTDƏ KİBER TƏHLÜKƏSİZLİYİN VƏ KİBER RİSKLƏRİN TƏŞKİLİNİN QİYMƏTLƏNDİRİLMƏSİ"

mövzusunda

MAGİSTR DİSSERTASİYA İŞİ

İxtisasın şifri və adı: 060409 Biznesin idarəedilməsi

İxtisaslaşma: Kibertəhlükəsizlik

Qrup: A19/21

Magistrant
Abbasov Hüseyn Qurban

_____imza

Elmi rəhbər
t.e.f.d. Əbdiyeva - Əliyeva Günay Əlişan

_____imza

Proqram rəhbəri
i.f.d. Qəzənfərli Mirvari Xəqani

_____imza

Kafedra müdiri
dos. Məmmədova Sevər Mömin

_____imza

BAKI – 2023

Təşəkkürnamə

Tədqiqat işinin aparılmasında nəzəri və praktiki biliklərin əldə olunması istiqamətində yardım göstərən Günay Əbdiyeva Əliyeva, həmçinin praktiki tərəfinin təşkilində böyük dəstəyi olan "Cahan Holding" İT departament rəhbəri İlham Əliyevə təşəkkür edirəm.

ŞİRKƏTDƏ KİBER TƏHLÜKƏSİZLİYİN VƏ KİBER RİSKLƏRİN TƏŞKİLİNİN QİYMƏTLƏNDİRİLMƏSİ

Xülasə

Dissertasiya işinin aktuallığı: Şirkətdə kibertəhlükəsizliyin və kiber risklərin qiymətləndirilməsi həssas məlumatları qorumaq və biznesin nüfuzuna və maliyyə sabitliyinə xələl gətirə biləcək kiberhücumların qarşısını almaq üçün çox vacibdir. Kibertəhlükələr inkişaf etməyə davam etdikcə, şirkətlərin sistemlərində və şəbəkələrində zəiflikləri müəyyən etmək üçün müntəzəm qiymətləndirmələr aparması vacibdir.

Dissertasiya işinin məqsədi: Rəqəmsal dünyada potensial insidentlərə qarşı öncədən hazırlıqlı olmaq üçün baş verən ən geniş təsirli hücum növləri ilə tanış olub, tətbiq oluna biləcək avadanlıq və proqramların iş prinsiplərini öyrənməklə daha dəqiq və operativ şəkildə təşkilatları qorumaqdır.

Dissertasiya işində istifadə edilmiş biznes tədqiqat metodları: Cahan Motors MMC daxilində fişinq hücum simulyasiyası həyata keçirilmişdir. Bu, Cahan Motors MMC-ə öz kibertəhlükəsizlik müdafiələrini qiymətləndirməyə və uğurlu fişinq hücumların ehtimalını azaltmağa imkan vermişdir.

Dissertasiya işinin məhdudiyyətləri: Mükəmməl səviyyəyədə qorunmaq üçün kibertəhlükəsizlik sistemlərinin standartlara uyğun səviyyədə qurulması və yeni texnologiyalardan istifadəsi yüksək xərclərə səbəb olur və nəticədə təşkilatlar tərəfindən istifadəsinə üstünlük verilmir.

Dissertasiya işinin praktik nəticələri: Təşkilata dəyə biləcək maddi və mənəvi zərərlərin qarşısını almaq məqsədi ilə rəqəmsal mühitdə təhlükəsizlik səviyyəsini yüksəltməklə mövcud olan kibertəhlükəsizlik standartlarına riayət etmək zəruridir.

MÜNDƏRİCAT

Giriş

Mövzunun aktuallığı: Şirkətdə kibertəhlükəsizlik və kiberrisklərin idarə edilməsinin qiymətləndirilməsi müasir biznes əməliyyatlarının mühüm tərkib hissəsidir. Biznes əməliyyatları üçün texnologiyaya və internetə artan etibarla şirkətlər əməliyyatlarını poza biləcək və potensial olaraq əhəmiyyətli maliyyə itkilərinə səbəb ola biləcək yeni və inkişaf edən kibertəhlükələrlə üzləşirlər.

Dissertasiya işinin məqsədi: Bu işin məqsədi təşkilatları kibertəhlükəsizliyin əhəmiyyəti və effektiv kiberrisklərin idarə edilməsi təcrübələrinin zəruriliyi haqqında maarifləndirmək və məlumatlandırmaqdır.

Dissertasiya işi kiberhücumların artan təhlükəsini və onların şirkətin əməliyyatlarına, reputasiyasına və nəticələrinə təsirini vurğulamaq məqsədi daşıyır. O, həmçinin şirkətlərin təhlükəsizlik vəziyyətini mütəmadi olaraq qiymətləndirməklə, kiber risklərin idarə edilməsi üzrə ən yaxşı təcrübələri tətbiq etməklə və kiberhücuma cavab planı hazırlamaqla kibertəhlükəsizliyə proaktiv yanaşmanın zəruriliyini vurğulayır.

Dissertasiya işi müxtəlif auditoriyalar, o cümlədən biznes sahibləri, rəhbər şəxslər və şirkətin informasiya və texnologiya sistemlərinin təhlükəsizliyinə cavabdeh olan hər kəs üçün nəzərdə tutulub. Mövzuya hərtərəfli baxış təqdim etməklə, bu iş təşkilatlara kibertəhlükəsizliyin əhəmiyyətini və özlərini kibertəhlükələrdən qorumaq üçün atacaqları addımları anlamağa kömək etmək məqsədi daşıyır.

Tədqiqatın predmeti: Dissertasiyasının işinin tədqiqat predmeti şirkətlərdə kibertəhlükəsizliyin və kiberrisklərin idarə edilməsinin mövcud vəziyyətinin dərk edilməsinə və mövcud təcrübələrin effektivliyinin qiymətləndirilməsinə yönəlmişdir. Bu tədqiqatın əsas məqsədi kibertəhlükəsizlik və kiberrisklərin idarə edilməsində ən mühüm problemləri və qabaqcıl təcrübələri müəyyən etmək və şirkətlər üçün təhlükəsizlik vəziyyətini yaxşılaşdırmaq üçün praktiki tövsiyələr hazırlamaqdır.

Tədqiqatın obyekti: Cahan Motors MMC-də kibertəhlükəsizlik müdafiəsini qiymətləndirmək üçün fişinq hücumu simulyasiyası həyata keçirilmişdir. Bu

proaktiv tədbir zəiflikləri müəyyən etməyə, təhlükəsizliyi gücləndirməyə və gələcəkdə uğurlu fişinq hücumları riskini minimuma endirməyə imkan verdi.

Elmi yenilik: Dissertasiya işi cari kibertəhlükəsizlik və kiber risklərin idarə edilməsi təcrübələrindəki boşluqları və zəif nöqtələri müəyyən edə bilər. Bu çatışmazlıqları vurğulayaraq, şirkətlərin kibertəhlükəsizlik vəziyyətini gücləndirə biləcək təkmilləşdirmələri təklif edir. Bu, daha effektiv risklərin idarə edilməsi çərçivələrinin hazırlanmasını, yeni texnologiyaların və strategiyaların qəbulunu və şirkətdə daha güclü kibertəhlükəsizlik mədəniyyətinin yaradılmasını əhatə edə bilər.

İşin praktiki əhəmiyyəti: Dissertasiya işi şirkətlərin mövcud kibertəhlükəsizlik və kiberrisklərin idarə edilməsi təcrübələrini necə qiymətləndirə və təkmilləşdirilməsi lazım olan sahələri müəyyənləşdirə biləcəyinə dair praktiki fikirlər verə bilər. Mövcud təcrübələrin effektivliyini qiymətləndirməklə, tədqiqat şirkətin kibertəhlükəsizlik mövqeyini gücləndirə biləcək təkmilləşdirmələr təklif edə bilər. Məsələn, dissertasiya yeni texnologiyaların və strategiyaların qəbulunu, daha effektiv risklərin idarə edilməsi çərçivələrinin işlənib hazırlanmasını və şirkət daxilində daha güclü kibertəhlükəsizlik siyasəti yaradılmasını tövsiyə edə bilər.

Tədqiqatın elmi və nəzəri əsasları: Dissertasiya işinin nəzəri əsaslarının işlənib hazırlanması prosesində Türkiyə və digər ölkələrdən olan mütəxəssislər tərəfindən hazırlanmış kitab, məqalə və digər materiallar kimi müxtəlif mənbələrdən istifadə edilərək tədqiqatı aparılmışdır.

İşin struktur və həcmi: Dissertasiya işi giriş, üç fəsil, nəticə və təfliklər, dissertasiya işində istifadə olunmuş ixtisarlar və tədqiqat işində istifadə olunan ədəbiyyatların siyahısından ibarətdir. Giriş hissəsində tədqiqatın aktuallığı, məqsədi, predmeti, obyekti, elmi yenilik, praktiki əhəmiyyəti və nəzəri əsasları haqqında qısa məlumat verilmişdir.

Birinci fəsil, üç alt başlıqdan ibarət olmaqla, informasiya təhlükəsizliyi, kiber təhlükəsizliyin əsas konsepsiyaları və korporativ kiber təhlükəsizliyin əhəmiyyəti haqqında ümumi anlayış verilmişdir.

İkinci fəsildə Korporativ şəbəkə təhlükəsizliyi, kibertəhlükəsizlik texnologiyaları və kibertəhlükəsizlik çərçivələri haqqında məlumatlar qeydə

alınmışdır.

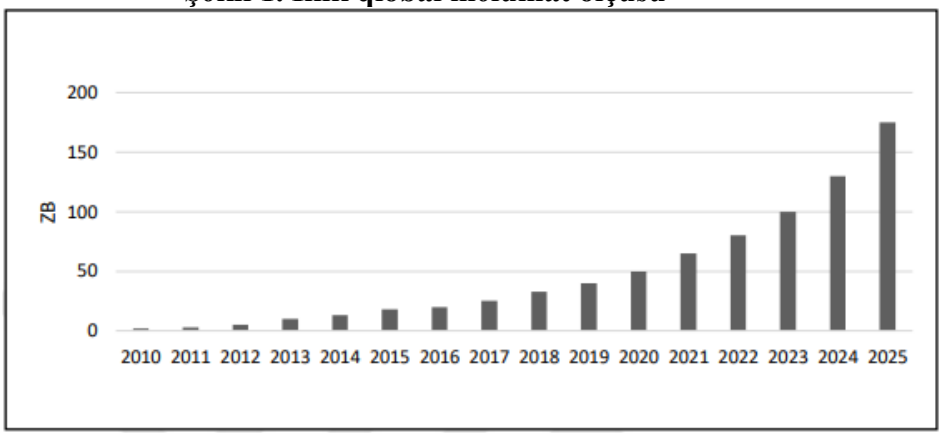
Üçüncü fəsildə isə təşkilatlara yönəlmiş fişinq hücumlarını anlayaraq fişinq hücum simulyasiyası (Cahan Motors MMC timsalında) həyata keçirilmişdir.

FƏSİL 1. ŞİRKƏTDƏ KİBER TƏHLÜKƏSİZLİK VƏ İNFORMASİYA TƏHLÜKƏSİZLİYİ

1.1 İnformasiya Təhlükəsizliyi Və Əsas Konsepsiyalar

Məlumat (Data) - Müasir şəraitdə inkişaf etmiş kimi xarakterizə edilən bu cəmiyyətin keyfiyyətinə yiyələnməsində ən mühüm amil onların sahib olduqları məlumatların miqdarıdır. Ona görə də bu günün ən mühüm kapitalı məlumatdır. Tarixən bütün əsas iqtisadiyyatlar məlumata əsaslanmışdır. Məlumat subyekt-obyekt münasibətləri nəticəsində yaranan müxtəlif məhsullardır. Bir subyekt obyektə əlçatan olduqda, məlumat və məlumatların həcmi kəskin şəkildə artır və növbəti bir neçə il ərzində parabolik artım gözlənilir. 2022-ci ildə istehsal olunan məlumat ölçüsü 63 ZetteBayt (63 trilyon GB) olduğu halda, 2025-ci ildə istehsal olunan məlumat ölçüsünün 175 ZetteBayt olacağı gözlənilir (Şəkil 1).

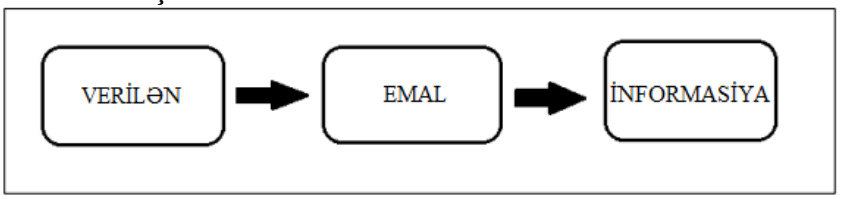
Şəkil 1. İllik qlobal məlumat ölçüsü



Mənbə: The Digitization of the World From Edge to Core.

Verilənlər informasiyanı aşkar etmək üçün emal edilməli olan rəqəmlərə və mətnlərə aiddir. Verilənlər; İnformasiya emal edilməsi nəticəsində yaranan məlumat dəstidir. Hər bir informasiya verilən olsa da, hər bir verilən informasiya deyil. İnformasiyanın əldə edilməsi prosesi aşağıdakı Şəkil 2-də göstərilmişdir.

Şəkil 2. Məlumatın əldə edilməsi



Mənbə: Müəllif tərəfindən tərtib edilmişdir.

İnformasiya Təhlükəsizliyi - İnformasiya təhlükəsizliyi məlumatların məxfiliyini, bütövlüyünü və əlçatanlığını təmin etmək, arzuolunmaz şəxslərin məlumatlara daxil olmasının qarşısını almaq və təşkilatda məlumatı əlçatanlıq səlahiyyətinə malik olan şəxslərin bu məlumatlara çıxışına icazə vermək üçün alətlərin və siyasətlərin strateji idarə edilməsidir.

Təşkilatlarda biznesin davamlılığı üçün geniş şəkildə məlumat istifadə olunur. Məlumatdan interaktiv istifadənin artması xidmətlər, təşkilatlar və ölkələr arasında məlumat ötürülməsinin sürətlənməsi ilə məlumatın təhlükəsiz saxlanması ehtiyacları qarşılaya bilməyəcək hala gətirdi. İnformasiyanın təhlükəsizliyini təmin etmək üçün həm məlumatın emal edildiyi yerdə təhlükəsiz saxlanılması, həm də ötürülmə zamanı baş verə biləcək hücumlara, dəyişikliklərə, pozuntulara və əldə etmələrə qarşı təhlükəsizliyini təmin etmək lazımdır. Bu nöqtədə informasiya təhlükəsizliyi prinsipləri ortaya çıxır. İnformasiya təhlükəsizliyi mövzusu araşdırılanda görünür ki, əksər mənbələr informasiya təhlükəsizliyini təmin etmək üçün üç elementi qeyd edir. Bunlar ingiliscə "CIA" sözlərinin baş hərfləri ilə ifadə edilir.

İnformasiya Təhlükəsizliyi Prinsipləri:

Məxfilik - Məxfilik informasiyanın icazəsiz şəxslərin girişinə bloklanma kimi ifadə edilir. Bu, həssas məlumatların arzuolunmaz insanlara çatmasının qarşısını almaq üçün lazımdır. Məlumatların emalının hər bir mərhələsində lazımi məxfilik səviyyəsinin təmin edilməsi icazəsiz girişin qarşısını alır. Şəbəkədəki sistemlərdə və cihazlarda məxfilik səviyyəsi məlumat ötürüldükdə və təyinat yerinə çatdıqda tətbiq edilməlidir.

Təşkilatların informasiya sistemlərində olan məlumatlar rəqiblərin öz üstünlükləri üçün istifadə edəcəkləri məlumatları, korporativ işçilərin şəxsi məlumatlarını və müştəri məlumatlarını ehtiva edə bilər. Məxfi məlumat çox vaxt qiymətlidir və buna görə də məxfi məlumatı olan təşkilatlar tez-tez kiberhücumlara məruz qalırlar (Altınkaynak M.,2020: s.10).

Təşkilatların öz məxfiliyini təmin etmək üçün görüdüyü bəzi tədbirlər:

Şifrələmə - Şifrələmənin təmin edilməsi informasiya təhlükəsizliyində məxfiliyin təmin edilməsi üçün ən mühüm tədbirlərdən biridir. Bu ehtiyat tədbiri hər

bir mümkün platforma üçün həyata keçirilməlidir. Fərdi kompüter əməliyyat sistem girişləri, disklər, veb-saytlar, portallardan başqa obyektlərə və fiziki məlumat mərkəzlərinə giriş də yoxlanılmalı və nəzarət edilməlidir.

İki faktorlu autentifikasiya - İki faktorlu autentifikasiya iki faktorlu bir addımla şəxsiyyətin təsdiqini təmin edən təhlükəsizlik tədbiridir. Şifrələmə ilə məlumatların təhlükəsizliyini təmin etmək mümkündür, lakin istifadəçi adı və şifrənin hansısa yolla təcavüzkarların əlinə keçməsi ehtimalı başqa bir təhlükəsizlik tədbirinin görülməsinə səbəb olub. İstifadəçi adı və şifrəni bilməklə sistemə daxil olmaq istəyərkən, sorğu edən şəxsin hüquqi şəxs, yoxsa təcavüzkar olduğu bilinmir. İki faktorlu autentifikasiya ilə hüquqi şəxsin sorğu verdiyini sübut edərək sistemə daxil olmaq mümkündür (https://www.cisa.gov/cybersecurity).

İki faktorlu autentifikasiya istifadəçi adı və şifrə ilə giriş sorğusu göndərildikdən sonra sistemdə qeydiyyatdan keçmiş mobil telefon nömrəsi, e-poçt ünvanı və ya Google Authenticator-dan alınacaq parolla daxil olmağa imkan verir.

Məlumatların ehtiyat nüsxəsinin çıxarılması - Məlumatların ehtiyat nüsxəsinin çıxarılması məlumatın nüsxələrinin saxlandığı yerdən başqa fiziki və ya virtual saxlama vahidlərində qorunmasına deməkdir. Məlumatların ehtiyat nüsxəsi olmadan məlumatların bərpası çox xərcli, yavaş və hətta mümkün olmaya bilər. Məlumatların müntəzəm olaraq saxlanması, qorunması və ehtiyat nüsxəsinin çıxarılması vacibdir.

Müntəzəm ehtiyat nüsxələri proqram və avadanlıq xətaları, viruslar, haker hücumları, elektrik enerjisinin kəsilməsi, insan səhvi nəticəsində baş verə biləcək zərər və itki risklərindən qorunmanı təmin edir. Ehtiyat nüsxələri çıxarılmış məlumatların qorunan mühitlərdə saxlanması təmin edilməlidir.

Qarşılıqlı məlumatların təhlükəsizliyi - Təşkilatlar və şəxslər bizneslərinin tələb etdiyi kimi kritik məlumatları bir yerdən digər yerə köçürərkən və ya bir sistemə daxil olarkən sessiya məlumatları şifrələnmədən yazıla bilər. Bu sessiya məlumatı üçün təhlükəsizlik tədbirləri görülməzsə, bu məlumat hücumçular tərəfindən "Man-in-the-middle attack (ortadakı adam hücumu)" ilə əldə edilə bilər. Məlumatı qorumaq üçün məlumatlar SSL sertifikatı ilə şifrələnməlidir.

Qarşılıqlı əlaqədə olan internet şəbəkəsi təhlükəsizliyi olmayan və ya zəif olan şəbəkədirsə, təcavüzkarlar şəxsi kompüter ilə internet arasına müdaxilə edərək məlumatları əldə edə bilərlər. Məlumatların etibarlılığı üçün təhlükəsizliyi olmayan internet şəbəkələrinə qoşulmaq təhlükə yarada bilər (Başaran A.,2019: s.55).

Bütövlük - Bütövlük məlumatın düzgünlüyünü təmin etmək mənasına gəlir. Məlumatın yalnız səlahiyyətli şəxslər tərəfindən dəyişdirilməsi şərtdir. Məlumatların bütövlüyü təmin edildikdə, məlumatların nə tezlikdə və nə qədər vaxta əldə olunmasından asılı olmayaraq, saxlanılan məlumat tam, dəqiq və etibarlı qalacaqdır.

Fiziki bütövlüy - Bu, məlumatların götürüldüyü və saxlandığı yerin fiziki mühafizəsidir. Sel, zəlzələ, elektrik kəsilməsi kimi fövqəladə vəziyyətlərdə fiziki bütövlük təhlükə altında olu. Fövqəladə hallar üçün zəruri fiziki infrastruktur və bütövlük təmin edilməlidir.

Məntiqi bütövlük - Məntiqi bütövlük verilənlərin dəyişməz və etibarlı olduğunu sübut edir. Məntiqi bütövlüyü təmin

etmək üçün məlumatların bir dəfədən çox siyahıya alınmaması, cədvəldə heç bir sahənin boş olmaması, mövcud olmayan məlumatların verilənlər bazasına daxil edilməməsi, məlumatların formatının, növünün və həcminin məhdudlaşdırılması kimi amillər nəzərə alınmalıdır.

Əlçatanlıq - Əlçatanlıq səlahiyyətli istifadəçilər tərəfindən tələb olunan məlumatın həmişə əlçatan olması deməkdir. Məlumatı saxlamaq və emal etmək üçün istifadə olunan hesablama sistemləri, onu qorumaq üçün istifadə olunan təhlükəsizlik nəzarəti və onu daşımaq üçün istifadə olunan rabitə kanalları düzgün işləməlidir.

Məlumatın əlçatanlığını qorumaq üçün görülən tədbirlər idarə edilə bilən və davamlı olmalıdır. Zəruri hallarda kritik məlumatlara daxil ola bilməmək biznes əməliyyatlarının dayanmasına səbəb ola bilər, ona görə də məlumatların bütövlüyünün davamlılığı təşkilatlar üçün əsas prioritetlərdən biri olmalıdır. Lazım olduqda məlumatlara çıxışın olmamasının nəticələri birbaşa təşkilata təsir edir.

