AZƏRBAYCAN RESPUBLİKASI TƏHSİL NAZIRLİYİ

AZƏRBAYCAN DÖVLƏT İQTİSAD UNİVERSİTETİ

«MAGİSTRATURA MƏRKƏZİ »

AMİN ŞIXƏLİZADƏ

MÖVZU: «**İnformasiya təhlükəsizliyinin müasir problemləri və həlli metodlarının qiymətləndirilməsi**»

MAGİSTR DİSSERTASİYASI

İxtisasın şifri və adı: 060632 - "İnformasiya texnologiyaları və sistemləri mühəndisliyi"

İxtisaslaşmanın adı: "İnformasiyanın mühafizəsi və təhlükəsizliyi"

Elmi rəhbər: **f.r.e.n., dos.Abdullayev A.X.**

Magistr proqramının rəhbəri: **f.r.e.n., dos. Əliyeva T.Ə.**

Kafedra müdiri: **tex.e.d., akad. Abbasov Ə.M.**

BAKI-2020

MÜNDƏRİCAT

GİRİŞ

Mövzunun aktuallığı. Müasir dövrdə məlumat ən vacib təşkilat aktivlərindən biridir. Bir təşkilat üçün məlumat dəyərlidir və müvafiq qaydada qorunmalıdır.Təşkilatdakı məlumatların və əməliyyat prosedurlarının bütövlüyünü, məxfiliyini təmin etmək üçün sistemləri, əməliyyatları və daxili nəzarəti birləşdirməkdir. İnformasiya təhlükəsizliyi tarixi kompüter təhlükəsizliyi tarixindən başlayır.İnformasiya texnalogiyaların çox sürətlə inkşafı daha çox məlumatların daşınmasına zərurət yaradır və daşınan məlumatların məxviliynin, gizliliyinin təmin eidlməsi prosesi çətinləşdirir.Məlumat çox vacib amildir buna misal olaraq kriptavalyuta və kart hesablarını göstərmək olar.Bu məlumatın əldə edilməsi üçün çox cəhdlər göstərilir,məlumatların gizliyininin pozulması üçün çoxlu müasir üsullar inkşaf etməkdədir buna qarşılıq olaraq məlumatların şifrələnməsi üçün bir çox metodlar təklif edilmişdir. Məlumat hər hansı bir təşkilatın ən vacib maddi aktivlərindən biridir və digər aktivlər kimi rəhbərliyin də onu lazımi qaydada qoruması məsuliyyət daşıyır. Itkin məlumatlar haqqında gələn xəbərlər, çox sayda həssas məlumatlar və müştəri məlumatlarını daşıyan informasiya texnologiyasına tamamilə etibar etdikləri üçün qurumları qorxudur. Kompüterlərin istifadəsi kompüter mərkəzləri ilə məhdudlaşdıqda və fiziki hesablama infrastrukturu üçün kompüter stendlərinin təhlükəsizliyi 1980-ci ilə aiddir. Bununla birlikdə, internetin açıqlığı daxili məlumat saxlama ilə prosesləri sadələşdirdi, eyni zamanda bu, informasiya təhlükəsizliyi baxımından da böyük bir zəiflikdir.İnternet etibarlı bir qrupdan etibarən milyonlarla tez-tez ünsiyyət quran anonim istifadəçi ilə ünsiyyət mübadiləsi ilə inkişaf etmişdir. İnternetdə olanlar məlumat çatışmazlığından narahat olmurlar, lakin rast gəldikləri həddən artıq lazımsız məlumatları idarə etməkdən daha çox narahatdırlar. Morris Worm 1988-ci ildə hazırlanmış və sistemlərin 10% -ni yoluxduran ilk internet qurd idi.O vaxtdan bəri bu hadisələr getdikcə daha mürəkkəb və bahalı olmağa başladı. Bununla mübarizə aparmaq üçün informasiya təhlükəsizliyi mövzusunda məlumatlılıq artdı və bir çox təşkilatlar məlumatlarının prioritetləşdirilməsi üçün səy göstərdilər.İnfosec adı ilə də bilinən informasiya

təhlükəsizliyi, rəqəmsal və rəqəmsal olmayan cihazlara yönəlmiş təhdidləri aşkar etmək, sənədləşdirmək, qarşısını almaq və onlara qarşı mübarizə aparmaq üçün strategiyalar, alətlər və siyasətlərin formalaşdırılması prosesidir. İnformasiya təhlükəsizliyi bilavasitə kontekstdə məlumatın ötürülməsindən, işlənməsindən və ya saxlanmasından asılı olmayaraq qorumaq üçün yaxşı müəyyən edilmiş təhlükəsizlik proseslərini qurmaqdır.

Tətqiqatın məqsədi və vəzifəsi. Informasiyanın təhlükəsizliyinin inkşaf etdirilməsinə təsir edən amillər, informasiya təhlükəsizliyinin qarşısında duran əsas problemlərin müəyyənləşdirilməsi və onlara qarşı tədbirlər toplusunu təşkil edir.

Tətqiqatın predmeti və obyekti. Tətqiqatın predimeti informasya təhlükəsizliyinə qarşı duran real təhlükələrin analizi və müasir həll metodlarının formalaşmasının əsasları.

Tətqiqatın obyekti informasiyadır.Müasir dövrdə ən vacib məsələ informasiyanın saxlanması, emal olunması və daşınması zamanı informasiya təhlükəsizliynin təminatıdır.

Tətqiqatın nəzəri əsasları. Nəzəri əsasları kimi informasiya təhlükəsizliyi inkşafı və kiber hücumlar qarşı tədbirlərin görülməsi üçün Azərbaycan və dünya ailmlərin araşdırmaları, məqalələri istifadə edilmişdir.

Tətqiqatın metodoloji bazası.İnformasiya təhlükələri və təhlükələrə qarşı görülmüş tədbirlərin, vasitələrin tarixi inkşafı və informasiya təhlükəsizlinin təyin edən vasitələrin işləmə mexanizmin analizi,təhlükəzilik probelmin tətqiqində istifadə edilən kriptoqrafik metodların analizi, sintezi,zamanla yeniləri ilə əvəzlənməsi üçün tələblərin zərurəti istifadə edilməklə ümumiləşdirilmiş, həmçinin xarici ölkə mühəndislərin, alimlərin elmi əsərləri və məqalələri təşkil edir.

Tədqiqatın elmi yeniliyi və praktiki əhəmiyyəti. Işin elmi yeniliyi informasiya təhlükəsizliynin zəruri əsasları, təhlükəsizlik qarşısında duran müasir problemlər və həll yollar,yeni kriptoqrafik metodaların tətqiq edilməsindən ibarətdir. Dünya üzrə informasiyanın əladə edilməsi və ya pozulması üçün cəhdlərin növləri sadalanmışdır, onlara qarşı vasitələr və tədbirlər toplusu qeyd edilmişdir.

Praktiki əhəmiyyət olaraq ənənəvi təhlükəsizlik metod və tədbirblərin yeni növ kiber hücumlardan müdafiə olunmaq üçün daha optimal şifrələmə alqoritmlərdən istifadə edərək elektron əməliyyatların daha təhlükəsiz, müdaxiləsiz icrasına təminat verir.İnformasiya təhlükəsizliyi çox vacib məqam olduğundan texniki tədbirlərlə yanaşı mütəmadı şəkildə işçi heyyətinə yeni müdafiə tədbirlərin aşılanmasını ifadə edir.

İnformasiya mənbəyi. müxtəlif beynəlxalq təşkilatların dövrü nəşirləri, Azərbaycan Respublikası Rabitə və Yüksək Texnologiyaları Naziliyinin məlumatları, Beynəlxalq Telekommunikasiya Birliyinin saytından, müxtəlif xarici ədəbiyyatlar və məqalələrdən ibarətdir.

Tətqiqat işin strukturu. Aparılmış tətqiqat işi giriş, üç fəsil, nəticə və təkliflər eyni zamanda ədəbiyyat siyahısından ibarətdir. Girişdə işin aktuallığı, tətqiqatın istiqamətləri göstərilir və tədqiq ediləcək problemlər müəyyənləşdirilir.

Magistr dissertasiya işinin birinci fəsili, informasiya təhlükəsizliyi sistemi, informasiya təhlükəsizliyi prinsipləri,informasiya təhlükəsizliyi tədbirləri, İnformasiya təhlükəsizliyi vasitələri, identifikasiya, giriş nəzarəti araşdırılmışdır

Dissertasiya işinin ikinci fəsli, internet şəbəkəsində informasiya təhlükəsizliyi, şəbəkə təhlükəsizliyi vəziyyətinin məlumatlılığı və müdaxilənin aşkarlanması, sosial mühəndislik hücumları, təchizat zəncirinə hücumlar, iot və infrastruktur hücumları, şəxsiyyət və mobil doğrulama, sıfır gün təhdidlərinin və polimorf hücumların artması, kiber həhlükəsizlik problemləri araşdırır

Dissertasiya işinin üçüncü fəsli, internet şəbəkə təhlükəsizliyinin üstünlükləri, internet şəbəkə təhlükəsizliyi alətləri və texnikaları, internet şəbəkəsində kiberhücuma qarşı effektiv mübarizə aparma üsualları, internet şəbəkəsində informasiyanın qorunması üçün əsas kriptoqrafik metodlar, internet şəbəkəsində ssl sertifikatı vasitəsilə məlumatın təhlükəsiz ötürülməsini araşdırır.

I FƏSİL. İnformasiya təhlükəsizliyi konsepsiyasi.

1.1. İnformasiya təhlükəsizliyi sistemi.

İnformasiya sistemlərinin təhlükəsizliyi, INFOSEC olaraq da bilinir, kompüterlər, şəbəkələr və istifadəçilərin qorunmasına yönəldilən informasiya texnologiyaları (İT) sahəsindəki geniş bir mövzudur. Demək olar ki, bütün müasir şirkətlər, eləcə də bir çox ailə və fiziki şəxslər, rifahları üçün rəqəmsal risklərlə bağlı narahatlıqlarını əsaslandırdılar. Bu təhdidlər hər cür formada və ölçüdə ola bilər, misal olaraq verilənlər bazasında gizli məlumatların oğurlanmasını, zərərli proqramların bir maşına quraşdırılması və qəsdən xidmətin pozulmasını qeyd etmək olar.

INFOSEC-in ən çox tanınan elementlərindən üçü məxfilik, bütövlük və mövcudluqdur. Bu, İT təhlükəsizlik peşəsinin əsas məqsədi, məlumatın bir sistem istifadəçilərinə başqa bir tərəf tərəfindən pozulmadan və oğurlanmadan əldə edilməsini təmin etməkdir.

Son zamanlarda böyük şirkətlərdə və digər qurumlarda baş verən məlumat pozuntuları informasiya sistemlərinin təhlükəsizliyi ictimai diqqətə çatdırılsa da, İnformasiya sistemlərinin təhlükəsizliyi on illərlə ardıcıl olaraq artan bir riskdir. Müştəriləri haqqında fərdi məlumatları, xüsusən şəxsiyyət və ya ödəmə ilə bağlı məlumatları saxlayan hər hansı bir iş, hack səbəb olduğu potensial ictimaiyyətlə əlaqələr kabusundan narahatdır. Şirkətləri, şəbəkələri zərərli proqramla zədələnmiş olduqda bir çox potensial gəlir və əmlakı da itirə bilər. Rəqəmsal təhdidlər davamlı təkamül və inkişaf vəziyyətindədir, bu səbəbdən xüsusi təhlükəsizlik mütəxəssislərinə müraciətlər artmaqdadır.

İnternet və inteqrasiya edilmiş, interaktiv sistemlərin bu çağında informasiya təhlükəsizliyi əsas məsələdir. Bir sıra iri korporasiyalar çox sayda insanı potensial şəxsiyyət oğurluğuna məruz qoyan təhlükəsizlik uğursuzluqlarına uğramışlar. Çevik müəssisə ardıcıl olmalıdır informasiya təhlükəsizliyi sistemi və bu meneceri rol əsaslı dostuq təmin etməlidir. Ardıcıl bir memarlıq mürəkkəbliyi azaldır və buna görə də qoruma üçün potensial nəzarəti təmin edir. Bu səlahiyyətli, təşkilatlararası giriş

asanlığını təmin edir və daxilolmaları və cəhd edilən pozuntuları aşkar etmək və yeni təhlükələrə cavab vermək üçün səmərəli və effektiv texniki xidmət və monitorinqi dəstəkləyir.Ardıcıl bir arxitekturada, nəzarət edilən bir hərəkət tələbini müvafiq bir səlahiyyət səviyyəsinə qaldırmaqla xüsusi halların avtorizasiya edilməsi prosesləri, məsələn, səlahiyyətli həddi aşan müştəri sifarişi və ya xərc tələbi və ya məhdudlaşdırılan bir fəaliyyət göstərilməlidir.Rol əsaslı giriş nəzarəti menecerlərə bir şəxsə uyğun icazəni tez və asanlıqla təmin etməyə və ya artıq uyğun olmayan avtorizasiyaya xitam verməyə imkan verir. Avtorizasiya giriş icazəsi vericisini dəqiq müəyyənləşdirməlidir.Rol əsaslı avtorizasiya dəstəyi prosesləri idarəetmə nəzarəti və şəxslərə verilən giriş icazəsi barədə məlumatlılığı artıra bilər və işçilər tapşırıqları dəyişdirdikdə və ya şirkətdən ayrıldıqda icazələri daha etibarlı şəkildə ləğv edə bilər.

1.2. İnformasiya təhlükəsizliyi prinsipləri

İnformasiya təhlükəsizliyinin əsas komponentləri ən çox Mərkəzi Kəşfiyyat İdarəsinin üçlüyü ilə əlaqələndirilir: məxfilik, bütövlük və mövcudluq.

1.1 Mərkəzi Kəşfiyyat İdarəsinin üçlüyü

Availability - Mövcudluq

Integrity - Bütövlük

Confidentially - Məxfilik

- **Məxfilik**, bəlkə də informasiya təhlükəsizliyi barədə düşünəndə dərhal ağla gələn üçlüyün əsas elementidir. Məlumat əldə etmək üçün səlahiyyətli olanlar bunu edə bildikdə məxfidir; məxfiliyi təmin etmək üçün məlumatları əldə etməyə çalışanları müəyyənləşdirmək və icazəsi olmayanların cəhdlərini bloklamaq lazımdır. Şifrələr, şifrələmə, identifikasiya və nüfuz hücumlarına qarşı qorunma məxfiliyi təmin etmək üçün hazırlanmış bütün üsullardır.
- **Bütövlük,** məlumatların düzgün vəziyyətdə saxlanılması və ya təsadüfən və ya zərərli yolla dəyişdirilməsinin qarşısını almaq deməkdir. Məxfililiyi təmin edən bir çox üsul da məlumatların bütövlüyünü qoruyacaqdır - axı, bir haker daxil ola bilmədiyi məlumatları dəyişə bilməz, lakin bütövlüyün müdafiəsini təmin edən digər vasitələr də var: çeklər məlumatları yoxlamağa kömək edə bilər

məsələn bütövlüyü, və versiyaya nəzarət proqramı və tez-tez yedəkləmə, lazım olduqda məlumatların düzgün bir vəziyyətə gətirilməsinə kömək edə bilər. Bütövlük rədd etmə anlayışını da əhatə edir: məlumatlarınızın bütövlüyünü, xüsusən də hüquqi müstəvidə qoruduğunuzu *sübut* edə bilməlisiniz.

- **Mövcudluq** məxfiliyin güzgü şəklidir: məlumatlarınızın icazəsiz istifadəçilər tərəfindən əldə olunmadığından əmin olmalısınız, eyni zamanda müvafiq icazəsi olanlar tərəfindən əldə *edilə* biləcəyinə əmin olmalısınız. Məlumatların mövcudluğunu təmin etmək, şəbəkə və hesablama mənbələrini gözlədiyiniz məlumatların əldə olunması həcminə uyğunlaşdırmaq və fəlakətlərin qarşısını almaq üçün yaxşı bir izləmə siyasətini həyata keçirmək deməkdir.

İdeal bir dünyada məlumatlarınız həmişə məxfi, düzgün vəziyyətdə və mövcud olmalıdır praktikada, əlbəttə ki, tez-tez hansı informasiya təhlükəsizliyi prinsiplərinin vurğulanacağı və məlumatlarınızı qiymətləndirməyi tələb edən seçimlər etməlisiniz. Məsələn, həssas tibbi məlumatları saxlayırsınızsa, məxfiliyə diqqət yetirirsiniz, halbuki maliyyə qurumu heç kimin bank hesabına yanlış kredit verilməməsini təmin etmək üçün məlumatların bütövlüyünü vurğulaya bilər [5].

İnformasiya təhlükəsizliyi siyasəti, müəssisənin özünün xüsusi ehtiyaclarına və sorğularına əsasən hansı məlumatların qorunması və hansı yollarla qorunması lazım olduğunu müəyyənləşdirən sənəddir. Bu siyasətlər kibertəhlükəsizliyin təmin edilməsi vasitələrinin alınması ilə əlaqədar təşkilatın qərarlarını istiqamətləndirir, həmçinin işçilərin davranışlarını və məsuliyyətlərini müəyyən edir.

Digər şeylər arasında şirkətinizin informasiya təhlükəsizliyi siyasətinə aşağıdakılar aid edilməlidir:

- Infosec proqramının məqsədini və ümumi hədəflərinizi izah edən bir şərh,
- Birgə anlaşmanı təmin etmək üçün sənəddə istifadə olunan əsas terminlərin tərifləri
- Kimin hansı məlumatları əldə etdiyini və hüquqlarını necə qura biləcəyini müəyyənləşdirən bir giriş nəzarəti siyasəti
- Bir parol siyasəti

- A data dəstək və əməliyyatlar data ehtiyacı olanlara həmişə mövcud olmasını təmin etmək üçün planlaşdırırıq
- Məlumatların qorunmasına gəldikdə işçilərin rolu və məsuliyyəti , o cümlədən məlumat təhlükəsizliyinə cavabdeh olanlar

Yadda saxlamağınız vacib olan bir şey, bir çox şirkətin bəzi kompüter xidmətlərini yayımladığı və ya məlumatları buludda saxladığı bir dünyada, təhlükəsizlik siyasətiniz yalnız sahib olduğunuz aktivlərdən daha çoxunu əhatə etməlidir. Amazon Web Servis (AWS) instansiyalarında saxlanan məlumatları şəxsən müəyyənləşdirməkdən həssas korporativ məlumat əldə etmək üçün identifikasiya etməyi tələb edən üçüncü tərəf podratçılarına qədər hər şeylə necə münasibət quracağınızı bilməlisiniz.

1.3. İnformasiya təhlükəsizliyi tədbirləri

Kibertəhlükəsizliyə aid bütün texniki tədbirlər müəyyən dərəcədə informasiya təhlükəsizliyinə toxunur, ancaq böyük ölçüdə infosec tədbirləri haqqında düşünməyə dəyər. Məlumat təhlükəsizliyi hər kiçik biznes sahibi üçün vacib bir sahə olmalıdır.Faktiki olaraq saxladığınız bütün vacib məlumatları - maliyyə qeydlərindən tutmuş müştərilərin şəxsi məlumatlarına nəzər yetirdikdə - bir pozuntunun niyə işinizə ciddi zərər verə biləcəyini görmək çətin deyil.

- **Texniki tədbirlərə** məlumatları qoruyan aparat və proqram təminatı daxildir (şifrələmədən güvənlik divarlarına (firewall) qədər hər şey).Firewall zəruridir, çünki şəbəkə trafikinizi - daxil olan və çıxanları qorumağa kömək edir. Hakerlərin müəyyən veb saytları bloklamaqla şəbəkənizə hücumunu dayandıra bilər. Ayrıca şirkətinizin şəbəkəsindən xüsusi məlumatların və məxfi e-poçtların göndərilməsinin məhdudlaşdırılması üçün proqramlaşdırıla bilər.
- **Təşkilati tədbirlərə** hər şöbədə bəzi işçilərin vəzifələrinin infosec hissəsi ilə yanaşı, informasiya təhlükəsizliyinə həsr olunmuş daxili bölmənin yaradılması da daxildir.

- **İnsan tədbirləri** istifadəçilərə düzgün infosek təcrübələri ilə bağlı məlumatlandırma təhsili vermək daxildir
- **Fiziki tədbirlərə** ofis yerlərinə və xüsusən məlumat mərkəzlərinə daxil olmağa nəzarət daxildir
- **Etibarlı Antivirus Proqramı quraşdırın.** Yaxşı, etibarlı bir antivirus proqramı hər hansı bir kiber təhlükəsizlik sisteminin əsas zəruridir. Bundan əlavə, anti-malware proqram təminatı da vacibdir. Təhlükəsizlik şəbəkənizdən keçərlərsə istenmeyen hücumları müdafiə etmək üçün son sərhəd kimi çalışırlar.Virus və zərərli proqram, reklam proqramları və casus proqramları aşkar etmək və aradan qaldırmaqla işləyirlər. Zərərli yükləmələri və e-poçtları da tarayır və süzürlər [6].
- **Kompleks şifrələrdən istifadə edin.** Demək olar ki, hər bir kompüter və İnternet əsaslı tətbiqetmə ona daxil olmaq üçün bir açar tələb edir. Təhlükəsizlik suallarına cavablar və ya şifrələr olsun, hakerlərin onları sındırmasını çətinləşdirmək üçün mürəkkəb olanlar yaratdığınızdan əmin olun.Təhlükəsizlik suallarına cavab almaq üçün pulsuz onlayn tərcümə vasitələrindən istifadə edərək onları başqa dilə tərcümə etməyi düşünün. Bu, onları proqnozlaşdırılmayan və deşifr etməkdə çətinlik çəkə bilər və sosial mühəndisliyə daha az həssas ola bilər.Şifrələrinizdən əvvəl vvə ya sonra boş yerdən istifadə etmək də hakerin atılması üçün yaxşı bir fikirdir. Bu yolla, şifrənizi yazsanız da, təhlükəsiz olacaq, yalnız ön və sonda boşluğa ehtiyac olduğunu biləcəksiniz. Üst və alt hərflərin birləşməsindən istifadə, alfasayısal simvol və işarələrdən istifadə etməkdən əlavə kömək edir.
- **Şifrələmə proqramını quraşdırın.** Gündəlik kredit kartlarına, bank hesablarına və sosial təminat nömrələrinə aid məlumatlarla əlaqəli olsanız, şifrələmə proqramının olmasının mənası var . Şifrələmə kompüterdəki məlumatları oxunmayan kodlara dəyişdirərək məlumatları təhlükəsiz edir.Bu şəkildə məlumatlarınız oğurlanarsa belə, haker üçün faydasız olardı, çünki məlumatların şifrəsini açmaq və məlumatları deşifrə etmək açarları olmurdu.

- **Şübhəli elektron poçtlara məhəl qoyma.** Şübhəli görünüşlü e-poçtları, məlum bir göndərəndən olduğu kimi görünsə də, heç vaxt açmamağı və cavab verməməyi vərdiş halına gətirin. E-poçtu açsan da, şübhəli bağlantıları vurma və qoşma yükləməyin. Bunu etmək, "phishing aldatmacaları" daxil olmaqla, onlayn maliyyə və şəxsiyyət oğurluğunun qurbanına çevrilə bilər.Fişinq e-poçtları, bank və ya işlə məşğul ola biləcəyiniz biri kimi etibarlı göndəricilərdən gəlir. Bunun sayəsində haker bank hesabı məlumatları və kredit kartı nömrələri kimi şəxsi və maliyyə məlumatlarınızı əldə etməyə çalışır.Əlavə təhlükəsizlik üçün, hər 60 - 90 gündə bir e-poçt parolunuzu dəyişdirdiyinizdən əmin olun. Bundan əlavə, fərqli e-poçt hesabları üçün eyni şifrəni istifadə etməkdən çəkinin və parolunuzu heç vaxt yazmayın.
- **Daimi ehtiyat nüsxəsini çəkin.** Hər həftə ya məlumatlarınızı xarici bir sabit diskə və ya buludunuza özünüzün nüsxəsini çıxarın və ya məlumatlarınızın etibarlı şəkildə saxlanmasını təmin etmək üçün avtomatlaşdırılmış ehtiyat nüsxələrini təyin edin.Bu yolla, sistemləriniz çöksə belə, məlumatlarınızı hələ də sizinlə təhlükəsiz saxlayırsınız.
- **Təhlükəsiz noutbuklar və smartfonlar.** Ətraflarında gəzdirmək asan olduğuna görə, noutbuk və smartfonlar bir çox dəyərli məlumatların içində bir cəhənnəm saxlayır və bu da itirilmə və ya oğurlanmaq riski daha yüksəkdir. Hər iki cihazın qorunması şifrələmə, parol qorunması və "uzaqdan silmək" seçimini təmin edir.
- **İşçilərə Kiber Təhlükəsizlik Siyasətlərini izah edin.** Ofis sistemləri və İnternetdən istifadə nöqtələrini və dəyərlərini əks etdirən yazılı bir kiber təhlükəsizlik siyasətinə sahib olmaq faydalıdır, lakin kifayət deyil. Bunun təfərrüatlarını işçilərinizə çatdırmağı və başa düşmələrini təmin etməlisiniz ki, təcrübədə tətbiq edə bilsinlər. Bu cür siyasətlərin təsirli olmasının yeganə yolu budur. Məzmunun aktuallığına görə mütəmadi olaraq bu siyasətləri düzəldin.

İnformasiya təhlükəsizliyinin təmin edilməsi üçün həmçinin aşağıdakı tədbirlər görülməlidir.

- Daxili audit
- Daxili texniki test
- İT meneceri, müvafiq hesabat hazırlamaq üçün İT şöbəsinin mənbələrini təmin edir
- Firewall auditləri uyğunluğu yoxlanılır və lazım olduqda icazələr dəyişdirilir
- Giriş hüquqları, davamlı iş ehtiyacı üçün müvafiq işçilər ilə nəzərdən keçirilir. Heç bir əsaslı ehtiyac olmadıqda, hüquqlar dərhal İT şöbəsi tərəfindən silinir
- Hər hansı bir iş stansiyasında araşdırma icazəsiz fəaliyyət göstərirsə, araşdırılmalı və lazımi hallarda intizam tənbehi də daxil olmaqla müvafiq tədbirlər görülməlidir
- Xarici audit
- Xarici texniki sınaq

1.4. İnformasiya Təhlükəsizliyi Vasitələri

Məlumatların məxfiliyini, bütövlüyünü və əlçatanlığını təmin etmək üçün təşkilatlar müxtəlif vasitələrdən birini seçə bilər. Bu vasitələrin hər biri sonrakı hissədə müzakirə ediləcək ümumi məlumat təhlükəsizliyi siyasətinin bir hissəsi kimi istifadə edilə bilər.

İnformasiya təhlükəsizliyini qorumaq üçün ən yaxşı vasitələr

- Şəbəkə Təhlükəsizliyi Monitorinq vasitələri
- Şifrələmə vasitələri
- Veb Zərərlilik Tarama vasitələri
- Şəbəkə Müdafiə Simsiz Alətlər
- Paket Sniffers
- Antivirus Proqramı
- Firewall
- PKI xidmətləri

- İdarə olunan aşkarlama xidmətləri
- Nüfuz testi

İnformasiya Təhlükəsizliyi üçün göstərişlər. Məlumat təhlükəsizliyinizi yaxşılaşdırmaq üçün izləyə biləcəyiniz bəzi ümumi tövsiyələr var. Bəzilərinə baxaq:

- Nə düşünsən də, hakerlər üçün cəlbedici bir hədəfsən. "Mənə olmayacaq" kəlməsi bir daha tətbiq edilmir
- Heç vaxt cihazlarınızı baxımsız buraxmayın. Kompüterinizi, planşetinizi və ya telefonunuzu tərk edərkən heç kim istifadə edə bilməyəcəyi üçün onları kilidləyin
- Yüklədiyiniz şeylərə diqqət yetirin. Yeni bir veb saytdan bir şey yükləməzdən əvvəl onu Google-da axtarmağa və sual verməyə çalışın, bu təhlükəsizdir
- İnternetdən yükləmək barədə danışarkən, e-poçt qoşmalarında vurduğunuz şeylərə diqqət yetirin. Fayl hər hansı bir şəkildə şübhəlidirsə, onu vurmayın. Qoşmanın götürəcəyi veb sayt URL-lərini iki dəfə yoxladığınızdan əmin olun
- Mütəmadi olaraq məlumatlarınızın ehtiyat nüsxəsini çıxarın. Antivirus proqramı quraşdırıb yeniləməyinizə əmin olun
- Həmişə güclü bir şifrə istifadə edin. Bunun üçün bir parol meneceri quraşdıra bilərsiniz
- Flash sürücüyü kompüterinizə qoşarkən diqqətli olun. Hakerlər zərərli proqramları yoluxmuş USB sürücülər vasitəsi ilə yaya bilərlər.