Məlumatların əlçatmazlığı əlaqəli iş xətlərinə təsir göstərə və təşkilatın

strukturuna zərər verə bilər. Məlumatlara daxil olmaq istəyinin səbəbi müştəriyə xidmət etməkdirsə, daha yaxşı məhsul və xidmətlər təklif olunmaya bilər və gələcək iş imkanları əldən verilə bilər.

Biznes uğurunun ən vacib elementlərindən biri brend və reputasiyadır. Formalaşması və inkişafı üçün çox səy və vaxt tələb edən brendinq və reputasiya anında yox ola bilər.

Bir şirkətin köhnə brend dəyərini və reputasiyasını bərpa etmək çox çətindir, o, qalıcı ziyanlar verə və hətta təşkilatın sonunu gətirə bilər. Məlumatların harada saxlandığı və etibarlı şəkildə əldə oluna biləcəyi təmin edilməli və qanuni öhdəliklər çərçivəsində tədbirlər görülməlidir.

1.2 Kiber Təhlükəsizlik Və Əsas Konsepsiyalar

Bu bölmədə kibertəhlükəsizlik və kibertəhlükəsizliyin əsas konsepsiyaları olan kiber məkan, kiber təhlükə, kiberhücum, kiber silah, kibermüharibə kimi əsas anlayışlar müzakirə olunacaq.

Kibertəhlükəsizlik - Kibertəhlükəsizlik kiber mühiti, təşkilatı və istifadəçi aktivlərini qorumaq üçün istifadə edilə bilən alətlər, siyasətlər, təhlükəsizlik konsepsiyaları, təhlükəsizlik tədbirləri, təlimatlar, risklərin idarə edilməsi, tədbirlər, təlimlər, ən yaxşı təcrübələr, təminat və texnologiyalar toplusudur. Kibertəhlükəsizlik kiberhücum riskini azaltmaq və sistemlərin, şəbəkələrin və texnologiyaların icazəsiz istismarından qorunmaq məqsədi daşıyır (Başaran A.,2021: s.29).

Kiberməkan internet, telekommunikasiya şəbəkələri, kompüter sistemləri, inteqrasiya olunmuş prosessorlar və nəzarətçilər də daxil olmaqla, bir-biri ilə əlaqəli informasiya texnologiyaları infrastrukturları şəbəkəsindən ibarət informasiya mühiti daxilində qlobal məkandır.

Kiber təhlükə məlumatlara zərər vermək, məlumatları oğurlamaq və ya ümumilikdə rəqəmsal mediaya zərər vermək məqsədi daşıyan bir təhlükədir. Kiber təhlükələrə kompüter virusları, məlumatların pozulması, xidmətdən imtina (DoS) hücumları və digər hücum vektorları daxildir. Kiber təhlükələr həmçinin

informasiya texnologiyaları aktivinə, kompüter şəbəkəsinə, əqli mülkiyyətə və ya hər hansı həssas məlumatlara icazəsiz daxil olmaq, zədələmək, pozmaq və ya oğurlamaq məqsədi daşıyan uğurlu kiberhücum ehtimalına aiddir.

Kiberhücum kompüterləri və ya kompüter sistemlərini yararsız hala salmaq, məlumatları oğurlamaq və ya əlavə hücumlara başlama məqsədli edilən bir cəhdidir. Kibercinayətkarlar kiberhücum etmək üçün müxtəlif üsullardan, o cümlədən zərərli proqram, fişinq, ransomware, adam-in-the-middle hücumu və digər üsullardan istifadə edirlər.

Kiber silah kiberhücumun bir hissəsi kimi hərbi və ya kəşfiyyat hədəfləri üçün istifadə edilən zərərli proqram agentləridir. Kiber silahlar dövlət və ya qeyri-dövlət təşkilatları tərəfindən dəstəklənir.

Kiber müharibə bir millətin və ya beynəlxalq təşkilatın kiber silahlardan və digər hücum vektorlarından istifadə edərək başqa ölkənin və ya təşkilatın sistem, şəbəkə və texnologiyalarına zərər vurma cəhdidir. Dövlətlər kiber əməliyyatlardan istifadəni araşdırdıqca və imkanları birləşdirdikcə, kiber əməliyyatın bir nəticəsi və ya onun bir hissəsi kimi ortaya çıxan fiziki münaqişə və zorakılığın yaranması ehtimalı artır. Bununla belə, müharibənin miqyasını proqnoz etmək mümkün deyildir, ona görə də kiber müharibədə qeyri-müəyyənliklər daimidir.

Haker - Haker texniki problemi aradan qaldırmaq üçün kompüter, şəbəkə və ya digər bacarıqlardan istifadə edən şəxsdir. Texniki bacarıqları olan hər kəsi haker adlandırmaq olar, lakin adətən öz bacarıqlarından sistemlərə və ya şəbəkələrə hücum etmək və icazəsiz giriş əldə etmək üçün istifadə edənlər kimi tanınırlar. Haker insanlara zərər vermək üçün fişinq hücumu etmək və ya sistemləri yararsız hala gətirməklə məlumatları oğurlaya və fidyə toplamaq üçün bu sistemləri girov saxlaya bilər.

Haker termini tarixən bölücü bir termindir, bəzən texniki problemlərə yanaşmada yüksək bacarıq və yaradıcılıq nümayiş etdirən birinə heyran olmaq üçün istifadə olunur, lakin bu termin daha çox bu bacarıqdan qeyri-qanuni və ya qeyri-etik məqsədlər üçün istifadə edən insanları təsvir etmək üçün istifadə olunur.

Haker termininin müxtəlif şərhlərinin olması insanların niyyətlərinə görə

adların verilmə zərurətinə səbəb olub. Hakerlər ağ papaq, boz papaq və qara papaq olmaqla üç yerə bölünür (https://www.scmagazine.com/).

Ağ papaqlı haker - Etik hakerlər olaraqda adlandırılan ağ papaqlı hakerlər təhlükəsizlik sistemlərinə giriş əldə edərkən heç bir zərərli niyyəti olmayan insanlardır. Ağ papaqlı hakerlər adətən bir təşkilatda maaş qarşılığında işləyən şəxslərdir və sistemləri daha güclü və hücumlara qarşı daha dayanıqlı etmək üçün çalışırlar. Mümkün hücumlar baş verməmişdən əvvəl sistemlərdəki zəiflikləri tapan, qabaqlayıcı işlər görən, hücum zamanı və hücumdan sonra lazımi tədbirləri görən işçilərdir. Ağ papaqlı hakerlər sistemlərin təhlükəsizliyi üçün sistemlərə sızmaq lazım olduqda lazımi icazələri əldə etməklə bunu edirlər.

Qara papaqlı haker - Qara papaqlı hakerlər zərərli niyyətlə kompüter şəbəkələrinə icazəsiz giriş əldə edən cinayətkarlardır. Onlar həmçinin faylları məhv edən, kompüterləri kilidləyən, parolları, kredit kartı nömrələrini və digər şəxsi məlumatları oğurlayan zərərli proqramlardan istifadə edə bilərlər. Qara papaqların motivasiyası maddi qazanc, qisas almaq və ya sadəcə xaos yaratmaq ola bilər. Bəzən motivasiya həm də ideoloji ola bilər və rəqiblər hədəfə alına bilər.

Boz papaqlı haker - Boz papaq hakerlərinin fəaliyyəti ağ papaq və qara papaq haker fəaliyyətlərinin qarışığıdır. Boz papaqlı hakerlər tez-tez təşkilatların icazəsi olmadan sistemlərə nüfuz edir və təhlükəsizlik zəifliklərini axtarırlar. Onlar adətən problem və zəiflikləri təşkilata bildirib, aşkarlanan zəifliklərə görə pul tələb edə bilərlər. Boz papaqlı hakerlər təşkilat bildirişə cavab vermədikdə və ya hər hansı səbəbdən aralarında fikir ayrılığı yarandıqda, əldə etdikləri məlumatları internetdə dərc edə bilərlər. Bu məlumat qara papaqlı hakerlərin əlində olarsa, təşkilata böyük ziyan dəyə bilər. Boz papaqlı hakerlər niyyətlərində zərərli deyillər, tapdıqları təhlükəsizlik boşluqlarından təşkilata zərər vermək üçün istifadə etmirlər, lakin Müəssisədən icazə tələb olunduğu üçün icazəsiz giriş halında cinayətkar sayılırlar.

1.3 Korporativ kiber təhlükəsizlik və onun əhəmiyyəti

Təşkilatın ən mühüm məqsədlərindən biri qərar qəbul etmək üçün etibar edə biləcəyi məlumat və sistemlərin davamlı mövcudluğunu qorumaqdır. Digər tərəfdən

kiberhücumlar davamlı olaraq inkişaf edir və dəyişir, təcavüzkarlar isə sistemləri yararsız vəziyyətə salmaq, məxfi məlumat əldə etmək, maliyyə qazancı təmin etmək əsaslı motivasiya qaynaqlarına sahib olmaqla davamlı olaraq yeni hədəflər axtararkən təşkilatları daim risk altına salırlar. Daim inkişaf edən təhdid mühiti qarşısında təşkilatlar adekvat kibertəhlükəsizlik tədbirləri görmədikləri təqdirdə məxfi məlumatların ifşası, maliyyə itkiləri, reputasiya itkisi kimi ciddi zərərlərlə üzləşə bilərlər. Bu səbəbdən kibertəhlükəsizlik biznesin müvəffəqiyyətini təmin edən iş davamlılığı axtarışında yüksək səviyyəli rəhbərlik tərəfindən prioritet məsələyə çevrilmişdir (Mitnick K., 2011: s.57).

Müəssisələrdə kibertəhlükəsizlik komandaları :

Kibertəhlükəsizlik sahəsində çalışan komandalar üzərlərinə götürdükləri öhdəliklərə görə fərqlənirlər. Bu komandaların adları rənglərlə ifadə olunur.

Qırmızı komanda - Potensial təcavüzkarların alət və üsullarından istifadə edib, onları təqlid edərək təşkilatın təhlükəsizlik səviyyəsini sınaqdan keçirən komandalardır. Testlər potensial təcavüzkarların davranış və üsullarını ən real şəkildə təqlid etməklə həyata keçirilir. Bir təcavüzkar rolunu öz üzərinə götürərək, təşkilatlara kibertəklükəsizlik cəhətdən təhdid yarada biləcək vəziyyətləri ortaya çıxartmaq üçün çalışır. Qırmızı komandanın fəaliyyətindən maksimum fayda real simulyasiyanı təmin etmək üçün təşkilatın müdafiə infrastrukturu haqqında biliyi olmayan komandaların birləşdirilməsi ilə əldə edilir.

Qırmızı komandanın fəaliyyətinin uğurlu və təsirli olması üçün hücum edənlərin istifadə edə biləcəyi bütün taktika, texnika və prosedurları bilmək lazımdır. Mümkün məlumat pozuntularının aşkarlanması və mümkün təhlükəsizlik zəifliklərinin aşkarlanması ilə yanaşı, həm də hücumların aşkarlanması və qarşısının alınması üzrə fəaliyyətlərin sürətləndirilməsi nəzərdə tutulur.

Təşkilatlar qırmızı komanda fəaliyyətləri ilə hücumları təqlid edərək müdafiə üsul və texnikalarını inkişaf etdirir. Qırmızı Komandanın bu hücumları simulyasiya etmək üçün istifadə etdiyi metodologiyalar var.

Qırmızı komanda metodologiyasının təfərrüatları aşağıdakılardır:

Kəşfiyyat: Bu, qırmızı komanda əməliyyatında ilk və ən kritik mərhələdir. Bu

mərhələ hədəf haqqında mümkün qədər çox məlumat toplamağa yönəlmişdir. Bu addım həmçinin xüsusi hədəfə aid alətlərin yaradılmasını və ya əldə edilməsini əhatə edir.

Silahlanma: Kəşfiyyat fəaliyyətlərindən əldə edilən məlumatlara əsaslanaraq, bu, hədəf üçün xüsusi komanda yaradılması və idarəetmə mərkəzlərinin qurulması mərhələsidir. Bu addımlar adətən proqram və aparat zərərvericilərinin hazırlanması, RFID (Radiotezlik identifikasiyası) klonlama cihazlarının hazırlanması, sosial mühəndislik üçün ssenarilərin hazırlanması, saxta insanlar və ya şirkətlərin yaradılması daxildir.

Çatdırılma: Kritik mərhələlərdən biri olan çatdırılma mərhələsi əməliyyatın hədəflə ilk təmasına aiddir və bu, bütün prosesin aktiv şəkildə başlandığını göstərir. Qırmızı komandaların bu mərhələdə müəyyən edilmiş ssenarilərdəki hədəflərə çatmaq üçün hədəf şəxs və ya təşkilatlara yönəlmiş fiziki olaraq şəxsiyyət vəsiqələrinin klonlanması, üz-üzə və ya kommunikasiya kanallarında sosial mühəndislik hücumları, texnologiya infrastrukturundakı zəiflik və ya zəifliklərin təhlili kimi tədbirlər görülür.

İstismar: Göndərmə fazasında görülən hərəkət və ya hərəkətlərin uğuru nəticəsində texnologiya infrastrukturundan hədəfə çıxış əldə etmək cəhdidir. Bu addımda hazırlanmış zərərli proqram təminatları müvafiq hədəfə yönləndirilir.

Əmr və Nəzarət: Hədəf sistem və ya sistemlərdə işləməyə başlayan zərərli proqram təminatının əmr və idarəetmə serverləri ilə əlaqə saxladığı mərhələdir. Bu mərhələ üçün yaradılmış əmr və idarəetmə serverləri normal şəraitdə leqal sistemlər kimi görünür. Bundan əlavə, təcavüzkar tərəfindən yaradılan şəbəkə trafikinin leqal şəbəkə trafiki kimi görünməsi üçün səylər göstərilir.

Obyektiv irəliləmə: Bu, təşkilat tərəfindən müəyyən edilmiş məqsədə çatmaq üçün işin başladığı addımdır. Məqsəd mümkün qədər tez və ifşa edilmədən müvafiq hədəfə çatmaqdır (https://www.zdnet.com/topic/security/).

Mavi komanda - Mavi komanda həm həqiqi hücumçulara, həm də qırmızı komandaya qarşı müdafiə edən qrupu ifadə edir. Onlar təhlükəsizlik səviyyəsini artırmağa və işlədikləri təşkilatı müdafiə etməyə çalışan komanda olub, mümkün

hücum səthlərini azaldırlar. Qırmızı komanda və mavi komanda birlikdə işlədikdə maksimum fayda təmin edilir. Qırmızı komanda oxşar texniki və xarakterik xüsusiyyətlərə malik hücumçuları və hücumları təqlid edərkən, mavi komanda daha güclü cavab vermək üçün müdafiə mexanizmlərinin çatışmayan nöqtələrini nəzərdən keçirib dəyişdirməyin yollarını tapır .

Mavi komandanın cavab strategiyası yaratması üçün hücumçuların taktika və prosedurlarından xəbərdar olmalıdırlar.

Mavi komandanın izlədiyi metodologiya aşağıdakı kimidir:

1. Hadisələrin təhlil edilməsi, əsaslandırılması və tədbir görülməsi üçün sübutların qeydə alınmasını təmin etməlidir.

2. Siqnallar cari hadisən ilə kompromis göstəricilər (IOC) üsuluyla vəziyyətlə əlaqələndirilməli və yoxlanılmalıdır.

3. Mavi komandanın kompromis göstəricilər ilə nə edəcəyini müəyyən etməsi lazımdır.

4. Hadisə ilə bağlı əlavə araşdırma tələb oluna bilər, bu zaman əməliyyatları vacibliyinə görə sıralamaq lazımdır.

5. Pozuntuların aradan qaldırılması və düşmənin təcrid edilərək zərərsizləşdirilməsi üçün plan hazırlanmalıdır.

Mavi komandalarda tələb olunan bacarıqlar aşağıdakılardır:

1. Kiber Təhlükə Ovçuluğu: Avtomatlaşdırılmış təhlükəsizlik həllərindən yayınan təhdidlərin proaktiv aşkarlanması və zərərsizləşdirilməsidir. Kiber təhdidlərin sürətlə artması kiber təhlükə ovçularına ehtiyacı da artırır. Qayda və imza əsaslı üsullarla təmin edilən təhlükəsizlik tədbirləri ilə yanaşı, təhdid ovçularının işə götürülməsi təşkilatların təhlükəsizlik səviyyələrini artırır.

   Müəssisələrdə uzun müddət təsbit edilmədən fəaliyyətə davam edən hücumların müəyyən edilməsində klassik avtomatlaşdırılmış üsullar yetərli olmasa da, şəbəkədə meydana gələn hər hansı qarşılıqlı gizli təhdidlər kiber təhlükə ovlama üsulu ilə təhlil edilə bilər. Kiber təhlükə ovlanması hücum baş verməzdən əvvəl potensial təhlükələri aşkar edir,

təcavüzkarların davranışları, hədəfləri və metodları haqqında yetərli məlumat toplayır və lazımi qabaqlayıcı tədbirlər görür.

2. İnsidentə Reaksiya: Hadisəni aşkar etmək, təhlil etmək, müdafiə etmək və müdaxilə etmək üçün texniki fəaliyyətlərdir. Hadisə idarəçiliyi hadisəni effektiv və aktiv şəkildə idarə etmək üçün əvvəlcədən hazırlanmış prosedurlardır (https://krebsonsecurity.com/).

   İnsidentə reaksiya hadisəni təhlil etmək üçün lazım olan bütün texniki komponentlərdir. Hadisə idarəçiliyi isə hadisəni sakit və səmərəli şəkildə həll etmək üçün lazım olan kommunikasiya koordinasiyası və planlaşdırma funksiyalarıdır. İnsidentə reaksiya verən şəxslərin şəbəkə məlumatı, log təhlili və məhkəmə ekspertiza bacarıqlarının (forensic) yüksək səviyyədə olması gözlənilir. Hadisə idarəçiliyi isə komandanın planlı şəkildə hərəkət edə bilib, lazımi müdaxilələri həyata keçirə bilməsi və tək başına işləyə bilməsi üçün kifayət qədər məlumata malik olduqlarını hiss etdirən tamamlayıcı roldur.

3. Təhdid Kəşfiyyatın Təhlili: Təhdid kəşfiyyatın analtiki kiber təhlükələri, zərərli proqram təminatını aşkarlayır və kibertəhlükəsizlik hadisələri ilə bağlı təhlükə səviyyəsini təhlil edir. Təşkilatların kibertəhlükəsizlik risklərinə qarşı hansı aktivlərin qorunması və təhdidlərə qarşı prioritetlərin müəyyən edilməsi ilə bağlı öhdəlikləri var. Təhdid kəşfiyyatı üzrə analtikin kibertəhlükəsizlik və kompüter şəbəkələrində təcrübəli olması şərtdir. Kibertəhlükəsizlik və kompüter şəbəkələrində təcrübə təhdidləri tam başa düşmək üçün lazım olan anlayışı təmin etməyə kömək edir. Təhdid kəşfiyyatı analitikləri təhdidləri aşkar edib, riskləri müəyyən etmələri üçün işlərinə maksimum dərəcədə fokslanmalı və ağır iş yükünü idarə etməyə hazır olmalıdırlar.

4. Rəqəmsal Məhkəmə Analizi: Rəqəmsal məhkəmə ekspertizası tez-tez kompüter cinayətləri ilə əlaqəli rəqəmsal cihazlarda tapılan materialların bərpasını əhatə edən məhkəmə ekspertizası sahəsidir. Rəqəmsal məhkəmə analizi isə kompüterlərdə və ya oxşar rəqəmsal mühitlərdə tapılan

rəqəmsal sübutlarla əlaqəli faktların müəyyən edilməsi, bərpası, araşdırılması, yoxlanılması və təqdim edilməsini əhatə edən məhkəmə ekspertizası sahəsidir. Bu, elmi cəhətdən qəbul edilmiş və təsdiq edilmiş proseslərdən istifadə edərək rəqəmsal sübutların müəyyən edilməsi, qorunması, araşdırılması və təhlili ilə əlaqədardır.

Rəqəmsal məhkəmə analizinin düzgün aparılması üçün müəyyən proseslərə əməl edilməlidir. Analiz edə bilmək üçün ilk növbədə kütləvi informasiya vasitələri ələ keçirmək lazımdır. Vasitələr ələ keçirildikdən sonra məlumatların bir nüsxəsi təhlükəsiz mühitə göndərilməli və orijinal vasitələr saxtakarlığa qarşı tədbirlər görülərək saxlanmalıdır. Beləliklə kopyası alınan faylı orjinal faylın sürəti ilə birə-bir olub-olmadığını müqayisə etmək olar. Rəqəmsal məhkəmə ekspertizasında araşdırılan faylın dəyişdirilib-dəyişdirilmədiyini sübut etmək vacibdir, buna görə də orijinal faylın kopyalanan fayllarla müqayisəsi vaxtaşırı aparılmalıdır. Bu proseslər gerçəkləşdirildikdən sonra, sürəti çıxarılmış vasitələr məhkəmə ekspertizasına məruz qalma səbəbinə görə təhlil edilməli və sübutlar toplanmalıdır (https://threatpost.com/).

Vasitələrdəki şəkillər, e-poçtlar, yazışmalar, internetə çıxış, sənədlər və s. təhlil edilərək sübutlar toplanmalıdır. Bundan əlavə, vasitələrdə silinmiş məlumatlar aşkar edilməli və bərpa edilməlidir. Bu sübut dəyəri olan məlumatları ehtiva edə bilər və sübutları aradan qaldırmaq üçün məlumatlar silinə bilər. Silinmiş məlumatların bərpası vacibdir. İstintaq başa çatdıqdan sonra aparılan işlərin və nəticələrin hesabatı verilməlidir.

5. Zərərli proqram təminatı təhlili: Zərərli proqram təminatı istifadəçilərin razılığı və məlumatı olmadan kompüter sisteminə zərər vermək üçün nəzərdə tutulmuş proqram təminatlarıdır. Zərərli proqram təminatlarının təhlili bu proqram təminatlarının potensial təsirlərini və necə işlədiyini öyrənmək prosesidir. Zərərli proqram təminatı birdən çox texnika ilə təhlil edilə bilər. Hansı texnikadan istifadə etmək seçilmiş hədəfdən asılı olur. Bu proqram təminatları təhlilinin məqsədi adətən şəbəkə hücumlarına

cavab vermək üçün lazım olan məlumatları təmin etməkdir. Zərərli proqram təminatı sistemə yoluxmuşsa, bu proqram təminatının hansı sistemlərə təsir etdiyini müəyyən etmək və yenidən sistemə daxil olmasının qarşısını almaq üçün bəzi təhlillər aparılır.

6. Tam Avtomatlaşdırılmış Təhlil: Tam avtomatlaşdırılmış analiz metodunda zərərli proqram təminatları avtomatlaşdırılmış proqram təminatları ilə analiz edilir. Bu analiz üsulu digərlərindən daha sürətli nəticələr verir. Bundan əlavə, hazır hesabatlar təqdim etməsi əlavə zəhməti aradan qaldırır. Ancaq bəzi zərərli proqram təminatları bu alətlərlə analiz edildiyini anlaya və göstərdiyi fəaliyyətləri sonlandıra. Bu, zərərli proqram təminatları haqqında tam və dəqiq məlumat verməyi çətinləşdirir.
7. Statik Analiz: Proqramı icra etmədən davranışını müşahidə etmək və təhlil etmək statik analiz adlanır. Statik analiz faylı heç bir alətə analiz etdirmədən statik olaraq zərərli proqram təminat kodunun içərisindəki imzaları, sözləri, mənbə kodunu, funksiyaları və başlıqları araşdıraraq edilən təhlildir. Statik analiz ilə analiz edilən faylın zərərli fayl olub-olmaması, şəbəkə trafiki və funksionallıq kimi bəzi məlumatlar əldə edilə bilər. Statik analiz zərərli proqram təminatını işə salmadan lazımi araşdırmalar etdiyi üçün zərərli proqram təminatının analiz edilən mühitə vura biləcəyi zərərlər aradan qaldırılır. Statik analiz mürəkkəb, yerinə yetirilməsi çətindir və təhlili aparılarkən bəzi vacib məqamlar nəzərdən qaçırıla bilər. Zərərli proqram təminatının analiz edilməməsi üçün bu proqram təminatını inkişaf etdirən insanlar tərəfindən qarışıqlıq və paketləmə kimi üsullarla onu oxunmaz hala gətirməyə çalışılır. Qarışıqlıq mənbə kodunun funksionallığını pozmadan oxunmaz hala gətirmək prosesidir. Bu üsullarla aşkarlanmağı gecikdirmək və tərs mühəndisliyi çətinləşdirmək mümkündür (https://www.darkreading.com/).

   Zərərli proqram təminatının gizlətmək istənən hissələrinə faydasız kodlar əlavə etməklə bu program təminatında qarışıqlıq yaradaraq, onun şərhini və təhlilini çətinləşdirmək mümkündür.

8. Dinamik Analiz: Proqramı icra edərək davranışını müşahidə etmək və təhlil etmək dinamik analiz adlanır. Dinamik analiz monitorinq edilən proqramın icrası zamanı əldə edilən URL, yaradılmış və əldə edilmiş fayllar, ötürülən məlumat və s. kimi təfərrüatlı məlumatları təmin edir. Fayl işləyərkən olduğu mühitə zərər verə bilər, buna görə də icra və təhlil prosesləri emulyator, simulyator, virtual maşın vasitəsilə həyata keçirilməlidir. Fayl işləyərkən URL-lər, fayllar, qeyd dəftəri və şəbəkə trafiki kimi ətraflı məlumatlar əldə edilə bilər. Bəzi zərərli proqram təminatları isə bu cür mühitlərdə işlədiyini anlayıb zərərli davranışlardan qaçaraq normal davranır. Dinamik analiz statik analizdən daha asan və effektivdir. Dinamik analiz ilə zərərli davranışları gizlənmiş (obfuscation) faylların da təhlili edilərək zərərli davranışları aşkarlamaq mümkündür. Zərərli proqram təminatını tam təhlil etmək üçün həm statik həm də dinamik analiz aparılmalıdır. Tək analiz üsulu zərərvericinin mümkün davranışını aşkar etməyə bilər, ona görə də zərərvericilərin analizində hər iki analiz üsulundan istifadə edilməlidir. Standarta görə dinamik analiz statik analizdən sonra aparılmalıdır.
9. Tərs mühəndislik: Tərs mühəndislik, istehsal mərhələlərini və necə işlədiyini başa düşmək üçün mövcud sistemin, cihazın və ya obyektin təbəqə-təbəqə tədqiqidir. Bu prosesin tərs mühəndislik adlandırılmasının səbəbi dizayn prosesinin tərs istiqamətdə aparılmasına əsaslanmasıdır. Tərs mühəndislik prosesi proqram təminatı, maşınlar, hərbi texnologiyalar, memarlıq strukturları və hətta bioloji hərəkətlər də daxil olmaqla əksər şeylərə tətbiq oluna bilər. Tərs mühəndislik digər üsullarla müqayisədə daha mürəkkəb, çətin və vaxt aparan bir üsuldur.

   Lisenziyalı proqramları lisenziyasız istifadə etmək (crack) üçün də tərs mühəndislikdən istifadə olunur. Proqramın mənbə kodunda şifrələnmiş sahə aşkar edildikdən sonra bu sahəni neytrallaşdırmaq üçün mənbə kodunda müxtəlif tənzimləmələr aparılır.

Təşkilatlarda təhlükəsizliyi təhdid edən elementlər və hücum vektorları:

Kiberhücumlar - Serverlər, fərdi kompüterlər, kompüter şəbəkələri və ya şəbəkə infrastrukturu, məlumat sistemləri kimi hədəflərə müxtəlif zərərli proqram təminatları və üsullarla qeyri-qanuni və ya icazəsiz giriş cəhdləridir. Kiberhücumlar maliyyə fırıldaqçılığı, həssas məlumatların əldə edilməsi, Təşkilatların və ya fərdlərin fəaliyyətini pozmaq kimi səbəblərlə edilir. Kiberhücumlara qarşı tədbir görülmədiyi təqdirdə, bu hücumlar maliyyə fırıldaqlığı, məlumat və ya şəxsiyyət oğurluğu kimi cinayətlərlə nəticələnir (https://www.securityindustry.org/).

Kiberhücumlar ilə fiziki-hərbi hücumlar arasında qarşı tərəfə zərər vermək kimi mühüm üzvi əlaqənin olduğunu söyləmək olar. Tarixdəki müharibələr araşdırıldığında, müharibələrdə təsirli strategiya və taktikalardan istifadə edildiyi görülür. Eynilə, təcavüzkarlar xüsusi hallar istisna olmaqla, zəruri hallarda effektiv zərərli proqram təminatları və metodlardan istifadə edirlər.

Texnologiya inkişaf etdikcə kiberhücumların tezliyi və əhatə dairəsi də zamanın şərtlərinə uyğun olaraq dəyişdi. Bir vaxların sadə zərərli proqram təminatı dəyişərək günümüzdə milli cinayət sindikatları və dövlətlər tərəfindən məqsədyönlü kiberhücumların bir hissəsinə çevrildi (Kennedy D., O'Gorman J., Kearns D., 2011: s.48).

Kiberhücum vektorları:

İyləmə - İyləmə vektoru təcavüzkarın yerli şəbəkələr daxilində trafikə nəzarət etməklə məlumat əldə etmə üsuludur.

1. Passiv İyləmə: Hub üzərində məlumat toplama prosesi passiv iyləmə adlanır. Təcavüzkar özünü həmin şəbəkənin cihazı kimi tanımlayaraq, digər cihazların məlumat mübadiləsini gözləyir. Digər cihazlar məlumat mübadiləsi etməyə başladıqda, təcavüzkar hub vasitəsilə məlumat əldə edir.
2. Aktiv İyləmə: Switch üzərində məlumat toplama prosesi aktiv iyləmə adlanır. Təcavüzkar şəbəkədəki trafiki özünə yönəltmək üçün switch'ə müdaxilə edərək, trafikin öz üzərindən keçməsini təmin edir. Beləliklə, təcavüzkar bütün şəbəkə haqqında məlumat əldə edə bilər.

3. ARP Zəhərlənməsi: ARP cədvəli media girişinə nəzarət ünvanlarını (MAC) və switch məlumatlarını ehtiva edən cədvəldir. Şəbəkədə məlumat mübadiləsi bu cədvəldən istifadə etməklə aparılır. ARP zəhərlənməsi təcavüzkarın ARP cədvəlini manipulyasiya edərək trafiki özünə yönləndirməsidir. ARP cədvəlini doldurmaq üçün yayım edilir. Arp cədvəlinin yayım sorğularını azaltmaq və lazım olduqda daha sürətli cavab vermək üçün qeydlər keş yaddaşda saxlanılır. Yeni yayım edilərkən yeni uyğunluqlar tutulduqda keş yenilənir. Təcavüzkar bu yayımlar zamanı saxta IP-MAC uyğunluqlarını cavab olaraq göndərərək keşi manipulyasiya edə bilər.
4. Domen Adı Sisteminin Zəhərlənməsi: Domen adı sistemləri internet saytlarının ünvanlarının indeksləşdirildiyi serverlərdir. Daxil ediləcək sayt ünvanları domen adı sistemləri vasitəsilə İP ünvanlarına çevrilir və sayta giriş bu İP ünvanlar vasitəsilə təmin edilir. Domen adlarını yadda saxlamaq IP ünvanlarını yadda saxlamaqdan daha asan olduğuna görə domen adı texnologiyası yaradılmışdır. Domen adlarını mobil nömrə bələdçisi kimi düşünmək olar. Mobil nömrə bələdçisində zəng ediləcək adlar əslində ad deyil, nömrələrdir. Beləliklə, domen adı sistemlərini mobil nömrə bələdçilərinə bənzətmək olar.

   Domen zəhərlənməsi domen adı sistemlərindəki zəifliklərindən istifadə edib internet trafikini leqal olanlardan saxta olanlara yönləndirərək həyata keçirilən hücum növüdür. Təcavüzkar yerli şəbəkədə yayım etməklə öz kompüterini şlüz kimi təqdim edir. Şəbəkədəki digər cihazlar internetə daxil olarkən şlüzdən istifadə edirlər. İnternetə giriş sorğusu edildikdə özünü şlüz kimi təyin edən təcavüzkar bütün trafikə nəzarət edə bilər. Təcavüzkar zərərçəkəni başqa serverə yönləndirərək daxil olan sorğuları qəbul edib məlumatıları ələ keçirir. Başqa bir üsul isə domen adı sistemi manipulyasiya edilərək domen adı qeydlərini dəyişdirməkdir. Beləliklə, zərərçəkən hər hansı sorğu ilə müraciət

etdikdə, o, daxil olmaq istədiyi sayta deyil, təcavüzkarın yönləndirdiyi sayta daxil olacaqdır. Təcavüzkarın yönləndirdiyi sayt çox vaxt zərərçəkənin daxil olmaq istədiyi saytın surəti olduğu üçün zərərçəkən saytın başqa sayt olduğunu anlamayacaqdır.

Yönləndirilən saytın idarəsi təcavüzkarın əlində olduğu üçün saytda yazılacaq parollar, kredit kartı məlumatları, şəxsi məlumatlar, mobil telefon nömrəsi kimi məlumatlar təcavüzkar tərəfindən əldə edilir.

Xidmətdən imtina - Xidmətdən imtina bir mənbədən edilən sorğular nəticəsində göstərilən xidmətin yararsız hala salınmasına və ya yavaşlamasına səbəb olan hücum növüdür. TCP bağlantılarında 3 tərəfli əl sıxma (3 way handshake - SYN,SYN-ACK,ACK) qurulmalıdır.

DoS hücumunda şəbəkə autentifikasiya mesajı olan SYN-ACK qaytarma trafikinə qarşılıqsız sorğular göndərərək sistemləri yararsız vəziyyətə gətirmək məqsədi daşıyır. Qayıdış ünvanını tapa bilməyən sistem müəyyən müddət ərzində sorğularına cavab verilməsini gözləyir və cavab gəlmədiyi halda əlaqə dayandırılır. Sistem əlaqəni dayandırdıqda, təcavüzkar qayıdış ünvanlarına daha çox keçərsiz autentifikasiya mesajı göndərir. Beləliklə, sistemin daha çox məşğul edilib xidmətin yavaşlaması və ya yararsız hala salınması təmin edilir.

Paylanmış Xidmətdən imtina - Paylanmış xidmətdən imtina hücumu bir neçə mənbədən edilən sorğular nəticəsində göstərilən xidmətin yararsız hala salınmasıdır. Paylanmış xidmətdən imtina hücumu təcavüzkarın bunu tək başına edə bilməyəcəyi qədər çox böyük hücumdur. Bu səbəbdən də müxtəlif üsullarla ələ keçirilən cihazların köməyi ilə həyata keçirilir. Təcavüzkar hədəf xidmətə hücum edəcəyi zaman hücuma hazır olan sistemlər aktivləşdirilir. Hədəf hücumu həyata keçirənləri zombi cihazlara çevrilmiş sistemlər olaraq aşkar etsə də, əslində arxa planda zombi cihazlarını aktivləşdirən təcavüzkardır. Buna görə də əsl hücum edənləri müəyyən etmək çox çətindir. Zombi cihazlarının sayı nə qədər çox olarsa, hücumun təsiri də bir o qədər çox olar (https://www.sans.org/).

Paylanmış xidmətdən imtina hücumlarını trafikdə hərəkət halında olan avtomobillərə bənzətmək olar. Yol avtomobil tutumuna malikdir, əgər

avtomobillərin sayı yolun nəqliyyat vasitəsi tutumundan azdırsa, hərəkət axıcıdır. Avtomobillərin sayı tutumun sayına yaxınlaşırsa, o zaman hərəkət yavaşlamağa başlayır. Tutumu doldurduqda və ya tutumu aşdıqda, nəqliyyat vasitələrinin hərəkəti dayanır (Mitnick K., 2017: s.87).

İP ünvan saxtakarlığı - İP ünvanının saxtalaşdırılması şəbəkə paketinin mənbə İP ünvanını manipulyasiya etmək və ya onun saxta mənbədən gəldiyi təəssüratı yaratmaq aktıdır. Başqa sözlə desək, bu, təhlükəsizlik tədbirlərini saxtalaşdırmaq və ya yan keçmək üçün göndərənin İP ünvanının saxtalaşdırılması prosesidir.

İP ünvanı şəbəkəyə qoşulmuş hər bir cihaza təyin edilmiş unikal rəqəmsal identifikatordur. Şəbəkə rabitəsində göndərici və qəbuledicinin ünvanı kimi xidmət edir. İP ünvanlarının saxtalaşdırılması həm qanuni, həm də zərərli məqsədlər üçün istifadə edilə bilər.

Qanuni hallarda, İP saxtakarlığı şəbəkə testi, sazlama və ya anonimlik məqsədləri üçün istifadə edilə bilər. Məsələn, tədqiqatçılar və ya sistem administratorları müəyyən onlayn resurslara daxil olarkən şəbəkə təhlükəsizlik tədbirlərini qiymətləndirmək və ya şəxsiyyətlərini qorumaq üçün İP ünvanlarını saxtalaşdıra bilərlər (https://owasp.org/).

Bununla belə, İP ünvanlarının saxtalaşdırılması çox vaxt zərərli fəaliyyətlərlə əlaqələndirilir:

1. Xidmətdən imtina (DoS) hücumları: Hücumçular mənbə İP ünvanını aldada bilər, hədəf sistemləri böyük həcmdə trafiklə doldura bilər. Hədəf sistem tez-tez həddən artıq yüklənir, çünki saxta paketləri qanuni paketlərdən ayırmaq qabiliyyəti yoxdur, bu da xidmətdən imtina ilə nəticələnir.

2. Paylanmış xidmətdən imtina (DDoS) Hücumları: DoS hücumlarına bənzəyir, lakin bir neçə mənbədən əlaqələndirilir. Hücumçular qurğular şəbəkəsini ələ keçirir (adətən zərərli proqramdan istifadə edir) və İP saxtakarlığından istifadə edir, bu da hücumun mənşəyini izləməyi çətinləşdirir.

3. Məlumat Oğurluğunda İP Spoofinqi: Təcavüzkarlar İP əsaslı autentifikasiyaya əsaslanan təhlükəsizlik tədbirlərindən yan keçmək üçün İP

ünvanlarını saxtalaşdıra bilərlər. Etibar etdiyimiz İP ünvanını saxtalaşdırmaqla onlar icazəsiz giriş əldə edə və ya icazəsiz hərəkətlər edə bilərlər.

4. Təhlükəsizlik və ya filtrlərdən yayınma: İP saxtakarlığı İP əsaslı qaydalara və ya qara siyahılara əsaslanan firewallları və ya şəbəkə filtrlərini keçmək üçün istifadə edilə bilər. Mənbə İP ünvanını saxtalaşdırmaqla təcavüzkarlar trafikin səlahiyyətli mənbədən gəldiyi təəssüratı yaradaraq təhlükəsizlik tədbirlərindən yan keçə bilərlər.

Müasir İnternet kontekstində İP ünvanlarının saxtalaşdırılmasının həyata keçirilməsi müxtəlif təhlükəsizlik mexanizmlərinin və texnologiyalarının tətbiqi ilə əlaqədar olaraq çox vaxt daha mürəkkəb olsa da. Bununla belə, İP saxtakarlığı hələ də şəbəkə administratorları və təhlükəsizlik mütəxəssisləri üçün narahatlıq yaradır və saxta İP trafikini aşkar etmək və azaltmaq üçün əks tədbirlərdən istifadə olunur.

Sosial mühəndislik - Sosial mühəndislik əsasən insanları manipulyasiya edib təhlükəsizlik tədbirlərindən yan keçməklə təşkilatlara sızmağa yönəlmiş hücum vektorudur. Bir çox sosial mühəndislik istismarı insanların kömək etmək istəyinə arxalanaraq həyata keçirilir. Təcavüzkarlar çox vaxt bu yöntəmə üstünlük verilir, çünki insanların zəifliklərindən istifadə edərək təşkilatlara daxil olmaq şəbəkə və proqram təminatının təhlükəsizlik tədbirlərinin zəifliklərini tapmaq və istismar etməkdən daha asandır. Təşkilatın informasiya təhlükəsizliyi səviyyəsinin ən zəif nöqtəsi insandır. İnsanları aldatmaq təhlükəsizlik cihazlarından yan keçməkdən çox daha asandır. Təşkilata yaxınlaşan pizza kuryeri olduğunu idda edən şəxsə güvənib şəxsiyyətinin təsdiq edilmədən içəri buraxılması, onun yarada biləcəyi risklərə qarşı təşkilat təhlükəsizlik cəhətdən həssas olacaq. Belə olan halda qapı və pəncərələrdə kilid, gözətçi iti, siqnalizasiya sistemi, tikanlı hasar və ya silahlı mühafizə personalının olmasının heç bir əhəmiyyəti qalmayacaq.

Sosial mühəndislik hücumundan əvvəl hədəf haqqında məlumat toplamaq lazımdır. Hədəf haqqında toplanan bu məlumatların köməyi ilə hədəflə əlaqələr qurulur və hücum həyata keçirilir. Hücum edildikdən sonra qanuni öhdəliklərə məruz qalmamaq üçün iz buraxılmadan çıxış təmin edilməlidir.

Arxa Qapı - Arxa qapı istehsalçılar tərəfindən qəsdən və ya istəmədən

sistemə əlavə olunmaqla icazəsiz girişlə təhlükəsizlik tədbirlərindən yayınma üsuludur. Bu üsul təşkilata kartlı keçid sistemi ilə səlahiyətləndirilərək daxil olan şəxslərin keçid sistemi olmayan başqa bir qapıdan keçməsini bənzətmək olar. Normal şəraitdə hər kəs kart keçid sistemindən istifadə etməli və giriş icazəsinin olub-olmadığı yoxlanmalıdır, lakin arxa qapıdan daxil olmaqla, kart keçid sistemindən yan keçilir. Arxa qapılar fiziki (hardware) və ya proqram təminatınlı yaradıla bilər. Prosessor, ram, ana plata, əməliyyat sistemi, proqram təminatında arxa qapılara rast gəlmək olar. Sistemdə istifadə edilən portlar vasitəsi ilə proqram təminatındakı müxtəlif zəifliklərdən istifadə edərək bu vəziyyəti yaratmaq olar.

Arxa qapılar aşkar olunmadığı müddətcə yalnız yaradıcılara məlumdur. Arxa qapılarla sistemlər nəzarət altına alına və idarə oluna, məlumat sızıntıları edilə və viruslar tərəfindən kompleks hücumlar üçün istifadə edilə bilər. Arxa qapıları aşkar etmək çox çətindir lakin onların yarada biləcəyi təsir böyükdür.

Sıfırıncı gün - Sıfırıncı gün hücumları bəzən hələ kəşf olunmamış təhlükəsizlik zəifliklər, bəzən isə kəşf olunmuş, lakin təcavüzkarlara məlum olmayan təhlükəsizlik zəifliklər kimi müəyyən edilir. Bu təhlükəsizlik açığının sıfır gün kimi təyin edilməsinin səbəbi proqram təminatı, cihaz, əməliyyat sistemi yeniləmələrindən dərhal sonra, yəni 0-cı gündə təcavüzkarlar yeni çıxmış yeniləmələrin zəifliklərini axtarmağa başlayırlar (Çıtak Ö., 2018 s.120).