1.5. İdentifikasiya

Birini tanımağın ən yaygın yolu, xarici görünüşləridir, amma kompüter ekranının arxasında və ya ATM-də oturan birini necə müəyyənləşdiririk? Doğrulama üçün vasitələr, məlumatları əldə edən şəxsin həqiqətən özünü təqdim etdiklərini təmin etmək üçün istifadə olunur.

Doğrulama üç və ya bir neçə amil arasında birini tanımaqla həyata keçirilə bilər: bildikləri bir şey, sahib olduqları bir şey və ya olduqları bir şey. Məsələn, bu gün ən çox yayılmış identifikasiya forması istifadəçi identifikatoru və şifrəsidir. Bu

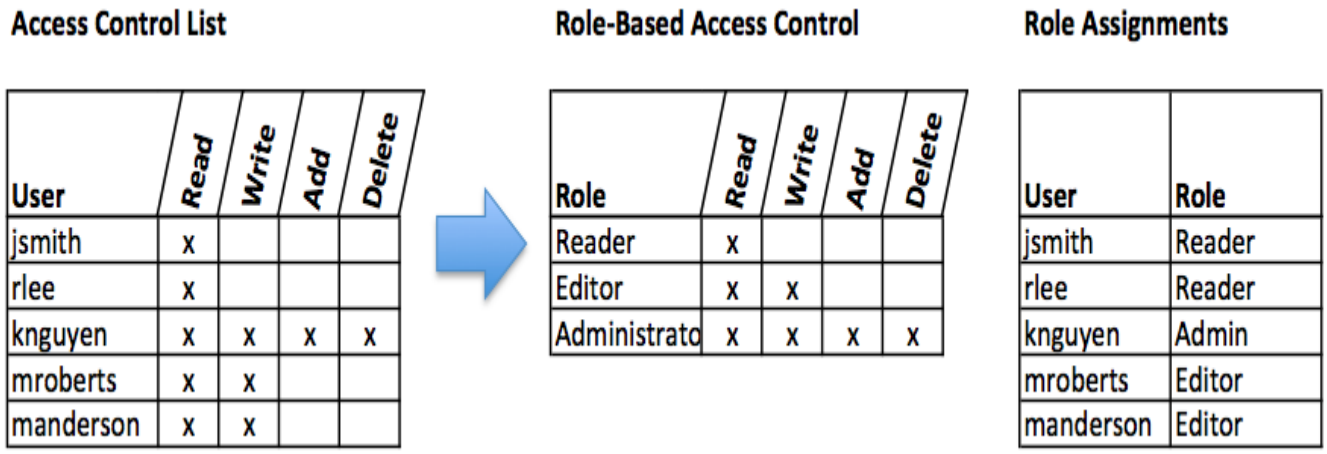
vəziyyətdə identifikasiya istifadəçinin bildiyi bir şeyi (onların şəxsiyyət və şifrələrini) təsdiq etməklə edilir. Lakin bu identifikasiya forması güzəştə getmək asandır (yan çubuğa baxın) və bəzən daha güclü identifikasiya formaları tələb olunur. Birisini yalnız açar və ya kart kimi bir şeylə eyniləşdirmək problemli ola bilər. Bu identifikasiya etiketi itirildikdə və ya oğurlandıqda şəxsiyyət asanlıqla oğurlana bilər. Son amil, bir şey olduğundan, güzəştə getmək çox çətindir. Bu amil istifadəçi göz taraması və ya barmaq izi kimi fiziki bir xüsusiyyətdən istifadə edərək müəyyən edir. Bir istifadəçini eyniləşdirmək üçün daha etibarlı bir yol çox amil identifikasiyası etməkdir. Yuxarıda sadalanan iki və ya daha çox amili birləşdirərək kiminsə səhv məlumat verməsi daha çətin olur. Buna bir nümunə RSA SecurID bir işarəsinin istifadəsi ola bilər. RSA cihazı əlinizdədir və hər altmış saniyədə yeni bir giriş kodu yaradacaqdır. RSA cihazından istifadə edərək bir məlumat mənbəyinə daxil olmaq üçün bildiyiniz bir şeyi, dörd rəqəmli PİN ilə cihazın yaratdığı kodla birləşdirirsiniz. Düzgün kimlik üçün yeganə yol, həm də kod bilmədən edir və RSA cihaz olan.

1.6. Giriş Nəzarəti

Bir istifadəçi təsdiqləndikdən sonra növbəti addım yalnız uyğun informasiya mənbələrinə daxil ola biləcəklərini təmin etməkdir. Bu giriş nəzarətinin tətbiqi ilə həyata keçirilir. Giriş nəzarəti hansı istifadəçilərin məlumatları oxumaq, dəyişdirmək, əlavə etmək və ya silmək hüququna sahib olduqlarını müəyyənləşdirir. Bir neçə fərqli giriş nəzarət modeli mövcuddur. Burada ikisini müzakirə edəcəyik: girişə nəzarət siyahısı (ACL) və rol əsaslı giriş nəzarəti (RBAC) [8].

Bir təşkilatın idarə etmək istədiyi hər bir məlumat mənbəyi üçün müəyyən tədbirlər görmək imkanı olan istifadəçilərin siyahısı yaradıla bilər. Bu girişə nəzarət siyahısı və ya ACL. Hər bir istifadəçi üçün oxumaq, yazmaq, silmək və ya əlavə etmək kimi xüsusi imkanlar təyin olunur. Yalnız bu imkanları olan istifadəçilərə bu funksiyaları yerinə yetirmək üçün icazə verilir. Bir istifadəçi siyahıda deyilsə, informasiya mənbəyinin olduğunu bilmək qabiliyyətinə də sahib deyillər. ACLs anlamaq və saxlamaq üçün sadədir. Ancaq bunların bir neçə çatışmazlığı var. Əsas çatışmazlıq odur ki, hər bir məlumat mənbəyi ayrıca idarə olunur, buna görə bir

təhlükəsizlik administratoru böyük bir məlumat dəstinə bir istifadəçi əlavə etmək və ya çıxarmaq istəsə, bu olduqca çətin olacaq. İstifadəçilərin və mənbələrin sayı artdıqca ACL-lərin saxlanılması çətinləşir. Bu, rola əsaslanan giriş nəzarəti və ya RBAC adlanan giriş nəzarətinin təkmilləşdirilmiş metoduna səbəb oldu. RBAC ilə, müəyyən bir istifadəçiyə bir məlumat qaynağına giriş hüququ vermək əvəzinə, istifadəçilər rollara təyin olunur və daha sonra bu rollara giriş verilir. Bu idarəçilərə istifadəçiləri və rolları ayrıca idarə etməyi asanlaşdırmaq və təhlükəsizliyi artırmaqla idarə etməyə imkan verir.



ACL və RBAC müqayisəsi

1.7. İzləmə

İnformasiya təhlükəsizliyi üçün digər vacib bir vasitə, bütün təşkilat üçün hərtərəfli ehtiyat planıdır. Korporativ serverlərdəki məlumatların təkcə nüsxəsi deyil, təşkilat daxilində istifadə olunan fərdi kompüterlər də yedəklənməlidir. Yaxşı bir ehtiyat plan bir neçə komponentdən ibarət olmalıdır.

- Təşkilati informasiya mənbələri haqqında tam məlumat. Təşkilat əslində hansı məlumatlara malikdir? Harada saxlanılır? Bəzi məlumatlar təşkilatın serverlərində, digər məlumatlar istifadəçilərin sabit disklərində, bəziləri buludda, bəziləri isə üçüncü tərəf saytlarında saxlanıla bilər. Bir təşkilat, yedeklenmesi lazım olan bütün məlumatların tam bir inventarını aparmalı və bunun ən yaxşı yolunu müəyyənləşdirməlidir.

- Bütün məlumatların müntəzəm olaraq yedeklənməsi. Yedekləmə tezliyi məlumatların şirkət üçün nə qədər əhəmiyyətli olduğuna və şirkətin itirilmiş hər hansı bir məlumatı əvəz etmək qabiliyyəti ilə birləşdirilməlidir. Tənqidi məlumatlar gündəlik yedeklenməlidir, halbuki daha az tənqidi məlumatlar həftəlik yedeklənə bilər.
- Yedək məlumat dəstlərinin kənarda saxlanması. Yedekləmə məlumatlarının hamısı, məlumatların orijinal nüsxələri ilə eyni bir yerdə saxlanılırsa, zəlzələ, yanğın və ya tornado kimi bir hadisə həm orijinal məlumatları, həm də nüsxəni çıxardar! Yedek planının bir hissəsinin məlumatları kənar bir yerdə saxlamaq vacibdir.
- Məlumatların bərpası testi. Müntəzəm olaraq, bəzi məlumatları bərpa etməklə ehtiyat nüsxələri sınaqdan keçirilməlidir. Bu, prosesin işləməsini təmin edəcək və təşkilata ehtiyat planına inam verəcəkdir.

II FƏSİL İnternet şəbəkəsində informasiya təhlükəsizliyinin analizi

2.1. İnternet şəbəkəsində informasiya təhlükəsizliyi

İnternet təhlükəsizliyi, onlayn rejimdə aparılan əməliyyatların təhlükəsizliyini təmin etmək üçün həyata keçirilən müxtəlif təhlükəsizlik tədbirlərini özündə cəmləşdirən kompüter təhlükəsizliyinin bir qoludur. Prosesdə internet təhlükəsizliyi brauzerlərə, şəbəkəyə, əməliyyat sistemlərinə və digər tətbiqlərə yönəlmiş hücumların qarşısını alır. Bu gün müəssisələr və hökumətlər, kiberhücumlardan və internetdən qaynaqlanan zərərli proqramlardan qorunmaqdan daha çox narahatdırlar. İnternet təhlükəsizliyinin əsas məqsədi İnternetdən gələn hücumları dayandıra biləcək dəqiq qaydalar və qaydalar yaratmaqdır.

İnternet təhlükəsizliyi, onlayn olaraq ötürülən məlumatların qorunması üçün müəyyən mənbələrə və meyarlara əsaslanır. Mühafizə üsullarına Pretty Good Privacy (PGP) kimi müxtəlif şifrələmə növləri daxildir. İnformasiya texnologiyaları inqilabı bu gün dünyada insan ünsiyyətində böyük dəyişikliklər etdi. Xüsusilə son illərdə bulud hesablamasının, böyük məlumatların, İnternet əşyalarının və mobil terminalların sənayeləşmə anlayışlarının dərin tədqiqatları rəqəmsal məlumatların idarə edilməsini yeni bir strateji idarəetmə nöqtəsi halına gətirdi və şəbəkə təhlükəsizliyi problemi də alındı. Daha geniş bir dairədə daha çox diqqət. 2013-cü ilin iyun ayında “prizmadan planı” nın ifşa olunması informasiya təhlükəsizliyini iqtisadi maraqdan milli təhlükəsizlik səviyyəsinə gətirdi. 2014-cü ilin fevral ayında "mərkəzi şəbəkə təhlükəsizliyi və məlumat qrupu" nun yaradılması, Çində İnternetin milli şüurunun oyanışını qeyd etdi və milli məlumat təhlükəsizliyi strategiyasının əhəmiyyətini vurğuladı.Mütəşəkkil zərərli şəbəkə hücumunun qarşısını necə almaq təhlükəsizlik sahəsində ən çox müzakirə olunan mövzuya çevrildi [14].

Şəbəkə təhlükəsizliyi mövzusunda araşdırmalar, məlumat şəbəkələrinin yarandığı gündən başladı. Şəbəkə ölçüsü və tətbiqinin eksponensial böyüməsi, xüsusən OSI modelinə əsaslanan statik İnternet fiziki bağlantı şəbəkəsində qurulan təsadüfi dinamik giriş əlaqəsi, şəbəkə təhlükəsizliyinin öyrənilməsini çətinləşdirir. 1960-cı illərdən əvvəl, şəbəkə təhlükəsizliyi araşdırmalarının ilk mərhələsi kimi qəbul

edilə bilən sistemin məxfiliyini, bütövlüyünü və əlçatanlığını təmin etmək üçün mütləq təhlükəsizlik sistemini necə yaratmaq və dizayn zəifliyini azaltmaqdır. Ancaq insanlar qısa müddətdə praktik əməliyyatın mümkünsüzlüyünü başa düşdülər. Zərərli müdaxilənin olması, müdaxiləni vaxtında aşkar etmək və müvafiq tədbirlər görmək məqsədi ilə təhlükəsizlik köməkçisi sistemi qurmaq düşüncəsini doğurur. Ən tipik tətbiq müdaxiləni aşkaretmə sistemidir (IDS). Giriş aşkarlanması Andersonun Texniki Tədqiqat Hesabatı və sonrakı tədqiqatları iki kateqoriyaya bölmək olar: anomaliya aşkarlanması və səhv istifadə. Hazırda əksər tədqiqat müəssisələrinin və kommersiya təşkilatlarının IDS-ləri bu iki kateqoriyaya əsaslanır. Giriş aşkarlama texnologiyası, şəbəkə hücumları baş verdikdə şəbəkə təhlükəsizliyini təmin etmək üçün proqnozlaşdırıcı xəbərdarlıq məlumatı verir, ancaq divar ətrafında gizli hücum və çox addımlı mürəkkəb hücumla əlaqəli bir şey etmək çox zəifdir. Belə bir passiv müdafiə texnologiyası real vaxt aşkarlanmasında qənaətbəxş deyil. Bu əsasda, 1990-cı illərdən sonra üçüncü mərhələ tədqiqatlarının diqqəti passiv müdafiədən aktiv təhlilə keçdi, hacker texnologiyasının inkişafından yaranmışdır. Niyyət, şəbəkə hücumlarının baş verməsindən əvvəl vahid təhlükəsizlik qiymətləndirməsini aparmaq, müdafiə strategiyasını hazırlamaq və ya zədələnmiş şəbəkəni nəzərə alaraq əvvəlcədən təyin edilmiş xidmət funksiyasını verməkdir. 1990-cı ildə, Bass ilk Cyber vəziyyət Awareness CSA, belə ki, insanlar daha yaxşı şəbəkə təhlükəsizliyi vəziyyəti tutmaq və gələcək istiqamətləri, a proqnozlaşdırmaq olar ki, müəyyən dərəcədə şəbəkə təhlükəsizliyi tədqiqatları və digər fənlərin inteqrasiyasına kömək edir. İnkişaf, xüsusən də bəzi inkişaf etmiş stoxastik modellərlə birləşmə nəzəri irəliləyişə səbəb oldu. Bununla birlikdə, əksəriyyəti praktik tətbiqetmədə və sistematik ekspozisiyalarda bir neçə irəliləyiş ilə qiymətləndirmə alqoritmini optimallaşdırmaq üçün CSA konseptual modelinə əsaslanır.

2.2. Şəbəkə təhlükəsizliyi vəziyyətinin məlumatlılığı və müdaxilənin aşkarlanması

Müdaxiləni aşkar etmə sisteminin (IDS) ümumi modeli ilk olaraq Denning tərəfindən təklif edilmişdir. Onun əsas ideyası, vahid saat şərti ilə yenilənə və dəyişdirilə bilən adi qaydalar toplusunu qurmaqdır. Bundan sonra, məlumat şəbəkə prosesi qeydlərindən bir agent tərəfindən toplanır və müəyyən edilmiş qaydalarla müqayisə edilir və sonra bütövlüyü, məxfiliyi və mənbələrin mövcudluğunu pozmağa çalışan fəaliyyət dəsti olub olmadığı müəyyən edilir. IDS quruluşu əsasən üç növə bölünə bilər: host əsaslı aşkarlama, şəbəkə əsaslı aşkarlama və agent əsaslı aşkarlama. Ev sahibi əsaslı aşkarlama əsasən bir ana üzərində olan proses qeydləri məlumatlarına uyğundur. Bu açıq şəkildə şəbəkə mühitində təhlükəsizlik tələblərinə cavab vermir; beləliklə, şəbəkə əsaslı aşkarlama, şəbəkə trafiki və protokol məlumatları kimi host əsaslı aşkarlanmaya bəzi elementlər əlavə edildikdən sonra qurulur; lakin, paylanmış sistemlərin tədricən istifadəsi ilə, paylanmış hostlardakı IDS-lər, agent əsaslı aşkarlamanın formalaşmasına kömək edən məlumatların qarşılıqlı əlaqəsinə ehtiyac duyur. Texniki olaraq, IDS əsasən iki növə bölünür, anormal müdaxilə aşkarlanması və sui-istifadə müdaxilə aşkarlanması. Anormal davranış normal və ya zərərsiz davranışın tərsidir, buna görə anormal davranış aşkarlanmasında təyin olunan qayda sistemin normal işləmə rejimidir. Normal modeldən sapma aşkar edildikdə həyəcan siqnalı yaranır. Bu metodun üstünlüyü ondan ibarətdir ki, hər hansı bir kəşfiyyat davranışı müəyyən edilmiş "normal" hərəkətə əlavə olaraq qeyd ediləcəkdir. Lakin sistemin normal rejimi dinamik olduğuna görə aşkaretmə modelinin qurulmasının əvvəlində tamamilə normallaşdırıla bilmədiyi üçün daha yüksək "saxta həyəcan siqnalı" olacaq; sui-istifadə davranış anormal və ya zərərli davranışdır, buna görə sui-istifadə davranış aşkarlanması qaydası sistem zərərli davranış modelidir. Zərərli naxışa uyğun davranış aşkar edildikdə həyəcan yaradır. Aydın uyğunlaşma vəziyyətində, bu metod, xüsusilə tipik məlum hücum hücum modeli üçün yüksək dəqiqliyə malikdir. Ancaq böyük bir "itkin hesabat nisbəti" var, çünki müxtəlif

aqressiv davranışlar fonunda zərərli davranışın bütün nümunə ümumiləşdirməsini passiv şəkildə həyata keçirmək demək olar ki, mümkün deyil.

2.3. İnternet Təhlükəsizlik Cihazları və İş üçün Proqram

Bu gün müəssisələr və hökumət təşkilatları üçün istifadə edilə bilən müxtəlif İnternet təhlükəsizlik cihazları və vasitələrinə ehtiyac duyulur. Bir növü müdaxiləni aşkar etməyə kömək etməlidir, digəri isə müdaxilənin qarşısını almağa kömək etməlidir. Bu vasitələr İT işçilərinə problemləri tanımaqda və kompüter şəbəkələrini təhdidlərdən təhlükəsiz saxlamaqda çox kömək edəcəkdir.

İnkişaf etmiş proqramların bir sıra təhdidləri tanıya və hücumları qarşısını ala bilməsi nəzərdə tutulur. Bütün prosesə virusların, casus proqramların, zərərli proqramların, qurdların və s. Aşkarlanması daxildir. Təsbit alətləri sistemi yaxından izləyəcək və sistem qrupunun şəbəkədə zərərli bir fəaliyyət baş verdikdə məsələyə baxması üçün həyəcan siqnalı qaldıracaqdır. Digər tərəfdən, qarşısının alınma sistemləri (anti-malware sistemləri) canlı izləmə imkanı verir və hücumların qarşısını almaq potensialına malikdir.

Comodo Internet Security Suite, kompüterdə saxlanılan həssas məlumatları oğurlaya biləcək onlayn hücumlardan və zərərli proqramların əksəriyyətindən qoruyur. Təhlükəsizlik dəsti, hakerlərin maliyyə detallarına və şəxsi məlumatlara girməsini möhkəm şəkildə dayandıracaq.

İnternetdən yaranan zərərli proqram bir girov kimi bir sistemi saxlaya bilər və pul tələb edə bilər, istifadəçilərin hesablama vərdişləri, internet fəaliyyəti, tuş vuruşları və s. Comodo İnternet Təhlükəsizlik Açar Xüsusiyyətləri aşağıdakılardır:

- Antivirus: PC-də gizlədilən hər hansı bir zərərli proqramı izləyir və məhv edir.
- Anti-Spyware: casus proqram təhdidlərini aşkar edir və hər bir infeksiyanı məhv edir.
- Anti-Rootkit: Kompüterinizdə rootkitləri tarar, aşkar edər və aradan qaldırar.
- Bot qorunması: Zərərli proqramı kompüterinizi zombi halına salmağın qarşısını alır.

- Müdafiə +: Quraşdırmadan əvvəl kritik sistem sənədlərini qoruyur və zərərli proqramları bloklayır.
- Avtomatik Sandbox Texnologiyası: Naməlum faylları heç bir zərər verə bilməyəcəyi bir mühitdə işlədir.
- Yaddaş Firewall : Mükəmməl tampon daşma hücumlarına qarşı qabaqcadan qorunma.
- Zərərli proqram Zərər vermədən əvvəl zərərli prosesləri öldürür.

2.4. İnformasiya təhdidlərinin növləri.

İnformasiya təhlükəsizliyinin müasir problemləri əsasən aşağıdakı 5 əsas Kiber Təhdidlərdən ibarətdir:

1. Sosial Mühəndislik Hücumları
2. Təchizat Zəncirinə hücumlar
3. IoT və İnfrastruktur Hücumları
4. Şəxsiyyət və Mobil Doğrulama
5. Sıfır gün təhdidlərinin və polimorf hücumların artması

Rəqəmsal olaraq daha çox bağlandıqca, daha həssas oluruq. Bağlı bir şey hədəfdir. 2018-ci ildə pozuntuların sayı heyrətləndirici nisbətlərə çatdı. Çox sayda yeni hücum vektoru ilə 2019 daha pis olacağını vəd edir. Budur bilməli olduğunuz 5 təhdiddir.

2.4.1. Sosial Mühəndislik Hücumları (Social Engineering Attacks)

2.1

Sosial mühəndislik, insan qarşılıqlı əlaqəsi nəticəsində həyata keçirilən zərərli fəaliyyətlərin geniş spektri üçün istifadə olunan bir termindir. Təhlükəsizlik səhvləri və ya həssas məlumatlar verməklə istifadəçiləri aldatmaq üçün psixoloji manipulyasiyadan istifadə edir.

Sosial mühəndislik hücumları bir və ya daha çox addımda baş verir. Cinayətkar əvvəlcə nəzərdə tutulan qurbanı, hücumun davam etdirilməsi üçün lazım olan giriş nöqtələri və zəif təhlükəsizlik protokolları kimi zəruri məlumat toplamaq üçün araşdırır. Daha sonra təcavüzkar qurbanın etimadını qazanmaq və həssas məlumatları aşkar etmək və ya kritik mənbələrə giriş vermək kimi təhlükəsizlik təcrübələrini pozan sonrakı hərəkətlərə təkan vermək üçün hərəkət edir. Sosial mühəndisliyin xüsusilə təhlükəli olanı, proqram və əməliyyat sistemindəki zəifliyə deyil, insan səhvlərinə güvənməsidir. Qanuni istifadəçilər tərəfindən edilən səhvlər çox az proqnozlaşdırılır, bu, zərərli proqram əsaslı müdaxilədən daha çox müəyyənləşdirilməsini və qarşısını almağı çətinləşdirir [10].

Kiber cinayətkarlar getdikcə mürəkkəb vasitələrdən, o cümlədən Süni intellektdən istifadə edərək, korporasiyaların və işçilərin sosial media saytlarında təsadüfən yerləşdirdikləri məlumatlar üçün interneti gəzdirirlər. Bu məlumat, ehtimal

ki, məlumatın fişinq və nizə dişli hücumlarında istismar edildiyi yeni ildə yeni bir təhlükə vektoruna çevriləcəkdir.

Sosial mühəndislik hücumları çox müxtəlif formalarda olur və insan qarşılıqlı əlaqəsinin olduğu hər yerdə edilə bilər. Aşağıdakı rəqəmsal sosial mühəndislik hücumlarının ən çox yayılmış beş formasıdır:

Bayındır **(**Baiting).Adından göründüyü kimi, qarmaqarışıq hücumlar qurbanın acgözlüyünə və ya maraqlanmasına təsir etmək üçün yalan vədlərdən istifadə edir. Onlar istifadəçiləri şəxsi məlumatlarını oğurlayan və ya sistemlərini zərərli proqramlarla vuran bir tələyə salırlar.

Ən çox təhqir edilmiş bir şəkildə zərərli proqramı dağıtmaq üçün fiziki media istifadə olunur. Məsələn, təcavüzkarlar yemi - adətən zərərli proqram təminatı ilə yoluxmuş flash sürücüleri, potensial qurbanların onları görmək üçün əmin olduqları yerlərdə (məsələn, vanna otağı, liftlər, hədəflənmiş şirkətin park yeri) tərk edirlər. Yiyənin, şirkətin əmək haqqı siyahısı kimi təqdim etdiyi etiket kimi orijinal bir görünüşü var.

Qurbanlar yemi maraqla qarşılayır və bir işə və ya ev kompüterinə daxil edirlər, nəticədə sistemə avtomatik zərərli proqram quraşdırılır.

Yalançılıq fırıldaqları mütləq fiziki dünyada həyata keçirilməməlidir. Yeməyin onlayn formaları zərərli saytlara yol açan və ya istifadəçiləri zərərli proqramla yoluxmuş bir tətbiq yükləməsini təşviq edən cəlbedici reklamlardan ibarətdir.

Qorxudan istifadə edin **(**Scareware). Qorxu qurbanlarının saxta həyəcan siqnalları və uydurma təhdidlərlə bombardman edilməsini nəzərdə tutur. İstifadəçilər, sistemlərinin zərərli proqramlarla yoluxduğunu düşündükləri üçün aldadırlar və bu, heç bir fayda olmayan (günahkardan başqa) və ya zərərli proqramın özüdür. Qorqud proqramı, aldatma proqramı, yaramaz skaner proqramı və fırıldaqçı proqram olaraq da adlandırılır.

Ortaq bir nümunə, vebdə gəzərkən brauzerinizdə görünən qanuni görünüşlü pop-up plakatlar, "Kompüteriniz zərərli casus proqramları ilə yoluxmuş ola bilər" kimi mətnləri göstərir. Aləti sizin üçün (tez-tez zərərli proqramla) quraşdırmağı təklif edir və ya kompüterinizi yoluxdurduğu zərərli sayta yönəldəcəkdir.

Qorxu proqramı, səhv xəbərdarlıqları həyata keçirən və ya istifadəçilərə dəyərsiz / zərərli xidmətlər almaq təklifləri verən spam e-poçt vasitəsi ilə də paylanır.

Bəhanə gətirmək**.** Burada təcavüzkar bir sıra ağılla hazırlanmış yalanlar vasitəsilə məlumat əldə edir. Fırıldaqçılıq çox vaxt bir cinayətkar tərəfindən, vacib bir vəzifəni yerinə yetirmək üçün zərərçəkmişdən həssas məlumatlara ehtiyac olduğunu iddia edərək başlanır.

Təcavüzkar, adətən, işçiləri, polis, bank və vergi işçilərini və ya bilmək hüququ olan digər şəxsləri təqib edərək öz qurbanlarına etimad yaratmağa başlayır. Sınaqçı zərərçəkənin şəxsiyyətini təsdiqləmək üçün lazımlı sualları soruşur, bunun vasitəsilə vacib şəxsi məlumatları toplayırlar.

Sosial təminat nömrələri, şəxsi ünvanlar və telefon nömrələri, telefon qeydləri, işçilərin məzuniyyət tarixləri, bank qeydləri və fiziki bir bitki ilə əlaqəli təhlükəsizlik məlumatları kimi bu cür hiylələrdən istifadə edərək toplanır.

Fişinq **(**Phishing). Ən populyar sosial mühəndislik hücum növlərindən biri kimi, fişinq dolandırıcıları, təcavüzkarlıq, maraq və qorxu hissi yaratmağa yönəlmiş e-poçt və mətn mesajı kampaniyalarıdır. Daha sonra, həssas məlumatları aşkar etmək, zərərli saytlara bağlantıları tıklamaq və ya tərkibində zərərli proqramları olan əlavələri açmaqla nəticələnir.

Nümunə, bir onlayn xidmət istifadəçilərinə, tərəflərinə təcili olaraq hərəkət etməyi tələb edən bir siyasət pozuntusu haqqında xəbərdarlıq edən bir e-poçt, məsələn tələb olunan parol dəyişikliyi. Buraya qanunsuz versiyasına bənzər bir qeyri-qanuni veb saytın bağlantısı daxildir - cəsarətlənməyən istifadəçinin cari etimadnamələrini və yeni şifrələrini daxil etmələrini tələb edir. Forma təqdim edildikdə məlumat təcavüzkara göndərilir.