Bu yeniləmələrdə aşkar edilən boşluqlar “Zero Day” adlanır. Təcavüzkarlar tərəfindən boşluq müəyyən edildikdən sonra zəifliyin yerləşdiyi və hücumun ediləcəyi hədəflər müəyyən edilir. Hədəflərə proqram təminatı vasitəsilə avtomatlaşdırılmış kütləvi hücumlar təşkil edilə bilər.

Zəifliklər adətən istismara çevrilməzdən əvvəl proqram dəstəyi qrupu tərəfindən düzəldilə bilər, lakin tez bir zamanda tədbir görülməzsə, zəiflik istismara çevrilərək təşkilata böyük ziyan vura bilər. Sıfır gün hücumlarına qarşı tədbir görülməsi istənirsə, əvvəlki versiyadan gəlmək tövsiyə olunur. Əgər yeni buraxılmış versiyalardakı boşluqlar hələ məlum deyilsə, lakin əlaqəli versiyada zəiflik məlumdursa, yeniləmələr təxirə salınmadan aparılmalıdır.

Zərərli Proqram Təminatı - Azərbaycan dilinə zərərli proqram təminatı

kimi tərcümə edilən “Malware” **mal**icious soft**ware** sözlərinin birləşməsindən yaranıb məlumatları oğurlamaq, giriş nəzarətlərindən yan keçmək, nəzarəti ələ keçirmək və sistemlərə zərər vermək üçün istifadə olunan proqram təmintalarıdır.

Zərərli proqram təminatları hərəkətlərinə, məqsədlərinə və təsirlərinə görə müxtəlif adlar altında qruplaşdırılır. Bu qruplaşmalar aşağıda qeyd edilmişdir.

1. Reklam proqram təminatı: Reklam vermək məqsədi ilə sistemlərə daxil olan və arzuolunmaz şəkildə avtomatik olaraq reklamları açan zərərli proqram təminatlarıdır. Bu zərərli proqram təminatları adətən veb brauzerlərdə pop-up və ya yeni veb səhifə kimi açıla bilər. Adətən internetdən yüklənmiş pulsuz proqramların üzərində gəlir və tətbiqi pulsuz edərək reklam yayımlarından gəlir əldə edir. Bu proqramlar bezdirici və arzuolunmaz vəziyyətlər yarada bilər.
2. Troya atı: İstifadəçilərə zərərli proqram təminatını yükləmək və quraşdırmaq üçün təhlükəsiz hesab edilən fayl və ya proqramlarda gizlədilən zərərli proqram təminatlarıdır. Trojan atı zərərli proqram təminatları ilə sistemə uzaqdan daxil olmaq, şəxsi və maliyyə məlumatları oğurlamaq, müxtəlif növ xüsusiyyətdə zərərli proqramlar quraşdırmaq, faylları dəyişdirmək, istifadəçinin ekran və klaviaturasına nəzarət etmək və hətta DDoS hücumlarında istifadə üçün sistemləri anonimləşdirmək mümkündür.
3. Qurd: Qurdlar özünü bir şəbəkədən digərinə köçürə bilən avtonom zərərli proqramlardır. Qurdlar diqqəti cəlb etməmək və aşkarlanması çətin olması üçün sistemin istifadə olunmayan və görünməyən hissələrindəki qaynaqlardan istifadə edərək yayılır. Buna görə də, sistemdə aşkar edilməsi çox çətindir, nəzarətsiz yayılma halında həddindən artıq resurs istifadəsindən qaynaqlanan yavaşlıq səbəbi ilə fərq edilə bilər. Qurdlar yoluxmuş sistemin e-poçt ünvanlarına əlavələri olan e-poçt məktubları göndərməklə də yayıla bilər.
4. Fidyə proqram təminatı: Fidyə proqram təminatı yoluxmuş sistemi şifrələyib kilidləyən zərərli proqram təminatıdır. Sistemdəki

məhdudiyyətləri aradan qaldırmaq və sistemə yenidən giriş əldə edilməsi qarşılığında ödəniş tələb edən, təşkilata maddi və reputativ zərər verən proqram təminatıdır.

5. Kök istifadəçisi: Rootkitlər sistemlərə uzaqdan girişi təmin edən və onlara nəzarət edən proqram təminatlarıdır. Rootkitlər əməliyyat sistemində giriş və nəzarət hüquqlarına malikdir. Əksər rootkit maliyyə və şəxsi məlumat əldə edə biləcəkləri fidyə proqram təminatı, düymə yazıcı kimi zərərli proqramlar üçün sahib olduqları giriş və nəzarət hüquqlarından istifadə edərək arxa qapılar yaradırlar. Bu yaradılmış arxa qapılar vasitəsilə məlumatlar sızdırıla və ya daha effektiv viruslar yoluxduraraq maliyyə gəliri əldə etməyin yolları axtarıla bilər. Bu zərərli proqram təminatları viruslar və qurd zərərvericiləri kimi özlərini kopyalayıb çoxalda bilməzlər, onlar adətən qanuni proqram təminatının içərisində gizlənərək sistemlərə yoluxmağa çalışırlar.
6. Düymə yazıcı: Düymə yazıcıları klaviaturadan edilən hər vuruşu izləyib qeyd etmək üçün istifadə olunan proqram təminatlarıdır. Bu proqramıar həssas məlumatların toplanması, maliyyə məlumatları və parolların əldə edilməsi kimi məqsədlər üçün hakerlər tərəfindən casus proqram kimi istifadə olunur. Düymə yazıcı proqram təminatının növündən asılı olaraq o, müəyyən proseslərdə ekran görüntülərini və veb səhifələrini yadda saxlaya bilir ki, hansı parolların hansı sayta daxil edildiyini müəyyən etmək mümkün olsun. Klaviatura hərəkətlərini düymə yazıcı proqram təminatı ilə yanaşı kompüterlərə qoşulacaq aparat qurğusu ilə də qeyd etmək mümkündür.
7. Xəta: Xətalar kompüter proqram təminatındakı kodlaşdırma səhvləridir. Bu cür proqram təminatı səhvlərinə çox əhəmiyyət verilmədiyi hallarda onların təsiri çox böyük ola bilər. Məlum zərərli proqramlardan fərqli olaraq, proqram xətalarının hansı təsirə malik olacağı dəqiq bilinməyə bilər. Proqram təminatı səhvləri ölümcül qəzalara, partlayışlara, sistem çökmələrinə və bu kimi hadisələrə səbəb ola bilər. Proqram təminatı

xətaları aşkar edildikdən sonra istehsalçı tərəfindən səhvin aradan qaldırıldığına dair yeniləmələr hazırlanmalı və bu yeniləmələr sistemlərdə quraşdırılmalıdır.

Kiberhücum üsulları:

Kiberhücumlar həyata keçirərkən vektorlar və zərərvericilərlə birlikdə istifadə edilə bilən bəzi kiberhücum üsulları var. Alınan təhlükəsizlik tədbirləri tam təhlükəsizliyi təmin edə bilir, təhlükəsizlik tədbirlərində yarana biləcək zəifliklər isə bəzi üsullardan istifadə edilərək aradan qaldırılmağa çalışılır.

Kobud güc hücumu - Kobud güc hücumu, düzgün olanı tapana qədər parolların və ya şifrələmə açarlarının bütün mümkün kombinasiyalarını sistematik şəkildə sınamağı əhatə edən kiberhücum texnikasıdır. Bu, təcavüzkarın avtomatlaşdırılmış alətlər və ya skriptlərdən istifadə edərək çoxlu sayda parol və ya açarları yaradaraq tez cəhd etdiyi metodik və hərtərəfli yanaşmadır.

Kobud güc hücumunun əsas məqsədi sistemə, hesaba və ya şifrələnmiş məlumatlara icazəsiz giriş əldə etməkdir. Bütün mümkün kombinasiyaları sistematik şəkildə sınamaqla təcavüzkar təhlükəsizlik tədbirlərindən yan keçməyə və düzgün parol və ya açarı tapmağa ümid edir.

Kobud güc hücumlarının mühüm aspektləri və versiyaları bunlardır:

1. Şifrəyə kobud güc hücumu: Bu ssenaridə təcavüzkar istifadəçinin parolunu tapmaq üçün hərflər, rəqəmlər və simvollar kimi simvolların müxtəlif kombinasiyalarını sınamağa çalışır. Adətən ümumi parollar, lüğət sözləri və ya əvvəllər sızdırılmış parolların siyahıları ilə başlayır və uğursuz olduqda daha mürəkkəb birləşmələrə keçir. Şifrə kobud güc hücumları tez-tez e-poçt hesabları, sosial media profilləri və ya bank sistemləri kimi onlayn hesablara qarşı istifadə olunur.

2. Etibarnamənin silinməsi: Bu texnika əvvəlki məlumat sızıntılarından istifadəçi adlarının və parolların böyük siyahısının istifadəsini nəzərdə tutur. Təcavüzkar bu etimadnamələri müxtəlif onlayn xidmətlərə qarşı avtomatik sınaqdan keçirərək istifadəçilərin parolları təkrar istifadə etdiyi hesabları tapmağa çalışır.

3. Şifrələmə açarlarına kobud güc hücumu: Bu tip hücum şifrlənmiş

məlumatın şifrəsini açmaq üçün bütün mümkün şifrələmə açarlarını sınamağa yönəlib. Şifrələmə alqoritmi və ya açar uzunluğu zəif olduqda tez-tez istifadə olunur. Şifrələmə açarlarının kobud güc hücumu ilə deşifrə edilməsi, xüsusilə güclü şifrələmə alqoritmləri və uzun açar uzunluqları ilə çox vaxt və resurs tələb edə bilər.

4. Paylanmış kobud güc hücumu: Prosesi sürətləndirmək və aşkarlanmamaq üçün təcavüzkarlar iş yükünü bir çox sistem və ya botnetlər arasında paylaya bilərlər. Hər bir sistem və ya bot mümkün kombinasiyaların bir hissəsini sınayaraq, hücumu daha səmərəli edir.

Kobud güc hücumlarından qorunmaq üçün bir sıra qabaqlayıcı tədbirlər görülə bilər:

1. Güclü şifrə siyasətləri: İstifadəçiləri böyük və kiçik hərflərin, rəqəmlərin və simvolların qarışığı ilə mürəkkəb parollar seçməyə təşviq edin. Parol uzunluğu və mürəkkəblik tələblərini tətbiq etməklə təcavüzkarların parolları təxmin etməsini çətinləşdirin.

2. Hesabın bloklanması və vaxt məhdudiyyətləri: Müəyyən sayda uğursuz giriş cəhdindən sonra hesabı bloklayan və ya müvəqqəti olaraq söndürən mexanizmləri tətbiq edin. Bu, təcavüzkarların müxtəlif parolları dəfələrlə sınamasının qarşısını alır.

3. Məhdud cəhd: Müəyyən vaxt çərçivəsində giriş cəhdlərinin sayını məhdudlaşdırmaqla avtomatik kobud güc hücumlarının qarşısını alın. Bu, hücum edənləri ləngidir və hücumu daha az real edir.

4. İki Faktorlu Doğrulama (2FA): Əlavə təhlükəsizlik qatını əlavə etmək üçün çox faktorlu autentifikasiyanı aktivləşdirin. 2FA ilə istifadəçilər parolundan əlavə, mobil cihazına göndərilən müvəqqəti kod kimi əlavə yoxlama metodu təqdim etməlidirlər.

5. Hücumun Aşkarlanması Sistemləri (IDS) və Hücumun Qarşısının Alınması Sistemləri (IPS): Şəbəkə trafikindəki nümunələri və anomaliyaları təhlil edərək kobud güc hücumlarını aşkarlaya bilən şəbəkə monitorinq sistemlərini tətbiq edin və bloklayın.

6. Daimi Yeniləmə: Təcavüzkarların istifadə edə biləcəyi hər hansı zəifliyi

aradan qaldırmaq üçün proqram təminatını, əməliyyat sistemlərini və tətbiqləri güncəl saxlayın.

Kobud güc hücumları, xüsusən güclü parollar və ya şifrələmə açarlarını hədəfə aldıqda resurs tələb edən və vaxt aparan ola bilər. Bununla belə, təhlükəsizlik üzrə ən yaxşı təcrübələri tətbiq etməklə və ayıq-sayıq qalmaqla, fərdlər və təşkilatlar bu cür hücumlara məruz qalmalarını əhəmiyyətli dərəcədə azalda bilərlər.

Saytlararası skript - Saytlararası skript, zərərli skriptlərin veb sayt məzmununa daxil edildiyi inyeksiya hücumunun bir növüdür. Təcavüzkar bir veb səhifəyə zərərli skriptlər əlavə etməklə, veb brauzerdə zərərli skriptlərin işlədilməsini gözləyir. Bu hücum hədəf zərərli skriptləri ehtiva edən veb səhifəyə daxil olduqda baş tutur. Veb səhifə zərərli skriptləri istifadəçinin brauzerinə çatdırmaq üçün bir vasitəyə çevrilir.

Saytlararası skript hücumları ilə hücumun şiddətindən asılı olaraq təcavüzkar istifadəçi hesablarını ələ keçirə, troyanları saytda aktivləşdirə, səhifə məzmununu dəyişdirə, istifadəçilərin şəxsi məlumatlarını mənimsiyə, kuki məlumatlarını ələ keçirə, qurbanı təqlid edərək hesablardan sui-istifadə edə bilər. Saytlararası skript öz daxilində Yansıdılan Saytlararası Skript (Reflected XSS), Saxlanılan Saytlararası Skript (Stored XSS) və Obyekt Modelli Saytlararası Skript (DOM Based XSS) kimi qruplara bölünür.

SQL inyeksiyası - SQL verilənlər bazasından məlumatların silinməsi, dəyişdirilməsi, əlavə edilməsi, siyahıya alınması kimi əməliyyatlar üçün istifadə edilən proqramlama dilidir. SQL inyeksiya verilənlər bazasına girişdə təhlükəsizlik zəifliyinin manipulyasiyasıdır. SQL inyeksiya zəifliyi proqram təminatının verilənlər bazası ilə qurduğu əlaqələrdə istifadəçidən aldığı parametrləri kifayət qədər təhlükəsiz səviyyədə təşkil etməməsi nəticəsində yaranır.

Bu inyeksiya ilə proqramda istifadəçinin edə biləcəyi demək olar ki, hər şey təcavüzkarın əmrinə çatdırılır və təcavüzkar istənilən məlumatı silmə, oxuya, əlavə edə və ya dəyişdirmə səlahiyyətinə malik olur. SQL inyeksiya hücumlarında ən kritik məqam istifadəçinin imtiyazlarında açıq olan modullardır. Açıq modullardan istifadə etməklə admin qruplarına yeni istifadəçi təyin edərək uzaqdan iş masası

idarəetmə icazəsi (Remote Desktop Protocol - RDP) verilə bilər. Serverə yüklənəcək xüsusi skript dillər ilə də serverin idarə edilməsi ələ keçirilə bilər. Bu boşluqdan istifadə etməklə təcavüzkarlar arxa qapılar yarada və serverə sıza bilərlər. Təcavüzkarlar həmçinin serverdəki mənbə kodunda dəyişikliklər etməklə, ziyarətçilərin brauzer zəifliyindən istifadə edərək ziyarətçilərin kompüterlərinə sıza bilərlər.

Saytlararası sorğu saxtakarlığı (XSS) - Bu, veb proqramlarında ümumi təhlükəsizlik zəifliyi növüdür. XSS, təcavüzkar etibarlı veb-saytlara zərərli skriptləri (adətən JavaScript) yeritdikdə və onları istifadəçinin brauzeri tərəfindən icra etdikdə baş verir. XSS hücumları həssas məlumatların oğurlanması, sessiyanın oğurlanması, veb-saytın pozulması və hətta zərərli proqramların yayılması kimi ciddi nəticələrə səbəb ola bilər.

1. XSS necə işləyir: XSS hücumları veb tətbiqinin istifadəçi tərəfindən təmin edilən məlumatlara etibarından istifadə edir. Hücum adətən giriş sahələrinə, URL parametrlərinə və ya digər istifadəçiyə göstərilən veb səhifələrin dinamik şəkildə yaradılan və göstərilən hissələrinə zərərli kodu yeritməklə həyata keçirilir. Qurban yoluxmuş səhifəyə daxil olduqda, zərərli kod brauzerdə işlədilir və təcavüzkarın həssas məlumatlara daxil olmasına və ya istifadəçi adından icazəsiz hərəkətlər etməyə imkan verir.

2. XSS Hücum Növləri:

a. Gizli XSS: Yerləşdirilmiş zərərli kod daimi olaraq hədəf serverdə saxlanılır və istifadəçilər müəyyən bir səhifəyə daxil olduqda və ya müəyyən məzmuna baxdıqda xidmət göstərir.

b. Reflected XSS: Enjekte edilmiş zərərli kod URL-də və ya digər girişdə olur və cavab olaraq server tərəfindən dərhal qaytarılır. Qurban hücumu həyata keçirmək üçün zərərli yükü ehtiva edən xüsusi linki tıklamalıdır.

c. DOM Əsaslı XSS: Hücum veb səhifənin Sənəd Obyekt Modeli (DOM) daxilində baş verir. Zərərli kod səhifə yükləndikdən sonra səhifənin strukturunu və məzmununu dəyişdirərək təcavüzkarın

səhifənin davranışını dinamik şəkildə dəyişməsinə imkan verir.

3. Təsir və Nəticələr:

XSS zəiflikləri müxtəlif zərərli təsirlərə malik ola bilər, məsələn:

a. Məlumat Oğurluğu: Təcavüzkarlar giriş məlumatları, şəxsi məlumatlar və ya maliyyə məlumatları kimi həssas istifadəçi məlumatlarını oğurlaya bilərlər.

b. Sessiyanın oğurlanması: İstifadəçi seanslarını oğurlamaqla təcavüzkarlar qurbanı təqlid edə və onların adından hərəkətlər edə bilərlər.

c. Zərər: Hücumçular veb-saytın görünüşünü və ya məzmununu dəyişdirərək etibardan sala və ya yalan məlumat yaya bilər.

d. Zərərli proqramların paylanması: Zərərli kodu yeritməklə, təcavüzkarlar istifadəçiləri zərərli vebsaytlara yönləndirə və ya zərərli faylların endirilməsinə səbəb ola bilər.

4. Qarşısının alınması və azaldılması:

XSS hücumlarının qarşısını almaq üçün veb tərtibatçıları və idarəçiləri aşağıdakı təhlükəsizlik tədbirlərini həyata keçirməlidirlər:

a. Daxiletmənin Təsdiqlənməsi: İstifadəçi tərəfindən təmin edilən bütün məlumatları veb səhifələrdə göstərilməzdən əvvəl yoxlayın və silin.

b. Çıxışın Kodlaşdırılması: İstifadəçi tərəfindən yaradılan məzmunu düzgün kodlaşdırmaqla onun icra edilə bilən kod kimi şərh edilməsinin qarşısını alın.

c. Məzmun Təhlükəsizliyi Siyasəti (CSP): Veb səhifəyə yüklənməsinə icazə verilən məzmun mənbələrini müəyyən edən ciddi CSP tətbiq edin.

d. HTTP kukiləri: XSS hücumları vasitəsilə sessiya kukilərinin oğurlanmasının qarşısını almaq üçün yalnız HTTP kukilərindən istifadə edilməlidir.

e. Daimi Təhlükəsizlik Yoxlamaları: Veb tətbiqlərində XSS

zəifliklərini aşkar etmək və düzəltmək üçün müntəzəm təhlükəsizlik yoxlamaları həyata keçirin.

XSS hücumları veb tətbiqləri üçün ümumi və əhəmiyyətli bir təhlükədir. Təcavüzkarların istifadə etdiyi üsulları başa düşmək və müvafiq təhlükəsizlik tədbirlərini tətbiq etməklə, tərtibatçılar və idarəçilər XSS zəifliklərı riskini azalda və istifadəçi məlumatlarını və sistemlərini istismardan qoruya bilərlər.

Qabaqcıl davamlı təhlükə - Qabaqcıl davamlı təhlükə qabaqcıl texnikaya malik sistemlərdə qalıcı olmağı hədəfləyən təhdidlərdir. Qabaqcıl davamlı təhdidlər çox vaxt adi hakerlər tərəfindən deyil, hökumətlər və ya korporasiyalar tərəfindən maliyyələşdirilən qruplar tərəfindən həyata keçirilir. Bu hücumları həyata keçirib nəticə almaq üçün birdən çox hücum vektor və texnikasına ehtiyac duyulur. Bu hücum təhlükəsinin qabaqcıl və davamlı ifadələri ehtiva etməsi aşağıda izah edilən səbəblərlə əlaqəlidir. Bu hücumları həyata keçirmək üçün tələb olunan qabaqcıl alətlər və üsullar çox yüksək maliyyə ilə təmin edildiyi üçün hücumun adının ilk ifadəsi də "Qabaqcıl" olaraq təyin olunmuşdur. Davamlı ifadəsi isə bu hücumların məqsədə çatmaq üçün son dərəcə davamlı və daimi olması səbəbi ilə təyin edilmişdir. Sistemlərə daxil olduqdan sonra müdaxilə aşkarlama sistemlərindən yayınmaq üçün sistemlərdə kifayət qədər uzun müddət qalmağa çalışırlar. Aşkarlanma ehtimalını azaltmaq və müvəffəqiyyət nisbətini artırmaq üçün fəaliyyətlərini aşağı səviyyədə və yavaş-yavaş davam etdirirlər.

Təhdid həssas məlumatların sızdırılması, kritik komponentlərin və ya tapşırıqların bloklanmasıdır. Təcavüzkarlar tərəfindən çoxsaylı hücum vektorları ilə kritik məlumatları aşkar etmək, kritik bir tapşırığı zəiflətmək və maliyyə qazancı əldə etmək mümkündür. Məqsədə çatmaq üçün aşağıda qeyd olunan mərhələlər həyata keçirilməlidir.

1. Kəşfiyyat: Uğurlu bir hücum həyata keçirmək üçün hədəf haqqında məlumat əldə edilməlidir. Hədəf haqqında nə qədər çox məlumat toplanarsa, hücumun uğurlu olma ehtimalı bir o qədər yüksək olacaqdır. Hədəf haqqında məlumat Linkedin, Facebook və s. kimi ictimaiyyətə açıq mənbələrdən alına bilər.

2. Giriş Nöqtəsi: Hədəf haqqında məlumat toplandıqdan sonra hansı hücum vektorları ilə sistemə necə daxil olunacağına qərar verilir. Ümumiyyətlə, sistemə daxil olmaq və şəbəkəyə arxa qapılarla sızmaq üçün sosial mühəndislik və sıfırcı gün hücum vektorlarından istifadə edilir.
3. Komanda və İdarəetmə Server Kommunikasiyası: Şəbəkəyə sızdıqdan sonra, şəbəkəyə əmr və idarəetmə vasitələri ilə nəzarət edilməlidir. Bu əmrlər və idarəetmələr uzaq server IP-ləri vasitəsilə təmin edilir və bunun üçün də komanda və idarəetmə serverləri ilə əlaqənin qurulmnası tələb olunur.
4. Yanaşı Hərəkət və Davamlılıq: Təcavüzkar şəbəkəyə sızdıqdan sonra o, imkanlarını genişləndirməyə və gücləndirməyə çalışır. Təcavüzkar bunun üçün daxili şəbəkədə yanal kəşfiyyat işləri apararaq sistemləri ələ keçirir və səlahiyyət imtiyazları artırılmağa çalışır. Kəşf zamanı əldə edilən şəxsi məlumatlar yüksək səlahiyyətli istifadəçi hesablarına əlçatanlıq qazandırır, bu da daha çox sistemə girişi təmin edir.
5. Hədəfin Müəyyən Edilməsi: Bu, vacib ola biləcək aktivlərin və məlumatların kəşf mərhələsidir. Bu mərhələdə məlumat fayllarına və şəbəkələrə icazəsiz giriş sorğuları yarana bilər. Təcavüzkarın icazəsiz giriş sorğuları səbəbindən aşkarlanma ehtimalı yüksəkdir.
6. Məlumat sızması: İstənilən hədəfə çatdıqda və ya məlumatı əldə etdikdə, təcavüzkar bir qaçış planı qurmalı və geridə qoyduğu izləri silməlidir, beləliklə, təcavüzkarın şəxsiyyətini və vurulan zərəri müəyyən etmək çətinləşir. Bəzi hallarda təcavüzkarlar uzunmüddətli giriş əldə etmək istəyə və arxa qapılar sayəsində uzun müddət ərzində giriş təmin edilərək məlumatlar sızdırıla bilər.

   APT hücumlarına məruz qalan əksər təşkilatlar hücuma məruz qaldıqlarından xəbərsiz olurlar. Təhlükəsizlik cihazları tərəfindən APT hücumlarının aşkarlanmasını təmin etmək üçün qayda siyahıları hazırlanmalıdır.

FƏSİL 2. KORPORATİV KİBER TƏHLÜKƏSİZLİK TƏRƏFİNDƏN KİBER HÜCUMLARIN TƏHLİLİ

2.1 Korporativ Şəbəkə Təhlükəsizliyi və Kiber Təhlükəsizlik Texnologiyalari

Getdikcə rəqəmsallaşan dünyamızda korporativ şəbəkələrin təhlükəsizliyi son dərəcə vacibdir. Kiber təhdidlərin artması ilə müəssisələr rəqəmsal aktivlərini və həssas məlumatlarını qorumaq üçün fəal olmalıdırlar. Bu fəsildə korporativ şəbəkə təhlükəsizliyi, kibertəhlükəsizlik texnologiyalarının əhəmiyyəti və bizneslərin kiberhücum riskini minimuma endirmək üçün atdığı addımlar müzakirə olunacaq.

Korporativ şəbəkə təhlükəsizliyinin əhəmiyyəti - Korporativ şəbəkəsinin təhlükəsizliyi müəssisələr üçün həyati önəm daşıyır. Kiber təhdidlər getdikcə təkmilləşib və mürəkkəbləşdikcə, ciddi maliyyə itkisi, nüfuza ziyan vurma və əməliyyatların pozulması riski artır. Güclü şəbəkə təhlükəsizliyi strategiyasının həyata keçirilməsi təkcə dəyərli şirkət məlumatlarını qorumur, həm də müştərilərin etibarını qorumağa kömək edir.

Korporativ şəbəkələr üçün kibertəhlükəsizlik texnologiyaları - Korporativ şəbəkə təhlükəsizliyini gücləndirməyə kömək etmək üçün geniş çeşiddə kibertəhlükəsizlik texnologiyaları mövcuddur. Ən təsirli vasitələrdən bəziləri bunlardır:

1. Təhlükəsizlik divarları: Təhlükəsizlik divarları korporativ şəbəkənizlə ictimai şəbəkə arasında maneə rolunu oynayır. Əvvəlcədən müəyyən edilmiş təhlükəsizlik qaydalarına uyğun olaraq daxil və xaric şəbəkə trafikinə nəzarət edir və idarə edir.

2. Müdaxilənin aşkarlanması və qarşısının alınması sistemləri: Bu texnologiyalar trafiki təhlil edərək şübhəli fəaliyyətləri aşkar edir və şəbəkəyə icazəsiz girişin qarşısını alır.

3. Şifrələmə: Şifrələmə həssas məlumatların yanlış əllərə keçməsinin qarşısını almaq üçün düzgün şifrə açma açarı olmadan məlumatı oxunmayan koda çevirməyə kömək edir.

4. Çox faktorlu autentifikasiya: Çox faktorlu autentifikasiya şəbəkəyə və ya

sistemə daxil olmamışdan əvvəl istifadəçilərdən iki və ya daha çox autentifikasiya metodu təqdim etmələrini tələb etməklə təhlükəsizlik səviyyəsini artırır.

5. Son nöqtə təhlükəsizlik həlləri: Bu yöntəm korporativ şəbəkəyə daxil olan noutbuklar və mobil qurğular kimi fərdi cihazların təhlükəsizliyini təmin edir və icazəsiz girişin və məlumat sızmasının qarşısını alır.

Korporativ kibertəhlükəsizlik strategiyasının gücləndirilməsi - Korporativ şəbəkələri effektiv şəkildə qorumaq üçün təhlükəsizliyə çox təbəqəli yöntəmlə yanaşmaq lazımdır. Bunun üçün müəssisələrin ata biləcəyi bəzi addımlar bunlardır:

1. Proqram təminatı və aparat təminatını mütəmadi olaraq yenilənməsi: Zəifliklәri minimuma endirmək üçün bütün sistemlərin, cihazların və proqramların ən son təhlükəsizlik verisyaları ilə yeniləndiyinə əmin olunmalıdır.

2. İşçilərin təlimi: Mütəmadi olaraq işçilərə kibertəhlükəsizliyin əhəmiyyəti və təhlükəsiz onlayn davranış məzmunlu təlimlər keçirilməlidir.

3. Hadisəyə cavab planı: Kibertəhlükəsizlik insidentlərini müəyyən etmək, onlara cavab vermək və onlardan bərpa etmək üçün hərtərəfli plan hazırlanmalıdır.

4. Müntəzəm təhlükəsizlik auditləri: Şəbəkə təhlükəsizliyinizi müntəzəm olaraq yoxlayaraq potensial zəifliklәri və təkmilləşdirmə sahələri müəyyənləşdirilməlidir.

Şəbəkə girişinə nəzarət - Şəbəkə girişinə nəzarət anlayışı təhlükəsiz və davamlı şəbəkə mühitini qorumaq üçün vacibdir. Bu anlayış cihazları və istifadəçiləri müəyyən etmək, autentifikasiya və avtorizasiya etmək üçün sistematik yanaşma təqdim edir və yalnız etibarlı qurumların şəbəkənizə daxil olmasını təmin edir. Təşkilatlar şəbəkə girişinə nəzarət sistemlərini tətbiq etməklə icazəsiz giriş, məlumatların pozulması və kiber təhdidlər riskini azalda bilər. Şəbəkə girişinə nəzarət sistemlərinin əsas xüsusiyyətlərinə real vaxt rejimində monitorinq, son nöqtə uyğunluğunun yoxlanılması və avtomatik düzəliş daxildir. Şəbəkələrdə əşyaların interneti (IoT) cihazları və öz cihazını gətir (BYOD) siyasətləri olsa belə, şəbəkə girişinə nəzarət həssas məlumatların və resursların qorunması üçün kritik komponent olaraq qalır və nəticədə təşkilatları rəqəmsal mühitdə uğur qazanmaq

üçün gücləndirir (Engebretson P., 2013: s.44).

Virusdan mühafizə proqramı - Rəqəmsal dünya genişləndikcə viruslar və zərərli proqramlar təhlükəsi daha da böyüyür və antivirus proqram təminatları məlumatların, məxfiliyin və sistemin bütövlüyünün qorunması üçün əvəzsiz vasitəyə çevrilir. Bu proqram təminatları zərərli proqramları aşkar etmək, qarşısını almaq və aradan qaldırmaq üçün nəzərdə tutulmuş və kompüter sistemlərinizin və şəbəkələrinizin təhlükəsizliyini təmin edir.

Antivirus proqramının əsasını mütəmadi olaraq yenilənən məlum təhdidlər bazası təşkil edir, ona görə də proqram virusların, qurdların, troyanların, ransomware və digər zərərli proqramların imzalarını skan edərək cihazlarınızı yoxlaya bilər. Real vaxt rejimində qorunma potensial təhdidləri aşkar etmək və zərər verməzdən əvvəl onları bloklamaq üçün sistemlərinizi daim izləyən vacib xüsusiyyətdir.

Virusdan qorunma proqramının əsas komponentlərindən biri öncədən bilinməyən təhdidləri müəyyən etmək üçün alqoritmlərdən istifadə edən evristik analizdir. Şübhəli faylların və proqramların davranışını təhlil edərək, evristik təhlil hələ müəyyən edilməmiş yeni zərərli proqramları aşkarlaya və zərərsizləşdirə bilər.

Bundan əlavə, antivirus proqram təminatları adətən e-poçt filtri, təhlükəsizlik divarı inteqrasiyası və sistem optimallaşdırma alətləri kimi əlavə təhlükəsizlik xüsusiyyətlərini ehtiva edir. Bu proqram təminatları çox səviyyəli müdafiəni təmin edən və geniş spektrli kibertəhlükələrdən qoruyan hərtərəfli təhlükəsizlik paketi təklif edir (Özkaya E.,2019: s.155).

Bununla belə, yalnız antivirus proqram tıminatlarına etibar etmək kifayət deyil. Optimal təhlükəsizliyi qorumaq üçün istifadəçilər təhlükəsiz axtarış vərdişlərini mənimsəməli, etibarsız mənbələrdən faylları yükləməməli, proqram təminatı və əməliyyat sistemlərini mütəmadi olaraq yeniləməli və məlumatların ehtiyat nüsxəsini çıxarmalıdır. Güclü antivirus proqram təminatını sağlam düşüncəli onlayn təcrübələrlə birləşdirərək, rəqəmsal dayaqlarınızı gücləndirə və getdikcə daha düşmən olan rəqəmsal mühitdə qiymətli aktivlərinizi qoruya bilərsiniz.

Məlumat sızmasının və itkisinin qarşısının alınması - Təşkilatlar məlumatın fasiləsiz mübadiləsi üzərində inkişaf edir, lakin bu mübadilə təşkilatları

əhəmiyyətli risklərə məruz qoya bilər. Bu risklərdən biri məlumat sızması və həssas məlumatların arzuolunmaz şəxslərə icazəsiz ötürülməsidir. Təşkilatlar tənzimləyici standartlara riayət etmək, öz əqli mülkiyyətlərini və müştərilərin etibarını qorumaq üçün məlumat sızmasının qarşısının alınmasına üstünlük verməlidirlər.

Məlumat sızması insan səhvi, konfiqurasiya səhvləri və kiberhücumlar da daxil olmaqla müxtəlif yollarla baş verə bilər. Riskləri minimuma endirmək üçün təşkilatların qəbul edə biləcəyi bəzi təcrübələr bunlardır:

1. İşçilərin maarifləndirilməsi: İşçilər məlumatların mühafizəsi siyasətləri və prosedurları haqqında maarifləndirilməli və ciddi təhlükəsizlik protokollarına əməl etməyin vacibliyini anlamalıdırlar. İşçilərin inkişaf edən təhdidlər və texnikalardan xəbərdar olmasını təmin etmək üçün müntəzəm olaraq təlim yeniləmələri həyata keçirilməlidir.
2. Şifrələmə və məlumat təsnifatı: Saxlama və ötürmə zamanı həssas məlumatların şifrələndiyinə əmin olunmalıdır. Məlumatların həssaslığına görə təsnif edilməsi və ciddi giriş nəzarətinin tətbiqi icazəsiz girişin və ya məlumat ifşasının qarşısını almağa kömək edə bilər.
3. Müntəzəm təhlükəsizlik qiymətləndirmələri: Potensial zəiflikləri müəyyən etmək, təhlükəsizlik siyasətlərini nəzərdən keçirmək və məlumat axınlarını təhlil etmək üçün müntəzəm auditlər və qiymətləndirmələr aparılmalıdır. Bu, potensial məlumat sızması nöqtələrini aşkar edə və vaxtında məlumat sızmasının qarşısının alınmasını təmin edə bilər.
4. Məlumat itkisinin qarşısının alınması (DLP) həllərinin tətbiq edilməsi: Real vaxt xəbərdarlıqları və qabaqcıl analitika ilə məlumat sızmasını izləmək, aşkar etmək və qarşısını almaq üçün DLP alətləri tətbiq edilməlidir.
5. Hadisələrə cavab planı: Məlumat sızması hadisələrini effektiv şəkildə idarə etmək və potensial zərəri minimuma endirmək üçün güclü insidentə cavab planı hazırlanmalıdır.

Təşkilatlar məlumat sızmasının qarşısının alınması yanaşmasından fəal istifadı etmelidirlər. Qeyd olunan təcrübələri mənimsəməklə, müəssisələr məlumat sızması

riskini əhəmiyyətli dərəcədə azalda, öz nüfuzunu və uzunmüddətli uğurlarını qoruya bilərlər.

Təhlükəsizlik divarı - Şirkətlər ünsiyyət, əməkdaşlıq və ticarət üçün internetə olan bağlılığı getdikcə artırırlar. Bu isə şirkətlərə yönəlik kibertəhlükələrin riskini daha da artırır. Bu təhlükələrdən qorunmağın ən təsirli yollarından biri şirkətin şəbəkə infrastrukturunda təhlükəsizlik divarlarının tətbiqidir.

Təhlükəsizlik divarı əvvəlcədən müəyyən edilmiş təhlükəsizlik qaydalarına əsasən daxil və xaric olan şəbəkə trafikini izləyən və idarə edən təhlükəsizlik tədbiridir. Etibarlı daxili şəbəkə ilə etibarsız xarici şəbəkələr arasında maneə rolunu oynayan təhlükəsizlik divarları icazəsiz girişin, məlumatların pozulmasının və digər zərərli fəaliyyətlərin qarşısını almaq üçün mühüm qorunma təbəqəsini təmin edir.

Bir neçə növ təhlükəsizlik divarı mövcuddur və hər birinin güclü və zəif tərəfləri var. Şirkətlərdə ən çox istifadə edilən növlərə aşağıdakılar daxildir:

1. Paket filtrləmə təhlükəsizlik divarları: Bu təhlükəsizlik divarları IP ünvanı, protokol və ya port nömrəsi kimi müəyyən edilmiş meyarlara əsasən icazə vermək və ya rədd etmək üçün məlumat paketlərini yoxlayır.
2. Status məlumatı yoxlayan təhlükəsizlik divarları: Bu təhlükəsizlik divarları aktiv bağlantıların vəziyyətini izləyir və paketə icazə verilib-verilməməsi barədə qərar vermək üçün bu məlumatdan istifadə edir.
3. Proksi təhlükəsizlik divarları: Bu təhlükəsizlik divarları zərərli məzmunun sistemə daxil olmasının qarşısını almaq üçün şirkətin daxili şəbəkəsi ilə internet arasında vasitəçilik edən filtrləmə xidmətini təqdim edir.
4. Ən son nəsil təhlükəsizlik divarları (NGFW): Bu qabaqcıl təhlükəsizlik divarları müdaxilənin qarşısının alınması, paketlərin dərin təftişi və tətbiq məlumatlılığı kimi əlavə funksionallığı ənənəvi təhlükəsizlik divarlarının xüsusiyyətləri ilə birləşdirir.

Şirkətin şəbəkə infrastrukturunda təhlükəsizlik divarlarının tətbiqi möhkəm kibertəhlükəsizlik strategiyasının qurulmasında mühüm addımdır. Bununla belə, heç bir təhlükəsizlik tədbiri fərdi şəkildə tam qorunma təmin edə bilməz. Buna görə də,

təhlükəsizlik divarları son nöqtənin qorunması, müdaxilənin aşkarlanması sistemləri və müntəzəm təhlükəsizlik auditləri kimi digər təhlükəsizlik tədbirləri ilə birləşdirilməlidir.

Nəticədə, təhlükəsizlik divarları şirkətin rəqəmsal aktivlərini qorumaq və şəbəkə bütövlüyünü təmin etmək üçün əvəzsiz alətlərdir. Müvafiq təhlükəsizlik divarları həllini tətbiq etməklə və bunu hərtərəfli kibertəhlükəsizlik strategiyası ilə birləşdirməklə şirkətlər kibertəhlükələrə məruz qalmalarını əhəmiyyətli dərəcədə azalda və öz qiymətli məlumat və resurslarını qoruya bilərlər.

Proksi server - Şirkətlər rəqabətə davamlı olmaq üçün daim uyğunlaşmalı və yeniliklər etməlidir. Müəssisələrin iş tərzini dəyişdirən belə yeniliklərdən biri də proxy serverlərin istifadəsidir. Proksi server müştəri ilə internet arasında vasitəçidir və şirkətlərə onlayn fəaliyyətlərini effektiv şəkildə idarə etməyə və təhlükəsizliyini təmin etməyə imkan verir. Proksi serverdən istifadənin əsas üstünlüyü onun təmin etdiyi əlavə təhlükəsizlik səviyyəsidir. Proksilər şirkətin daxili şəbəkəsi ilə internet arasında bufer rolunu oynayaraq kiberhücumlar və məlumatların pozulması riskini azaltmağa kömək edir. Bundan əlavə, proksilər zərərli veb-saytlara girişi bloklaya və arzuolunmaz məzmunu filtrləyərək təşkilatın rəqəmsal aktivlərini daha da qoruya bilər.

Proksi serverlər tez-tez daxil olan veb məzmunu keşləməklə şirkətin şəbəkə performansını yaxşılaşdıra bilər. Bu, internetdən məlumatların axtarışını sürətləndirir, daha sürətli axtarışa və məhsuldarlığın artmasına səbəb olur. Bundan əlavə, proksilər şəbəkə trafikini daha bərabər paylayaraq sıxlığın qarşısını alır və bütün istifadəçilər üçün ən yaxşı performansı təmin edir.

Şirkətlər proksi serverlərdən istifadə edərək işçilərin internet istifadəsinə nəzarət edə bilərlər. Proksilər əlaqəli olmayan veb-saytlara girişi məhdudlaşdırmaqla şirkəti bu veb-saytlardan gələ biləcək təhlükələrdən qoruyur.

Şirkətin IP ünvanını gizlətməklə, proksi serverlər onlayn olaraq anonimlik və məxfilik səviyyəsini təmin edə bilərlər. Bazar araşdırması və ya rəqabət təhlili aparan müəssisələr üçün bu, onlara anonim məlumat toplamaq imkanı yaradır. Bu üstünlüklərə baxmayaraq, şirkətlərdə proxy serverlərdən istifadə ilə bağlı potensial

çatışmazlıqlar var. Əsas narahatlıqlardan biri şirkəti təhlükəsizlik təhdidlərinə məruz qoya bilən yanlış konfiqurasiya riskidir. Həmçinin, bəzi proksi serverlər istifadəçi məlumatlarını saxlaya bilər ki, bu da məxfiliklə bağlı narahatlıqları artırır. Bu riskləri azaltmaq üçün şirkətlər güclü proksi serverlərə investisiya etməli və ciddi təhlükəsizlik tədbirləri həyata keçirməlidir (https://cloudsecurityalliance.org/).

Müdaxilənin aşkarlanması və qarşısının alınması sistemləri - Müdaxilənin aşkarlanması və qarşısının alınması sistemləri şəbəkə üzərindən ötürülən hər bir məlumat paketini təhlil edən və zərərli məzmun, şübhəli trafik və təhlükəsizlik pozuntularını ehtiva edən paketləri aşkarlayan və qarşısını alan sistemdir. Bu sistemlər şəbəkəni qorumaq üçün müxtəlif aşkarlama və qarşısının alınması üsullarından istifadə edir. Ümumi iş prinsipi qara siyahı üsuludur.

İmzaya əsaslanan üsullar keçmişdə aşkar edilmiş təhdidlərin imzalarından istifadə edir. Bu imzalar sistemin məlumat bazasında saxlanılır. Şəbəkə trafiki təhlil edilərkən bu verilənlər bazasındakı imzalarla müqayisə edilir və uyğun gələn trafik olduqda sistem konfiqurasiyasına uyğun olaraq lazımi tədbirlər görülür.

Anomaliyaya əsaslanan yanaşma şəbəkədə hər hansı anomaliya və gözlənilməz davranışa nəzarət edir. Normal olmayan davranış aşkar edilərsə, sistem konfiqurasiyasına uyğun olaraq lazımi tədbirlər görülür.