Fərqli və ya yaxın olan mesajların, фишингу kampaniyalardakı bütün istifadəçilərə göndərildiyini nəzərə alaraq, onları aşkar etmək və bloklamaq təhlükə mübadiləsi platformalarına girən poçt serverləri üçün daha asandır.

Nizə fişinqi **(**Spear phishing**)**

Bu, təcavüzkarın müəyyən şəxsləri və ya müəssisələri seçdiyi фишинг fırıldaqçılığının daha hədəfli bir versiyasıdır. Daha sonra mesajlarını hücumlarını daha az fərqləndirmək üçün xüsusiyyətlərinə, iş mövqelərinə və qurbanlarına aid əlaqələrə əsaslanaraq düzəldirlər. Nizə fişinqi günahkarın adına daha çox səy tələb edir və çəkilmək üçün həftələr və aylar çəkə bilər. Bacarıqla həyata keçirildikdə, aşkarlamaq və daha yaxşı müvəffəqiyyət nisbətlərinə sahib olmaq daha çətindir.

Bir nizə nişanlanması ssenarisi, bir təşkilatın İT məsləhətçisini təqlid etmək, bir və ya daha çox işçiyə bir e-poçt göndərən bir təcavüzkarı əhatə edə bilər. Bu, məsləhətçinin normal olaraq yazdığı və imzalanmasıdır, bununla da qəbuledicilərin orijinal mesaj olduğunu düşünərək aldadır. Mesaj, alıcılardan şifrələrini dəyişdirməyi xahiş edir və onları təcavüzkarın indi etimadnamələrini ələ keçirdiyi zərərli səhifəyə yönləndirən bir keçid təmin edir.

Sosial mühəndislər sxemləri həyata keçirmək və qurbanlarını tələlərinə çəkmək üçün maraq və qorxu kimi insan hisslərini manipulyasiya edirlər. Buna görə, bir e-poçt ilə həyəcanlandığınızda, bir veb saytında göstərilən bir təklifə cəlb olunanda və ya yalançı rəqəmsal media ilə qarşılaşdığınız zaman ehtiyatlı olun. Ayıq olmaq, özünüzü rəqəmsal aləmdə baş verən bir çox sosial mühəndislik hücumlarından qorumağa kömək edə bilər.

Üstəlik, aşağıdakı məsləhətlər sosial mühəndislik işlərinə münasibətdə sayıqlığınızı artırmağa kömək edə bilər.

- Şübhəli mənbələrdən e-poçt və əlavələr açmayın - sual göndərənini bilmirsinizsə, bir e-poçta cavab verməyinizə ehtiyac yoxdur. Əgər siz onları tanıyırsınızsa və onların mesajlarına şübhə ilə yanaşsanız, xəbərləri telefon vasitəsilə və ya birbaşa xidmət təminatçının saytı kimi digər mənbələrdən çap edib təsdiqləyin. Unutma ki, e-poçt ünvanları hər zaman pozulur; etibarlı bir mənbədən gələn bir elektron poçt, hətta təcavüzkar tərəfindən başlatılmış ola bilər.

- Multifaktorlu identifikasiyadan istifadə edin - Məlumat təcavüzkarlarının axtardıqları ən qiymətli parçalardan biri istifadəçi etimadnaməsidir. Multifaktorlu identifikasiyanı istifadə etmək, sistemin güzəşt vəziyyətində hesabınızın qorunmasını təmin edir. Imperva Login Protect , tətbiqləriniz üçün hesab təhlükəsizliyini artıra bilən asan bir 2FA həllidir.
- Cazibədar təkliflərdən ehtiyatlanın - Təklif həddən artıq cəlbedici səslənirsə, fakt kimi qəbul etməzdən əvvəl iki dəfə düşünün. Mövzunun Googling, qanuni bir təklif və ya tələ ilə məşğul olub olmadığınızı tez bir zamanda müəyyənləşdirməyə kömək edə bilər.
- Antivirus / antimal proqram proqramınızı yeniləyin - Avtomatik yeniləmələrin cəlb olunduğundan əmin olun və ya hər gün ən son imzaları ilk dəfə yükləməyi vərdiş halına gətirin. Yeniləmələrin tətbiq olunduğundan əmin olmaq üçün vaxtaşırı yoxlayın və sisteminizi mümkün infeksiyalar üçün tarayın
- Lisenziyanızı iş yerinizdən uzaqda olduğunuz zaman kilidləyin.
- Hansı şəraitdə bir qəribin binaya daxil ola biləcəyinizi və ya verməyiniz lazım olduğunu başa düşmək üçün şirkətinizin məxfilik siyasətini oxuyun.

2.4.2. Təchizat Zəncirinə hücumlar

Korporasiyalar öz perimetrlərini və hücum səthlərini sərtləşdirməyə davam etdikdə, cinayətkarlar getdikcə risklərin tam anlaşılmadığı həssas təchizat zəncirinə baxırlar. Getdikcə bu tədarük zəncirindəki satıcılar şirkətin öz zəifliyi və risk profilinin bir hissəsi kimi qəbul ediləcəkdir. Cinayətkarlar korporasiyalar haqqında kritik məlumatlar əldə etmək üçün tədarük zəncirindən getdikcə daha çox istifadə edəcəklər.

Bir dəyər zənciri və ya üçüncü tərəf hücumu da adlandırılan bir tədarük zənciri hücumu, sisteminizə və məlumatlarınıza girmə imkanı olan bir tərəfdaş və ya provayder vasitəsilə sisteminizə daxil olduqda baş verir. Bu, son bir neçə ildə tipik müəssisənin hücum səthini kəskin şəkildə dəyişdirdi, daha çox təchizatçı və xidmət təminatçısı əvvəlkindən daha həssas məlumatlara toxundu.Təchizat zəncirinin hücumu ilə əlaqəli risklər yeni hücum növləri, təhdidlər barədə ictimaiyyətin

xəbərdarlığı və tənzimləyicilərin nəzarəti artması səbəbindən heç vaxt yüksək olmamışdır. Bu vaxt, təcavüzkarlar mükəmməl bir fırtına yaratdıqca əvvəlkindən daha çox sərvət və vasitəyə sahibdirlər.

Təchizatçılar tərəfindən baş verən böyük kiber pozuntulara son yoxdur. 2014 Hədəf pozuntusu , bir HVAC satıcısının təhlükəsizliyi səbəb oldu. Bu il, Equifax nəhəng pozuntusunu istifadə etdiyi xarici proqram təminatında qüsurla günahlandırdı. Daha sonra veb saytındakı zərərli bir yükləmə bağlantısını başqa bir satıcıya günahlandırdı.Daha sonra böyük korporasiyalar, siyasətçilər və məşhurlar tərəfindən dəniz vergisindən yayınma haqqında ətraflı məlumat verən 13 milyondan çox sənəd olan Cənnət Sənədləri var idi. Mənbə Keçən ilki Panama Papers kimi , ən zəif bağlantı olan bir hüquq firması idi.

Bu təcrid hallar deyil. Ponemon İnstitutu tərəfindən 2018-ci ilin payızında aparılan bir araşdırmaya görə , təşkilatların 56 faizində satıcılardan biri səbəb olan bir pozuntu var. Bununla yanaşı, hər bir təşkilatda həssas məlumatlara sahib olan üçüncü şəxslərin ortalama sayı 378-dən 471-ə yüksəldi. Bu rəqəm bir az aşağı ola bilər. Şirkətlərin yalnız 35 faizində həssas məlumatları paylaşdıqları üçüncü tərəflərin siyahısı var.Şirkətlərin yalnız 18 faizi bu satıcıların öz növbəsində bu məlumatları digər tədarükçülərlə paylaşdıqlarını bildiklərini söyləyir. Bu bir problemdir, çünki müştərilərin məlumatları itirən şirkətin tədarükçüsü olub-olmaması, şirkətin özü deyil.Bu səbəblərə görə şirkətlər üçüncü tərəf risklərinə daha çox diqqət yetirirlər. 2018-ci ilin Dekabr ayında Ponemon İnstitutu Kiber Risk Hesabatı üçüncü şəxslər tərəfindən məxfi məlumatların qeyri-qanuni istifadəsi və ya icazəsiz paylaşılmasının 64 faizi ilə İT mütəxəssisləri arasında 2019 üçün ikinci ən böyük təhlükəsizlik narahatlığı olduğunu təsbit etdi. Qırx faizi son 24 ayda üçüncü tərəflə əlaqəli insident yaşadıqlarını söylədi.Təchizatçı münasibətləri dayandırıldıqda risklərin bitmədiyini düşündüyünüz zaman problem daha da ağırlaşır. Bu payız, Dominonun Avstraliyada bir təhlükəsizlik pozuntusu oldu və keçmiş bir təchizatçı sisteminin müştəri adlarını və e-poçt ünvanlarını sızdırdığını söylədi. "Təqdim etdiyim müqavilələrin əksəriyyətində satıcı ləğvinin çətin prosesini idarə etmək üçün adekvat detallar

yoxdur" deyir Bred Keller, Prevalent, Inc üçüncü tərəf strategiyasının baş direktoru.Üstəlik, tənzimləyicilər getdikcə üçüncü tərəf risklərinə baxırlar. Keçən il New York Dövlət maliyyə tənzimləyiciləri, New Yorkdakı bir maliyyə firmalarından, təchizatçılarının kiber təhlükəsizlik qorumalarının paralel olmasını təmin etmələrini tələb etməyə başladılar.Üçüncü tərəf risk tənzimləmələri hələ başlanğıc mərhələsindədir və bir çox şirkət bu riskləri yaxşı idarə edə bilmir, Thales e-Security-də strategiya və marketinq üzrə VP Peter Galvin qeyd edir ki, “bir çox şirkət riskləri başa düşmür və pozuntuların artacağını görüb və daha çox tədbirlər görəcəklər."
Mütəxəssislər, daha çox tənzimləyicinin şirkətlərdən bu günkü kimi olduğundan daha çox üçüncü tərəf riski ilə əlaqədar daha çox şey etmələrini tələb etməyə başlayacaqlarını gözləyirlər. "Bu gördüyümüz davam edən bir tendensiya oldu" dedi Focal Point Data Risk, MMC-nin məlumatların məxfiliyi praktikası rəhbəri Eric Dieterich.

Demək olar ki, hər bir şirkət kənar proqram və hardware istifadə edir. Artıq heç kim bütün texnologiyasını sıfırdan qurmur, açıq mənbə iqtisadiyyatında bir bum sayəsində. Ancaq bu zehniyyətə xeyli risk var. Satın alınan hər bir cihaz, yüklənən hər bir tətbiq yoxlanılmalı və potensial təhlükəsizlik risklərinə nəzarət edilməlidir və bütün yamalar yenilənməlidir.

Aprel ayında Flashpoint Intelligence araşdırmaçıları, cinayətkarların , məşhur kredit mənbəyi olan Magento e-ticarət platformasına qarşı hücumları gücləndirdiyini , kredit kartı qeydlərini qırmaq və kriptovalyutaya yönəlmiş zərərli proqram quraşdırmaq üçün şiddətli parol tətbiq etdiklərini söylədi.
Tədqiqatçılar ən azı 1000 güzəştli Magento idarəetmə panelini aşkar etdilər və dərin vebdə və qaranlıq vebdə platformanın özünə olan maraqın 2016-cı ildən bəri davam etdiyini söylədi. Bundan əlavə, Powerfront CMS və OpenCart-a da böyük maraq var.
Keçən il Magento Community Edition-da bir CSRF zəifliyi 200.000 onlayn pərakəndə satışa məruz qaldı. İstismar edilsə, qüsur, həssas müştəri məlumatlarını ehtiva edən verilənlər bazalarını ifşa edərək, sistemin tam güzəştinə icazə verə bilər.

Magento-nun ticari versiyası eyni əsas kodu paylaşdığı üçün müəssisələrin əməliyyatlarına da ciddi təsir göstərildi.

Yalnız bir şirkətin öz məlumatları risk altındadır, ancaq nöqsanlı bir proqram və ya hardware komponenti bir məhsula yapışdırılarsa, bu, daha çox təhlükəsizlik problemlərinə səbəb ola bilər. Təhlükəsizlik arxa planına yoluxmuş bir kompüter çipi, güclü identifikasiyası olmayan bir kamera və ya pis bir proqram komponenti geniş ziyan verə bilər. Heartbleed səhv , məsələn, Oracle, VMware və Cisco daxil olmaqla bir çox əsas satıcılar tərəfindən web və mobil cihazlar, eləcə də proqram milyonlarla təsir etdi.

Convey, üçüncü tərəfin pozulması səbəbindən məxfi məlumatları və ya həssas intellektual mülkiyyəti (IP) itirməkdən də narahat olduğunu qeyd etmişdir.

Bir çox şirkət, tədarükçülərin cavab verməli olduğu keyfiyyət standartlarına malikdir. Cisco təhlükəsizlik üçün eyni yanaşmanı istifadə edir.Əsas yanaşama olaraq dözümlülük səviyyəsinə çatdıqdan sonra, dözümlülük səviyyəsindən yuxarıda və ya altındasınızsa, ölçməyə başlaya bilərsiniz. Dözümlülük həddindədirsə, birlikdə oturub bunu necə həll etmək üçün birlikdə işləmək olar.

Tək, düzəldilmiş bir təşkilat fərdi tətbiqlərdən bütöv məlumat mərkəzlərinə qədər hər şeyin bulud təminatçılarına keçdiyi bir rəqəmsal ekosistemlə əvəz olundu. "Qorumalı olduğunuz şey ətrafınızdan o qədər də kənarda deyil", CyberGRX baş direktoru Fred Kneip deyir. "Və hakerlər ağıllıdırlar. Ən az müqavimət yoluna gedirlər."Kneip deyir ki, indi də bulud effektiv gəlir. Və bir avtomobil xətti üçün bir IoT qaynaq aləti standart parametr, proqnozlaşdırma baxımını edə bilməsi üçün istehsalçıya diaqnostika göndərilməsində istifadə eidlir.

Peşəkar xidmətlər göstərən firmalar daha az etibarlı ola bilərlər

"Təhlükəsizlik həqiqətən ən zəif əlaqə olduğu qədər yaxşıdır" deyə təhlükəsizlik satıcısı CrowdStrike, Inc satış mühəndisliyi EMEA direktoru John Titmus bildirir. Təchizat zəncirvari hücumları daha da genişlənir və tezliyi və incəliyi ilə artır. Risklərin mahiyyətini anlamalı və ətrafındakı bir təhlükəsizlik xəritəsi hazırlanmalıdır.Daha böyük servis şirkətləri də həssasdır. Verizon pozulması altı

milyon müştəri qeydlər cəlb, Nice Systems, müştəri xidməti analitik provayderi səbəb oldu. Nice, hesabı və şəxsi məlumatları daxil edən altı aylıq müştəri xidməti zəngləri ictimai Amazon S3 saxlama serverinə qoydu.

"Kaspersky Laboratoriyasının əsas təhlükəsizlik tədqiqatçısı Kurt Baumgartner," daha çox təchizat tərəfi təşkilatının təcavüzkarlar tərəfindən vurulduğunu görsək təəccüblənməyəcəyik.

Üçüncü tərəf riskini necə idarə etmək olar: İlk addımlar

Üçüncü tərəfin kiber təhlükəsizlik riskinə düzgün nəzarət yalnız uyğunluq üstünlüklərindən əlavə divident ödəyir. Ponemon hesabatına görə əslində pozuntu ehtimalını azaldır. "Bir pozuntu hadisəsini 20 faiz bəndi azaltmaq olar" deyə Dov Goldman, araşdırmaya sponsorluq edən Opus Global, Inc. şirkətindəki yeniliklər və ittifaqlar üzrə VP deyir.

Xüsusilə, bir şirkət bütün təchizatçılarının təhlükəsizlik və məxfilik siyasətlərini qiymətləndirirsə, pozuntu ehtimalı 66 faizdən 46 faizə düşür. Buna bütün tədarükçülər daxildir, deyə Goldman əlavə edib.

Goldman bildirir ki, "Böyük münasibətlər ən böyük risk olmaya bilər". Ən böyük tədarükçülərin, ehtimal ki, artıq hazırlanmış kiber təhlükəsizlik müdafiəsinə sahib olması mümkündür.Ancaq daha kiçik təşkilatlara baxsanız, onlarda kiber təhlükəsizlik nəzarəti yoxdur, hər bir təşkilatda miqyasından asılı olmayaraq müəyyən səviyyədə təhlükəsizlik normaları təyin edilməli və həyata keçirilməlidir.

Bir şirkət bütün satıcıların kim olduğunu və hansının həssas məlumatlara sahib olduğunu başa düşdükdən sonra təhlükəsizlik səviyyələrini qiymətləndirməyə kömək edəcək müxtəlif vasitələr mövcuddur. Məsələn, bəzi şirkətlər təchizatçıları ilə xidmət səviyyəsində razılaşmalara təhlükəsizlik də daxil edirlər, bulud təhlükəsizlik şirkəti Evident.io-nun baş direktoru Tim Prendergast bildir ki, “Təhlükəsizliyə təminat verən provayderlərdən razılaşmanın tələbində inkşaf görülür. Onlar bu provayderlərdən tərəfdaşlarına oxşar nəzarət tətbiq etmələrini xahiş edirlər. Biz bu müqavilələrin hüquqi kaskadını görürük."

Satıcılardan özünü qiymətləndirmə, müştəri ziyarətlərinə və yoxlamalarına icazə verilməsi və ya kiber sığorta almaq tələb oluna bilər. Bəzən daha incə bir qiymətləndirmə lazımdır. "Biz bir çox şirkətin öz xidmət təminatçılarında yoxlamalar apardığını gördük" dedi Kudelski Təhlükəsizlik tədqiqat direktoru Rayan Spanier.

Kiçik müştərilər isə bu cür təsir bağışlamaya bilər.Həm də təhlükəsizlik ilə yaxşı bir iş gördüyünüzü bildiyiniz şirkətlərlə məhdudlaşa bilərsiniz, çünki çox deyil onlardan indi. "Bundan əlavə, təhlükəsizlik ballarını təmin edən təşkilatlar da var. Məsələn, BitSight Technologies və SecurityScorecard xaricdən satıcılara, şəbəkələrinin hücumlara nə qədər etibarlı olduğuna dair reytinq şirkətlərinə baxır.

Daha dərin qiymətləndirmələr üçün, satıcıların daxili siyasət və proseslərinə baxaraq, Deloitte və CyberGRX satıcıları müştərilərin hər birinə ayrıca cavab verməkdən xilas edərək araşdırmaları və davam edən qiymətləndirmələri etmək üçün bir araya gəldilər.Şirkətlər bu gün üçüncü tərəflərin kiber risklərinə davamlı idarə edilməli olan bir iş riski kimi yanaşmalıdırlar, Aetna'nın CSO Jim Routh,CyberGRX Birjası bütün şirkətlərə bu yanaşmanı etməyə imkan verir.

Bir neçə maliyyə sənayesi qrupu oxşar bir şey edir. Noyabr ayında American Express, Bank of America, JPMorgan və Wells Fargo TruSight adlı bir satıcı qiymətləndirmə xidmətini yaratmaq üçün birləşdilər. İyun ayında Barclays, Goldman Sachs, HSBC və Morgan Stanley IHS Markit şirkətindən Bilinən Üçüncü Tərəf risk idarəetmə həllində səhm aldıqlarını açıqladılar.

Şirkətlər üçüncü tərəflərin məxfi məlumatlara necə daxil olmalarını nəzərdən keçirməlidirlər ki, yalnız düzgün insanlar məlumatları yalnız təsdiq edilmiş məqsədlər üçün əldə edə bilsinlər. Ponemon'un Kiber Risk Hesabatına görə respondentlərin 42 faizi, üçüncü tərəflərin məxfi məlumatlara girişi üzərində nəzarəti yaxşılaşdırdıqlarını söylədi.

2.4.3. IoT və İnfrastruktur Hücumları (IoT and Infrastructure Attacks)

İnfrastrukturumuzu idarə edən köhnə sistemlərlə birlikdə, İnternet Şeyi (IoT) təşkil edən ucuz və etibarsız cihazların yayılması Yeni ildə mükəmməl bir fırtına yaratmaq üçün birləşir. Cinayətkarlar şirkətləri, şəhərləri və hətta ölkələri girov saxlayaraq bu

cür sistemləri ələ keçirdikləri üçün Ransomware-nin daha yüksək olması ehtimalı yüksəkdir. Attribution çox çətin olacaq və bununla da cinayətkarları və millətləri əhatə edir.

Things of Internet (IoT) kiber cinayətkarlar üçün əsas hədəfə çevrilib. IoT cihazlarında təkrar təhlükəsizlik hadisələri IoT hücumlarının artan bir tendensiyasını təmsil edir.

İstehlakçı, müəssisə və səhiyyə təşkilatlarında əlaqəli cihazların yayılması və daxili zəifliklər kiber cinayətkarlar veb kameralar, ağıllı TV, marşrutlaşdırıcılar, printerlər və hətta bir cihaz kimi güzəştə getmək üçün Sıfır günlük hücum edə biləcəyi bir təhlükəsizlik kor nöqtəsi yaratdı.

Bağlı cihazların yaratdığı 10 ciddi təhlükənin siyahısı:

Smart Təhlükəsizlik Kameraları**.** Ağıllı təhlükəsizlik kameraları ilə kiber təhlükəsizlik məsələsi Xiaomi Mijia'nın həssaslıqlarına məruz qaldıqdan sonra müştəriləri həyəcanlandırdı. Hadisə, evinin ətrafındakı Google Nest Hub və bir neçə digər Xiaomi Mijia kamerasına sahib olan Dio-V, kameralarından məzmunu Google Nest Hub-a ötürdüyü zaman təsadüfi olaraq digər insanların evlərindən şəkillər aldığını iddia etdikdən sonra aydınlaşdı.Bu ağıllı təhlükəsizlik kameralarının bir problem yaratdığı ilk hadisə deyil.

Amazon-a məxsus bir ev təhlükəsizliyi məhsulları təmin edən Ring, təhlükəsizlik kameralarında qurbanların xəsarət almasına səbəb olan çoxsaylı hack hadisələri barədə xəbərlər üçün ABŞ -da bir sinif davası ilə vuruldu.

Kibertəhlükəsizlik firmasının Bitdefender-in təhlükəsizlik tədqiqatçıları Amazon-un Ring Video Doorbell Pro-dakı bir qüsuru aşkarladı və bildirdilər ki, bu da hakerlərə istifadəçinin Wi-Fi şəbəkəsinə və ona qoşulmuş digər cihazlara icazəsiz giriş verə bilər. Hal-hazırda, bütün Ring Doorbell kameraları məsələni yüngülləşdirmək üçün Amazon-dan təhlükəsizlik yamağı aldı.

Ayrıca Tenable zəiflik təsbit firmasının tədqiqatçıları Amazon şirkətinə məxsus Blink XT2 təhlükəsizlik kamera sistemlərində yeddi kritik zəifliyi aşkar etdilər. İstismar edildiyi təqdirdə, zəifliklər hakerlərə kamera görüntülərini uzaqdan

görmək, səs çıxışı dinləmək və yoluxmuş cihazı xidmətdən yayımlanan rədd hücumlarını (DDoS) başlatmaq üçün istifadə edə bilər.Buna cavab olaraq Amazon, zəifliklər üçün yamalar yaydı və istifadəçilərini cihazlarını 2.13.11 və ya daha sonra versiyasını yeniləməyə çağırdı.

HakerlərFaks maşınlarını "Faksploit" edə bilərlər**.** Check Point-in təhlükəsizlik tədqiqatçıları Yaniv Balmas və Eyal Itkin, faks maşınlarında bir hackerin sadəcə bir telefon xətti və bir faks nömrəsindən istifadə edərək bir şirkətin şəbəkəsi vasitəsi ilə məlumatları oğurlamasına imkan verə biləcək təhlükəsizlik zəifliklərini tapdılar . Tədqiqatçılar, həmçinin DEFCON 26 konfransında Hewlett Packard hamısı in-bir printerdə təhlükəsizlik qüsurlarından necə istifadə edə bildiklərini nümayiş etdirdilər.

Potensial təhlükəni izah edən tədqiqatçılar, təcavüzkarların xüsusi yaradılan zərərli proqram təminatı ilə kodlaşdırılmış görüntü fayllarını faks vasitəsi ilə hədəf şəbəkələrə göndərə biləcəyini söylədi. Faks maşınındakı çatışmazlıqlar, həssas məlumatları poza biləcək və ya bağlı şəbəkələr arasında pozulmalara səbəb ola biləcək zərərli proqramı faylları deşifrə etməyə və bunları yaddaşına yükləməyə imkan verir.

Smart TV**.** FTB-nin məlumatına görə, ağıllı televiziyalar təhlükəsizlik məsələlərinə bir neçə göz yumur və laqeyd yanaşırlar. Bildirilib ki, təhlükəsizlik bir neçə ağıllı televiziya istehsalçısı üçün müxtəlif təhlükələrə qarşı həssas hala gətirir. Hakerlər, kanalları və ya səs səviyyəsini dəyişdirmək üçün təmin edilməmiş televizorunuzu idarə edə bilməz, həm də quraşdırılmış kamera və mikrofondan istifadə edərək gündəlik hərəkətlərinizi və danışıqlarınızı izləyə bilər.

Ağıllı ampüller. Birdən çox hesabat ağıllı ampullərdə təhlükəsizlik zəifliklərini açıqladı. San Antonio Texas Universitetinin (UTSA) bir araşdırma mütəxəssisi Murtuza Jadliwala görə, hakerlər , evdə mövcud olan digər bağlı İoT cihazlarını istismar etmək üçün, ampullərdən yayılan infraqırmızı görünməz bir işıq vasitəsilə əmrlər göndərərək infraqırmızı effektiv ağıllı ampülləri güzəştə gedə bilərlər.

Ağıllı Ev həssasdır. Onların Smart Home quraşdırma naməlum intruders tərəfindən hacklandi sonra Milwaukee-based neçə dəhşətli hadisə yaşadı.Cütlük Samantha və

Lamont Westmoreland, hakerlərin əlaqəli cihazları güzəştə apararaq ağıllı evlərini ələ keçirdiklərini bildirdilər. Təcavüzkar, mətbəxdəki bir kamera vasitəsi ilə danışarkən video sistemindən yüksək səs səviyyəsində narahat musiqi səsləndirdi, həmçinin termostatı istifadə edərək otaq temperaturunu 90 dərəcə Farenheitə dəyişdirdi.

Əvvəlcə cütlük bunun texniki bir dəyişik olduğunu düşündü və şifrələrini dəyişdirdi, amma məsələ davam etdi. İkili daha sonra, kiminsə Wi-Fi və ya Nest sistemini ələ keçirdiyini başa düşdükdən sonra şəbəkə identifikatorlarını dəyişdirdi.

Smartfonun Mikrofonu Akustik Yan-Kanal Hücumunu başlamaq üçün istifadə edilə bilər. İngiltərə və İsveçdən olan akademik tədqiqatçılar, cihazın parol və kodlarını oğurlamaq üçün bir smartfonun mikrofonundan istifadə edə biləcək bir zərərli proqram hazırladılar . Tədqiqatçılar, "Toxunuşunuzu Eşitmə: Smartfonlardakı Yeni Akustik Yan Kanal" adlı hesabatında, istifadəçilərin sensor ekranlarında istifadəçilərin nə yazdıqlarını təqdim edən ilk akustik yan kanal hücumunu tapdıqlarını iddia etdilər.Hakerlər şəxsiyyətinizi və bank məlumatlarını bir qəhvə maşınından oğurlaya bilərlər.Xüsusi tətbiqlərdən istifadə edərək internetə qoşulmuş ağıllı qəhvə maşınları, sahibinin bankı və ya kart məlumatlarını oğurlamaq üçün hakerlər tərəfindən hədəfə alına bilər.Təhlükəsizlik nəhəngi Avastın icraçı direktoru Vince Steckler, ağıllı qəhvə maşınlarının sahiblərinə telefonlarını istifadə edərək uzaqdan idarə etməyə imkan verdiklərini söylədi . İstifadəçilər Amazon-un Alexa kimi virtual köməkçi proqramla əlaqəli olduqları təqdirdə maşınlara vokal əmrləri də verə bilərlər.