E-poçt təhlükəsiz şəbəkə keçidi - Zərərli məzmunlu məktublar hakerlər tərəfindən korporativ şəbəkələrə sızmaq, məlumatları oğurlamaq, korporativ nüfuzunu korlamaq və qurumun nüfuzuna xələl gətirmək üçün tez-tez istifadə olunur. Elektron məktubların hədəfinin insanlar olduğu və insanı aldatmağın sistemi aldatmaqdan daha asan olduğu bilindiyi üçün zərərli məzmunlu elektron məktubların hədəf son istifadəçiyə ötürülməsinin qarşısını almaq lazımdır. Buna görə də, e-poçt təhlükəsizlik şlüzünün istifadəsi çox vacib məsələdir.

E-poçt təhlükəsizlik şlüzü təşkilatı arzuolunmaz zərərli məzmundan qorumaq və onun nəzərdə tutulan alıcılara çatmasının qarşısını almaq üçün istifadə edilən sistemdir. Zərərli, arzuolunmaz məzmunu olan e-poçtlar şirkət siyasətini poza bilən, zərərli proqram və ya arzuolunmaz məlumatları ehtiva edən e-poçtlardır.

Bu sistemlər bir neçə moduldan ibarət ola bilər. Zərərli proqram filtri e-poçtda

zərərli proqramı aşkarlayır və zərərli e-poçtun alıcılara çatmasının qarşısını alır. Zərərli e-poçtların alıcılara çatma riskini azaltmaq üçün e-poçtun təhlükəsizlik şlüzündə antivirus imza verilənlər bazasını yeniləmək və hər bir e-poçtu yoxlamaq lazımdır (Erickson J., 2008: s.83).

Son nöqtənin aşkarlanması və cavabı - Son nöqtənin aşkarlanması və cavabı (EDR) anlayışı şəbəkələrini inkişaf edən kibertəhlükələrdən qorumaq istəyən şirkətlər üçün kritik təhlükəsizlik tədbiridir. EDR bütün dünyada şirkətlərin həssas məlumatlarını və aktivlərini qorumaq üçün güclü və proaktiv həll yolu təqdim edir. Bu təhlükəsizlik tədbiri şirkətlərə son nöqtə cihazlarını hədəf alan kiberhücumları aşkarlamağa, cavab verməyə və qarşısını almağa kömək edir.

Son nöqtələr - kompüterlər, noutbuklar və mobil cihazlar şirkət məlumatlarına birbaşa çıxışı sayəsində kiberhücumlara qarşı xüsusilə həssasdır. EDR potensial təhlükələri ən erkən mərhələlərdə aşkar etmək, təhlil etmək və zərərsizləşdirmək üçün nəzərdə tutulmuşdur, beləliklə, təhlükəsizlik qrupları pozuntularla tez bir zamanda məşğul ola və zərəri məhdudlaşdıra bilər.

EDR-nin əsas funksionallığı son nöqtə fəaliyyətlərini daim izləmək və təhlil etməkdir. Maşın öyrənməsi və süni intellektdən istifadə edərək, EDR alətləri anomaliyaları aşkarlaya, şübhəli davranışı qeyd edə və təhlükəsizlik qruplarına real vaxtda xəbərdarlıq verə bilər. Bu proaktiv yanaşma potensial təhdidlərə sürətli reaksiya verir və hakerlər üçün əlçatanlığı minimuma endirir.

EDR alətləri son nöqtə fəaliyyətlərinə dərindən nəzər salmaqla analitiklərə hücumların miqyasını və xarakterini başa düşməyə və müvafiq tədbirlərin görülməsini təmin etməyə imkan verir (https://www.securityforum.org/).

Təhlükəsizlik məlumatı və hadisələrin idarə edilməsi - SIEM sistemləri potensial təhlükəsizlik insidentlərini müəyyən etmək üçün şəbəkə cihazları, serverlər və proqramlar kimi çoxsaylı mənbələrdən əldə edilən gündəlik məlumatları toplayan, əlaqələndirən və təhlil edən hərtərəfli həllyoludur. SIEM sistemlərinin işləmə prinsipi aşağıdakı kimidir:

1. Günlük məlumat toplanması və idarə edilməsi: Sistem müxtəlif mənbələrdən günlük məlumatları toplayır və onları vahid formata çevirib təhlil və əlaqələndirməyi asanlaşdırır.
2. Hadisələrin əlaqələndirilməsi: Toplanmış günlük məlumatları əvvəlcədən müəyyən edilmiş qaydalar və nümunələrlə müqayisə edərək təhlükəsizlik hadisəsini müəyyən edir.
3. Xəbərdarlığın yaradılması: Potensial hadisə aşkar edildikdə, SIEM sistemi təhlükəsizlik qrupu hadisəyə uyğun cavab verə bilməyi üçün xəbərdarlıq yaradır (https://www.cisecurity.org/).
4. Hadisələrə Cavab: SIEM sistemləri adətən təhlükəsizlik qruplarına, insidentlərə cavab verməyə kömək edən həyata keçirilə bilən anlayışlar və düzəliş tövsiyələri verən alətləri əhatə edir.
5. Hesabat və Analitika: SIEM sistemi təhlükəsizlik hadisələri və tendensiyaları haqqında hesabatlar yaradır, təhlükəsizlik qruplarına və rəhbərliyə şirkətin təhlükəsizlik vəziyyəti haqqında məlumat əldə etməyə və əsaslandırılmış qərarlar qəbul etməyə imkan verir.

Şirkətlərdə SIEM tətbiqinin üstünlükləri - SIEM sisteminin tətbiqi şirkətlər üçün aşağıda qeyd olunan bir sıra üstünlüklər təklif edir.

1. Təkmilləşdirilmiş təhlükənin aşkarlanması: Çoxsaylı mənbələrdən məlumatların toplanması və təhlili ilə SIEM sistemləri fərdi təhlükəsizlik həllərinin qaçıra biləcəyi təhdidləri aşkarlaya və ümumi təhlükənin aşkarlanması imkanlarını artıra bilər.

2. Daha sürətli insident reaksiyası: SIEM sistemləri tərəfindən yaradılan xəbərdarlıqlar təhlükəsizlik qruplarına insidentlərə tez reaksiya verməyə və təhlükəsizlik pozuntusunun potensial təsirini minimuma endirməyə imkan verir.

3. Tənzimləmə uyğunluğu: Bir çox sənayedə məlumatların təhlükəsizliyi üçün ciddi tənzimləmə tələbləri var və SIEM sistemləri şirkətlərə ətraflı hesabatlarda və audit yollarına uyğunluğu nümayiş etdirməkdə kömək edə bilər.

4. Artırılmış əməliyyat səmərəliliyi: Günlük məlumatların toplanması, təhlili və xəbərdarlığın yaradılmasını avtomatlaşdıraraq, SIEM sistemləri təhlükəsizlik

qruplarının diqqətini digər strateji vəzifələrə yönəltmək üçün imkan yaradır.

5. Daha yaxşı qərarların qəbulu: SIEM sistemləri tərəfindən təqdim edilən hesabatlar və analitiklər təhlükəsizlik qruplarına və idarəçilərə şirkətin təhlükəsizlik vəziyyəti haqqında dəyərli anlayışlar təqdim edərək, onlara təhlükəsizlik siyasətləri və investisiyalar haqqında əsaslandırılmış qərarlar qəbul etməyə kömək edir.

2.2 Korporativ Kibertəhlükəsizlik Çərçivələri

Təşkilatlar kibertəhlükəsizlik risklərini effektiv şəkildə müəyyən edə, qiymətləndirə və azalda bilməsi üçün əhatəli kibertəhlükəsizlik çərçivələri qəbul etməlidirlər.

Korporativ kibertəhlükəsizlik çərçivələri kibertəhlükəsizlik risklərini idarə etmək üçün strukturlaşdırılmış və sistematik yanaşma təklif edir. Bu çərçivələr təşkilatların möhkəm və effektiv kibertəhlükəsizlik proqramını yaratmaq və saxlamaq üçün istifadə edə biləcəyi təlimatlar, ən yaxşı təcrübələr və standartlar toplusudur. Bu çərçivələr idarəetmə, risklərin idarə edilməsi, uyğunluq, insidentlərə reaksiya və təhlükəsizlik əməliyyatları kimi bir sıra kibertəhlükəsizlik sahələrini əhatə edir. Hərtərəfli kibertəhlükəsizlik çərçivəsinin qəbul edilməsi təşkilatlar üçün öz aktivlərini qorumaq və kibertəhlükəsizlik risklərini effektiv şəkildə idarə etmək üçün vacibdir.

Hər birinin öz təlimatları və tələbləri olan bir sıra korporativ kibertəhlükəsizlik çərçivələri mövcuddur. Ən çox tanınan çərçivələrə aşağıdakılar daxildir:

1. Milli Standartlar və Texnologiya İnstitutu (NIST) Kiber Təhlükəsizlik Çərçivəsi
2. Mərkəzi İnternet Təhlükəsizliyi (CIS)
3. Beynəlxalq Standartlaşdırma Təşkilatı (ISO) 27001
4. Ödəniş Kart Sənayesi Məlumat Təhlükəsizliyi Standartı (PCI DSS)
5. Kritik Təhlükəsizlik Nəzarətləri (CSC)

Milli Standartlar və Texnologiya İnstitutu (NIST) Kiber Təhlükəsizlik

Çərçivəsi - Milli Standartlar və Texnologiya İnstitutunun (NIST) Kibertəhlükəsizlik Çərçivəsi təşkilatlarda kibertəhlükəsizlik risklərinin idarə edilməsi üçün hərtərəfli, riskə əsaslanan yanaşmadır. Dövlət və özəl sektorlar arasında əməkdaşlıq prosesi vasitəsilə hazırlanmış bu çərçivə biznes və dövlət qurumlarının kibertəhlükəsizlik mövqeyini yaxşılaşdırmaq üçün standarta çevrilmişdir. NIST kibertəhlükəsizlik çərçivəsi istənilən ölçüdə və ya sənayedə təşkilatların ehtiyaclarına uyğunlaşdırıla bilən çevik və genişlənə bilən bir həll təqdim edir .

NIST kibertəhlükəsizlik çərçivəsi beş əsas funksiyadan ibarətdir. Bu funksiyalar təşkilatlara kibertəhlükəsizlik insidentlərini müəyyən etmək, qorumaq, aşkar etmək, reaksiya vermək və bərpa etmək üçün strukturlaşdırılmış yanaşma təmin edir. Beş əsas funksiya bunlardır:

1. Müəyyən etmə: Bu funksiyaya təşkilatın aktivlərini, sistemlərini və məlumatlarını başa düşmək, eləcə də onların üzləşdiyi potensial riskləri müəyyən etmək daxildir. Müəyyən etmə funksiyası risklərin qiymətləndirilməsi və aktivlərin idarə edilməsi kimi mövzuları əhatə edir.
2. Qoruma: Bu funksiya kritik aktivlərin və sistemlərin məxfiliyini, bütövlüyünü və əlçatanlığını təmin etmək üçün mühafizə tədbirlərinin həyata keçirilməsinə diqqət yetirir. Qoruma funksiyası girişə nəzarət, məlumat təhlükəsizliyi və işçilərin təlimi kimi mövzuları əhatə edir.
3. Aşkarlama: Bu funksiya potensial kibertəhlükəsizlik insidentlərinin vaxtında tanınmasına diqqət yetirir. Aşkarlama funksiyası davamlı monitorinq, anomaliyaların aşkarlanması və təhlükəsizlik hadisələrinin təhlili kimi mövzuları əhatə edir (https://www.nist.gov/topics/cybersecurity).
4. Cavab vermə: Bu funksionallığa aşkar edilmiş kibertəhlükəsizlik insidentlərinə cavab vermək üçün planın hazırlanması və həyata keçirilməsi daxildir. Cavab vermə funksiyası hadisəyə cavab planlaması, ünsiyyət və təhlil kimi mövzuları əhatə edir.
5. Bərpa etmə: Bu funksiyaya kibertəhlükəsizlik hadisəsindən sonra normal əməliyyatların bərpası və təşkilatın təcrübədən öyrənməsinə imkan

yaradılması daxildir. Bərpa etmə funksiyası bərpa planının hazırlanması, həyata keşirilməsi və hesabat verilməsi kimi mövzuları əhatə edir.

Nəticə olaraq NIST kibertəhlükəsizlik çərçivəsinin tətbiqi təşkilatlar üçün kibertəhlükəsizlik risklərinə proaktiv yanaşmaq üçün mühüm addımdır. Bu hərtərəfli yanaşmaya riayət etməklə təşkilatlar ümumi təhlükəsizlik vəziyyətini təkmilləşdirə, tənzimləyici tələblərə əməl edə və maraqlı tərəflərə inam yarada bilər.

Mərkəzi İnternet Təhlükəsizliyi (CIS) İdarəsi - Mərkəzi İnternet Təhlükəsizliyi müxtəlif sənaye sahələrində təşkilatların kibertəhlükəsizlik vəziyyətinin yaxşılaşdırılmasına həsr olunmuş qeyri-kommersiya təşkilatıdır. CIS-nin kibertəhlükəsizliyə nəzarət çərçivəsi təşkilatları möhkəm kibertəhlükəsizlik əsası ilə təmin edən prioritetləşdirilmiş ən yaxşı təcrübə tədbirlər toplusudur. Bu nəzarətlər təşkilatlara ən çox yayılmış kibertəhlükələri və zəiflikləri müəyyən etmək və aradan qaldırmaqla təhlükəsizlik vəziyyətini yaxşılaşdırmaqda kömək etmək üçün nəzərdə tutulub (Hadnagy C., 2018: s.143).

Çərçivə üç kateqoriyaya bölünən nəzarətlərdən ibarətdir: Əsas, təməl və təşkilati. Əsas nəzarətə aparat və proqram təminatı aktivlərinin inventarlaşdırılması və nəzarəti, təhlükəsiz konfiqurasiya və davamlı zəifliyin idarə edilməsi kimi kritik təhlükəsizlik tədbirləri daxildir. Təməl nəzarət e-poçt və veb brauzerin qorunması, məlumatların bərpa imkanları və təhlükəsiz şəbəkə infrastrukturu kimi aspektləri həll edir. Təşkilati nəzarət isə insidentlərə cavab tədbirlərinin planlaşdırılması, nüfuz testi və işçilərin təliminin vacibliyini vurğulayır.

<u>Təşkilatlar CIS kibertəhlükəsizliyi çərçivəsinin tətbiqindən necə faydalana bilər?</u>

1. Gücləndirilmiş təhlükəsizlik: CIS nəzarətləri ən çox yayılmış kibertəhlükələrin həllinə sistemli və prioritet yanaşma təklif etmək üçün nəzərdə tutulmuşdur. Bu nəzarətləri həyata keçirməklə təşkilatlar məlumatların pozulması, maliyyə itkiləri və nüfuzun zədələnməsi risklərini effektiv şəkildə azalda bilər.
2. Xərc səmərəliliyi: Çərçivə təşkilatlar üçün kibertəhlükəsizlik mövqeyini gücləndirmək üçün xərc baxımından sərfəli üsul təqdim edir. MDB

Nəzarətlərinin həyata keçirilməsi təşkilatların təhlükəsizlik texnologiyalarına, kadrlara və təlimlərə investisiyanın və resursların səmərəli şəkildə bölüşdürülməsini təmin etməyə kömək edə bilər.

3. Sənaye qaydalarına uyğunluq: GDPR, HIPAA və PCI DSS kimi bir çox tənzimləyici orqanlar və sənaye standartları təşkilatlardan güclü kibertəhlükəsizlik tədbirləri görmələrini tələb edir. CIS nəzarətlərinin həyata keçirilməsi təşkilatlara bu tələblərə uyğunluğu nümayiş etdirməyə və potensial olaraq cərimələrdən yayınmağa kömək edə bilər.
4. Miqyaslılıq və çeviklik: CIS kibertəhlükəsizliyə nəzarət çərçivəsi bütün sənaye təşkilatlarına uyğun şəkildə uyğunlaşdırıla bilər. Modul yanaşma təşkilatlara öz unikal risk profillərinə və biznes ehtiyaclarına əsaslanaraq xüsusi nəzarət vasitələrinə üstünlük verməyə və onlara diqqət yetirməyə imkan verir.
5. Tərəfdaşlıq və məlumat mübadiləsi: CIS idarəetmələrindən istifadə edərək təşkilatlar ən yaxşı bilik, təcrübə və tətbiqləri paylaşan kibertəhlükəsizlik mütəxəssisləri icmasına qoşulurlar. Bu əməkdaşlıq yanaşması kibertəhlükəsizlikdə davamlı inkişafı və yeniliyi təmin edir

Beynəlxalq Standartlaşdırma Təşkilatı (ISO) 27001 - ISO 27001 Beynəlxalq Standartlar Təşkilatı (ISO) və Beynəlxalq Elektrotexniki Komissiya (IEC) tərəfindən hazırlanmış beynəlxalq səviyyədə tanınmış standartdır. Bu standart təşkilat daxilində İnformasiya Təhlükəsizliyi İdarəetmənin (ISMS) yaradılması, həyata keçirilməsi, saxlanılması və davamlı təkmilləşdirilməsi üçün çərçivə təmin edir. ISO 27001 standartı risklərin idarə edilməsi yanaşmasına əsaslanaraq xüsusi təhlükəsizlik tələblərini və risklərini həll edə bilməsi üçün hər miqyaslı təşkilata tətbiq olunması nəzərdə tutulmuşdur (McNab C., 2016: s.112).

<u>ISO 27001-in tətbiqinin üstünlükləri:</u>

1. Təkmilləşdirilmiş təhlükəsizlik: ISO 27001 təşkilatın informasiya təhlükəsizliyi risklərinin idarə edilməsinə kompleks yanaşma təqdim edir. Standartı tətbiq etməklə təşkilatlar potensial təhdidləri, zəiflikləri və onların informasiya aktivlərinə təsirləri müəyyən edə və bu riskləri azaltmaq üçün

müvafiq nəzarət vasitələri hazırlaya bilərlər. Bu, həssas məlumatları qorumağa, təhlükəsizlik insidentləri ehtimalını azaltmağa və işin davamlılığını təmin etməyə kömək edir.

2. Tənzimləmə uyğunluğu: Məlumatların qorunmasına və məxfiliyə artan diqqətlə təşkilatlar müxtəlif tənzimləmə tələblərinə tabe olurlar. ISO 27001-in tətbiqi tənzimləyicilərə və maraqlı tərəflərə təşkilatın informasiya təhlükəsizliyinə ciddi yanaşdığını və uyğunluq öhdəliklərini yerinə yetirmək üçün möhkəm struktura malik olduğunu nümayiş etdirə bilər.
3. Təkmilləşdirilmiş reputasiya: ISO 27001 sertifikatının əldə edilməsi təşkilatın informasiya təhlükəsizliyinə sadiqliyini nümayiş etdirən mühüm mərhələdir. Bu, təşkilatın reputasiyasını yaxşılaşdıra, müştərilər və tərəfdaşlar arasında inam yarada və bazarda rəqabət üstünlüyü təmin edə bilər.
4. Xərclərə qənaət: ISMS-in tətbiqi təşkilatlara məlumat pozuntularının və təhlükəsizlik insidentlərinin qarşısını almağa kömək edir. Bu da maliyyə itkilərinin, hüquqi cəzaların və reputasiyaya dəyən zərərin qarşısını alır. Riskləri proaktiv şəkildə idarə etməklə və potensial problemləri artmazdan əvvəl həll etməklə, təşkilatlar informasiya təhlükəsizliyi ilə bağlı ümumi xərcləri azalda bilər.

<u>ISO 27001 Tətbiq Addımları:</u>

1. Yüksək idarəetmə dəstəyinin təmin edilməsi: ISO 27001-in tətbiqində ilk addım yüksək idarəetmənin öhdəliyini və dəstəyini qazanmaqdır. Bu, effektiv ISMS-nin yaradılması və saxlanılması üçün lazımi resursların və təcrübənin olmasını təmin etmək vacibdir.
2. Risk qiymətləndirilməsinin həyata keçirilməsi: Təşkilatlar öz məlumat aktivləri üçün riskləri müəyyən etməli və qiymətləndirməlidirlər. Bura təhlükəsizlik insidentlərinə səbəb ola biləcək təhdidlərin və zəifliklərin müəyyən edilməsi və təşkilata potensial təsirlərin qiymətləndirilməsi daxildir.
3. Risk azaltma planının hazırlanması: Risklərin qiymətləndirilməsinə əsaslanaraq, təşkilatlar müəyyən edilmiş riskləri azaltmaq üçün lazım olan

nəzarət və tədbirləri özündə əks etdirən risk azaltma planı hazırlamalıdır. Bura ISMS-nin tətbiqi ilə məşğul olan işçilərin rol və məsuliyyətlərinin müəyyən edilməsi daxildir.

4. Nəzarətlərin həyata keçirilməsi: Təşkilatlar siyasətləri, prosedurları və texniki tədbirləri ehtiva edə biləcək lazımi nəzarətləri həyata keçirməklə risk azaltma planını səfərbər etməlidir.
5. Monitorinq və təhlilin keçirilməsi: Müntəzəm monitorinq və təhlil ISMS-nin effektivliyini təmin etmək və təkmilləşdirilməli sahələri müəyyən etmək üçün vacibdir. Bura daxili auditlərin və rəhbərliyin nəzərdən keçirilməsi və aşkar edilmiş uyğunsuzluqların aradan qaldırılması daxildir.
6. Sertifikatlaşdırma: ISMS tam şəkildə tətbiq edildikdə və səmərəli fəaliyyət göstərdikdə, təşkilatlar müstəqil audit aparmaq üçün akkreditə olunmuş sertifikatlaşdırma orqanını işə götürərək ISO 27001 sertifikatına nail ola bilərlər.