“Qəhvə maşınları təhlükəsizlik üçün nəzərdə tutulmamışdır. Şəbəkəyə girmək üçün əlavə vektorlardır. Və siz onları qoruya bilməzsiniz”deyə Stekler media açıqlamasında bildirib.

Bağlı printerlər. Quocirca təhlükəsizlik araşdırma firmasının fikrincə, bir təşkilatın şəbəkəsinə qoşulmuş printerlər kiberhücumların potensial vektorudur. Quocirca, "Qlobal Çap Təhlükəsizliyi Landşaftı, 2019" adlı hesabatında , bağlı printerlərin yaratdığı təhlükəsizlik zəifliklərinə toxundu.Hesabatda Böyük Britaniya, ABŞ, Fransa və Almaniyadakı müəssisələrin 60 faizinin 2019-cu ildə çapla əlaqəli məlumat

pozuntusuna məruz qaldığı, bunun nəticəsində şirkətlərin orta hesabla 400.000 ABŞ dollarından artıq dəyər itkisi ilə nəticələndiyi vurğulanmışdır.

Ağıllı Dinamiklər Hack edilə bilər. Wu HuiYu və Qian Wenxiang, Tencent Blade təhlükəsizlik tədqiqatçılar məruz bir smart natiq hack necə DEFCON təhlükəsizlik konfransında bir canlı nümayiş smart natiqlər ətrafında zəifliklərin. Komanda hücum proqramını təqdim etmək üçün Amazon Echo ağıllı dinamiklərindən istifadə etdi.

Tədqiqatçılar bir hücum proqramı ilə qurulmuş zərərli cihaz əlavə edərək dinamikdən əl çəkdi. Təqdimatdan əvvəl tapdıqlarını Amazon-a bildirdilər və Amazon problemləri həll etmək üçün təhlükəsizlik yamağı itələdi.

İnternetə qoşulmuş qaz stansiyaları belə hücümlara həssasdır. Trend Micro-un tədqiqatçıları aşkarladılar ki, hakerlər IoT əsaslı kiberhücumlara başlamaq üçün internetə bağlı yanacaqdoldurma məntəqələrini hədəf alırlar .

Onun da hesabatda , "Things İnternet Kibercinayətkarlıq Yeraltı, " Trend Micro mandat smart metr ilə ölkənin bütün elektrik metr əvəz Rusiya hökumətinin yeni direktiv, faydalanmışdır necə rus hakerlər təsvir. Trend Micro, Rusiyanın qaranlıq veb-forumlarında olan hakerlərin ağıllı sayğacların istifadəsi barədə məlumat istədiklərini bildirdi. Bəzi hakerlər yeraltı bazar forumlarında hətta dəyişdirilmiş ağıllı sayğacları satırlar. Tədqiqatçılar, həmçinin qaz nasosunun sındırılması ilə bağlı dərsləri, o cümlədən bağlı sayğacları necə sındırmağın addım-addım prosedurlarını gördüklərini aşkar etdilər.

2.4.4.Şəxsiyyət və Mobil Doğrulama

Şifrələrin məhdudluğunu və şəxsiyyət idarəetməsinin getdikcə buludda hərəkət etdiyini başa düşdüyümüzdə, mobil cihaz identifikasiyası partlaya bilər. Heç olmasa başlanğıcda, bu keçidin bir hissəsinin istismar olunacağını, xüsusən də etibarsız yanaşmaların tətbiq olunduğunu gözləyin. Üzün tanınması və biometriya hələ də sürətli inkişaf mərhələsindədir və həqiqi etibarlı vəziyyətə gəlmədi.

2.4.5. Sıfır gün təhdidlərinin və polimorf hücumların artması

Son bir ildə ən çox görülən hücumlar, kritik aktivləri güzəşt etmək üçün göndərilməmiş yeni zəifliklərin istifadə edildiyi sıfır günlük təhdidlərin istismarı idi.

"Polimorfik Hücumlar" vəziyyətində istismar üçün istifadə olunan kod effektiv idarəetmə və bərpaedilmənin qarşısını almaq üçün sürətlə və avtomatik olaraq dəyişir. 2019-cu ildə bunun yüksək sürətlə davam edəcəyini gözləyin. Zaman təzyiqləri ilə mürəkkəbləşən proqram təminatına olan yüksək tələbat bir çox aşkarlanmamış zəifliklərə səbəb olur.

Tərifinə görə, identifikasiya həqiqətin və ya obyektin kimliyini təsdiqləmə prosesidir. Texniki baxımdan, istifadəçinin şəxsiyyətini təsdiqləyən bir proqram və ya bir prosesdir. Bildiyimiz kimi, istifadəçi xüsusi seanslarını və ya məlumat toplusunu qorumaq üçün ehtiyac duyan bütün kompüter sistemlərinin istifadəçilərə giriş üçün bir növ identifikasiya mexanizmini tələb etməsi lazımdır. Bu, müştəri-server əsaslı sistemlər, həmçinin veb effektiv portallar üçün doğrudur. Tətbiqetmə proqramı və sistemlərinin ümumi təhlükəsizliyində autentifikasiya mühüm rol oynayır. Onun məqsədi, ilk növbədə, icazəsiz şəxslərin sistemə girməməsi və səlahiyyətli şəxsin ehtiyac duyduğu mənbələrə daxil olmasını təmin etmək üçün istifadə olunur. Doğrulanmanın bütün şifrələrə aid olduğu həmişə güman edilir. Bu müəyyən dərəcədə doğrudur, tezliklə bunun xaricində mexanizm öyrənəcəyik. Təhlükəsizlik problemlərini anlamaq üçün əvvəlcə autentifikasiya prosesinin işini başa düşməliyik.
Tipik bir identifikasiya sisteminin necə işlədiyinə baxaq. Xahiş edirəm Şəkil 1-ə baxın. İstifadəçi identifikasiya yoxlayıcısı ilə özünü təsdiqləməyə çalışır. Doğrulama, ilk növbədə istifadəçi adresi və parol kimi etimadnaməsini təmin etmək üçün təhlükəsizliyi təmin edən bir proqram sistemidir. İstifadəçi identifikasiya moduluna göndərilən məlumatları daxil edir. Bu modul istifadəçinin etimadnaməsi haqqında məlumatı olan bir geribildirim identifikasiyası verilənlər bazasına aiddir. Bu məlumat keçmişdə istifadəçinin profili qurulanda yaradıldı. Verilənlər bazası girişləri və təqdim olunan məlumatlar müqayisə edildikdən və uyğun olduğu aşkarlandıqdan sonra istifadəçiyə bir mö'cüzə təqdim olunur. Bu işarə indi istifadəçinin aktiv sessiyasının bir hissəsinə çevrilir və hər bir sonrakı tələb üçün identifikasiya prosesini ləğv edir. Bu nümunə bir istifadəçinin proqram sistemi ilə təsdiqlənməsi prosesini təsvir edir. Bir proqram sisteminin digər proqram sistemlərini də təsdiqlədiyi

vəziyyətlər var. Şəkil 2-də göstərildiyi kimi, təhlükəsizliyin gücləndirilməsi baxımından fərqli OSI qatlarında işləyən və hər biri fərqli bir məqsəd üçün identifikasiya üçün bir çox protokol mövcuddur. Doğrulama 3-cü təbəqədən 7-ci qatadək baş verə bilər. Aşağıda geniş istifadə olunan bir neçə yüksək səviyyəli identifikasiya növləri var.

Giriş identifikasiyası - Bu tip adi istifadəçi və şifrə birləşməsindən, eləcə də captcha şəkillərindən, biometrikadan, smart kartlardan, pin nömrələrdən və s. İstifadə kimi müasir təhlükəsizlik vasitələrindən ibarətdir. Bu sistem istifadə olunan müştəri server sistemləri və veb əsaslı sistemlərdən ibarətdir. Birinci səviyyəli müdafiə.

Şəbəkə identifikasiyası - Bu növ çoxsaylı OSI qatlarında fəaliyyət göstərir və şəbəkə mənbələrinə daxil olma üçün istifadəçi şəxsiyyətini yoxlayır. Adətən əməliyyat sistemi şəbəkə sürücüsü və protokol yığını köməyi ilə bu işi görür. Məsələn, bir istifadəçi bir payı təsdiqlədikdə və bağlandıqdan sonra o seans üçün yenidən etimadnaməsi tələb olunmur.

IP identifikasiyası - Bu metod aşağı şəbəkə qatlarında işləyir və ilk növbədə mənbəyi və təyinat IP məlumatlarını təsdiqləmək üçün istifadə olunur. Buna əsas IPSec və ya Kerberos təhlükəsizlik modullarından istifadə etməklə və ya bəzi hallarda açıq açar kriptoqrafiyasından istifadə etməklə əldə edilir.

Uzaqdan identifikasiya - Bu növ, məlumat ötürülməsi üçün bir-birinə məlumat verən uzaq kompüter sistemləri arasında identifikasiya üçün istifadə olunur. Adətən virtual özəl şəbəkələr (VPN) bu identifikasiyadan istifadə edir və PAP və ya CHAP protokollarından istifadə edə bilər.

HTTP ünsiyyət üçün əsas protokol olduğu internet dünyasında tətbiq və sessiya təbəqəsinin təhlükəsizliyi əsas yer tutur. Veb portalların müxtəlif identifikasiya mexanizmlərindən də istifadə etdiyini qeyd etmək vacibdir. Aşağıda geniş istifadə olunan bir neçə standart növ var.

Basic Authentication - Bu tip Base-64 kodlanmış aydın mətn parollarından istifadə edir. Bu, ümumiyyətlə veb serverlərin əksəriyyəti üçün standart metoddur.

Digest - Bu növ əsasa bənzəyir, ancaq şifrələr qaralama üsullarından istifadə edərək şifrələnir.

Forma əsaslanan - Bu üsulda, HTTP protokolunun POST əmri, HTML şəklindəki məlumatları server tərəfindəki qəbuledici veb səhifəyə təqdim etmək üçün istifadə olunur. Forma əsaslı identifikasiya düz HTTP kanalında və ya qorunan SSL kanalında baş verə bilər.

NTLM - Bu nəqliyyat qatında və sessiya qatında işləyən bir Microsoft mülkiyyət protokoludur və HTTP protokolu tərəfindən veb portallar üçün identifikasiyanı həyata keçirmək üçün bir vasitə kimi istifadə edilə bilər. Onun əsas istifadəsi pəncərələr və ya pəncərədən kənar müştərilər arasında identifikasiyanı həyata keçirməkdir.

Müştəri sertifikatları - SSL bir veb hosting serverinin şəxsiyyətini təsdiqləmək üçün istifadə edilsə də, müştəri sertifikatı həmin veb sayta daxil olan istifadəçi üçün eyni şeyi edir. Adətən bir müştəri sertifikatı bahalı smart kartları və ya etibarlı informasiyanı dəyişdirmək üçün iqtisadi vasitə kimi istifadə olunur. Müştəri sertifikatları SSL və ya TLS protokolu üzərində həyata keçirilir və problemə cavab vermə prosesində iştirak etmək üçün brauzer dəstəyinə ehtiyac duyulur.

Əvvəllər qeyd edildiyi kimi, identifikasiya prosesi bir proqram tətbiqi və ya sisteminin təmin edilməsində vacib bir komponentdir. Beləliklə, identifikasiya prosesinin özü təmin edilməsi, hətta vacib və vacib vəzifəyə çevrilir. Bunun səbəbi, müvəffəqiyyətli bir identifikasiya sisteminə nüfuz etmənin ciddi zərər verə biləcəyi. Bir haker həssas məlumatlar əldə edə bilər və dəyərli məlumatları silə, dəyişdirə və ya poza bilər. Bundan əlavə, haker şəxsiyyət və ya pul oğurluğu kimi şəxsi ziyanla nəticələnən birinin şəxsiyyətini qəbul edə bilər. Hack edilmiş şəxsiyyət bir şəbəkə və ya server idarəçisidirsə, zərərlər təsəvvür xaricindədir.

Təhlükəsizlik nöqteyi-nəzərindən yuxarıda müzakirə etdiyimiz identifikasiya prosesinə başqa bir nəzər salaq. Şəkil 1-ə istinad edərək, prosesi həssas hala gətirə biləcək üç kritik hack nöqtəsi (qırmızı nömrələrlə qeyd olunur) var. Istifadəçi etimadnaməsini yazarkən, bunlar bir brauzer skripti və ya hücum adam tərəfindən

əldə edilə bilər. Eynilə, etimadnamələr tel üzərindən ötürüldükdə, bunları orta hücumda olan bir adam tuta bilər. Nəhayət, etimadnamələr bazadakı girişlərlə müqayisə edildikdə, uğurlu bir nüfuz əldə etmək üçün dəyişdirilə bilər. Bu, paket toplamaq və paket hazırlamaqdan məlumat toplamaq və idarə etmək üçün istifadə edildiyini göstərir və nəticədə autentifikasiya mexanizmini həssas vəziyyətə gətirir. İndi bir neçə identifikasiya hücum növünü ətraflı şəkildə müzakirə edək.

Bypass hücumu - İnsan təbiətinə görə, hakerlər əvvəlcə təhlükəsizliyi pozmaq istəyirlər və identifikasiya bunun istisna deyil. Adətən identifikasiya bypassının kök səbəbi ya proqram sisteminin giriş siyasətlərini tətbiq edə bilməməsi və ya zəif dizayn edilmiş identifikasiya sistemi arxitekturasıdır. Məsələn, istifadəçi etimadnaməsini istifadə edərək autentifikasiyanı həyata keçirən bir veb kodun ciddi parol siyasətini tətbiq edə biləcəyi, ancaq boş bir şifrə verə bilməməsi və bununla da ciddi boşluq yaratması müşahidə olundu. Başqa bir nümunə olaraq, tez-tez inkişaf etdiricilər qorunan və qorunmayan faylları eyni qovluğa qoyaraq səhv buraxırlar və beləliklə veb kodu görünən və həssas hala gətirirlər. Bypass hücumları, ümumiyyətlə, güclü sənaye standartlarından daha çox, xüsusi identifikasiya sistemlərinə qarşı mühakimə olunur.

Şifrələr üçün qəddar qüvvə - Bir müştəri server proqram sistemində və ya veb portallarında parollar, bu gün belə bir təhlükəsizlik pozuntusunun bir nöqtəsidir. Təcavüzkarlar sadəcə təxmin etməklə yanaşı, minlərlə istifadəçi və şifrə birləşmələri ilə bəslənən skript və xüsusi proqram təminatlarından istifadə edirlər. Bu skriptlər hack ediləcək identifikasiya sisteminə qarşı işləyir. Əvvəlcə proqrama bütün İngilis dili sözlərinin birləşməsi verilir. Buna lüğət hücumu deyilir. Bunun ardınca ədədi dəyərlər və xüsusi simvollarla birlikdə çox istifadə olunan bir istifadəçi və parol etimadnaməsi yığılmışdır. Nəhayət, artıq müxtəlif insanlar tərəfindən istifadə edilən etimadnamələrin böyük məlumat bazaları sistemə girməyə çalışılır. Fikir, etimadnamələrin hər və mümkün birləşməsini bir iş birləşməsi işləməyincə sınamaqdır. çünki təsdiqləmə sistemi tərəfindən qəbul edilir. Bu səslənsə də, əslində çox mükəmməl bir iş olsa da, inkişaf etmiş hesablama gücü və şəbəkə genişliyi ilə,

identifikasiya mexanizmlərinə çatmaq daha asan oldu. Müasir təcavüzkarlar, fasilə vaxtını daha da azaltmaq üçün göy qurşağı masaları adlanan etimadnamə qablarından istifadə edirlər.

Sessiya qulaq asma - Doğrulama prosesi iki sistem arasındakı problem və cavabı ehtiva etdiyindən, etimadnamələr tel üzərindən keçir. Bir hacker bir paket ələ keçirmə vasitələrini yerləşdirə bilər və qurbanı şəxsiyyət məlumatlarını istifadə etməsini gözləyə bilər. Doğrulama prosesi davam edərkən, haker sessiyaları pozur və oradan etimad məlumatını deşifr edir. Məsələn, veb sayt SSL-dən çox olmayan sadə HTML formaları identifikasiyasından istifadə edərsə, asanlıqla ələ keçirilə bilən sadə aydın mətn parollarından istifadə edə bilər. İnkişaf etmiş bir formada, hacker sessiya ələ keçirmə hücumundan istifadə edə bilər, bunun nəticəsində təsdiqləmə prosesinin təsdiqlənməsi kimi alınan etibarlı əlamət ələ keçirilir və sessiyanı ələ keçirmək üçün istifadə olunur. Bundan sonra haker qurbanı təqlid etməklə sonrakı hərəkətləri edə bilər.

Təkrar hücum - Bu tip, sessiyanı ələ keçirməkdən bir qədər fərqlənən haker sadəcə müvəffəqiyyətli identifikasiyanın məlumatlarını qeyd edir və serverə və ya doğrulayıcıya yeni sorğu açır. Bu yeni tələblə yanaşı, hacker qeydə alınmış məlumatları saxta eyniləşdirmək və şəxsiyyətini dəyişdirmək üçün istifadə edir və bununla da zərərçəkən kimi eyni hüquqlara və çıxışlara sahib olur.

Cookie kəsişməsi - Bildiyimiz kimi istifadəçilərin etimadnamələrini daxil etmələrini tələb edən veb portallar, tez-tez istifadəçinin brauzerində saxlanan cookies-lərə etibar edirlər. Çərəzlərin zərərsiz bir məlumat parçası olduğu ehtimal edilsə də, bəzən hakerlər tərəfindən istifadə olunur. Bir çox saytlarda veb gəzən təcrübələri, ünvanları, ekranın mövzusu rəngləri və s. Kimi istifadəçi üstünlükləri saxlanılır, tez-tez istifadəçinin identifikasiyası əlaməti də çərəzlərdə saxlanılır. Bu mö'cüzə, istifadəçinin sistemə uğurlu girişinin nəticəsidir. Cookie-lər brauzerlər tərəfindən hər bir veb sorğuda veb serverlərə təqdim olunur və hackerlər tərəfindən tutuldu və ya brauzer tərəfində bir Trojan istifadə olunur. Doğrulama simvolu məlumatı

pozulduqdan sonra təcavüzkar onu qurbanı təqlid etmək və sonrakı hərəkətləri həyata keçirmək üçün istifadə edə bilər.

Doğrulama şəxsiyyəti - Keçmişdə orta hücumda olan bir kişinin gizli təbiətinə görə aşkarlamaq çox çətin olduğunu öyrəndik. Qabaqcıl bir hacker ortada bir adam ola bilər və şəbəkədə öz identifikasiya sistemini qura bilər və əvvəllər öyrəndiklərimizdən İP ləkələmək və digər üsullardan istifadə edərək trafiki yönləndirə bilər. Bir əlaqə quran və etimadnaməsini göndərməyə çalışan hər hansı bir qurban, bu məlumatı hakerə aşkar etməklə başa çatır. Bu tip hücumu həyata keçirmək bir qədər çətin olsa da, daxili narazı bir işçi üçün asanlıqla mümkündür.

Reflection hücum - Bu çox inkişaf etmiş bir hücum növüdür və mütləq veb texnologiyası ilə məhdudlaşmır. Xüsusi bir problem cavab proqramı identifikasiya sistemində zəifliklərdən istifadə etməyə çalışır. Haker əvvəlcə qurbanla əlaqə qurmağa başlayır. Qurban normal bir proses olaraq identifikasiya üçün hakerə müraciət edir. Bu vəziyyətdə haker, qurbanla yeni bir əlaqə açır və öz problemini göndərir. Yenidən normal bir identifikasiya prosesi olaraq hədəf ona etibarlı bir cavab ilə geri cavab verir. Haker bu cavabı ələ keçirir və ilk başlanan əlaqəyə göndərir. Çağırış və cavab tədbirləri həm qurbanın etibarlı identifikasiya parametrləri siyahısına düşdüyündən, bu hücumun qurbanı olur. Bu hücum nadir hallarda real həyatda istifadə olunur, ancaq zəif açar şifrələmə şifrələri üçün çox yaygındır.

Keylogger hücumu - Bu, arxa planda səssiz oturan və bütün tuş vuruşlarını qeyd edən bir istifadəçinin maşınlarına Trojan göndərildiyi məlum bir növüdür. Daha sonra veb saytdakı URL-lərin əldə edildiyi və daxil edilmiş sənədlər barədə bir hesabat yaradır və bu hesabatı səssizcə e-poçt vasitəsilə hakerə göndərir. Gizli rejimdə işləyən bir çox müasir casus, bir keylogger ehtiva edir. Adətən casuslar istifadəçinin baxış təcrübəsini aşkar etmək üçün düymələr yığırlar, lakin şifrələrin oğurlanmamasına zəmanət yoxdur.

Server tərəfi identifikasiyası hücumları - İndiyə qədər müştəri və tel üzərindəki hücumlar haqqında danışdıq. Bir veb server və ya LDAP server identifikasiyası həyata keçirərkən, təhlükəsizlik problemləri də ola bilər. Adətən, hakerlər bütün

etimad məlumat bazasını daha da aşkarlayacaq əsas identifikasiya serverinə daxil olmaq üçün inzibatçı şifrəsini oğurlamağa cəhd göstərəcəklər. İn-in-the-orta hücumlar tez-tez məlumatları açmaq və kök sisteminə giriş əldə etmək üçün istifadə olunur. Server tərəfi hücumları, adətən gizli limanları açan bir skript və ya serverdə quraşdırılmış bir Trojan ilə başlayır. Bundan sonra haker tələb olunan məlumatları əldə etmək üçün serverdəki əmrləri işlətmək üçün həmin limanlardan istifadə edir. Bu gün də müasir veb saytlar SQL əsaslı identifikasiyasından və ya SQL-dən etibarlılığı təsdiqləyən sənəd olaraq istifadə edən LDAP identifikasiyasından, və həssas olduğu aşkar edilir. Zərərli veb sorğuları və ya yalnış bir veb server istifadə edərək zərərli skript işlətmək, bu seriyanın veb hack məqaləsində öyrəndiyimiz kimi SQL məlumatlarının oğurlanmasına səbəb ola bilər. Bu vacib serverlərə güzəştə getmək kütləvi informasiya və məlumat oğurluğuna səbəb ola bilər.

FOSS sistemlərini qorumaq Doğrulama hücumlarını aşkarlamaq və həll etmək çətin olsa da, hər şəbəkə rəhbərinin öz infrastrukturlarında tətbiq etməli olduğu bir neçə profilaktik mexanizm var. Texnologiya menecmenti baxımından, hack nöqtələri üçün daha az sahə buraxdığına görə, çoxaltmaqdan daha çox bir şirkət üçün vahid identifikasiya sisteminin olması tövsiyə olunur. Texniki baxımdan istifadəçilərin şəxsiyyətini təsdiqləmək və üçün istifadə edilə bilən çox amil identifikasiya növlərini göstərən cədvələ baxıla bilər.

Qəti və mürəkkəb bir parol sxemindən istifadə, ümumiyyətlə, birinci müdafiə xəttidir. Şifrə müddəti və siyasət kilidi siyasəti də çox vacibdir. Mərkəzləşdirilmiş sistemdə saxlanılan şifrələrin şifrələnməsi zəruridir. Bütün bu yollar əl ilə və ya proqramlı bir qəddar güc şifrə hücumundan qorunmağa kömək edir. Doğrulama bir çox tərəfdən hack edilə bildiyindən, sistemləri identifikasiya bypass hücumundan qoruyan identifikasiya sisteminin dizaynını düzgün arxivləşdirmək və nəzarət etmək lazımdır. IPSec və Kerberos istifadə sessiyanın oğurlanması və qaçırılmasının qarşısını almağa kömək edə bilər. Sessiya əlamətlərindən və ya vaxt möhürləmə istəklərindən istifadə və vaxt ştamplarına əsaslanan səhv işləmə kimi fəndlər identifikasiya təkrar hücumuna qarşı riskləri azaltmağa kömək edə bilər.

Şəbəkə qatında, Linux FOSS sistemləri qaynaq ünvanı yoxlanışı adlanan daxili bir xüsusiyyət ilə gəlir. Bu açıldıqda daxili şəbəkədən gələn kimi görünən paketləri atmağa başlayan, lakin əslində olmayan bir kernel xüsusiyyətidir. Ubuntu və CentOS və s. Kimi son ləpələrin əksəriyyəti bunu dəstəkləyir, amma Linux distro dəstəyiniz yoxdursa, onu təkmilləşdirməyin vaxtıdır. Bu, ümumiyyətlə, hakerlər tərəfindən autentifikasiya hücumlarına nail olmaq üçün istifadə edilən paket ləkələmə şanslarını azaltmaq üçün bir addım atmağa kömək edir. "Nospoof on" əlavə etmək üçün hosts.conf faylı dəyişdirmək, başqa bir müdafiə səviyyəsidir. Sözsüz ki, sağlam və avtomatik açıq mənbəli təhlükəsizlik yama sistemi və antivirus yerləşdirilməsi vacibdir.Kiberhücumlardan 100 faiz qorunma yoxdur. Bununla birlikdə, yeni təhdidlər barədə daim məlumat vermək və təhlükəsizlik strategiyanızı şübhə altına almaqla riskləri çox azalda bilərsiniz.

2.4.5.1. Sıfır günlük istismar və hücumların artması

Effektiv kiber təhlükəsizlik təhlükəsizliyi strategiyasının formalaşdırılmasının bir hissəsi təşkilatınıza təsir edə biləcək təhdidləri başa düşmək deməkdir. Mürəkkəblik və təhlükə ilə böyüyən və davamlı inkişaf edən təhdidin bir növü, sıfır günlük istismar olaraq da adlandırılan sıfır günlük bir hücumdur. Bu zərərli hücumların adı, üçüncü tərəfin istismarından bəri neçə gün keçdiyindən və ya bir şirkətin təhlükəsizlik məsələsini həll etmək imkanın olmadığına aiddir. Bunun bariz nümunəsi, gündə bir hücum üçün həssas olan yeni proqram təminatının çıxarılmasıdır, çünki potensial problemlərin həllinə vaxt qalmamışdır.

Başqa bir misal, bir istifadəçi antivirus proqramı quraşdırdıqda. Ümumiyyətlə, proqram, sistemin qorunması üçün yeniləmələri tələb edən proqramın köhnə / əsas versiyasıdır. Bir sıfır günlük hücum / istismar, bir son hücum kitabxanasında yeniləmədiyi üçün bir kiberhücumçu sistemə güzəştə getdikdə baş verir. Ayrıca hardware özü haqqında da düşünə bilərsiniz; quraşdırılmış qorunması olmayan yeni bir kompüter, lazımi qaydada yenilənməyincə istismarın istənilən formasına

həssasdır. Tipik olaraq, sıfır günlük təhdidləri təyin etmək üçün üç ümumi yol vardır:

Sıfır günlük hücumlar: Bu, üçüncü tərəfin proqram təminatındakı zəifliklərdən istifadə edərkən baş verir. RansomWare buna misaldır. Sıfır günlük istismar: Sıfır günlük hücum və ya sıfır günlük hücum nəticəsində yaranan istismar Sıfır gün zəifliyi: İstismarçı hücum yaratmaq üçün günahkarlar tərəfindən aşkar olunan zəiflik. Bunlar təsəvvür etmək üçün rahat ssenarilər deyil. Daha böyük bir miqyasda, bir istismar şəbəkəni daha da istismar üçün açıq buraxdığından bir işə və onun infrastrukturuna ziyan vururlar. Bundan əlavə, sıfır günlük hücumlar müntəzəm olaraq bir müəssisəni qoruyub saxlaya bilər və daha çox zərər verə bilər (bunun səbəbi, bir iş sonradan daxil olacağımız hücumun qarşısını almaq əvəzinə 'reaksiya verməli' olur). Müvafiq cavab strategiyası olmadan, iş vaxtı zəmanət verilir. Kibertəhlükəsizliyin yaxşı strategiyası reaktiv yox, fəal yanaşma ehtiva etdiyindən bir təşkilat “arxadan işləməlidir”. Başqa sözlə, lazımi müdafiəyə sahib olmaq əvəzinə yeni bir təhlükəsizlik yamağı yaratmaq üçün vəsait və vaxt xərcləməlidirlər.

Necə olur?