Ödəniş Kart Sənayesi Məlumat Təhlükəsizliyi Standartı (PCI DSS) - Ödəniş Kart Sənayesi Məlumatlarının Təhlükəsizliyi Standartı (PCI DSS) kart sahibinin məlumatlarını emal edən, saxlayan və ya ötürən təşkilatlara təhlükəsiz mühitin qorunmasına kömək etmək üçün Ödəniş Kartı Sənayesi Təhlükəsizlik Standartları Şurası (PCI SSC) tərəfindən hazırlanmış qlobal miqyasda tanınan təhlükəsizlik standartları toplusudur. PCI DSS-nin əsas məqsədi məlumatların pozulması riskini azaltmaq və müştərilərin həssas məlumatlarını qorumaqdır. Onlayn əməliyyatlar eksponent olaraq böyüməyə davam etdikcə, təşkilatlar müştərilərinin məlumatlarını qorumaq və etibar yaratmaq üçün PCI DSS uyğunluğunun həyata keçirilməsinə və saxlanmasına üstünlük verməlidirlər (Sanders C., Smith J., 2013: s.152).

Standart altı nəzarət məqsədinə bölünmüş on iki əsas tələbdən ibarətdir:

1. Təhlükəsiz şəbəkə və sistemlərin qurulması və qorunması
   - Kart sahibinin məlumatlarını qorumaq üçün firewall konfiqurasiyasını quraşdırın və qoruyun.
   - Sistem parolları və digər təhlükəsizlik parametrləri üçün satıcı tərəfindən təmin edilmiş standart parametrlərdən istifadə etməyin.

2. Kart sahibinin məlumatlarını qorunması
    - Saxlanan kart sahibi məlumatlarını qoruyun.
    - Açıq, ictimai şəbəkələrdə kart sahibi məlumatlarının ötürülməsini şifrələyin.
3. Zəifliyin idarə olunması proqramının davam etdirilməsi
    - Bütün sistemləri zərərli proqramlardan qoruyun və antivirus proqram təminatlarını müntəzəm olaraq yeniləyin.
    - Təhlükəsiz sistemləri və proqramları inkişaf etdirin və qoruyun.
4. Girişə nəzarət tədbirlərinin həyata keçirilməsi
    - Biznes ehtiyacını bilməklə kart sahibi məlumatlarına girişi məhdudlaşdırın.
    - Sistem komponentlərinə girişi müəyyən edin və autentifikasiya edin.
    - Kart sahibinin məlumatlarına fiziki girişi məhdudlaşdırın.
5. Şəbəkələri mütəmadi olaraq izləmək və sınaqdan keçirmək
    - Şəbəkə resurslarına və kart sahibi məlumatlarına bütün girişləri izləyin və nəzarət edin.
    - Mütəmadi olaraq təhlükəsizlik sistemlərini və proseslərini sınaqdan keçirin.
6. İnformasiya təhlükəsizliyi siyasətini aparın
    - Təhlükəsizlik siyasətini yaradın, dərc edin və qoruyun.

<u>PCI DSS tətbiqinin üstünlükləri:</u>

1. Gücləndirilmiş təhlükəsizlik: PCI DSS-nin 12 tələbinin həyata keçirilməsi təşkilatın təhlükəsizlik mövqeyini gücləndirir, məlumatların pozulması riskini və onların gətirdiyi potensial maliyyə və reputasiya zərərini azaldır.
2. Təkmilləşdirilmiş müştəri etimadı: PCI DSS ilə uyğunluğu nümayiş etdirərək, təşkilatlar öz müştərilərinə məlumat təhlükəsizliyinə üstünlük verdiklərini bildirirlər.
3. Tənzimləmə uyğunluğu: PCI DSS adətən oxşar məqsədləri paylaşan Ümumi Məlumatların Qorunması Qaydası (GDPR) və Kaliforniya İstehlakçı

Məxfiliyi Aktı (CCPA) kimi digər məlumat qoruma qaydalarına riayət etmək üçün təşkilatlara kömək edir.

4. Azaldılmış maliyyə riski: PCI DSS-ə əməl edilməməsi ağır cərimələr, artan əməliyyat haqları və ya ödəniş kartı əməliyyatlarını emal etmək hüququnun itirilməsi kimi ciddi nəticələrə səbəb ola bilər. Təşkilatlar uyğunluğu təmin etməklə belə zərərli nəticələrin qarşısını ala bilərlər.

Nəticə olaraq, PCI DSS'ye uyğunluq, yalnız güclü bir təhlükəsizlik çərçivəsi təmin etməklə qalmaz, eyni zamanda müştəri güvənini və normativlərə uyğunluğu təmin edər. PCI DSS uyğunluğunun tətbiqi və saxlanması təşkilatlara həssas müştəri məlumatlarının idarə edilməsi ilə bağlı riskləri azaltmağa və rəqabətli biznes dünyasında uzunmüddətli uğur üçün mövqe tutmağa imkan verir.

Kritik Təhlükəsizlik Nəzarətləri (CSC) - Kritik Təhlükəsizlik Nəzarətlər (CSCs) təşkilatlara kibertəhlükələrə qarşı müdafiələrini gücləndirməyə kömək etmək üçün nəzərdə tutulmuş prioritet kibertəhlükəsizlik təcrübələridir. İnternet Təhlükəsizliyi Mərkəzi (CIS) tərəfindən hazırlanmış və dəstəklənən bu nəzarətlər potensial zəiflikləri aşkar etmək və aradan qaldırmaqla təşkilatların kibertəhlükəsizlik mövqelərini gücləndirmək üçün riskə əsaslanan çərçivə təmin edir.

1. Kritik Təhlükəsizlik Nəzarətlərinin Önəmi:

CSC-lərin tətbiqi təşkilatlara aktivləri, həssas məlumatları və biznesin davamlılığını qoruyan möhkəm və davamlı kibertəhlükəsizlik infrastrukturu yaratmağa imkan verir. Ən kritik və effektiv nəzarətlərə üstünlük vermək, təşkilatlara kibertəhlükəsizliyə edilən investisiyanın gəlirliliyini (ROI) maksimuma çatdırmaq üçün resursları səmərəli şəkildə ayırmağa imkan verir.

2. Təbəqəli Kibertəhlükəsizlik Yanaşması:

CSC-lər hər növ təbəqəli təhlükəsizlik yanaşmasını təqdim edir. Bu o deməkdir ki, təşkilatlar güclü müdafiə yaradan çoxsaylı tamamlayıcı nəzarətlər tətbiq etməlidir. Çünki bir tədbir uğursuz olsa belə, təhlükəsizliyi qorumaq üçün digərlərinin mövcud olması əsasdır.

3. Risk Əsaslı Prioritetləşdirmə:

CSC-lər təşkilatlara ilk növbədə ən kritik nəzarətlərə diqqət yetirməyə kömək edir,

daha aşağı prioritetli məsələlərə keçməzdən əvvəl onlara resursları səmərəli şəkildə bölüşdürməyə və yüksək prioritetli zəiflikləri həll etməyə imkan verir.

4. Daimi Yeniləmələr və Təkmilləşdirilmiş Nəzarətlər:

CIS müvafiq, effektiv və ən son təhlükə kəşfiyyatı, sənayenin ən yaxşı təcrübələri və texnoloji irəliləyişlərlə uyğunlaşmaq üçün CSC-ləri müntəzəm olaraq nəzərdən keçirir və yeniləyir.

5. Kritik Təhlükəsizlik Nəzarətlərinin Əsas Komponentləri:

CSC-lərin xüsusi sayı və tərkibi zamanla dəyişə bilsə də, əsas anlayışları geniş şəkildə aşağıdakı kateqoriyalara qruplaşdırmaq olar:

5.1 Aktivlərin idarə edilməsi: Aparat və proqram təminatı aktivlərinin düzgün idarə edilməsi təşkilatın təhlükəsizliyini qorumaq üçün vacibdir. Buraya dəqiq inventarların yaradılması və saxlanması, yalnız icazə verilmiş cihazlar və proqramlardan istifadə və köhnəlmiş aktivlərin dərhal çıxarılması və məhv edilməsi daxildir.

5.2 Zəifliyin idarə edilməsi: Aparat, proqram təminatı və konfiqurasiyalardakı zəifliklərin müntəzəm olaraq müəyyən edilməsi, qiymətləndirilməsi və aradan qaldırılması təşkilatın hücum səthini azaltmaq üçün çox vacibdir. Buraya zəifliklərin skan edilməsi, yamaqların və yeniləmələrin tətbiqi, təhlükəsizlik konfiqurasiyalarının müntəzəm nəzərdən keçirilməsi və yenilənməsi daxildir (https://www.issa.org/).

5.3 Girişə Nəzarət: İnformasiya sistemlərinə və məlumatlara çıxışın idarə edilməsi və nəzarəti həyati əhəmiyyət kəsb edir. Buraya güclü autentifikasiya və avtorizasiya mexanizmlərinin tətbiqi, həssas məlumatlara girişin yalnız ehtiyac olduqda icazəsi və administrator hesablarının və imtiyazlarının istifadəsinə nəzarət daxildir.

5.4 Şəbəkə Təhlükəsizliyi: Təşkilatlar öz şəbəkələrini icazəsiz girişdən qorumaq və təhdidlərin yayılmasından müdafiə etmək üçün güclü şəbəkə təhlükəsizliyi tədbirləri həyata keçirməlidir. Buraya təhlükəsizlik divarının, müdaxilənin aşkarlanması və qarşısının alınması sistemlərinin (IDPS), şəbəkənin bölünməsi və təhlükəsiz uzaqdan giriş həllərinin tətbiqi daxildir.

5.5 Son Nöqtə Təhlükəsizliyi: Masaüstü kompüterlər, noutbuklar və mobil cihazlar kimi son nöqtə cihazları virusdan qorunma proqram təminatları, son nöqtənin aşkarlanması və cavablandırılması (EDR) alətləri və müntəzəm proqram yeniləmələri kimi güclü təhlükəsizlik tədbirləri ilə qorunmalıdır.

5.6 Məlumatların qorunması: Təşkilatlar həssas məlumatları şifrələmə, məlumat itkisinin qarşısının alınması (DLP) texnologiyaları və təhlükəsiz məlumatların saxlanması və məhv edilməsi təcrübələri kimi üsullarla qorumalıdır (https://www.iacsit.org/).

5.7 Hadisələrə cavab və idarəetmə: Hərtərəfli insident cavab planının yaradılması və saxlanması təşkilatlara təhlükəsizlik insidentlərini tez bir zamanda aşkar etməyə, reaksiya verməyə, bərpa etməyə və potensial zərər və pozuntuları minimuma endirməyə imkan verir.

5.8 İşçilərin maarifləndirilməsi: İşçilərin müntəzəm kibertəhlükəsizlik təlimləri və maarifləndirmə proqramları ilə təmin edilməsi təhlükəsizlik yönümlü anlayışlar yaradır, insan səhvləri və daxili təhdidlər riskini azaldır.

Xülasə, kritik təhlükəsizlik nəzarətləri təşkilatlar üçün kibertəhlükəsizlik tədbirlərini prioritetləşdirmək və həyata keçirmək üçün sistematik və riskə əsaslanan yanaşma təmin edir. Bu nəzarətləri qəbul etməklə, təşkilatlar ümumi təhlükəsizlik vəziyyətini əhəmiyyətli dərəcədə yaxşılaşdıra, aktivlərini qoruya və uğurlu kiberhücumların ehtimalını azalda bilər.

FƏSİL 3. TƏŞKİLATLARA YÖNƏLMİŞ FİŞİNQ HÜCUMLARI VƏ SİMULYASİYASININ HƏYATA KEÇİRİLMƏSİ (CAHAN MOTORS MMC TİMSALINDA)

3.1 Təşkilatlara Yönəlmiş Fişinq Hücumları

Təşkilatlara yönəlik fişinq hücumu nədir? - Təşkilatlara qarşı fişinq hücumu bir kiberhücum növüdür ki, bu zaman hücumçular özlərini qanuni qurum kimi təqdim edərək, təşkilatla əlaqəli insanları giriş etimadnamələri, maliyyə məlumatları və ya şəxsi məlumatlar kimi həssas məlumatları təqdim etməyə inandırmağa çalışırlar. Fişinq hücumları e-poçt, telefon zəngləri, mətn mesajları və ya ani mesajlaşma platformaları kimi müxtəlif rabitə kanalları vasitəsilə həyata keçirilə bilər. Bu hücumlar çox vaxt insan psixologiyasından və etibarından istifadə edərək təşkilatları kiber təhlükəyə məruz qoyur.

Fişinq hücumlarının həssas məlumatların oğurlanması, təşkilatın sistemlərinə icazəsiz girişin əldə edilməsi və ya hədəf cihazlarda zərərli proqramların quraşdırılması kimi bir neçə hədəfi ola bilər. Bəzi hallarda, təcavüzkarlar maliyyə mənfəəti güdmək üçün məlumatları şəxsiyyət oğurluğunda və ya digər saxta fəaliyyətlərdə istifadə edə bilərlər. Digər hallarda, təcavüzkarlar korporativ casusluq, biznes əməliyyatlarını pozmaq və ya daha çox kiberhücumlara başlamaq kimi daha strateji niyyətə malik ola bilərlər.

Hər ölçülüdə və sənayedə olan təşkilatlar fişinq hücumlarına qarşı həssasdır. Bununla belə, maliyyə, səhiyyə və hökumət kimi bəzi sənayelər idarə etdikləri həssas məlumatların təbiətinə görə daha cəlbedici hədəflər ola bilər. Bundan əlavə, yüksək ictimai profilə, qlobal mövcudluğa və ya əhəmiyyətli əqli mülkiyyətə malik olan təşkilatlar da fişinq hücumlarına məruz qala bilər.

Təşkilatların bilməli olduğu bir neçə növ fişinq hücumu var:

1. Nizə fişinqi: Bu tip fişinq hücumu təşkilat daxilindəki xüsusi şəxsləri və ya şöbələri hədəf alır. Hədəflərini daha yaxşı araşdıraraq, təcavüzkarlar fişinq e-poçtlarını və ya mesajlarını daha real edir və uğur şanslarını artırırlar.

2. Balina ovu: Balina ovu hücumları təşkilat daxilində yüksək səviyyəli rəhbərləri və ya qərar qəbul edənləri hədəf alır. Təcavüzkarlar hücumun daha

etibarlı görünməsi üçün saxta veb-saytlar yaratmaq və ya saxta e-poçt ünvanlarından istifadə etmək kimi daha mürəkkəb yanaşmadan istifadə edə bilərlər.

3. Biznes E-poçt Fırıldaqçılığı (BEC): Bu tip hücumda təcavüzkar təşkilat daxilində yüksək səviyyəli icraçı və ya digər etibarlı şəxsi təqlid edirək adətən pul köçürmələri və ya həssas məlumatları aşkar etmək üçün işçiləri aldatmaq məqsədi daşıyır.

4. Klon fişinqi: Klon fişinqi təcavüzkarın əvvəllər hədəfə göndərilmiş qanuni e-poçtun demək olar ki, dəqiq surətini çıxarmasını nəzərdə tutur. Təcavüzkar linkləri və ya əlavələri zərərli proqram teminatları ilə əvəz edərək orijinal e-poçtu təqlid edir.

5. Vişinq: Vişinq və ya səsli fişinq telefon vasitəsilə həyata keçirilir. Təcavüzkar bank və ya dövlət agentliyi kimi etibarlı qurumu təqlid edərək, həssas məlumatları şifahi şəkildə əldə etmək üçün hədəfi manipulyasiya etmeyə cəhd edə bilər.

Təşkilatlara yönəlmiş fişinq hücumlarının təsiri:

Fişinq hücumları maliyyə itkilərindən tutmuş reputasiyaya zərər kimi ciddi nəticələr verə bilər. Uğurlu fişinq hücumunun təsiri təcavüzkarın məqsədləri, təşkilatın hazırlığı və pozulan məlumat və ya sistemlərin xarakteri kimi amillərdən asılı olaraq dəyişə bilər. Təşkilatlara yönəlmiş fişinq hücumlarının əsas təsirləri aşagıdakılardır:

1. Maliyyə itkiləri: Fişinq hücumları təşkilat üçün birbaşa maliyyə itkilərinə səbəb ola bilər. Təcavüzkarlar mənimsənilmiş giriş etimadnaməsini və ya maliyyə məlumatlarından istifadə edərək icazəsiz vəsait köçürmə əməliyyatları və ya icazəsiz alışlar edə bilərlər. Bundan əlavə, təşkilatlar hücumun araşdırılması, həlli və aradan qaldırılması ilə bağlı xərclərlə üzləşə bilər.

2. Məlumatların pozulması: Fişinq hücumlarının əsas hədəflərindən biri həssas məlumatlara icazəsiz giriş əldə etməkdir. Hücumçular müştəri məlumatları, işçilərin qeydləri və ya əqli mülkiyyət kimi məxfi məlumatları

mənimsəyərək qara bazarda satmaq və ya fırıldaqçılıq üçün istifadə edə bilərlər. Məlumatların pozulması təsirə məruz qalan təşkilatlar üçün əhəmiyyətli maliyyə və hüquqi məsuliyyətlə nəticələnə bilər.

3. Biznes davamlılığının pozulması: Fişinq hücumları kritik sistemlərə və ya məlumatlara təhlükə yaradaraq təşkilatın biznes davamlılığını poza bilər. Məsələn, təcavüzkarlar oğurlanmış etimadnamələrdən istifadə edərək sistemləri kilidləmək üçün ransomware'lər istifasdə edə bilər. Bu cür hücumlar bizneslərdə vaxt və məhsuldarlığ itkisinə səbəb ola və bərpa üçün əlavə xərclərlə nəticələnə bilər.

4. Reputasiyanın zədələnməsi: Uğurlu fişinq hücumunun təsirlərindən sonra müştərilər, tərəfdaşlar və ictimaiyyət tərtəşkilata qarşı məlumat və təhlükəsizliyi qorumaq qabiliyyətinə olan inamını itirə bilər. Bu inamsızlıq təşkilat reputasiyasının əhəmiyyətli dərəcədə zədələnməsi ilə nəticələnə bilər. Güvən və reputasiyanın bərpası uzun və maliyyətli prosesdir.

5. Rəqabət üstünlüyünün itirilməsi: Fişinq hücumları vasitəsilə əqli mülkiyyət və ya ticarət sirrinin mənimsənilməsi təşkilatın rəqabət üstünlüyünü təhlükə altına sala bilər. Rəqiblər mənimsənilmiş məlumatlardan istifadə edərək, rəqabət aparan məhsul və ya xidmətləri inkişaf etdirə, təşkilatın bazardakı mövqeyini və gəlirliliyini zədələyə bilər.

Xülasə, fişinq hücumları təşkilatlar üçün ciddi və geniş yayılmış mənfi nəticələrə səbəb ola bilər. Fişinqlə bağlı riskləri azaltmaq üçün təşkilatlar güclü təhlükəsizlik tədbirləri, işçilərin təlimi və insidentlərə cavab planlaması kimi addımlar atmalıdır. Potensial nəticələri başa düşmək və fişinq hücumlarından qorunmaq üçün qabaqlayıcı tədbirlər görməklə təşkilatlar bu təhlükələrə məruz qalmalarını və onların potensial zərərlərini əhəmiyyətli dərəcədə azalda bilər.

Təşkilatlara yönəlmiş fişinq hücumlarından qorunma - Fişinq hücumları kibertəhlükəsizlik zəiflikləri və sosial mühəndislik metodlarından istifadə etməklə insan səhvinə əsaslanır. Fişinq hücumlarından qorunmaq üçün işçilərin təlimi, texnoloji müdafiə və davamlı monitorinq kimi çoxşaxəli strategiyanın həyata keçirilməsi vacibdir.

1. İşçilərin təlimi: Fişinq hücumlarından qorunmağın ən təsirli yollarından biri işçiləri fişinqin təhlükələri haqqında maarifləndirmək və şübhəli e-poçtları müəyyən edib xəbər verməkdir. Aşağıdakı mövzuları əhatə edən müntəzəm təlim sessiyaları təklif edilməlidir:
    - Fişinq e-poçtlarının tanınması: İşçilərə e-poçt mənbəyinin düzgünlüyü, yanıltıcı e-poçt məzmunu və səhv yazılmış domen adları kimi fişinq e-poçtlarının əlamətlərini necə aşkar etməyi öyrədilməlidir.
    - Təhlükəsiz bağlantıların müəyyən edilməsi: İşçilərə e-poçt əlavələrində qeyd edilmiş URL'lərin düzgünlüyünün yoxlanılması və yalnız etibarlı mənbələrdən olan bağlantılara klik edilməsi öyrədilməlidir.
    - Şübhəli e-poçtları bildirlməsi: İşçilərin şübhəli fişinq e-poçtlarını İT departamentinə və ya təyin edilmiş təhlükəsizlik qrupuna bildirmələri təhlükəsizlik siyasətlərinə əlavə edilməlidir.
    - İki faktorlu autentifikasiyanı (2FA) tətbiq edilməsi: İşlə bağlı bütün hesablarda əlavə təhlükəsizlik səviyyəsi olan 2FA tətbiq edilməli və işçilər bundan istifadə etməyə təşviq edilməlidir.

2. Texnoloji müdafiə: Fişinq hücumlarından qorumaq üçün lazımi kibertəhlükəsizlik alətlərinə və proqram təminatlarına investisiya edilməlidir:
    - E-poçt filtrasiyası: Məlum fişinq domenlərini bloklamaq və fişinq əlamətləri daşıyan e-poçtları skan etmək üçün e-poçt filtrləmə alətlərindən istifadə edilməlidir.
    - Antivirus proqram təminatları: Fişinq e-poçtlarında tapıla bilən zərərli proqramlardan və digər təhlükəsizlik təhdidlərindən qorunmaq üçün antivirus proqram təminatı yenilənmiş versiyada saxlanılmalıdır.
    - Təhlükəsizlik divarı: Təşkilatınızın şəbəkəsinə girişi məhdudlaşdıraraq icazəsiz girişin qarşısını almaq üçün təhlükəsizlik divarı tətbiq edilməlidir.