Faydalı, aktiv strategiyaların hazırlanmasının bir hissəsi bu hücumların necə baş verdiyini anlamaqdır. Üçüncü tərəflər sistemlərə infiltrasiya etmək üçün bir sıra texnikalar tətbiq edirlər və biz sıfır günlük istismarın necə inkişaf etdiyinə dair kontekst təmin etmək üçün qısa şəkildə keçəcəyik. Təhlil və Hücum Testi - İlkin mərhələdə günahkarlar proqramda zəiflikləri tapmağa çalışırlar. Bunun üçün mənbə kodunu müşahidə edərək proqramın dərin təhlili tələb olunur və adətən mövzu (proqram mühəndisliyi kimi) barədə geniş bilik tələb olunur. Üçüncü tərəflər bunu həyata keçirmək üçün müxtəlif üsullar tətbiq edəcəklər və çox vaxt qeyri-adi davranışların aşkarlandığı yerlər olur.

Fuzz təhlili - Hücum testinə bənzər, fuzz testi, günahkar bir sistemə təsadüfi dəyərlər tətbiq edərək zəiflik tapmağa çalışdıqda baş verir. Proses tez-tez avtomatlaşdırılmış və ya alət köməyi ilə həyata keçirilir. Üçüncü tərəfin hücumunda müvəffəq olma şansı daha yüksək olarsa, bu nə qədər uzun olar. Yaratma - Zərərli tərəf uyğun giriş

nöqtələrini və ya zəifliklərini aşkar etdikdən sonra, sıfır günlük istismar yaradılır. Hücumlar üçün hazırlanan zərərli proqram çox vaxt olduqca mürəkkəb və aşkar etmək çətindir. Bu nöqtədə, sıfır günlük bir müdaxilənin qarşısını almaq çətindir. İcra və yerləşdirmə

- Zərərli proqramın hazırlanmasından sonra hədəf sisteminə çatdırılır. Mürəkkəblikdən asılı olaraq, bəzi təşkilatlar kritik sistemlərə güzəştə getməyincə təsirləndiklərini bilmirlər.

Heç bir iş kiber təhlükəsizlik təhlükəsi qarşısında çarəsiz hiss etmək istəmir. Xoşbəxtlikdən, bu halların baş verəcəyi təqdirdə sizin və təşkilatınızın atacağı bir neçə addım var . Bu vacibdir, çünki bütün sıfır günlük istismar bir şirkətin infrastrukturu səbəbindən baş vermir. Biznesiniz tərəfindən istifadə olunan hər hansı bir proqram, proqram və ya modul müvafiq qaydada yamansa həssasdır. Məsələn, şirkətinizin universal rabitə proqramlarından istifadə etdiyini düşünün. Bu platforma hədəfləmək üçün bir işçi girişi kimi istifadəçi məlumatlarını oğurlamaq istəyən zərərli proqram forması yaradılmışdır. Proqram təminatçısı bunun üçün düzəltmədiyini və sıfır günlük hücum baş verdiyini söylədi. Geliştirici problemi yamayanadək, proqram ya istifadə edilə bilməz və ya təhlükəli hücumlara qarşı həssas qalır.Bu məsələlərlə mübarizə aparmaq üçün, sıfır günlük hücumlarla qarşılaşdıqda bir neçə üsul lazımdır.

Ətraflı Monitorinq

Sıfır günlük bir istismarın erkən aşkarlanması üçün potensial bir həll monitorinqdir . Monitorinq bir ifadədir, lakin ümumiyyətlə proqram təminatı və şəbəkə infrastrukturunu əhatə edir. Məqsəd, gələn şəbəkə trafiki və ya bir tətbiqin davranışındakı dəyişikliklər kimi qeyri-adi davranışları müəyyənləşdirmək və bayraq etməkdir. Tez-tez müəssisə, infrastrukturu onlar üçün unikal olduğundan, monitorinq metodlarını inkişaf etdirməlidir. İdeya gələcəkdə qarşısını almaq üçün işləyərkən aşkarlanması üçün sıfır günlük hücumları xarakterizə etməkdir.

Davranışa əsaslanan aşkarlama

Yuxarıda göstərildiyi kimi, davranışa əsaslanan aşkarlama ilə sıfır günlük istismarın aşkarlanması bir proqram platforması ilə əlaqəli qeyri-adi hərəkətlərin

müəyyənləşdirilməsini əhatə edir. Buraya bir tətbiq və onun fayllarla qarşılıqlı əlaqəsi daxildir. Fikir bu davranışın zərərli olub olmadığına dair nəticə çıxarmaqdır.

AI əsaslı monitorinq / aşkarlama

Gündəlik istismarları aşkarlamağa çalışarkən təşkilatlar çoxsaylı problemlərlə üzləşdikləri üçün AI əsaslı monitorinq başqa faydalı bir həlldir. AI və ona cavab verən alqoritmlər, şübhəsiz ki, sıfır günlük hücumlarla qəribə davranış meyllərini effektiv şəkildə aşkar etməyin yeganə yollarından biridir. Hücumun aşkarlanması, qeyri-adi proqram davranışını xarakterizə etməyi tələb etdiyindən, AI monitorinqi bunu effektiv şəkildə həyata keçirə bilən yeganə tətbiqlərdən biridir.

Kadr təhsili və maarifləndirmə

Bir çox kibertəhlükəsizlik strategiyasında olduğu kimi, işçilərin ən yüksək səviyyədə məlumatlandırılması vacibdir. Komanda üzvlərinin - İT-dən idarəetmə səviyyəsinə qədər maarifləndirmə, sıfır günlük hücumlar və istismarların vurduğu ziyanı azaltmağa kömək edəcək başqa bir əsas yoldur. Sıfır günlük hücumlar baş verərsə, işçilər Yedəkləmə və Kəşf Bərpa (BDR) siyasətlərini dərindən dərk etməlidirlər. Bundan əlavə, sıfır günlük bir hücumun nə olduğunu və nəyin mənasını verdiyinə dair kurs biliklərinə sahib olmalıdırlar. Potensial müdaxilələrin və məlumat itkisinin qarşısını almağa kömək edəcək təlimatlar təyin edin.

Reaktiv Yeniləmə

Sıfır günlük bir hücum aşkar edildikdən sonra ən yüksək səviyyədə bir qətnamə əldə edilir. Bunun bir inkişaf etdiricidən ən yeni yamaq yüklənməsindən və ya daxili bir qətnamə əldə edilməsindən asılı olmayaraq, problemi həll etmək daha da kəsilmənin qarşısını alır. Ən son anti-malware proqramı ilə önləyici metodlar qurmaq da vacibdir, çünki onlar sizin ilkin müdafiə xəttinizdir [7].

Sıfır günlük istismar və hücumlar, hər hansı bir işə, təşkilata və müəssisəyə təsir edə biləcək nüanslı müasir təhdidlərdir. Çox vaxt müasir infrastruktura hücum edə bilərlər. Bir şəbəkə tərəfindən idarə olunan hər şey hücum üçün həssasdır. Sıfır günlük istismar zərərli proqramının bəzi formaları, Stuxnet virusu (kiber silah kimi təsnif edilə bilmək üçün kifayət qədər təhlükəlidir) kimi mürəkkəb tərəflər tərəfindən

hazırlanmışdır. Kiçikdən orta ölçülü bir işin Stuxnet kimi mürəkkəb bir şeyə qarşı çıxması çətin olsa da, hazır olmaq üçün pul ödəyir. Ransomware kimi xərcləmələr bir təşkilatın infrastrukturuna düzəlməz zərər verə bilər və nəticədə həddindən artıq maliyyə ziyanına səbəb olur.

Polimorf hücumların artması

2.4.5.2. Polimorfik zərərli proqramin tərifi

Polimorfik zərərli proqram aşkarlanmamaq üçün tanımlanan xüsusiyyətlərini daim dəyişdirən zərərli bir proqram növüdür. Zərərli proqramların çox yayılmış formaları viruslar, qurdlar, botlar, troyanlar və ya keyloggerlər də daxil olmaqla polimorf ola bilər. Zərərli proqramı bir çox aşkaretmə texnikasına tanınmaz hala gətirmək üçün polimorfik üsullar, fayl adları və növləri və ya şifrələmə açarları kimi tez-tez dəyişdirilə bilən xarakteristikaları özündə cəmləşdirir.

Polimorfizm antivirus proqramı kimi təhlükəsizlik həllərinə etibar edilən nümunə uyğunluğu aşkarlanmasının qarşısını almaq üçün istifadə olunur. Polimorfik zərərli proqramların müəyyən xüsusiyyətləri dəyişsə də, funksional məqsədi eyni qalır. Məsələn, polimorf virus aşkarlanmamaq üçün imzası dəyişsə belə cihazları yaymağa və yoluxdurmağa davam edəcəkdir. Yeni bir imza yaratmaq üçün xüsusiyyətləri dəyişdirərək, imza əsaslı aşkaretmə həlləri faylı zərərli olaraq tanımayacaqdır. Yeni imza müəyyən edilərək antivirus həllərinin imza bazasına əlavə olunsa da, polimorf zərərli proqram aşkar olunmadan imzaları dəyişdirməyə və hücumlar etməyə davam edə bilər.

2.4.5.3. Polimorfik zərərli proqramlarin nümunələri

Webroot tədqiqatçıları aşkarladılar ki, zərərli proqram infeksiyalarının 97% -i polimorf üsullardan istifadə edir . Bu taktikalardan bəziləri 1990-cı illərdən bəri davam edərkən, son on ildə təcavüzkar polimorfik zərərli proqramların yeni dalğası meydana çıxdı. Polimorfik zərərli proqramların bəzi yüksək profilli nümunələrinə aşağıdakılar daxildir:

- Fırtına Worm E-poçtu: 2007-ci ildə "Avropada fırtına əsən kimi 230 ölü" başlığı ilə göndərilən məşhur spam e-poçt, bir anda bütün qlobal zərərli

proqram infeksiyalarının 8% -i üçün cavabdeh idi. Mesajın əlavəsi açıldıqda, zərərli proqram qəbuledicinin kompüterinə wincom32 xidməti və troyan quraşdırır və onu bot halına gətirir. Fırtına qurdunun ənənəvi antivirus proqramı ilə aşkarlanmasının o qədər çətin olduğunun səbəblərindən biri, hər 30 dəqiqədə və ya bir dəfə istifadə olunan zərərli kod idi.

- CryptoWall Ransomware: CryptoWall, qurbanın kompüterindəki faylları şifrələyən və açılması üçün bir fidyə ödəməsini tələb edən polimorf bir fidyə proqramıdır. Cryptowall'da istifadə olunan polimorf inşaatçı, hər potensial qurban üçün mahiyyətcə yeni bir variantı hazırlamaq üçün istifadə olunur.

2.4.5.4. Polimorf zərərli proqramin yaratdiği təhlükə

Artıq bir çox zərərli proqram suşları polimorfik imkanlara malikdir, zərərli proqramı güzəştə getmədən əvvəl dayandırmaq və dayandırmaqda ənənəvi antivirus həllərini təsirsiz edir. İllər boyu zərərli proqramların qorunmasına dair adi müdriklik antivirus, firewall və IPS kimi profilaktik həllərə sərmayə qoymaqdır. Bununla birlikdə, bu həllər polimorfik zərərli proqramlara qarşı işləmir. Bu gün demək olar ki, bütün uğurlu hücumlarda bəzi polimorfik texnikalardan istifadə olunması, şirkətinizin bu həllərə güvəndiyi təqdirdə özünüzü hücuma açıq buraxdığınız deməkdir.

Hazırda Gartner , müəssisənin infosec xərcləməsinin 90% qarşısının alınması və 10% aşkarlama olduğunu təxmin edir. Bununla birlikdə, bu profilaktik mərkəzli yanaşma ilə müəyyən məhdudiyyətlər mövcuddur və xüsusilə polimorf zərərli proqram vəziyyətində bir çox profilaktik nəzarət vasitəsi zərərli fəaliyyətləri dayandıra bilmir.

2.4.5.5. Polimorf zərərli proqramlardan qorunmaq üçün ən yaxşi təcrübələr

Polimorfik zərərli proqramlardan qorunmaq, insanları, prosesləri və texnologiyanı birləşdirən müəssisə təhlükəsizliyinə layiqli bir yanaşma tələb edir. Zərərli proqramların qorunması üçün ən yaxşı təcrübələrdən tutmuş davranışa əsaslanan təsbit üçün ixtisaslaşmış həll yollarına qədər polimorfik zərərli proqramların qorunması üçün bir sıra ən yaxşı təcrübələr mövcuddur. Polimorf zərərli proqramlardan qorunmaq üçün bir neçə əsas tövsiyə:

- Proqramınızı bu günə qədər qoruyun: Zərərli proqram infeksiyalarının qarşısını almağa kömək edən sadə bir yol, şirkətinizin istifadə etdiyi müxtəlif tətbiqetmələr və proqram vasitələrini saxlamaqdır. Microsoft, Oracle və Adobe kimi müəssisə proqram istehsalçıları məlum zəifliklər üçün kritik təhlükəsizlik yamaları olan proqram yeniləmələrini müntəzəm olaraq buraxırlar. Təhlükəsizlik köhnəlmiş proqramları ilə köhnəlmiş bir proqram işlətmək, şirkətinizi müxtəlif zərərli proqram infeksiyalarına səbəb ola biləcək istismarlara açıq buraxır.
- Şübhəli bağlantıları və ya əlavələri vurmayın: phishing e-poçtları və ya digər istənməyən elektron rabitə zərərli proqramları yaymaq üçün istifadə olunan zərərli bağlantıları və ya əlavələri ehtiva edə bilər. Son istifadəçilərə şübhəli bağlantıları və əlavələri necə tanımaq barədə məlumat vermək, zərərli proqram hücumları üçün bu ümumi giriş vektorunu azaltmağa kömək edə bilər.
- Güclü şifrələrdən istifadə edin və onları müntəzəm olaraq dəyişdirin: Hesablarınızın etibarlı və bənzərsiz şifrələrlə qorunmasını təmin etmək zərərli proqramların qorunması üçün daha yaxşı bir tətbiqdir. Təhlükəsiz şifrələr haqqında son istifadəçiləri öyrədin və lazım olduqda çox faktorlu identifikasiya və ya etibarlı parol menecerləri kimi xüsusiyyətlərdən istifadə edin.
- Leverage Davranışlı Təsbit Alətləri: Polimorfik zərərli proqram ənənəvi antivirus alətləri tərəfindən aşkarlanmadan yayınmaq üçün yaradıldığından, bu təhlükə üçün ən yaxşı həllər inkişaf etmiş, davranışa əsaslanan aşkarlama metodlarından istifadə edir. Son nöqtə aşkarlanması və cavab və ya inkişaf etmiş təhdid qorunması kimi davranışa əsaslanan həll həllər, məlumatlarınızdan hər hansı birinə güzəştə getmədən əvvəl real vaxtda təhdidləri təyin edə bilər. Davranışa əsaslanan zərərli proqram təminatı , polimorfik hücumlarla mübarizə aparan ənənəvi imza əsaslı metodlardan daha doğrudur .

Polimorf zərərli programların yüksəlişi

Anti-malware proqramları bir imza istifadə edərək zərərli proqramları aşkarlayır. Zərərli proqramların əksəriyyəti anti-malware proqramlarını aşkar etməyə imkan verən unikal markerlərdən, kod nümunələrindən ibarətdir. Təcavüzkarlar, polimorfik zərərli proqram kimi yeni zərərli proqram növləri ilə gündəmə gələn zərərli proqram və anti-malware proqramları arasındakı funksionallıqdan xəbərdar oldular. Bu yeni növ zərərli proqram ənənəvi antivirus proqramı zərərli proqramı aşkar etmədən dayandırır.Polimorfik zərərli proqram, aşkarlanmadan qaçmaq üçün hər dəfə yerinə yetirildiyi zaman orijinal formasından dönə bilmə qabiliyyəti ilə hazırlanmış koddur. Unikal, dəyişən xüsusiyyətlərinə, fayl adları, növləri və ya şifrələmə açarları daxildir ki, zərərli proqram tanımadığı hala gətirilsin. Polimorfik zərərli proqramların tərkibinə daima dəyişən viruslar, qurdlar, troyanlar və ya casus proqramlar daxil ola bilər.Zərərli proqram işə salındıqda kod şifrələnir və icra edilməzdən əvvəl orijinal koduna baxılmır. Kodun görünüşü hər bir icra ilə dəyişsə də, funksiya vahid olaraq qalır. Məsələn, polimorfik bir casus proqram istifadəçinin şəxsi məlumatlarını əldə etməyə və təcavüz edənə göndərməyə davam edəcəkdir.Son bir neçə ildə polimorf viruslar təcavüzkarlar tərəfindən yayılan əsas zərərli proqramdır. Tədqiqatçılar aşkar etdilər ki, zərərli vasitələrin 97% -i polimorfik zərərli proqramlardan istifadə etməklə sərbəst buraxılır. 2007-ci ildə spam e-poçtu, Storm Worm Email, təxminən 8% qlobal zərərli proqram hücumlarının açarı oldu. E-poçt istifadəçi tərəfindən açıldıqda, istifadəçinin kompüterinə trojan quraşdırıldı və nəticədə bot oldu. Bu zərərli proqram, təxminən hər otuz dəqiqədə çevrilmə qabiliyyətinə görə aşkar etmək çətindi.Webroot hesabatına görə, polimorfizm 2016-cı ilin tendensiyalarından biri idi və Webroot tərəfindən aşkar edilən zərərli proqramların 94% -i yalnız bir dəfə görüldü. Polimorfik zərərli proqramlara qarşı mübarizə aparmaq üçün təşkilatlar şəbəkədəki bütün proqram və tətbiqləri yeniləməlidir. Sərbəst buraxılan təhlükəsizlik yamaları, təcavüzkarlar tərəfindən zərərli məqsədlər üçün istifadə edilə bilən və zəif olanları bağlamaq üçün vacibdir.Bütün işçilər ən yaxşı təhlükəsizlik praktikaları ilə bağlı mütəmadi olaraq təhsil almalıdırlar. Son istifadəçilər şübhəli bağlantıları və qoşmaları necə tanıya biləcəyini bilməli, beləliklə hücum şansını azaldır. Təcavüzkarlar eyni

zamanda çox faktorlu identifikasiya ilə güclü və etibarlı parollardan istifadə etməli və şifrələrini müntəzəm olaraq dəyişdirməlidirlər. Zərərli proqramlardan qorunmanın adi vasitələri polimorfik zərərli proqramlara qarşı təsirsiz hala gəlir. Antivirus, firewall və IPS kimi müdafiə ilə yanaşı, təşkilatlar davranışa əsaslanan aşkarlama vasitələrindən istifadə etməlidirlər.Polimorfik zərərli proqramların kod nümunələrini dəyişdirmək qabiliyyətinə görə və ənənəvi vasitələrin qarşısını almaq mümkün olduğu üçün davranışa əsaslanan aşkarlama həlli ən yaxşı yanaşmadır. Adi imza əsaslı metodlardan daha dəqiq olma qabiliyyətinə malikdir. Son nöqtə aşkarlanması və cavab vermə və ya inkişaf etmiş təhdid qorunması, məlumatları pozulmadan əvvəl zərərli proqramları aşkar edərək real vaxt rejimində təhlükələri təyin edə biləcək davranışa əsaslanan bir təsbitdir.

2.4.6. Kiber həhlükəsizlik problemləri

Kiber təhlükəsizlik ilə bağlı problemlər, köhnəlmiş proqram təminatından tutmuş, liderlik qruplarının dəstəyi olmaması kimi geniş miqyaslı mübarizələrə qədər ola bilər. Kiberhücumlar bu gün bir-biri ilə əlaqəli dünyanın ortaq bir xüsusiyyətinə çevrilib. Bir çox təşkilat məlumat əməliyyatlarını onlayn rejimə keçirdikcə, hücumların da həcmi artdı. 2016-cı ildən 2017-ci ilə qədər bildirilən hadisələrin ümumi sayı təxminən iki dəfə artdı və bu, bildirilməmiş hücumların sayını nəzərə almır. Bundan da pisi, bu hücumların çoxu özlərini müdafiə etmək üçün heç bir vasitə və ya strategiyaya sahib olmayan kiçik müəssisələri hədəf aldı.İşdə kibertəhlükəsizlik problemləri ilə məşğul olan şirkətlərin üzləşdikləri bir neçə həll yolu ilə qarşılaşdıqları bəzi problemlər.

2.4.6.1. Hədəf olduğunuzu tanımaq

Kiçik təşkilatlar həmişə aktivlərinin və məlumatlarının kiber cinayətkarlar üçün cəlbedici olduğunu həmişə dərk etmirlər. "Müasir iqtisadiyyatımızda, əksər şirkətlərdə təcavüzkarların istədikləri şeylər var - məlumat və pul. Kiber təhdidlərin həyəcan verici sürətlə irəlilədiyi heç kimə sirr deyil. Sosial mühəndislikdən, zərərli proqramlardan, sıfır günlük hücumlardan və ya DDoS hücumlarından asılı olmayaraq hər bir təşkilat - ölçüsündən və sənayesindən asılı olmayaraq risk altındadır. Müəssisə

səviyyəli təşkilatların bu irəliləyən təhdidləri azaltmaq üçün lazım olan mənbələrə sahib olmasına baxmayaraq, kiçik müəssisələr və başlanğıclar eyni zamanda məlumat pozuntusu və ya təhlükəsizlik hadisəsi ilə üzləşə biləcək dərəcədə eyni olduqlarını qəbul etməlidirlər. Hansı sənayedə olmağınızdan asılı olmayaraq, oğurlanacaq həssas aktivlər var. Qorunan sağlamlıq məlumatları, ödəmə kartı məlumatları, Sosial Təminat Nömrələri, doğum tarixi, telefon nömrələri, e-poçt ünvanları, təsdiq nömrələri, səyahət mükafatları nömrələri - zərərli hakerlər bunu istəyirlər və hansı sahədə olduğuna və ya olduğuna görə ayrı-seçkilik etməyəcəklər.Ancaq başlıqlarda müəssisə səviyyəli təşkilatların məlumat pozuntularını tez-tez gördüyümüz üçün kiçik və orta sahibkarlığın kiberhücumlar üçün hədəf olmadığını düşünmək asan ola bilər. Bu həqiqətdən daha da irəli gedə bilməz. Başlanğıc və kiçik müəssisələrin sahib olduğu aktivlər əhəmiyyətli dərəcədə fərqli ola bilsə də, bir çox kiber təhdid eyni qalır. Məsələn, bir şirkətin beş işçisi və ya 500 işçisi olmasından asılı olmayaraq bir məlumatın pozulmasına səbəb olan bir işçinin təhdidi hələ də iş yerlərini azaltmaq məcburiyyətindədir. Eynilə, zəif şifrələr, təsirsiz mobil cihaz siyasəti, həssas POS sistemləri və anlaşılmaz kiber təhlükəsizlik təhlükələri kimi şeylər bütün növ müəssisələrin məlumat pozuntusuna və ya təhlükəsizlik hadisəsinə məruz qalmasına səbəb ola bilər.

2.4.6.2. Kiber təhlükəsizlik qrupları tərəfindən maliyyələşdirilmir

"Onların şirkətləri miqyaslı kimi, fəal təhdidlər idarə heyəti və uyğunluq tələblərinə təlim arasında, bu overwhelmed almaq üçün kiber təhlükəsizlik komanda üçün asan," Andrew Douthwaite da CTO deyir VirtualArmour . "Yüksək təhsilli kiber təhlükəsizlik mütəxəssisləri üçün sıx bazar bu məsələdə kömək etmir."Douthwite deyir ki, bir çox kiber təhlükəsizlik qrupları günlərinin çoxunu yanğın söndürməklə keçir, gələcək strategiyalarını fəal inkişaf etdirmək və komanda üzvlərinə rəhbərlik etmək üçün az vaxt ayırır [25]. İrəliyə baxmağınız üçün vaxt və ya mənbələr olmadan, kiber təhlükəsizlik mütəxəssisləri uzun müddət təhlükəsizliyinə fayda gətirəcək tədbirlər görmək üçün mübarizə apara bilərlər.

2.4.6.3. Təhlükəsizlik yamaqları

"Müxtəlif təşkilatlara rəhbərlik etdiyim 100% zəiflik qiymətləndirməsindən, həmişə avadanlıqlarında olmayan adətən istifadəçi iş stansiyaları və noutbuklardakı təhlükəsizlik yamaları var" dedi Parney Cyber Solutions MMC-nin baş direktoru və kiber təhlükəsizlik üzrə ekspert Courtney Jackson. Cekson –un bildirdiyinə görə "Kiçik bir məsələ kimi görünə bilər, amma belə deyil".Təhlükəsizlik yamaları müəyyən edilmiş zəiflikləri aradan qaldırmaq üçün dərc olunur. Yeni təhlükəsizlik yamalarının quraşdırılmasının gecikməsi təşkilatların aktivlərini risk altına qoyur. Laks e-poçt təhlükəsizliyi

Raske bildirir: "Şübhəsiz ki, ransomware hər ölçüdə təşkilatların qarşılaşdığı ən böyük təhdidlərdən biridir". Bu günlərdə hər kəs hazır ransomware alıb öz hücumlarını həyata keçirə bilər.Raske, 2019 Verizon Məlumat Qəzasının Təhlili Hesabatlarının nəticələrinə istinad edir ki, ransomware zərərli şirkətlərin 24 faizini təşkil edir və bütün zərərli proqramların 90 faizi e-poçt vasitəsilə şəbəkələrə verilir.Bir şirkətin e-poçt təhlükəsizlik strategiyasını qulaqardına vurması olduqca ağılsız görünür, ancaq Raske bunun düşündüyünüzdən daha tez-tez baş verdiyini söyləyir.Təhlükənin qarşısını almaq üçün əsas e-poçt müştərilərində gördüyünüz ümumi e-poçt spam filtri kifayət deyil. E-poçt filtrləri zərərli mesajları dayandırmaq üçün inkişaf edir, lakin kibercinayətkarlar cihazlarda və şəbəkələrdə zərərli proqramları işə salmaq üçün əlavələrdən istifadə etməyə başladılar "dedi.Bir gündə bir təşkilata, içərisinə və içərisinə gedən e-poçtların daha çox həcmini nəzərə alsaq, bu zərər vermə şansı yüksək olan bir problem sahəsidir. "Sadə bir Microsoft Office makrosu bütün şəbəkəni ləğv edə bilər. Zərərli proqramın 40 faizindən çoxu əlavə olaraq göndərilir. "

2.4.6.4. "Ehtiyat planı" nı itirmək

360 şirkətin baş direktoru Marius Nel: "Əksər şirkətlər kiber təhlükəsizlik təşəbbüsünün bir hissəsi olaraq yedəkləmə sənədlərini görmürlər". O izah edir ki, insanlar tez-tez məlumatlarını qorumaq üçün sistemlərə və ya xidmətlərə güvənirlər və ardıcıl olaraq yedəkləməyi müvəffəqiyyətsiz olaraq etibarlı olaraq yedəkləməyi

unuturlar.Nel bildirir: "Sistem bütün digər xidmətlərin nəticədə uğursuz olacağını və yedəkləmə tələb olunacağını düşünən şəkildə qurulmalıdır".Bu yaxınlarda vurulan Baltimore City ransomware hücumunu edin, Həmid deyir. Fidyə vermədən və ya şifrəni açmaqdansa, məlumatlar əbədi olaraq silinir. Böyüməkdə olan xarici ehtiyat nüsxəsi *çox* vacibdir, lakin tez-tez diqqətdən kənarda qalır. "Həmid deyir ki, ransomware bütün bazarda var. “Müəssisələr bunu müştərilərindən və cəmiyyətdən gizlətmək üçün əllərindən gələni edirlər. Ancaq sonrakı qarışıqlığı təmizləyən komandadan gəldikdə sizə deyə bilərəm ki, əksər insanların düşündüklərindən daha çox yayılmışdır. "

2.4.6.5. BYOD Təhlükəsizlik

Douthwaite görə öz cihaz siyasətinizi bir çox şirkətdə məşhurdur. BYOD, işçiləri işlərini asanlaşdırmaq üçün ofisdə və ya uzaqdan işləmək üçün öz maşınlarından istifadə etməyə imkan verir. Ancaq bir çox müəssisə rəhbərləri bir BYOD mühitinin təşkilatlarına dəvət edə biləcəyi unikal təhlükələri qiymətləndirmirlər.Bir neçə ümumi mənada addımlar iş şəbəkələrini BYOD ilə əlaqəli təhdidlərdən daha yaxşı qoruya bilər.Bu tədbirlərdən bəziləri, iki faktorlu identifikasiyanı təmin edən və bütün cihazların davamlı olaraq yenilənməsini təmin etmək üçün şəbəkə girmə nəzarətini təmin edən rol əsaslı giriş ola bilər. Douthwite, güclü işçi şifrələrini tələb etməyi və şirkət məlumatlarını köhnə işçi cihazlarını təmizləmək üçün bir çıxış prosesinin olmasının da vacib olduğunu söylədi.

BYOD VoIP abunə

BYOD ifadəsinin başqa bir ümumi istifadəsi VoIP sənayesinə bağlıdır və bu ifadə VoIP abunə və ya planının müəyyən bir növünü təsvir etmək üçün istifadə olunur. VoIP xidmətinə qoşulduqda öz VoIP qurğusuna (SIP- qapalı cihaz) sahib olan abunəçilər BYOD-dan istifadə etdikləri zaman daha ucuz abunə planlarından yararlana biləcəklər - lakin bütün VoIP xidmət təminatçıları üçün xüsusi tarif planları təklif etmirlər .Öz avadanlıqları olan abunəçilər. BYOD abunəsi VoIP provayderi vasitəsi ilə mümkün deyilsə, özünüzün əvəzinə provayderin avadanlıqlarından istifadə etməlisiniz.

2.4.6.6. Korporativ təhlükəsizlik proqramının olmaması

Təhlükəsizliyə gəldikdə şirkətlərin qarşılaşdıqları təəccüblü bir məsələ rəsmi bir korporativ təhlükəsizlik proqramının olmamasıdır. "Hər bir şirkət, ölçüsündən asılı olmayaraq, məqbul istifadə, hadisələrə reaksiya, fiziki təhlükəsizlik və ən azı daha çox sahəni açıqlayan korporativ təhlükəsizlik siyasətinə sahib olmalıdır."Kiber təhlükəsizliyə bu fəal yanaşmanın bir çox müəssisənin əskiksiz tərkib hissəsidir.Orta bir iş icraçısının, iş yerlərində təsirli bir kiber təhlükəsizlik proqramının olmamasının, onları hücum və ya məlumat pozma riski altına aldığını başa düşülməlidir.

2.4.6.7. Kiber təhlükəsizliyə maliyyə problemi əvəzinə bir İT problemi kimi baxın

Bir çox müəssisə rəhbərləri hələ də kiber təhlükəsizliyə bir İT problemi kimi yanaşırlar, bu günlərdə, həqiqətən, alt xətt haqqında. "Kiber təhlükəsizlik hücumlarının əsas səbəbi maliyyə məsələsidir" Douthwite deyir. "Məlumatlar bir məlumat pozuntusunun orta dəyəri təxminən 4 milyon dollar olduğunu göstərir."Nel deyir ki, güclü kibertəhlükəsizliyi olan şirkətlər bunu işin hər tərəfinə qarışdıraraq "həyat tərzi" olaraq qəbul etdiklərini öyrəndilər. "Əslində, strateji düşüncə və davamlı taktiki hərəkətləri tələb edən bir iş riskini azaltma məşqidir."Bu işçilərin təlimini tələb edir. Nel deyir ki, son kiber təhlükəsizlik mövzusunda son istifadəçiləri öyrətmək bir təşkilatı qorumağın ən təsirli və ucuz yoludur.

2.4.6.8. Lövhədə təmsilçiliyin olmaması

Kennyhertz Perry, MMC-nin kiber təhlükəsizlik üzrə vəkili Braden Perry görə, bir çox şirkətin biznes prosesləri üçün *çox* möhkəm siyasət və prosedurlar var.Bu, inkişaf etmiş idarə heyəti üzvlərinin başa düşə biləcəyi bir şeydir. Ancaq İT bir iş adamı üçün fərqli bir dildir və təəssüf ki, idarə heyəti üzvlərinin əksəriyyəti bu məsələlərə məhəl qoymur və ya təxirə salır.

Perry, informasiya təhlükəsizliyi üçün inanılmaz, proaktiv bir planı olan bir iş IT şöbəsinin, resurs üzvləri və kiber təhdidləri başa düşmədikləri üçün lazım olan dəstəkləri əsla ala bilməyəcəyini söyləyir.

"İdarə heyətinin İT dilini biznesə və əksinə tərcümə etmək üçün təcrübəli bir İT və ya kiber təhlükəsizlik əlaqəsinə sahib olması daha vacib və demək olar ki vacibdir"

deyərək Perry bir problemi araşdırmaq üçün işə götürüldükdə, ümumiyyətlə bu İT şöbəsi və yüksək rəhbərlik arasında daha yaxşı rabitə olsaydı, işi öz həll edə bilərdi.

2.4.6.9. DDoS hücumları

Paylanmış xidmətdən imtina (DDoS) hücumları son bir neçə ildə kiber cinayətkarlığın ən məşhur formalarından birinə çevrildi. Onların tezliyində artdıqları şübhə doğurmasa da (2018 hadisələrin sayına görə yeni bir rekord vuracaq), DDoS hücumları, əsas saytları ələ keçirməyi bacardıqları zaman sıçrayışlı başlıqları düzəldir , hətta bir neçə nəfərə bunu edə bilsələr də. Dəqiqə. Bir DDoS hücumunun məqsədi, nəticədə çökənə qədər bir giriş tələbi ilə bir serveri çox yükləməkdir. Bu hücumlar ümumiyyətlə "botnetlər", zərərli proqram təminatı ilə yoluxmuş və bir hədəfə giriş sorğuları göndərmək üçün bir haker tərəfindən yönəldilmiş kompüterlər tərəfindən asanlaşdırılır. DDoS hücumlarının daha yeni, daha intensiv formaları “yadda saxlama, "Giriş sorğularını artırmaq üçün və terabaytdan çox trafikə sahib saytları su altında qorumaq üçün açıq qorunmayan, açıq mənbəli obyekt yaddaş sistemlərindən istifadə edir.

2.4.6.10. Zərərli proqram

Kiberhücumun klassik forması, zərərli proqram müxtəlif üsullarla bir sistemə daxil edilə bilər. E-poçt qoşmaları, proqram yükləmələri və əməliyyat sisteminin zəifliyi zərərli proqramların ən çox yayılmış mənbələridir. Quraşdırıldıqdan sonra, zərərli proqram qanuni koda qoşularaq digər sistemlərə yayılaraq özünü gizlədir. Zərərli proqramın məqsədi ümumiyyətlə kompüterə və ya sistemə icazəsiz daxil olmaqdır. İstifadəçinin şifrələmə ilə kritik məlumatlara girməsini rədd edən bir fidyə, kilidini açmaq üçün ödənilənə qədər son illərdə bir neçə yüksək profilli kiberhücumdan məsuldur. Lakin zərərli proqramların yeni növləri, o cümlədən troyanlar, viruslar və qurdlar, həm təşkilat, həm də şəxsləri təhdid etmək üçün davamlı olaraq ortaya çıxır.

2.4.6.11. Phishing Dolandırıcıları

Yaşlı bir fırıldaqçı, phishing hücumlarının rəqəmsal bir versiyası istifadəçiləri şəxsi məlumatlarını bölüşmək üçün bir yola salan linkə vurmağa inandırmaq üçün psixoloji manipulyasiya və aldatmağın müxtəlif formalarından istifadə edən e-poçt

mesajlarından ibarətdir. Müasir phishing mesajları inanılmaz dərəcədə mürəkkəbdir, əksər hallarda qanuni, etibarlı şirkətlərin elektron poçtları kimi təqdim olunur. Əksər internet istifadəçilərinin bu cür istəklərdən xüsusilə ehtiyatlı olduqlarını bildikləri halda, 2016 Verizon hesabatı , insanların adi bir marketinq e-poçtundan daha çox bir фишинг e-poçtunu vurma ehtimalının daha yüksək olduğunu açıqladı .

2.4.6.12. Daxili sui-istifadə

Hətta ən yaxşı kibertəhlükəsizlik tədbirləri işçilərin istifadə imtiyazlarından sui-istifadə etmək qərarı verdikdə təsirsiz ola bilər. Təhlükəsiz məlumatları açıq mənbələrə sızdıran insanlar bu cür sui-istifadə hallarının ən yeni nümunəsi ola bilərsə də, işçilərin bununla əlaqəli heç bir planı olmadan sadəcə həyati əhəmiyyətli məlumatları və məlumatları götürmələri daha yaygındır. Son araşdırmalar işçilərin 85 faizinin şəxsən yaratdıqları sənədləri və ya məlumatları, 30 faizi isə yaratmadığı məlumatları götürdüklərini müəyyən etdi. Bu məlumatlara strategiya sənədləri, müştəri məlumatları və hətta xüsusi mənbə kodu da daxil idi. Bəzən işçilər işdən çıxarılmasına cavab olaraq məlumat alarkən, onların 90 faizi bunu dayandırmaq üçün heç bir siyasət və ya texnologiya olmadığı üçün aldıqlarını bildirdi.

III FƏSİL. İnternet şəbəkəsində informasiya təhlükəsizliyinin müasir vasitələri.

3.1. İnternet şəbəkəsində infomasiya təhlükəsizliyi

Şəbəkə təhlükəsizliyi, şəbəkə trafiki də daxil olmaqla rəqəmsal aktivləri qorumaqla yanaşı, icazəsiz şəbəkə müdaxiləsinə nəzarət etmək, qarşısını almaq və cavab vermək üçün hazırlanmış alətlər, taktika və təhlükəsizlik siyasətlərini izah edən bir termindir. Şəbəkə təhlükəsizliyinə aparat və proqram texnologiyaları (fərasətli təhlükəsizlik təhlilçiləri, ovçular, hadisə cavabdehləri və s. Kimi mənbələr daxil olmaqla) daxildir və şəbəkənizi hədəfləyən potensial təhdidlərin hamısına cavab vermək üçün hazırlanmışdır.Başqa sözlə, səhv insanları həssas məlumatlarınızdan uzaqlaşdırmaq üçün istifadə etdiyiniz müdafiədir.Viruslar içəri girməyə çalışırlar,şəbəkə təhlükəsizliyi onları kənarda saxlayır. Yaxşı, bu tərif daxilində hər hansı bir şəbəkə təhlükəsizliyi strategiyasının əsasını təşkil edən üç əsas diqqət var: qorunma, aşkarlama və cavab.Mühafizə, şəbəkə müdaxiləsinin qarşısını almaq üçün hazırlanmış hər hansı bir vasitə və ya siyasəti əhatə edir. Aşkarlama, şəbəkə trafikini təhlil etməyə və zərər vermədən əvvəl problemləri tez bir zamanda müəyyən etməyə imkan verən qaynaqlara aiddir. Və nəhayət, *cavab* müəyyən edilmiş təhdidlərə reaksiya vermək və mümkün qədər tez həll etmək qabiliyyətidir.Təəssüf ki, əksər müəssisələr bunu necə düzgün edəcəyini bilmirlər. Əslində, ABŞ və Avropada 4,100 idarəçi, şöbə müdirləri, İT menecerləri və digər əsas mütəxəssislər arasında aparılan bir sorğuda məlum oldu ki , dörd təşkilatdan təxminən üçü (73 faiz) təcrübəsiz səviyyədə kiber təhlükəsizlik strategiyasını tətbiq edir. Bu artan təhlükədir, çünki şəbəkə pozuntuları baş verdikdə, məlumatların özündən daha çox təhlükə var.

3.2. İnternet şəbəkə təhlükəsizliyinin üstünlükləri

Şəbəkə təhlükəsizliyi təşkilatınızın yalnız həssas məlumatlarını deyil, ümumi fəaliyyətini, nüfuzunu və hətta işdə qalma qabiliyyətini qorumaq üçün mövcuddur. Davamlı əməliyyat qabiliyyəti və bütöv bir nüfuz effektiv şəbəkə təhlükəsizliyinin iki əsas faydasıdır [27].

Kiberhücumların qurbanı olan şirkətlər tez-tez özlərini içəridən şikəst, xidmət göstərə bilməyən və ya müştəri ehtiyaclarını səmərəli şəkildə həll edə bilməyən vəziyyətə

gətirirlər. Eynilə, şəbəkələr daxili şirkət proseslərində böyük rol oynayır və hücumlara məruz qaldıqda, bu proseslər bir təşkilatın iş aparmaq və ya hətta standart əməliyyatları davam etdirmək qabiliyyətini daha da çətinləşdirə bilər.Ancaq bəlkə daha da ziyanlı olan bir şəbəkə pozuntusunun işinizin *nüfuzuna* xələl gətirə biləcək təsiridir .Şəxsiyyət oğurluğu və şəxsi məlumatların oğurlanması ilə əlaqəli digər təhlükələrin getdikcə artdığını nəzərə alaraq, bir çox müştəri müəssisələrlə məlumat mübadiləsinə gəldikdə artıq tərəddüd edir. Kiberhücum baş verərsə, bu müştərilərin çoxu daha etibarlı alternativlərin lehinə geri çəkilə bilər.Dəyərli məlumatların itirilməsi və ya korlanması, müştəri xidmətlərinə və daxili prosesə ciddi ziyan vurmaqla yanaşı, digər zərərlər təmir olunduqdan sonra uzun müddət davam edə biləcək nüfuzlu ziyanla nəticələndi - şəbəkə təhlükəsizliyinə gəldikdə nəyin baş verdiyini görmək çətin deyil. . Əslində, SMB-lərin 66 faizinin məlumat pozuntusu yaşadıqdan sonra (müvəqqəti və ya daimi) bağlanmalı olduğu təklif edilmişdir. Və daha da böyük, daha çox qurulmuş müəssisələr əvvəlki vəziyyətlərini geri qaytara bilmirlər.Digər tərəfdən, düzgün siyasət və strategiyalarla birlikdə etibarlı şəbəkə təhlükəsizliyi proqram təminatı və kiberhücumlar baş verdikdə onların təsirinin minimum olacağını təmin edə bilər.

3.3. İnternet Şəbəkə Təhlükəsizliyi Alətləri və Texnikaları

Şəbəkəniz hər cür forma və ölçüdə təhdidlərlə üzləşir və buna görə hücumların hamısını qorumağa, müəyyən etməyə və cavab verməyə hazır olmalıdır. Ancaq reallıq budur ki, əksər şirkətlər üçün ən böyük təhlükə gecə-gündüz təhdid edən aktyorlar deyil, yaxşı maliyyələşdirilən və müəyyən səbəblərə görə xüsusi təşkilatları hədəf alan hücum edənlərdir. Bu səbəbdən, şəbəkə təhlükəsizlik strategiyanızın bu aktyorların istifadə edə biləcəyi müxtəlif üsulları həll edə bilməsi lazımdır.

3.3.1. Giriş nəzarəti

Təhdid aktyorları şəbəkənizə daxil ola bilmirsə, edə biləcəkləri zərərin miqdarı son dərəcə məhdud olacaqdır. Ancaq icazəsiz girişə mane olmaqdan əlavə, hətta *səlahiyyətli* istifadəçilərin də potensial təhdid ola biləcəyini unutmayın. Giriş nəzarəti, istifadəçi girişi və qaynaqları yalnız fərdi

istifadəçilərin vəzifələrinə birbaşa tətbiq olunan hissələrə məhdudlaşdırmaqla şəbəkənizin qorunmasını artırmağa imkan verir.

3.3.2. Antivirus proqramı

Viruslar, troyanlar, qurdlar, keylogger, casus proqram və s. Şəklində olan kompüter proqramları, kompüter sistemləri vasitəsilə yayılmaq və şəbəkələrə yoluxmaq üçün hazırlanmışdır. Anti-malware alətləri, təhlükəli proqramları müəyyənləşdirmək və yayılmasının qarşısını almaq üçün hazırlanmış bir növ şəbəkə təhlükəsizliyi proqramıdır. Anti-malware və antivirus proqramı şəbəkəyə zərərləri minimuma endirərək zərərli proqram infeksiyalarını həll etməyə kömək edə bilər.

3.3.3. Anomaliyanın aşkarlanması

Anomaliyanın tərifi "standart, normal və ya gözləniləndən fərqli olan bir şeydir." Şəbəkə sahiblərində bir anomaliyanı müəyyən etmək üçün normal və ya gözlənilən davranış anlayışı olmalıdır.Şəbəkə anomaliyası motorları şəbəkənizi analiz etməyə imkan verir ki, pozuntular baş verdikdə cavab verə bilmək üçün tez bir zamanda xəbərdar olursunuz.

3.3.4. Tətbiq təhlükəsizliyi

Bir çox təcavüzkar üçün tətbiqetmələr istismar edilə biləcək bir müdafiə zəifliyidir. Tətbiq təhlükəsizliyi şəbəkə təhlükəsizliyinizlə əlaqəli hər hansı bir tətbiq üçün təhlükəsizlik parametrlərini təyin etməyə kömək edir.

3.3.5. Məlumat itkisinin qarşısının alınması

Çox vaxt şəbəkə təhlükəsizliyindəki ən zəif əlaqə insan elementidir. DLP texnologiyaları və siyasəti işçiləri və digər istifadəçiləri həssas məlumatlardan sui-istifadə və bəlkə güzəştə getməkdən və ya deyilən məlumatları şəbəkədən kənarda saxlamağa qorumağa kömək edir.

3.3.6. E-poçt təhlükəsizliyi

DLP-də olduğu kimi, e-poçt təhlükəsizliyi insanla əlaqəli təhlükəsizlik zəifliklərini artırmağa yönəldilmişdir. Fişinq strategiyaları ilə (tez-tez çox mürəkkəb və inandırıcıdır), təcavüzkarlar e-poçt alıcılarını həssas məlumatları

bölüşməyə və ya səhvən hədəf şəbəkəyə zərərli proqram yükləməyə inandırırlar. E-poçt təhlükəsizliyi təhlükəli e-poçtları tanımağa kömək edir və hücumların qarşısını almaq və həyati əhəmiyyətli məlumatların paylaşılmasının qarşısını almaq üçün də istifadə edilə bilər.

3.3.7. Son nöqtə təhlükəsizliyi

İş dünyası getdikcə öz cihazınızı şəxsi və iş kompüter cihazları arasındakı fərq demək olar ki, mövcud olmayan nöqtəyə gətirir. Təəssüf ki, bəzən istifadəçilər iş şəbəkələrinə girmək üçün etibar etdikləri zaman fərdi qurğular hədəf olur. Son nöqtə təhlükəsizliyi uzaq qurğular və iş şəbəkələri arasında müdafiə qatını əlavə edir.

3.3.8. Firewalls

Firewalls şəbəkəniz və internet arasındakı sərhədləri qorumaq üçün istifadə edilə bilən qapılar kimi çox işləyir. Firewall şəbəkə trafikini idarə etmək üçün istifadə olunur, icazəsiz trafikə girişi maneə törədərkən səlahiyyətli trafikə imkan verir.

3.3.9. İntrüzsiyanın qarşısının alınması sistemləri

İntruziya qarşısının alınması sistemləri (müdaxilənin aşkarlanması da deyilir) şəbəkələrin trafikini / paketlərini daim araşdırır və təhlil edir ki, hücumlar tez müəyyənləşdirilib cavab verə bilsin. Bu sistemlər təhdidləri dərhal tanımaq üçün tez-tez məlum hücum metodlarının məlumat bazasını saxlayır.

3.3.10. Şəbəkəseqmenti

Şəbəkə trafikinin bir çox növü var, bunların hər biri fərqli təhlükəsizlik riskləri ilə əlaqələndirilir. Şəbəkə seqmenti, şübhəli mənbələrdən trafikə məhdudiyyət qoyarkən, düzgün trafikə doğru giriş imkanı verir.

3.3.11. Təhlükəsizlik məlumatları və hadisələrin idarə edilməsi

Bəzən sadəcə çox sayda müxtəlif vasitə və mənbələrdən düzgün məlumatları bir yerə **toplamaq** olduqca çətin ola bilər - xüsusən vaxt problem olduqda. SIEM alətləri və proqramları respondentlərə tez bir zamanda hərəkət etmələri üçün lazım olan məlumatları verir.

3.3.12. Virtual özəl şəbəkə (VPN)

VPN alətləri etibarlı şəbəkələr və son nöqtə cihazı arasındakı əlaqəni təsdiqləmək üçün istifadə olunur. Uzaqdan girişli VPN-lər, digər tərəflərin qulaq asmağına mane olmaq üçün şifrəli bir xətt yaradaraq identifikasiya üçün IPsec və ya Secure Sockets Layer (SSL) istifadə edir.

3.3.13. Veb təhlükəsizliyi

alətlər, aparatlar, siyasətlər və daha çox şeylər daxil olmaqla, veb təhlükəsizlik daxili şəbəkəyə qoşulduqda təhlükəsiz internet istifadəsini təmin etmək üçün müəssisələrin həyata keçirdiyi şəbəkə təhlükəsizlik tədbirlərini təsvir etmək üçün ədalətli bir müddətdir. Bu, veb-əsaslı təhdidlərin, şəbəkəyə daxil olmaq üçün giriş nöqtələri kimi istifadə edilməsinin qarşısını almağa kömək edir.

3.3.14. Simsiz təhlükəsizlik

Ümumiyyətlə, simsiz şəbəkələr ənənəvi şəbəkələrə nisbətən daha az etibarlıdır. Beləliklə, təhlükə iştirakçılarının əldə etməmələrini təmin etmək üçün ciddi simsiz təhlükəsizlik tədbirləri lazımdır.

3.4. İnternet şəbəkəsində kiberhücuma qarşı effektiv mübarizə aparma üsualları

3.4.1. Proqnozlaşdırma təhlili

Kiberhücuma qarşı effektiv mübarizə aparmaq üçün İT işçiləri hücumun nəyə bənzədiyini, baş vermə ehtimalı və haradan gəldiyini bilməlidirlər. Maşın öyrənməsi ilə idarə olunan proqnozlaşdırıcı analitik proqram məlum kiberhücumlar haqqında çoxlu məlumat toplaya bilər və nəticələrini mövcud təhlükəsizlik protokollarına tətbiq edə bilər. Bu, aktiv DDoS azaldılması üçün xüsusilə faydalıdır, çünki bu, kibertəhlükəsizlik sistemlərinə təhdidləri müəyyənləşdirməyə və sistemin aşılmazdan əvvəl trafikin yönləndirilməsi üçün aktiv tədbirlər görməyə imkan verir. Sürətli cavab müddəti kiberhücumların ən pis təsirinin qarşısını almaq üçün vacibdir. Bir pozuntu nə qədər uzun müddət aşkarlanmasa, məsələn, hər ölçüdə şirkətlər üçün baha ola biləcək daha çox məlumat güzəşt ediləcəkdir. Proqnozlaşdırıcı analitik uzaq əl

qruplarını verə bilər Hack hücumlarına qarşı fəal mübarizə aparmaq lazım olduqları əvvəlcədən xəbərdarlıq.

3.4.2. Tənqidi məlumatların ehtiyat nüsxəsini çıxarın

DDoS və ransomware hücumları halında, şirkətlərin məlumatların ehtiyat planının yerində olması vacibdir. Missiya kritik məlumatlarına çıxış əldə etmək, sistemlərin və xidmətlərin minimum iş vaxtı ilə tez bir zamanda geri qaytarılması və fəlakətli bir server çatışmazlığı ilə fərq arasındadır. Tez-tez həyati əhəmiyyətli məlumatları və aktivləri ayrıca və daha çox kənarda saxlayan sistemdə saxlayan hərtərəfli ehtiyat strategiyası ilə şirkətlər uzunmüddətli iş vaxtına səbəb olan kiberhücum riskinin qarşısını ala bilər. Məlumat mərkəzləri kibertəhlükəsizliyin və fiziki təhlükəsizliyin bir çox təbəqəsi ilə gücləndirilmiş geniş ehtiyat həll yollarını təmin edə bilər.

3.4.3. SLA təminatları

Bir çox təşkilat İT infrastrukturunu və ya məlumat əməliyyatlarını üçüncü tərəf şirkətlərinə verir. Bu, xərcləri və maddi-texniki yükü azalda bilər, eyni zamanda üçüncü tərəfin təhdidlərdən qorunmaq üçün eyni səviyyədə kibertəhlükəsizlik tədbirləri olmadıqda məlumatların məruz qalma riskini də təqdim edir. Bu problemin qarşısını almaq üçün şirkətlər, münasibətlərdə iştirak edən bütün tərəflərin təhlükəsizlik öhdəliklərini təmin etmək üçün xidmət səviyyələri razılaşmalarından (SLA) istifadə etməlidirlər. SLA bir kiberhücumun qarşısını ala bilməsə də, üçüncü tərəf təminatçılarının müəyyən təhlükəsizlik standartlarına riayət etməmələri və ya uyğunsuzluq üçün ciddi maliyyə nəticələrinin olması barədə hüquqi təminat verir.

3.4.4. Kiber Sığorta

Hacking bir çox sahələrdə qəbul edilən bir risk halına gəldikdə, bir çox şirkət, potensial maliyyə itkisindən qorumaq üçün sığorta planları alaraq cavab verdi. Kiber sığorta bazarının 2025-ci ilə qədər 20 milyard dollara qədər artacağı gözlənilir. Yalnız daha ümumi biznes planlarına əlavə edilən bir seçimdən sonra müstəqil kiber sığorta sığortası o qədər populyarlaşdı ki, bir çox yeni sığortaçılar bu bazara kapital qoymaq üçün bazara daxil olurlar. Uyğunluq qanunlarına görə sağlam təhlükəsizlik tədbirlərini həyata keçirməkdə çətinlik çəkən səhiyyə kimi sahələr üçün sığorta sürətli

şəkildə şirkətləri öz sistemlərindəki və ya təchizatçı və tərəfdaşlarından olan kiberhücumlardan qorumaq üçün zərurətə çevrilir [26].

3.4.5. "Bug Bounties"

Proqram kodundakı zəifliklərin müəyyən edilməsi yorucu və vaxt aparan bir proses ola bilər. Bir çox təşkilat, proqramları hakerlər tərəfindən istismar edilə bilən hər bir səhv və ya boşluğu aşkar etmək üçün zəruri olan ciddi araşdırmaya tabe etmək üçün resurslara sahib deyildir. Son illərdə, şirkətlər "səhv lütfü" proqramları vasitəsilə bu vəzifədən kənar olmaq qərarına gəldilər. Bu proqramlar, yaxşı niyyətli hakerləri həssaslıqlar və səhvlər üçün veb əsaslı proqramı ləkələməyə, təsdiqlənmiş səhvlər aşkar edildikdə nağd ödəmə təmin etməyə təşviq edir. Həm özəl şirkətlər, həm də dövlət qurumları proqram təminatlarını inkişaf etdirməyə kömək etmək üçün "səhv lütfü" siyasətini həyata keçirirlər.

3.4.6. Təlim və maarifləndirmə

Bir çox məlumat pozuntusu, şəbəkə sistemlərinə zərərli proqram təqdim edən fırıldaqçıların nəticəsidir. Fırıldaqçılar tərəfindən istifadə edilən son taktikalarla bağlı işçilərə maarifləndirmə, zərərli proqramlara məruz qalan bağlantıları vurma ehtimalını azaltmağa kömək edə bilər. Şirkət məlumatlarını düzgün idarə etməyi izah edən əsas məlumat təhlükəsizliyi siyasətinin həyata keçirilməsi daxili sui-istifadə təhlükəsini azaltmaq üçün də vacibdir. Təşkilatlar ilk növbədə həssas məlumatlara kimin girişi ilə bağlı daha ciddi olmalıdırlar. Bu strategiyalar insan səhvlərinin kiber təhlükəsizlik tədbirlərinə təsirini xeyli azalda bilər .Kiberhücumlar bu gün təşkilatlar üçün ciddi bir təhlükə olaraq qalsa da, məlumatların qorunması və xidmət müddətinin artırılması üçün səyləri artıra biləcək bir neçə həll yolu var. Ən son riskləri nəzərə alaraq şirkətlər həm özlərini, həm də müştərilərini zərərli məlumat pozuntularından və digər təhlükələrdən qorumaq üçün daha effektiv kiber təhlükəsizlik strategiyaları həyata keçirə bilərlər.