- DNS filtrasiyası: Məlum zərərli vebsaytlara girişi bloklamaq və fişinq e-poçtlarında zərərli linklərə klikləməyin qarşısını almaq üçün DNS filtrindən istifadə edilməlidir.
- Təhlükəsiz e-poçt portları: Fişinq e-poçtlarını işçilərin gələn qutularına çatmazdan əvvəl skan etmək və filtrləmək üçün təhlükəsiz e-poçt portlarından istifadə edilməlidir.

3. Davamlı monitorinq: Fişinq hücumlarına məruz qalmamaq üçün təşkilatınızın şəbəkəsini və sistemlərini davamlı olaraq izləyin:

- Loqları müntəzəm olaraq yoxlanılması: Birdən çox uğursuz giriş cəhdləri və ya icazəsiz məlumat ötürülməsi kimi qeyri-adi fəaliyyətlərin qarşısını almaq üçün sistem qeydlərinin yoxlanılması fişinq hücumunu da aşkarlaya bilər.
- Müntəzəm təhlükəsizlik yoxlamalarının aparılması: Potensial zəiflikləri və təkmilləşdirilməli sahələri müəyyən etmək üçün təşkilatın təhlükəsizlik tədbirlərinin müntəzəm yoxlanılması həyata keçirilməlidir.
- Yeniliklərdən xəbərdar olunması: Ən son fişinq hücum tendensiyaları və taktikalarından xəbərdar olunmalı və təşkilatın müdafiə strategiyaları müvafiq olaraq tənzimlənməlidir.

İşçilərin təlimi, texnoloji müdafiə və davamlı monitorinq kombinasiyasını həyata keçirməklə təşkilatlar fişinq hücumlarına məruz qalmalarını əhəmiyyətli dərəcədə azalda bilər.

3.2 Təşkilata Yönəlmiş Fişinq Hücum Simulyasiyası (Cahan Motors MMC Timsalında).

Fişinq hücum simulyasiyası nədir? - Fişinq hücumunun simulyasiyası təşkilatın işçilərinin və infrastrukturunun fişinq hücumlarına qarşı həssaslığını qiymətləndirmək üçün təhlükəsizlik mütəxəssisləri tərəfindən həyata keçirilən nəzarətli testdir. Real fişinq ssenarilərini simulyasiya etməklə, təşkilatlar təhlükəsizliklə bağlı məlumatlandırma təlimlərində zəif cəhətləri müəyyən edə və

bu təhdidlərə qarşı ümumi dayanıqlığı artıra bilərlər.

Fişinq hücum simulyasiyası haqqında (Cahan Motors MMC timsalında) - Simulyasiya Cahan Motors MMC-nin maliyyə departamentinin maliyyəcilərinə yönəlik Cahan Motors MMC-də həyata keçirilmiş fishinq hucumundan ibarətdir. Simulyasiya e-poçt vasitəsi ilə Cahan Motors MMC-nin tədarükcü şirkət əməkdaşı olduğunu iddia edən şəxsin saxta maliyyə məlumatı yeniləmə xəbərdarlığını və maliyyə vəsaitilərinin köçürülmə yolu ilə manimsəmə istəyini əhatə edən fişinq hücumundan ibarətdir.

Simulyasiyanın məqsədi - CM MMC-ə qarşı fişinq hücum simulyasiyasının məqsədi müəssisənin təhlükəsizlik vəziyyətini aşağıdakı yollarla qiymətləndirmək və yaxşılaşdırmaq üçün nəzərdə tutulmuşdur:

1. İşçilərin məlumatlılığının qiymətləndirilməsi: Simulyasiya işçilərin fişinq cəhdlərini tanımaq və hesabat vermək qabiliyyətini ölçməyə kömək edir. İşçilərin bilik boşluqlarının müəyyən edilməsi təşkilata təlim və maarifləndirmə proqramları yaradılmasında kömək edir.
2. Təlimin effektivliyinin ölçülməsi: CM MMC fişinq simulyasiyasının nəticələrindən istifadə edərək təhlükəsizlik şüurunun və təlim proqramlarının effektivliyini ölçməklə kibertəhlükəsizlik investisiyaları haqqında qərarlar qəbul edə bilər.
3. Təhlükəsizlik tədbirlərinin sınaqdan keçirilməsi: Simulyasiya CM MMC-ə e-poçt filtrləri, təhlükəsizlik divarları və müdaxilənin aşkarlanması sistemləri kimi mövcud təhlükəsizlik tədbirlərinin fişinq hücumlarını aşkar etmək və qarşısını almaqda effektiv olub-olmadığını yoxlamağa imkan verir.
4. Zəifliklərin aşkarlanması: CM MMC real həyatda olan fişinq hücumlarını simulyasiya etməklə, kibercinayətkarlar tərəfindən istifadə edilə bilən proseslər, siyasətlər və texnologiyalardakı potensial zəiflikləri müəyyən edə bilər.

Simulyasiyanın həyata keçirilməsi - Simulyasiya Cahan Holding İT departamentinin rəhbəri İlham Əliyevin icazəsi ilə Cahan Motors MMC-nin İT departamentdə mütəxəsis vəzifəsində işləyən Hüseyn Abbasov tərəfindən həyata

keçirilmişdir. Bu fişinq hücum simulyasiyasında e-poçt vasitəsi ilə CM MMC-nin maliyyə departamentinin əməkdaşı olan Günel Rəhimovaya saxta domenli e-poçt ünvanından göndərilən manipulasiya edici e-poçt məktubdan istifadə olunmuşdur.

Manipulasiya edici e-poçt məktubunun məzmunu:

Mövzu: Gözləyən faktura üçün ödəniş məlumatlarını yenilənməsi - Cahan Motors

Hörmətli Günel Rəhimova,

Ümid edirəm ki, gününüz yaxşı keçir. Mən Cheng Zhao, HONGQI Auto Suppliers'in mühasibat meneceri. Biz beş ildən artıqdır ki, Cahan Motors-a keyfiyyətli avtomobil və avtomobil ehtiyat hissələri təqdim edir və tərəfdaşlığımıza böyük əhəmiyyət veririk.

Son dövr üçün ödənişlə bağlı vacib bir məsələni diqqətinizə çatdırmaq istəyirəm ki, maliyyə əməliyyatlarımızdakı bəzi son dəyişikliklərə görə bank hesab məlumatlarımızı yeniləmişik. Düşünürəm ki, hələdə bizim yenilənmiş bank hesab məlumatımız sizin sisteminizə əlavə edilməyib və aşağıda qeyd olunan faktura üçün ödəniş hələ də gözlənilir.

Faktura No: CM-2023-993.

Sifarişlərinizin çatdırılmasında gecikmələrin qarşısını almaq üçün sisteminizdə bank məlumatlarımızı yeniləməyiniz xahiş olunur. Yeni hesab təfərrüatları aşağıdakılardır:

Bankın adı: China Construction Bank (CCB)

Hesabın Adı: HONGQI Auto Suppliers

Hesab nömrəsi: 9976843550

Yönləndirmə nömrəsi: 323959779

Swift Kodu: NBOTUS33

Lütfən, ödənişi CM-2023-993 nömrəli faktura üçün yenilənmiş hesaba mümkün qədər tez icra edin. Ödəniş emal edildikdən sonra ödəniş təfərrüatlarını və əməliyyat tarixini təsdiqləyən bu e-poçta cavab verin.

Hər hansı bir sualınız varsa və ya daha çox məlumata ehtiyacınız varsa, lütfən, +86 (131) 2234 4676 nömrəsi ilə birbaşa mənimlə və ya

support@hongqiautosuppliers.com ünvanında müştəri dəstək komandamızla əlaqə saxlaya bilərsiniz.

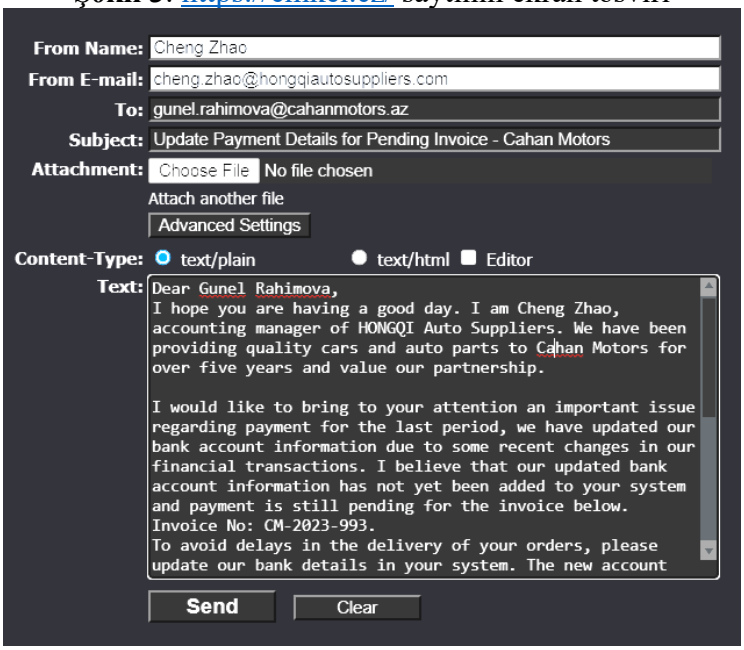
Hörmətlə

Cheng Zhao

1. Manipulasiya edici e-poçt məktubun icrası:

Manipulasiya edici e-poçt məktubunu saxta domenli e-poçt ünvanından göndərmək üçün https://emkei.cz/ saytındakı veb tətbiqdən istifadə olunmuşdur (**Şəkil 3**).

Şəkil 3. https://emkei.cz/ saytının ekran təsviri



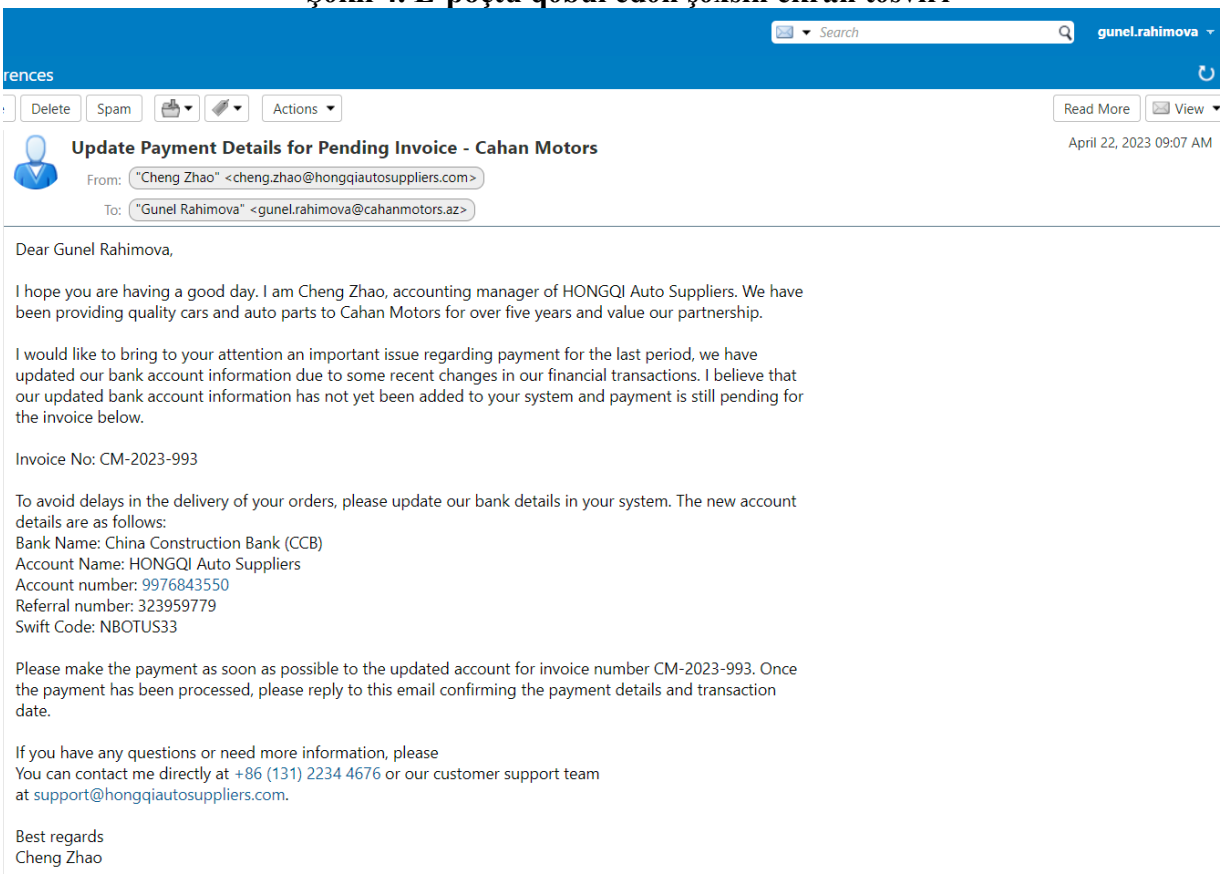
Mənbə: Müəllif tərəfindən tərtib edilmişdir.

Qeyd: E-poçt orjinallığını itirməmək üçün mövzu və məzmun İngilis dilində yazılmışdır.

Şəkil 3-də qeyd olunan veb tətbiqin "From Name" hissəsinə e-poçtu göndərən şəxsin adı (Cheng Zhao), "From E-mail" hissəsinə e-poçtu göndərən şəxsin e-poçt ünvanı (cheng.zhao@hongqiautosuppliers.com), "To" hissəsinə e-poçtu qəbul edən səxsin e-poçt ünvanı (gunel.rahimova@cahanmotors.az), "Subject" hissəsinə manipulasiya edici e-poçt məktubunun mövzusu (Gözləyən faktura üçün ödəniş məlumatlarını yenilənməsi - Cahan Motors) və "Text" hissəsinə isə manipulasiya edici e-poçt məktubunun məzmunu daxil edilir. Məlumatlar daxil edildikdən sonra e-poçt məktubunu göndərmək üçün "Send" düyməsi sıxılır. E-

poçt məktubu göndərildikdən sonra qarşı tərəfə aşağıdakı şəkil 4.-də göstərilən e-poçt məktubu çatır (**Şəkil 4**).

Şəkil 4. E-poçtu qəbul edən şəxsin ekran təsviri



Mənbə: Müəllif tərəfindən tərtib edilmişdir.

Fişinq hücum simulyasiyasının nəticəsi - MMC-nin maliyyə departament rəhbərinin təsdiqi olmadan məktubu alan şəxs sistemdə maliyyə məlumatlarını yeniləyə bilməz. Buna görə də əməkdaş təsdiq üçün məktubu maliyyə departament rəhbərinə yönləndirmişdir. Məktubu alan maliyyə departament rəhbəri HONGQI Auto Suppliers'in mühasibat meneceri olduğunu idda edən Cheng Zhao adlı şəxsi tanımadığından yönləndirilmiş məktubu təsdiqləməmişdir. Maliyyə departament rəhbəri Cheng Zhao adlı şəxsin şəxsiyyətini və tutduğu vezifəni dəqiqləşdirmək üçün HONGQI Auto Suppliers maliyyə deartament rəhberi ilə birbaşa əlaqə saxlamış və eyni zamanda məktubun qaynağının araşdırılması üçün İT departamentinə yönləndirmişdir. Göndərilən e-poçt məktubu araşdırıldıqdan sonra bu məktubun fişinq hücum cəhdi olduğu müəyyən edilmişdir.

Nəticə olaraq, fişinq hücum simulyasiyası CM MMC-ə öz kibertəhlükəsizlik müdafiələrini fəal şəkildə qiymətləndirməyə, uğurlu fişinq hücumların ehtimalını

azaltmağa və bu hücumların reputasiyaya potensial təsirini minimuma endirməyə imkan vermişdir.

NƏTİCƏ VƏ TƏKLİFLƏR

Günümüzdə informasiya texnologiyalarının fasiləsiz inkşafı nəticəsində, yeni kiber təhlükələr ortaya çıxır. Buna görə də təşkilatların təhlükəsizlik tədbirlərinə proaktiv və adaptiv yanaşmanı davamlı etmələri zəruridir.

Kibertəhlükəsizlikdə insan amili mühüm rol oynayır. İşçilərin təlimi və maarifləndirilməsi kiber insidentlərin qarşısının alınmasında həyati əhəmiyyət kəsb edir. Effektiv kiber risklərin idarə edilməsi şirkətin reputasiyasına, əməliyyatlarına və gəlirliliyinə birbaşa təsir etdiyi üçün ümumi biznes strategiyası və risklərin idarə edilməsi çərçivəsinə inteqrasiya edilməlidir. Standartlara və qaydalara uyğunluq daha yaxşı kibertəhlükəsizlik təcrübələrini təşviq edə və təşkilatın ümumi təhlükəsizlik vəziyyətinin yaxşılaşdırılmasına töhfə verə bilər.

Süni intellekt və maşın öyrənməsi kimi qabaqcıl təhlükəsizlik texnologiyalarına sərmayə qoymaq təşkilatlara qabaqcadan aşkarlama və reaksiya imkanlarını təmin etməklə yaranan təhlükələri öncədən görməyə kömək edə bilər.

Bu nəticələr və tövsiyələr kibertəhlükəsizlik və risklərin idarə edilməsi sahəsində ümumi tendensiyalara və ən yaxşı təcrübələrə əsaslanır və kibertəhlükəsizliklərə qarşı müdafiəsini gücləndirmək istəyən təşkilatların geniş spektri üçün tətbiq oluna bilər.

İXTİSARLAR

CIA - Confidentiality, İntegrity and Availability (Məxfilik, Tamlıq və Əlçatanlıq)

CIS - Center for Internet Security (Mərkəzi İnternet Təhlükəsizliyi)

CSC - Critical Security Controls (Kritik Təhlükəsizlik Nəzarətləri)

DoS - Denial of Service (Xidmətdən İmtina)

DDoS - Distributed Denial of Service (Paylanmış Xidmətdən İmtina)

DNS - Domain Name System (Domen adı sistemi)

IDS - Intrusion Detection System (Müdaxilənin Aşkarlanması Sistemi)

IP - Internet Protocol (İnternet Protokolu)

IPS - Intrusion Prevention System (Müdaxilənin Qarşısının alınması Sistemi)

ISO - International Organization for Standardization (Beynəlxalq Standartlaşdırma Təşkilatı)

NIST - National Institute of Standards and Technology (Milli Standartlar və Texnologiya İnstitutu)

PCI DSS - Payment Card Industry Data Security Standard (Ödəniş Kart Sənayesi Məlumat Təhlükəsizliyi Standartı)

SIEM - Security İnformation and Event Managment (Təhlükəsizlik Məlumatı və Hadisələrin İdarə Edilməsi)

SYN - Synchronization (Sinxronizasiya)

İSTİFADƏ EDİLMİŞ ƏDƏBİYYAT SİYAHISI

Türk dilində

1. Alper Başaran (2019). “Siber Kıyamet” Ankara, “Arion Yayınevi”, s. 55-61.
2. Alper Başaran (2021). “Siber Savaş Cephesinden Notlar” İstanbul, “Arion Yayınevi”, s.29-65.
3. Erdal Özkaya, Raif Sarıca, Şükra Durmaz (2019). “Siber Güvenlik” Ankara, “Buzdağı Yayınevi”, s.155-201.
4. Mustafa Altınkaynak (2020). “Uygulamalı Siber Güvenlik ve Haching”. Abaküs, s.10-38.
5. Ömer Çıtak (2018). “Ethical Haching” İstanbul. ”Abaküs”, s.120-152.

İngilis dilində

1. Kevin Mitnick (2011). "Ghost in the Wires: My Adventures as the World's Most Wanted Hacker" Boston, "Little, Brown and Company", s.57-65.
2. David Kennedy, Jim O'Gorman, Devon Kearns, (2011). "Metasploit: The Penetration Tester's Guide" California, "No Starch Press", s.48-52.
3. Kevin Mitnick (2017). "The Art of Invisibility: The World's Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data" Boston, "Little, Brown and Company", s.87-94.
4. Patrick Engebretson (2013). "The Basics of Hacking and Penetration Testing" Amsterdam, "Syngress", s.44-59.
5. Jon Erickson (2008). "Hacking: The Art of Exploitation" California, "No Starch Press", s.83-98.
6. Christopher Hadnagy (2018). "Social Engineering: The Science of Human Hacking" New Jersey, "Wiley", s.143-160.
7. Chris McNab (2016). "Network Security Assessment: Know Your Network" California, "O'Reilly Media", s.112-127.
8. Chris Sanders and Jason Smith (2013). "Applied Network Security Monitoring: Collection, Detection, and Analysis" Amsterdam, "Syngress", s.152-161.

Dolayı istinadların siyahısı

1. Cybersecurity and Infrastructure Security Agency (CISA) - https://www.cisa.gov/cybersecurity
2. National Institute of Standards and Technology (NIST) - https://www.nist.gov/topics/cybersecurity
3. Information Systems Security Association (ISSA) -
4. International Association of Computer Science and Information Technology (IACSIT) - https://www.iacsit.org/
5. Center for Internet Security (CIS) - https://www.cisecurity.org/
6. Information Security Forum (ISF) - https://www.securityforum.org/
7. Cloud Security Alliance (CSA) - https://cloudsecurityalliance.org/
8. Open Web Application Security Project (OWASP) - https://owasp.org/
9. SANS Institute - https://www.sans.org/
10. Security Industry Association (SIA) - https://www.securityindustry.org/
11. Dark Reading - https://www.darkreading.com/
12. Threatpost - https://threatpost.com/
13. KrebsOnSecurity - https://krebsonsecurity.com/
14. ZDNet Security - https://www.zdnet.com/topic/security/
15. SC Magazine - https://www.scmagazine.com/

İSTİFADƏ OLUNMUŞ ŞƏKİLLƏRİN SİYAHISI