Bu gün çox sayda məlumat fərdi və ya işləyən kompüterlərdən istifadə edilməklə işlənir, buna görə kompüter sistemlərinə hücumlar çox yayılmışdır. Hər il aktiv internet istifadəçilərinin sayı eksponent olaraq artır və bu səbəbdən şəbəkədə

işləyərkən təhlükəsizlik problemi daha da aktuallaşır. Təəssüf ki, internetdən istifadə zamanı kompüter təhlükəsizliyinin əsasları barədə istifadəçi məlumatları şəbəkənin inkişafı tempi və təhlükəsizlik təhdidlərinin uçqun kimi böyüməsindən geri qalır. Bu təhdidlərə aşağıdakılar daxildir: zərərli proqramlar (viruslar), İnternet saxtakarlığı; xidmət hücumlarının rədd edilməsi; pul oğurluğu; şəxsiyyət oğurluğu; informasiya mənbələrinə və sistemlərinə icazəsiz giriş; bilərəkdən yalan məlumatların yayılması. Bundan əlavə, İnternet istifadəçisinin məlumat təhlükəsizliyinə əsas təhdidləri, səlahiyyətli istifadəçilərdən və elektron məruz qalma üsullarından irəli gəldiyini bilirsiniz. Səlahiyyətli istifadəçilərdən: Hakerlər tərəfindən məlumatları bilərəkdən zədələmək və ya oğurlamaq. Ehtiyatsız hərəkətlər nəticəsində yaranan məlumatların pozulması. Elektron təsir üsulları: Kompüter virusları Spam Phishing İnternet üzərindən yayılan müxtəlif zərərli proqramların təhlükəsizlik təsirlərini nəzərdən keçirək. Zərərli proqram məlumatı çıxarmaq, təhrif etmək, silmək və ya dəyişdirməklə kompüterin, məlumatın və ya kompüter şəbəkəsinin sahibinə (ziyan). Microsoft Corporation təfsiri ilə "zərərli proqram" (zərərli proqram "zərərli proqram" üçün qısa) termini ümumiyyətlə tək bir kompüterə, serverə və ya kompüter şəbəkəsinə ziyan vurmaq üçün xüsusi olaraq hazırlanmış hər hansı bir proqram üçün ümumi qəbul edilmiş müddət kimi istifadə olunur. Bir virus, casus proqram və ya bu kimi şeylər olsun. Zərər növünə görə zərərli proqramlar bir neçə kateqoriyaya bölünə bilər. Zərərli proqramlar: sistemin işinə mane olur; kompüter resurslarını azaltmaq; məlumatlarla icazəsiz hərəkətlər etmək; istifadəçinin kompüterlə işini pozmaq. Yoluxmuş bir kompüterin işinə maneələr müxtəlif zərərli hərəkətlər ola bilər: CD-ROM tepsisini açmaqdan və bağlamadan başlayaraq məlumatların məhv edilməsi və aparat çatışmazlığı ilə bitənədək; müalicəsini çətinləşdirmək üçün antivirus saytlarının, antivirus proqramlarının və əməliyyat sisteminin inzibati funksiyalarının bloklanması kompüter tərəfindən idarə olunan istehsal proseslərinin təxribatı (tanınmış Stuxnet qurdu bunu etdi). Tez-tez, yoluxmuş bir fayl digər zərərli proqramları quraşdırır: şəbəkədən başqa bir daha zərərli proqramı yükləyib onu çıxartmaq və ya zərərli kod artıq faylın içərisindədir (damcı), çox vaxt zərərli

proqram kompüterin demək olar ki, bütün resurslarını tutur. Məlumatlarla icazəsiz hərəkətlərə aşağıdakılar daxildir: oğurluq, fırıldaqçılıq, qəsb və istifadəçiyə casusluq. Oğurluq üçün, sabit disk taramasından, tuş vuruşlarının qeydindən (Keylogger) istifadə edə bilərsiniz və istifadəçini tam olaraq orijinal mənbələri təkrarlayan saxta saytlara yönləndirə bilərsiniz. Dəyər və ya gizli məlumatların oğurlanması, müxtəlif xidmətlərin (e-poçt, təcili mesajlaşmalar, oyun serverləri, ödəniş sistemləri) hesablarının oğurlanması. Hesablar spam göndərmək üçün istifadə olunur və e-poçt vasitəsi ilə digər hesablardan şifrələr əldə edə bilərsiniz, virtual oyun əmlakı MMOG-da satıla bilər (Massively multiplayer online oyun). Zərərli proqram kompüterin kilidlənməsinə, şantaj və vəsaitin qəsb edilməsi üçün istifadəçi sənədlərinin şifrələnməsinə səbəb olur. Çox vaxt ödənişdən sonra kompüter ya kilidini açmayacaq və ya tezliklə ikinci dəfə kilidlənəcəkdir. Zərərli proqram telefon modulundan kibercinayətkarlar tərəfindən qeydə alınmış pullu nömrələrə bahalı zənglər etmək üçün istifadə edir və bu da telefon ödəmələrində xeyli miqdara səbəb olur. Məsələn, antivirusu təqlid edən, lakin heç bir faydası olmayan (saxtakarlıq proqramı və ya qorxudan proqram) ödənişli bir proqram yaratmaq mümkündür. Zərərli proqramlar digər qeyri-qanuni işləri də həyata keçirir: kompüterin özünün və ya onun vasitəsi ilə daxil olan üçüncü mənbələrin icazəsiz daxil olması, o cümlədən birbaşa kompüter nəzarəti (arxa adlandırılan yer), açıq vpn tunellərinin və kompüterdə ictimai proxy serverlərin təşkili. Yoluxmuş bir kompüter (botnetin bir hissəsi kimi) DDoS hücumlarını həyata keçirmək, e-poçt ünvanlarını toplamaq və spam yaymaq üçün istifadə edilə bilər bir botnetin bir hissəsi kimi. Bu cür fəaliyyətlər, həmçinin elektron səsvermənin yekunlaşdırılması, reklam pankartlarına basmaq; Bitcoin ödəmə sisteminin sikkələrini əmələ gətirir və hətta 25-ci çərçivənin bir insana zombi etmək effektindən istifadə edir [27]. Rootkit (rootkit, ingiliscə kök dəstindən, yəni "kök dəsti") - təcavüzkarın və ya zərərli proqramın izlərini gözdən yayınmaq üçün gizlətmək üçün hazırlanmış bir proqram və ya proqramlar. Ransomware (İngilis dilindən. Ransom - fidyə və proqram - proqram) bir ransomware kimi işləyən zərərli bir proqramdır. Botnet (robot və şəbəkədən doğulmuş Botnet) - çalışan botlarla

işləyən bir sıra sahiblərdən ibarət olan kompüter şəbəkəsidir - bağımsız bir proqramdır. Çox vaxt bir botnetin bir hissəsi olan bir qurbanın kompüterinə gizli quraşdırılmış və təcavüzkarın yoluxmuş kompüterin mənbələrindən istifadə edərək müəyyən hərəkətlər etməsinə imkan verən bir proqramdır. İstənməyən proqram, həqiqətən zərərli olmayan, lakin əsasən istənməyən sənədlər yaza bilər: yumorlu proqram, yəni istifadəçini narahat edən hər şeyi edir. Məsələn, Adware proqramı reklamları göstərir və Spyware proqramı istifadəçi tərəfindən icazəsiz məlumatları İnternet vasitəsilə göndərir. Sənədlərin "zəhərlənməsi" deyilən bir şey yaradılır, onları açan pozucu proqram yaradılır (məsələn, ölçüsü meqabaytdan az olan bir arxiv bir çox giqabayt məlumatı ehtiva edə bilər və onu çıxartdıqda arxivçi uzun müddət dondura bilər və ya hətta sərt disk daşması). Uzaqdan idarəetmə proqramları həm kompüterlə problemləri uzaqdan həll etmək üçün, həm də zərərli məqsədlər üçün istifadə edilə bilər. Bəzən öz "həyat dəstəyi" üçün zərərli proqram əlavə yardım proqramları quraşdırır: IRC müştəriləri, proqram yönləndiriciləri, açıq klaviatura ələ keçirmə kitabxanaları. Bu cür proqram zərərli deyil, lakin bununla birlikdə antiviruslar tərəfindən təyin olunan daha zərərli bir proqram quraşdırılıb. Hətta belə olur ki, yalnız bir skriptli skript zərərlidir, proqramın qalan hissəsi qanunidir. Zərərli proqramın yayılma metoduna görə təsnifatı: istismar, bu cür məlumatlarla işləyən bir proqram tərəfindən səhv qəbul edilən nəzəri cəhətdən zərərsiz məlumatlar toplusudur (məsələn, bir görüntü faylı və ya şəbəkə paketi). Burada zərər verən bir fayl deyil, bir səhv ilə proqramın uyğunsuz davranışı. İstismar da deyilənlər "zəhərlənmiş" məlumatlar yaratmaq üçün proqramlardır; bir proqramda məntiqi bir bomba müəyyən bir şərt altında tetiklenir, faydalı bir daşıyıcı proqram üçün ayrılmazdır; Trojan'ın öz yetişdirmə mexanizmi yoxdur; Kompüter virusu bir kompüter içində və çıxarıla bilən disklər vasitəsilə yayılır. İstifadəçinin özü yoluxmuş faylı şəbəkəyə yüklədiyi təqdirdə yerli şəbəkə vasitəsilə çoxalma mümkündür. Viruslar eyni vaxtda yoluxmuş olan faylların növünə (fayl, skript, açılış), fayllara qoşulma üsulu ilə (saxta, müşayiət edən və mənbə sənədinin üzərində yazılanlar) və s. Bölünür; şəbəkə qurdu şəbəkədən müstəqil şəkildə yayılmağı bacarır. Bunlar IRC, poçt, istismardan istifadə edərək

çoxalanlara bölünür və s. Zərərli proqram zəncirlər yarada bilər: məsələn, bir qurbanın kompüterində bir istismardan istifadə edərək qurdun əsas orqanını (proqram kodu) İnternetdən quraşdıran bir yükləyicisi yerləşdirilir. Kompüterinizə yoluxan proqramlar haqqında daha çox məlumat üçün Kompüter viruslarına baxın. İctimai Wi-Fi-dan etibarlı istifadə Bu gün bir çoxumuz noutbuk və ya smartfonlardan istifadə edərək İnternetdən istifadə edirik. Rahatlıq üçün, bir çox ictimai yerlərdə (kafelər, barlar, otellər, ticarət mərkəzləri və hətta tramvaylar) Wi-Fi-dan istifadə etmək və hava proqnozunu asanlıqla görmək, elektron poçtları yoxlamaq və ya sosial şəbəkəyə mesaj göndərmək mümkündür. Bununla birlikdə, ictimai bir Wi-Fi şəbəkəsində bir istifadəçi bir sıra təhdidlər gözləyə bilər. Wi-Fi cihazına (dizüstü kompüter, tablet və ya smartfon) qoşulduqda, Wi-Fi şəbəkəsində məlumat ötürməyə və almağa başlayırlar. Təcavüzkar xüsusi proqramlardan istifadə edərək şəbəkə vasitəsilə müxtəlif məlumatlar toplaya bilər: hansı qurğular bağlıdır, bağlı cihazlarda ictimai mənbələr (fayllar, qovluqlar, printerlər) olub-olmadığı, bu cihazların istifadəçiləri hansı saytlara daxil olurlar. Bu proqramlardan bəzilərini (Zenmap, Inssider, WiFi Analyzer) İnternetdə asanlıqla tapmaq mümkündür. Daha ciddi bir yanaşma ilə təcavüzkarlar giriş və giriş şifrələri haqqında da məlumat əldə edə bilərlər. Wi-Fi şəbəkəsini ictimai yerlərdə istifadə edərkən aşağıdakı qaydalara əməl olunmalıdır: Məlumatlarınıza girişi dayandırın, əks halda cihaz və ondakı məlumatlar təcavüzkarlar üçün asan yırtıcı hala gələ bilər. Windows ilə işləyən bir kompüterdə, paylaşma ayarında (İdarəetmə Paneli / Şəbəkə və İnternet), fayl paylaşımını söndürün və eyni zamanda şəbəkənin digər istifadəçilərinin kompüteri tapmasına mane olur. Bir VPN istifadə edin. VPN vasitəsi ilə ictimai İnternetdən istifadə daha təhlükəsizdir (bu ixtisarlar virtual özəl şəbəkə - özəl virtual şəbəkə deməkdir). VPN, pulsuz Wi-Fi-a qoşulsa belə, trafiki sözdə təhlükəsiz şəbəkə vasitəsilə yönləndirir. Tez-tez etibarlı və ictimai şəbəkələrdən istifadə etsəniz, VPN uyğun olacaq. Bu həm pulsuz, həm də pullu, daha etibarlı xidmətlərdən istifadə etmək üçün edilə bilər. Sonuncu, məsələn, məlumat trafikinin hansı ölkələrdən keçəcəyini seçməyə imkan verir və onlar məlumat ötürmə həcmini və sürətini məhdudlaşdırmır. Avtomatik olaraq Wi-Fi

şəbəkələrinə qoşulmaq arzuolunmazdır. Müasir noutbuklar, smartfonlar və planşetlər avtomatik olaraq açıq Wi-Fi nöqtələrinə qoşula bilər, lakin bu təhlükəli ola bilər. Bir cihaz, məlumatı oğurlamaq üçün xüsusi olaraq kibercinayətkarlar tərəfindən yaradılmış şəbəkəni ala bilər. Əksər müasir mobil cihazlarda şəbəkələrə avtomatik qoşulma standart olaraq dayandırılır, ancaq "Wi-Fi Quraşdırma" bölməsində bir daha yoxlamaq üçün bir neçə saniyə sərf etmək daha yaxşıdır. SSL istifadə edin. Bir çox sayt, server və istifadəçilər arasında şifrəli məlumat mübadiləsini təmin edən SSL kriptoqrafik protokolundan istifadə edir. Hər şey avtomatik olaraq baş verir, yalnız brauzer təhlükəsizlik parametrlərində "SSL" maddəsini yoxlamaq lazımdır. Bir brauzer quraşdırarkən ümumiyyətlə bu protokol default olaraq aktivdir. İki addımlı (iki faktorlu) identifikasiyanı (saytdakı icazə) laqeyd yanaşmayın. Çox vaxt, iki addımlı identifikasiya saytın əvvəlcədən qurulmuş şifrəni, habelə istifadəçi tərəfindən daxil edilmiş mobil telefon nömrəsinə SMS ilə göndərilən kodu istəməsi ilə nəticələnir. Beləliklə, kimsə bir şifrə oğurlayırsa, başqasının hesabından istifadə etmək kifayət etmir. İki addımlı autentifikasiya bir az daha çox vaxt tələb edir, əsəbi ola bilər (İnternet banklarının əksəriyyəti bu sxemdən istifadə edir. Bəzən onu silmək istəyərsiniz, amma bunu etmək çox vaxt mümkün deyil, çünki bu saytdakı avtorizasiya üçün əsas şərtlərdən biridir). Bunun könüllü olaraq edilə biləcəyi, məsələn, poçt, video hosting, sənədlər və milyonlarla insanın istifadə etdiyi bir çox digər xidmətin qoşula biləcəyi ikiqat giriş nəzarətini aktivləşdirmək vacibdir. Google mobil nömrəni daxil etməyi təklif edəcək və hesabı telefonla bağlamaq üçün tələb olunan altı rəqəmli kodu göndərəcək. Hesab daxil olmaq istəyərkən belə bir kod hər dəfə şifrə əlavə edilməlidir. Şəbəkənin adını göstərin. Bəzən fırıldaqçılar adından əslinə bənzər bir məlumat oğurluğu şəbəkəsi yarada bilərlər. Məsələn, rəsmi THOMSON şəbəkəsinə əlavə olaraq, fərdi məlumatları oğurlamaq və mobil cihaza icazəsiz daxil olmaq üçün təcavüzkarın yaratdığı şəbəkə ola bilən "THOMPSON" u görə bilərsiniz. Kafedə aşkar edilən Wi-Fi, ən kiçik bir şübhəyə belə səbəb olarsa, mütləq qurumun işçiləri ilə əlaqə qurmalı və şəbəkələrinin nə ilə çağırılacağını yoxlamaq lazımdır. Şifrələrinizi qoruyun. Əsas və çox sadə və vacib bir qayda: fərqli

saytlarda qeydiyyata alınan hesablar üçün eyni parol qoymayın. Tənbəl olmamaq və mürəkkəb şifrələrlə qarşılaşmamaq da vacibdir: böyük və kiçik hərflər və simvollarla qarışıq olan nömrələrdən istifadə edin. Bir çox parol varsa, onda onlarda qarışıqlıq yarana bilər. Bunu etmək üçün parol menecerindən istifadə edə bilərsiniz, məsələn KeePass və ya LastPass. Bu proqramlar pulsuzdur, hər ikisi də məlumatları şifrələyir, lakin bunu fərqli yollarla edirlər: KeePass şifrəli məlumatları kompüterdə, LastPass isə bulud serverində saxlayır. Metodların hər biri öz müsbət və mənfi cəhətlərinə malikdir, lakin ümumiyyətlə hər iki xidmət yüksək səviyyədə qorunma təmin edir. "Firewall" (firewall) yandırın. Bəzi əməliyyat sistemlərində daxil olan və çıxan İnternet əlaqələrini izləyən və kompüterdən məxfi məlumatların daxil olmasına və ya göndərilməsinin qarşısını alan daxili bir təhlükəsizlik duvarı var. Bir çox firewall proqramı var - həm pullu, həm də pulsuz. Firewall mütləq təhlükəsizliyə zəmanət vermir, ancaq açılmalı olan faydalı bir qoruyucu seçimdir. Windows-da, idarəetmə panelinin Sistem və Təhlükəsizlik bölməsində aktivdir. İnternet istifadəçisinin sağlamlığına təhlükələr İnternetin həddindən artıq, nəzarətsiz və əsassız istifadəsi istifadəçilərin zehni sağlamlığına təhdid yarada bilər. İnternet istifadəçisinin psixi sağlamlığına təhdidlər: psixikaya təsiri olan məlumatların yayılmasından çox məlumat; reallıqdan uzaqlaşma. Psixoloji təhlükəsizliyin, ilk növbədə kompüter və şəbəkə texnologiyalarının istifadəçilərinin psixoloji sağlamlığının təmin edilməsinin əsas problemi məlumat (idrak) həddindən artıq yüklənməsi probleminə çevrildi. Məlumat təqdim etmək üçün hiper mətn formatının spesifikliyi, İnternet istifadəçisi üçün "hiperspekstdə oriyentasiya itkisi problemi" (İngilis dilində itkin düşmə problemi) adlanan xüsusi bir psixoloji fenomenin ortaya çıxmasına səbəb oldu. Bu psixoloji fenomen istifadəçinin veb saytın informasiya məkanında yerini müəyyənləşdirə bilməməsi, daim eyni materiallara qayıtması, lazımi məlumat üçün hara getməli olduğunu başa düşməməsi (hətta harada olduğundan şübhələnsə də) özünü göstərir. araşdırılan hiper mətn məkanında bir şey), əvvəllər baxılmış mövzulara necə qayıdacağını bilmir, axtarışının ilkin motivlərini və baxılan veb səhifələrin məzmununu və s. Hiperspansiyada oriyentasiyanın itirilməsi tez-tez

baxılan materiallar arasındakı semantik əlaqələrin itirilməsinə səbəb olur və demək olar ki, həmişə onların məzmununu həddən artıq səthi qəbul etməyə səbəb olur. İkinci, daha az əhəmiyyətli bir problem, şəbəkədə psixoloji travmaya səbəb ola biləcək və ya istifadəçini hər hansı bir qanunsuz hərəkətə təhrik edə bilən məlumatın nəzarətsiz yayılmasıdır. Bu problemləri həll etmək üçün müxtəlif istifadəçi interfeyslərini yaxşılaşdırmaq, həmçinin məlumat axını verilən parametrlər dəsti ilə süzə biləcək tətbiqetmələrin yaradılması istiqamətində işlər uğurla aparılmışdır. Şəbəkəyə çox vaxt sərf edən bəzi İnternet istifadəçiləri sosial mühitdən kənarlaşmanın təsirini hiss edirlər. İnternetdən intensiv istifadənin təkliyə qədər sosial əlaqələrin daralmasına, ailə əlaqələrinin azalmasına və hətta depresif vəziyyətlərin inkişafına səbəb olduğu hallar var. İnternetin fərdi və qrup zehni fəaliyyətinə mənfi təsir göstərdiyinə dair başqa bir sübut da var. Məsələn, İnternetdən istifadənin uşaqların və yeniyetmələrin autizasiyasına töhfə verə biləcəyi, sosial uyğunlaşma proseslərində pozulmalara səbəb ola biləcəyi və s. Psixoloqlar, insan psixikasının virtual reallıq fenomeni ilə mürəkkəb əlaqəsini virtual aləmin dəyişdirilmiş şüur vəziyyətləri problemləri ilə mümkün əlaqəsi, ağrılı formaları qəbul edən İnternetdən nəzarətsiz psixoloji asılılıq barədə qeyd edirlər. Psixoloji təhlükə, İnternetdəki rol oyunlarının ələ keçirilməsi, onların antisosial davranışla mümkün əlaqəsi, şəxsiyyətinizi dəyişdirmək və ya birdən çox şəbəkə şəxsiyyəti yaratmaq üçün bir avatar kimi istifadə psixoloji motivasiya. İnternetin insana psixoloji təsirinin təhlükələrindən İnternetdə sərf olunan vaxtın özünü izləmək, hədəf, hədəf təyin etmək və İnternetdə əsaslı axtarış aparmaq qabiliyyətinin inkişaf etdirilməsindən xilas olmaq olar. İnternetin tələsik istifadəsi səbəbindən ortaya çıxan problemləri, valideynlər və psixoloqlarla müzakirə etmək vacibdir. İnternetdən istifadə zamanı hansı qaydalara əməl edilməlidir? İnternetdən etibarlı istifadənin ümumi qaydalarını artıq bilirsiniz: İnternetə qoşulmadan əvvəl, istifadəçinin kompüterində antivirus qorunmasının olub olmadığını yoxlamaq və təhlükəsizlik proqramının versiyasını yeniləmək lazımdır; istifadəçinin kompüterinə hər hansı bir faylın yüklənməsinə səbəb ola biləcək hiperlink aktivləşdirmək tövsiyə edilmir; İstifadəçinin kompüterinə

naməlum saytlardan proqram yükləmək tövsiyə edilmir; istifadəçi üçün tanımadığı saytlarda yerləşdirilən bannerlər (reklam və ya əyləncəli) aktiv edilməməlidir; istifadəçi üçün bilinməyən elektron poçt göndərişlərinə əlavə edilmiş sənədlərin açılması qadağandır; İnternetdə hər hansı bir şəxsi məlumatı bölüşmək tövsiyə edilmir; ümumiyyətlə istifadəçi adı və şifrə tələb edən etibarlı veb saytlardan istifadə etməklə etibarlı olmayan veb saytlar (əməliyyat təhlükəsizliyini təmin edən müəyyən sertifikatlar verə bilməyən saytlar) vasitəsilə hər hansı bir maliyyə əməliyyatının aparılması qadağandır. Şifrə ən azı səkkiz işarədən ibarət olmalıdır, verilmiş məktublar və nömrələr. Ən əsası, parol açıq bir şey olmamalıdır, bəzi sadə sözlər və ya tarixlər; İnternet vasitəsilə tanış olduğunuz bir insanla görüşməyə razılıq verməyin, fotoşəkilinizi İnternet dostlarınıza göndərməyin, ad, ünvanı, məktəb nömrəsi, sinif cədvəli və ya ailə məlumatları kimi qəribəliklərə yol verməyin. İnternetdə müəllif hüquqlarının qorunması İxtira və İnternetin sürətli və geniş yayılması bir əsər müəllifi ilə onun istehlakçısı arasındakı münasibətlərin qanuni tənzimlənməsi sahəsində informasiya ictimaiyyəti üçün olduqca ciddi suallar doğurdu. Kompüter şəbəkəsinin texnoloji əsası İnternetdə yerləşdirilən hər hansı bir məlumat obyektinin hər hansı bir kompüter cihazından şəbəkəyə qoşulmuş hər hansı digər kompüterə və ya gadget-a pulsuz kopyalanmasını təmin edir. Lakin bu, müəyyən edilmiş müəllif hüquqları qanunlarının pozulması demək deyil. Rusiya Federasiyasında müəllif hüququ Mülki Məcəllə və Müəllif hüquqları və əlaqəli hüquqlar haqqında qanunla tənzimlənir. Müəllif hüquqları obyektlərinə aşağıdakılar daxildir: ədəbi və bədii əsərlər (roman, şeir, məqalə və digər yazılı əsərlər; mühazirələr, nitqlər, xütbələr və digər şifahi əsərlər; dramatik, musiqi və dramatik əsərlər, pantomimalar, xoreoqrafiya və digər səhnə əsərləri, obyektlərin digər qrupları). ; kompüter proqramları; onların komponentlərinin seçilməsi və ya sadələşdirilməsi üzrə intellektual fəaliyyətin nəticəsi olduqda məlumatların (verilənlər bazasının) yığılması; digər əsərlər. Müəllif hüquqları mövzusundadır: adi mətbuat məlumatlarına xas olan günün və ya cari hadisələrin xəbərləri; xalq sənət əsərləri (folklor); dövlət orqanları tərəfindən öz səlahiyyətləri daxilində və rəsmi

tərcümələrdə dərc edilmiş siyasi, qanunvericilik, inzibati xarakterli rəsmi sənədlər (qanunlar, fərmanlar, fərmanlar, məhkəmə qərarları, dövlət standartları və s.); dövlət rəmzləri, dövlət mükafatları; dövlət orqanlarının, silahlı qüvvələrin və digər hərbi hissələrin rəmzləri və nişanları; ərazi icmalarının simvolları; Müəssisə, idarə və təşkilatların işarələri və işarələri; banknotları; nəqliyyat vasitələrinin cədvəlləri, televiziya və radio yayım cədvəlləri, telefon qovluqları və orijinallıq meyarlarına cavab verməyən və sui-generis hüququna tabe olan digər oxşar məlumat bazaları (bir növ qanun, xüsusi bir qanun növü). Yəni müəllif hüquqları obyektləri olduqca müxtəlifdir və yəqin ki, mədəniyyətin və cəmiyyətin inkişafı ilə yenə də yeni obyektlər görünəcəkdir. Beləliklə, qlobal İnternetin inkişafı ilə kompüter proqramları və məlumatların yığılması kimi obyektlər meydana çıxdı. Qanuna görə, bir əsərin rəqəmsal formada İnternetdə yayımlanması bir əsərin yayımı və ya onun paylanması hesab olunur və buna görə də müəllif hüquqları sahibinin icazəsi tələb olunur. Əsərin bir hissəsini və ya onun bir hissəsini müəllifin icazəsi olmadan İnternetdə yerləşdirmək qanun pozuntusudur və mənəvi ziyana və maddi ziyana (itirilmiş qazana) görə kompensasiya tələbi ilə məhkəməyə şikayət edilə bilər. İnternetdə ən çox yayılmış pozuntular bunlardır: müəllif və ya müəllif hüququ sahibinin əvvəlcədən icazəsi olmadan musiqi, bədii, ədəbi əsərlərin və ya kompüter proqramlarının qeyri-qanuni bərpası və surəti. Bu müəlliflərin maddi hüquqlarının pozulmasına səbəb olur. Bundan əlavə, plagiat getdikcə populyarlaşır. İnternetdə belə hərəkətlər müəlliflərin maddi və qeyri-maddi hüquqlarını pozur. Müəllif hüquqlarını qorumaq üçün aşağıdakı tədbirlərdən istifadə edilə bilər: pozuntudan əvvəlki mərhələdə: məhdud funksionallıq - müəlliflər sənədləri çap edə və ya kompüterin yaddaşında saxlaya bilməyən proqramları yayırlar; "Zaman bombası" - müəllif tam hüquqlu bir müəllif hüququ obyekti paylayır, lakin ona girişin mümkün olmayacağı bir tarix təyin edir; kopiya qorunması, yəni müəllif bir faylın kopyalana biləcəyini neçə dəfə təyin edir; kriptoqrafik zərflər - iş şifrələnir ki, şifrə açarından istifadə etməklə ona giriş mümkündür; rəsmi mənbədə materialın əvvəlcədən dərc edilməsi, işin müəyyən bir tarixdə mövcudluğunun təsdiqlənməsi, əsərin yaradıldığı tarixin notarius tərəfindən

təsdiqlənməsi, lazer diskinə yazılması və arxivə və ya veb depozitə yerləşdirilməsi. Klirinq mərkəzləri - müəllif mərkəzə işə öz hüquqlarını lisenziyalaşdırmaq hüququ verir, mərkəz istifadəçidən haqq alır və müəllif hüquqları sahibinə ötürür. pozuntudan sonra mərhələdə: agentlər, əvvəlcədən təyin edilmiş əmrləri avtomatik yerinə yetirən kompüter proqramlarıdır, məsələn, saxta əsərlərin nüsxələri üçün şəbəkəni axtarır; stenoqrafiya - məlumatların sənədlərdə gizlədilməsi prosesi, məsələn, əsərin müəllifinin "su nişanı", bu şəxsin bu işə müəllifliyinin sübutu olacaqdır; "Beacon", bir işə yerləşdirilən və icazəsiz istifadə zamanı işə salınan, müəllif hüququ pozucusunu tapmaq imkanı verən xüsusi bir etiketdir; kod sözlərindən istifadə. İnternetdəki müvafiq mətn verilənlər bazalarında mətnlərin müəllifliyini yoxlamaq üçün plagiat aşkarlama proqramından istifadə edə bilərsiniz.İnternet kompüter şəbəkəsinin insan fəaliyyətinin bütün sahələrində yayılması ilə şəbəkə istifadəçiləri tərəfindən müxtəlif dərəcələrdə açıq olan məlumatların təhlükəsizliyi xüsusi əhəmiyyət kəsb edir. Kiberməkanda dövlət sərhədləri yoxdur, kompüter məlumatlarına icazəsiz girişi həyata keçirən bir şəxs istənilən ərazidə yerləşə bilər, kompüter virusunun müəllifi onu populyar bir saytda yerləşdirə və bununla da onun müxtəlif ölkələrə daxil olmasını təmin edə bilər. İnformasiya təhdidini yaradan bu şərtlər qanunların uyğunlaşdırılmasını və vahidin yaradılmasını tələb edir [10]

Məlumat təhlükəsizliyi müasir sivilizasiyanın ən vacib məsələlərindən biridir. Bu müasir dünyada məlumatların əksəriyyəti internetdən istifadə edərək ötürülür və saxlanılır. Buna görə məlumatlarımızı icazəsiz girişdən qorumaq vacibdir. Kompüter alimləri məlumatları təmin etmək üçün müxtəlif növ mexanizmlər hazırlayırlar. Köhnə mexanizmlər müxtəlif növ icazəsiz hücumlar nəticəsində məhv edildiyindən, kompüter alimləri məlumatları qorumaq üçün yeni və müasir təhlükəsizlik mexanizmlərini inkişaf etdirir. Məlumat şifrələnir, buna görə icazəsiz istifadəçi faktiki məlumat ala bilmir və səlahiyyətli istifadəçi tərəfindən istifadə üçün şifrələnir. Kriptologiya həm kriptovalyutanı, həm də kriptovalyutanı əhatə edən etibarlı rabitələrin öyrənilməsidir. Şifrəli məlumatlar istifadəçiyə bu məlumatların istifadəsini təmin etmək üçün şifrələnməlidir. Şifrələmə - tərcümə

mətni və ya alqoritm əsasında düz mətnin və ya məlumatın geri dönüşümlü tərcümə yolu ilə bilinməyən formaya çevrilməsi, buna şifrələmə də deyilir. Digər tərəfdən şifrənin açılması şifrəli mətnin və ya məlumatların (şifrə mətni adlandırılan) orijinal mətnə və ya məlumatlara (düz mətn adlanır) tərcüməsidir, buna deşifrə deyilir. Təhlükəsizlik hücumlarından həssas məlumatların məxfiliyini təmin etmək üçün güclü bir məlumat şifrələmə və şifrəni açma texnikası tələb olunur.Müasir dövrdə məlumatların qorunması üçün əsasən aşağıdakı anlayışlardan istifadə edilir.

3.5. İnternet şəbəkəsində informasiyanın qorunması üçün əsas kriptoqrafik metodlar

Kriptoqrafiya kriptologiya və kriptovalyutanın fənləri ilə sıx bağlıdır. Kriptoqrafiyaya mikrodotlar, sözləri şəkillərlə birləşdirmək və məlumatı saxlama və ya tranzitdə gizlətməyin digər üsulları daxildir. Halbuki, bu günkü kompüter mərkəzli dünyada kriptovalyutası ən çox şifrə mətninə (adi mətn, bəzən açıq mətn adlandırılan) şifrə mətninə (şifrələmə adlanan bir proses), sonra yenidən (şifrələmə adı ilə tanınan) qarışdırılır. Bu sahə ilə məşğul olan insanlar kriptoqraflar kimi tanınırlar. Kriptoqrafiyanın əsas komponenti kriptovalyutadır.

Kriptoqrafik alqoritmlərin təsnif edilməsinin bir neçə yolu var. Bu sənədin məqsədləri üçün, şifrələmə və şifrəni açmaq üçün işlədilən açarların sayına görə təsnifləşdiriləcək və sonradan tətbiqi və istifadəsi ilə müəyyənləşdiriləcəkdir. Müzakirə ediləcək alqoritmlərin iki növüdür (Şəkil 3.1):

- Gizli Açar Kriptoqrafiyası (GAK): Həm şifrələmə, həm də şifrələmə üçün bir düymədən istifadə edir.
- Açıq Açar Kriptoqrafiyası (AAK): Şifrələmə üçün bir açar, digəri şifrələmə üçün istifadə olunur.

3.5.1. Gizli açar kriptoqrafiyası

Gizli açar kriptovalyutası ilə həm şifrələmə, həm də şifrələmə üçün istifadə olunur.Göndərici düz mətni şifrələmək üçün açardan (və ya bəzi qaydalar dəstindən) istifadə edir və şifrə mətnini qəbulediciyə göndərir. Alıcı mesajın şifrəsini açmaq və düz mətni bərpa etmək üçün eyni düyməni (və ya qaydaları) tətbiq edir. Hər iki

funksiya üçün bir açar istifadə edildiyi üçün gizli açar kriptoqrafiyası simmetrik şifrələmə adlanır.

Simmetrik açar / gizli açar şifrələrinin iki əsas növü var:

- Transpozisiya şifrələri
- Əvəzedici şifrələr
- Transpozisiya şifrələri

Transpozisiya şifrələri

Kriptoqrafiyada transpozisiya şifrəsi şifrələmə metodudur ki, düz mətn bölmələrinin (ümumiyyətlə simvol və ya simvol qruplarıdır) mövqeləri nizamlı bir sistemə uyğun olaraq dəyişdirilir və beləliklə şifrə mətnin permutasiyasını təşkil edir. Yəni bölmələrin sırası dəyişdirilir (düz mətn yenidən tənzimlənir). Transpozisiya şifrəsi düz mətndəki simvolları şifrə mətnini yaratmaq üçün yenidən dəyişdirir. Məktublar dəyişdirilmir.

Əvəzləmə şifrələri

A əvəz şirfəsi ciphertext istehsal düz metin simvol dəyişir. Düz mətn bölmələrinin sabit bir sistemə görə şifrə ilə əvəz edildiyi kodlaşdırma metodudur; "vahidlər" tək hərflər (ən çox yayılmışlar), hərflər cütü, hərflərin üçlüyü, yuxarıdakıların qarışıqları və sair ola bilər. Alıcı tərs əvəzləmə ilə mətni açır. Bir sıra müxtəlif növ əvəzedici şifrələr mövcuddur. Şifrə tək hərflər üzərində işləyirsə, sadə əvəzedici şifrə adlanır; Daha böyük hərf qruplarında işləyən bir şifrə poliqrafiya adlanır.

3.5.2. Açıq açar Kriptoqrafiyası

Açıq açar kriptovalyutasıbir cüt kriptoqrafik açar istifadə edən hər hansı bir şifrləmə sistemidir, bu sistemin sadəcə birinə sahib olduğu digərinin praktik hesablanmasına imkan vermir. Ümumiyyətlə açıq açar şifrələmə üçün istifadə olunur və geniş yayıla bilər, digəri - xüsusi açar, şifrəni açmaq üçün istifadə olunur və yalnız sahibinə məlumdur. Açıq açardan istifadə edərək istənilən şəxs sahibi üçün bir mesajı şifrələyə bilər və bu mesaj yalnız sahibinin şəxsi açarı ilə şifrələnə bilər. Beləliklə, müəyyən bir alıcı üçün nəzərdə tutulmuş bir mesaj şifrələnə bilər və ümumi serverlərdə

təhlükəsiz yerləşdirilə bilər, yalnız şəxsi açar sahibi onu oxuya bilər. İki fərqli qoşalaşmış açarın istifadəsinin bu sistemi asimmetrik açar şifrələmə alqoritmi adlanır. Simmetrik şifrələmə / deşifrə daha sadə alqoritmlərə əsaslanır və daha sürətli olur.

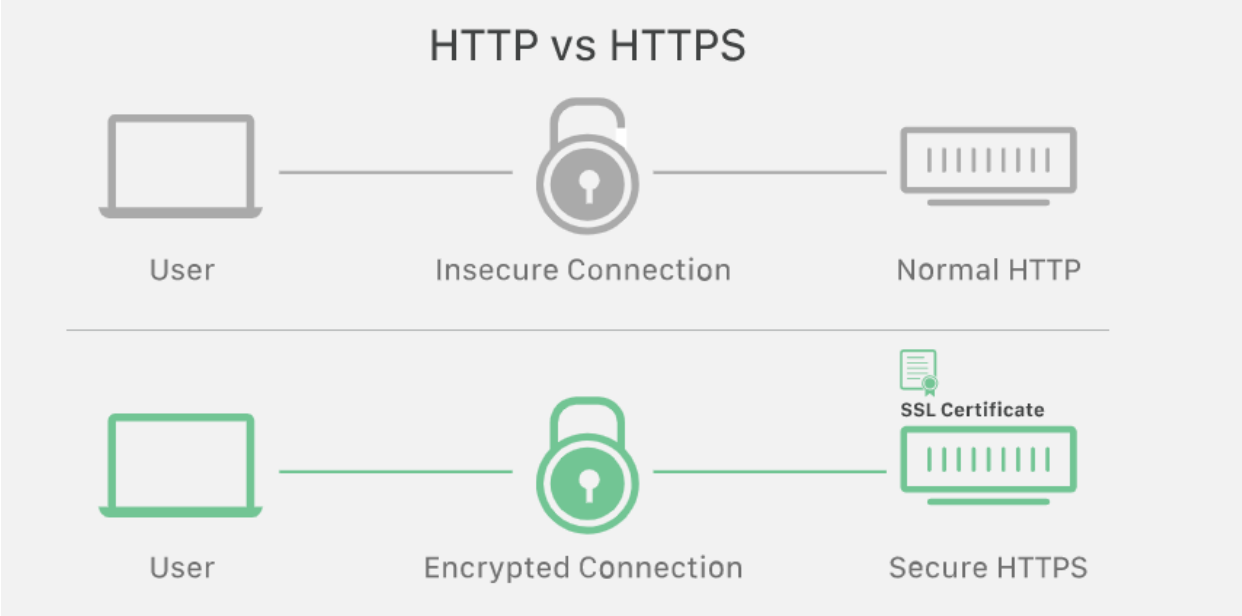
3.5.3. Elliptik əyri kriptoqrafiyası (ECC)

Bir elliptik əyri, xi müstəvisindəki $y^2 = x^3 + ax + b$ formanın cəbri tənliyini təmin edən nöqtələrin yeridir. A və b ədədlərinin hər bir seçimi fərqli elliptik əyrilər verir. X, y, a və b hər hansı bir sahədən ola bilər, yəni mürəkkəb sayı, həqiqi sayı, sonlu say və s.

3.6. İnternet şəbəkəsində SSL sertifikatı vasitəsilə məlumatın təhlükəsiz ötürülməsi.

3.6.1. SSL nədir

SSL və ya Secure Sockets Layer, şifrələməyə əsaslanan İnternet təhlükəsizliyi protokoludur. İlk dəfə 1995-ci ildə Netscape tərəfindən İnternet rabitələrində məxfilik, identifikasiya və məlumat bütövlüyünün təmin edilməsi məqsədi ilə hazırlanmışdır. SSL, bu gün istifadə olunan müasir TLS şifrələməsinin sələfidir[25].



3.1

Onlayn biznesin ən vacib komponentlərindən biri potensial müştərilərin alış-veriş etməkdə inamlı olduqları bir mühit yaratmaqdır. SSL sertifikatları etibarlı bir əlaqə quraraq inam zəmini yaradır. Ziyarətçilərin əlaqələrinin etibarlı olmasına əmin olmaq üçün brauzerlər ev göstəriciləri dediyimiz xüsusi vizual istəkləri təmin edir - yaşıl bir kiliddən markalı URL çubuğuna qədər bir şey.SSL sertifikatlarının əsas cütü var: açıq və gizli açar. Bu açarlar şifrəli bir əlaqə yaratmaq üçün birlikdə işləyir. Sertifikatda sertifikat / veb sayt sahibinin şəxsiyyəti olan "mövzu" adlandırılanlar da var.

Ümumilikdə yüksək dərəcədə məxfilik təmin etmək üçün SSL internet üzərindən ötürülən məlumatları şifrələyir. Bu o deməkdir ki, bu məlumatları ələ keçirməyə çalışan hər kəs yalnız şifrəsini açmaq mümkün olmayan simvol qarışıq bir qarışıq görəcəkdir.SSL, hər iki cihazın həqiqətən iddia etdikləri şəxslərdən olmasını təmin etmək üçün iki ünsiyyət qurğusu arasında bir əlaqə yaratma deyilən bir təsdiqləmə prosesini başlatır.SSL ayrıca məlumatların bütövlüyünü təmin etmək üçün məlumatları rəqəmsal şəkildə imzalayır, məlumatın nəzərdə tutulan alıcıya çatmamışdan əvvəl dəyişdirilmədiyini yoxlayır.SSL-in sonuncularından daha etibarlı bir neçə təkrarlama var. 1999-cu ildə SSL TLS olmaq üçün yeniləndi.

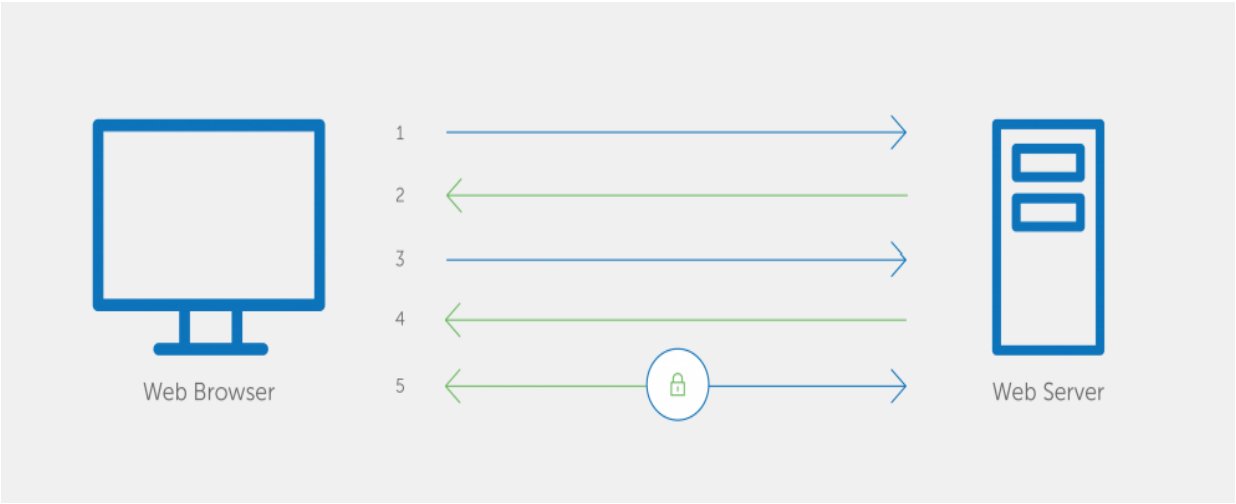
SSL həmçinin aşağıdakı əməliyyatları yerinə yetirir.

- Security Sockets Layer (SSL) bir server və bir müştəri arasında şifrəli bir əlaqə yaratmaq üçün standart bir texnologiyadır - adətən bir veb server (veb sayt) və bir brauzer və ya bir poçt serveri və bir poçt müştəri (məsələn, Outlook).
- SSL kredit kartı nömrələri, sosial təhlükəsizlik nömrələri və giriş etimadnaməsi kimi həssas məlumatların etibarlı şəkildə ötürülməsinə imkan verir. Normalda, brauzerlər və veb serverlər arasında göndərilən məlumatlar düz mətnlə göndərilir - qulaq asmaqda həssas qalır. Təcavüzkar bir brauzer və veb server arasında göndərilən bütün məlumatları ələ keçirə bilirsə, bu məlumatları görə və istifadə edə bilər.
- Daha dəqiq desək, SSL təhlükəsizlik protokoludur. Protokollar alqoritmlərin necə istifadə olunacağını təsvir edir. Bu vəziyyətdə SSL protokolu həm keçid, həm də ötürülən məlumatlar üçün şifrələmənin dəyişənlərini təyin edir.

- Bütün brauzerlər SSL protokolundan istifadə edərək təhlükəsiz veb-serverlərlə qarşılıqlı əlaqə qurma imkanına malikdir. Bununla birlikdə, təhlükəsiz bir əlaqə qura bilmək üçün brauzer və serverə SSL Sertifikatı deyilən bir şey lazımdır.
- SSL hər gün milyonlarla insanın İnternetdəki məlumatlarını, xüsusən onlayn əməliyyatlar zamanı və ya məxfi məlumat ötürərkən təmin edir. İnternet istifadəçiləri, onlayn təhlükəsizliklərini SSL ilə təmin edilmiş bir veb sayt və ya Genişləndirilmiş Doğrulama SSL ilə təmin olunan veb sayt ilə birlikdə gələn kilid simgesi ilə əlaqələndirməyə gəldilər. SSL ilə təmin olunan veb saytlar da http deyil, https ilə başlayır.

3.6.2. SSL necə işləyir

Bir brauzer SSL ilə təmin edilmiş bir veb saytına daxil olmağa çalışdıqda, brauzer və veb server bir SSL bağlantısı quraraq "SSL Əl ilə əlaqə və ya razılaşma" (SSL Handshake) adlanan bir prosesi istifadə edirlər.Qeyd edək ki, SSL Handshake istifadəçi üçün görünməz və dərhal baş verir.Əslində, SSL bağlantısını qurmaq üçün üç düymədən istifadə olunur: ictimai, özəl və sessiya düymələri. Açıq açar ilə şifrələnmiş hər hansı bir şey yalnız özəl açarla deşifrələnə bilər və əksinə.Şəxsi və açıq açar ilə şifrələmə çox emal gücünə sahib olduğundan, onlar yalnız simmetrik sessiya açarı yaratmaq üçün SSL Handshake zamanı istifadə olunur. Etibarlı bir əlaqə qurulduqdan sonra, sessiya açarı bütün ötürülən məlumatları şifrələmək üçün istifadə olunur.



3.2

SSL Handshake

1. Brauzer SSL (https) ilə təmin edilmiş bir veb serverə (veb səhifəyə) qoşulur.
2. Brauzer, serverin özünü tanımasını xahiş edir.
3. Server SSL Sertifikatının bir nüsxəsini, o cümlədən serverin açıq açarını göndərir.
4. Brauzer sertifikat kökünü etibarlı CA-lərin siyahısına və sertifikatın istənməmiş, geri çağırılmamış olduğunu və ümumi adın qoşulduğu veb sayt üçün etibarlı olduğunu yoxlayır. Brauzer sertifikata güvənirsə, serverin açıq açarından istifadə edərək simmetrik sessiya açarını yaradır, şifrələyir və geri göndərir.
5. Server şəxsi açarından istifadə edərək simmetrik sessiya açarını deşifrə edir və şifrəli seansa başlamaq üçün sessiya açarı ilə şifrələnmiş bir təsdiq göndərir.
6. İndi Server və Brauzer bütün ötürülən məlumatları sessiya açarı ilə şifrələyir.

NƏTİCƏ VƏ TƏKLİFLƏR

Aparılan araşdırma və analizlər göstərir ki, müasir dövdə informasiaynın qorunması məsələsi öz aktuallığını daha da möhkəmləndirir, informasiya təhlükəsizliyinin inkaşaf etdiriliməsi,yeni kriptoqrafik şifrələmə metodların istifadə edilməsinə çox böyük zərurət yaranır.

Nəticə kimi aşağıdakılar göstərilə bilər:

- Informasiya təhlükəsizliyinin səviyyəsinin yüksəldilməsi onlayın əməliyyatları həyata keçirilməsini, dövlət və özəl qurumlara aid dəyərli məlumatların çox rahat daşınmasına, məlumatın müəllif hüquqlarının qorunmasına təminat verir.
- İnformasiya təhlükəsizlinin yüksək səviyyədə təşkil edilməsi maddi və mənəvi zərərlərin qarşısının maksimum alınmasına həmçinin insanların şəxsi məlumatlarının yüksək səviyyədə qorunmasını təmin edir.
- Məlumatların gizliliyinin pozulması üçün hər zaman cəhdlər göstərilir və bu cəhtlər öz növbəsində dinamik inkşafdadır, kibertəhlükəsizlik heç bitməyən bir döyüşdür. Problemin daimi qətiyyətli həlli yaxın gələcəkdə tapılmayacaqdır.
- Fiziki şəxslərin, firmaların, dövlət qurumlarının və millətin kiber təhlükəsizliyi vəziyyətinin yaxşılaşdırılması, kibertəhlükəsizliyin pozulması ilə əlaqəli ola biləcək itki və zərərin azaldılmasında əhəmiyyətli dərəcəyə malikdir.
- İnformasiya təhlükəsizliyinin təkmilləşdirilməsi iki fərqli fəaliyyət növünü tələb edir: (a) təhlükəsizliynin yaxşılaşdırılması ilə bağlı bilinənlərdən daha səmərəli və daha geniş istifadə edilməsi üçün səylər və (b) təhlükəsizlik üçün yeni biliklərin hazırlanması səyləri.

İnformasiya təhlkükəsizlik üzrə aparılmış analiz və təhlillərin nəticəsi olaraq aşağıdakı tədbirlərin icrasına zərurət var.

- Yeni növ kiberhücumlara qarşı bütün vacib informasiyanın saxlanması və daşınması əməliyyatları müasir kriptoqrafik metodlar və protokollar(SSL/TLS) vasitəsilə həyata keçirilməlidir

- Informasiyanın texniki mühafizəsinin inşaf etdirilməsi ilə yanaşı içşi heyyətinə təhlükəsizlik tədbirləri aşılanmalıdır.Müasir dövrdə əsasən əksər hücüm metodlarında hədəf işçi komputeri seçilir və onun vasitəsilə şəbəkəyə sızıla bilir.
- Ən vacib məqamlardan biri də parollar statik deyil dinamiklyi təmin edilməlidir.Beynəlxalq standartlara əsasən parol dinamik olaraq məyyən vaxt intervalı üçün keçərli olmalıdır
- Mümkün qədər bütün doğrulanma əməliyyatları 3D təhlükəsilik metodu ilə həyata keçirilməlidir.Bu metodun tədbiqi xüsusən də bank əməliyyatlarının və işçilərin sistemə girişini daha da təhlükəsiz edir
- Məlumatların təhlükəsizliyinin digər yönü də məlumat itgisinin qarşısını almaqdır.Burada hər hansı kiberhücumdan söhbət getmir məlumatın saxlanıldığı diskin sıradan çıxması nəticəsində məlumat itgisi olar bilər,bunun qarşısını almaq üçün müasir arxivlənmə metodlarından istifadə edilməlidir
- Son dövrlərdə onlayn bank əməliyyatlarının, elektron ticarət proseslərinin çox sürətli inkşafı vacib informasiya mübadiləsinin kəskin artması kiberhücumların yeni metodlarnın inşkaf etməsinə səbəb olmuşdur.Bunun üçün ənənvi təhlükəsizlik tədbirlərdən deyil yeni kriptoqrafi metodlardan istifadə edilməlidir.

ƏDƏBİYYAT SİYAHISI

1. P.W. Singer. Cybersecurity and Cyberwar: What Everyone Needs to Know(r), 120-128 səh.
2. Richard A. Cyberwar: The Next Threat to National Security & What to do about It, 324-330 səh.
3. Adam Shostack. Designing for Security, 56-60 səh.
4. Chris McNab. Network Security Assessment, 71-75 səh.
5. Stuart McClure, Joel Scambray, George Kurtz. Network Security Secrets and Solutions, səh 61.
6. Michael Sikorski. Practical Malware Analysis 65-72 səh.
7. Michael Sikorski. Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software, 231-245 səh.
8. Ross J. Anderson. Security Engineering: A Guide to Building Dependable Distributed Systems 2nd, fəsil 6,13
9. Andrew Jaquith. Security Metrics: Replacing Fear, Uncertainty, and Doubt 95-102 səh.
10. Christopher Hadnagy. Social Engineering: The Art of Human Hacking ,fəsil 7
11. Mary Aiken, The Cyber Effect, 121-134 səh.
12. Christopher Hadnagy. The Science of Human Hacking, 170-176 səh.
13. www.ict.az - Informasiya texnalogiyalar instutu sayıtı
14. www.krebsonsecurity.com
15. www.mincom.gov.az - Azərbaycan Respublikası Nəqliyyat,Rabitə və Yüksək Texnalogiyalar Nazirliyi sayıtı
16. www.nsa.gov - Beynəlxaq təhlükəsizlik agentliyi sayıtı
17. www.proofpoint.com
18. Анисимов А. А. Менеджмент в сфере информационной безопасности: Учебное пособие / А. А. Анисимов. – М.: Интернет-Университет Информационных Технологий; БИНОМ. Лаборатория знаний, 2009. – 176 с.: ил., табл. – (Основы информационных технологий).

19. Арзуманов С. В. Оценка эффективности инвестиций в информационную безопасность [Электронный ресурс]. // Экономически оправданная безопасность. – 2005. - №1.- Режим доступа: http://www.inside-zi.ru/pages/1_2005/23.html
20. Галатенко В. А. Основы информационной безопасности. Курс лекций. Учебное пособие – 3 изд. / В.И. Галатенко. - М.: Интернет-Университет Информационных Технологий», 2006. -264 с.
21. Клаверов В.Б. Проблемы противодействия компьютерной преступности / Клаверов В.Б. [Электронный ресурс]. – Режим доступа: http: // www.securitylab.ru / contest / 382194.php.
22. Томас Т.Л. Сдерживание асимметричных террористических угроз, стоящих перед обществом в информационную эпоху / Мировое сообщество против глобализации преступности и терроризма. Материалы международной конференции. М., 2002
23. Воробьев В. В. Преступления в сфере компьютерной информации (юридическая характеристика
24. Юсупов Р.М., Шишкин В.М. Информационная безопасность и кибербезопасность: семантический конфликт или сосуществование // Информатизация и связь. - № 6 – 2013. С. 8-13.
25. Шишкин В.М., Гололобова О.В. О понятии «критичность» в информационной безопасности // Материалы конференции «Региональная информатика – 2004» (СПб, 22-24 июня 2004 г.) – СПб.: 2004.
26. Юсупов Р.М., Шишкин В.М. Информационно-коммуникационные технологии и национальная безопасность – противоречивая реальность // Информатизация и связь, № 1, 2010. - С. 27-35.
27. Фесечко А.И. Оптимизация защитных мероприятий по безопасности жизнедеятельности людей.Надёжность и качество-2011: труды Международного симпозиума: в 2 т./ под ред. Н.К.Юркова. – Пенза: Изд-во ПГУ, 2011. – 2 т. – С.30-31.

28. Шишкин В.М. Показатели надёжности и безопасности: возможности нелинейного перехода.Надёжность и качество -2011: труды Международного симпозиума: в 2 т./ под ред. Н.К.Юркова. – Пенза: Изд-во ПГУ, 2011. – 1 т. – С.100-102.

Резюме

Целью исследования является выявление фактов, влияющих на развитие информационной безопасности и основных проблем, стоящих перед безопасностью, оптимальный способ реализации существующих инструментов против них, а также анализ новых криптографических методов.

В этой научной работе говорится о преимуществе сравнения новых криптографических методов в традиционных методах безопасности. Например: для ограничения кибер-ущерба, повышения уровня защиты информационной безопасности и предотвращения ущерба от киберпреступности

Это исследование также предоставляет информацию о научных и исследовательских областях криптографии.

Доказано, что информационная безопасность является очень важным моментом, и необходимо изучать криптографические методы и протоколы.

Проанализировано предотвращение потери ценной информации, внутренний и внешний аудит.

Summery

The purpose of the investigation is to identify the facts that affect the development of information security and the main problems facing security, the optimal way to implement existing tools against them, and the analysis of new cryptographic methods.

In this scientific work is spoken the advantage of comparing new cryptographic methods in traditional security methods. For example: To limit cyber damage, increase information security protection level and avoid cybercrime damages.

This investigation also provides information on the scientific and research areas of cryptography.

It has been proved that information security is a very important point and it is necessary to study cryptographic methods and protocols.

Analyzed loss prevention of valuable information, internal and external auditing.