Kiber təhlükəsizlik nədir?

Kiber təhlükəsizlik kompüterlərin, serverlərin, mobil qurğuların, elektron sistemlərin, şəbəkələrin və məlumatların ziyankar hücumlardan qorunması təcrübəsidir. İnformasiya texnologiyaları təhlükəsizliyi və ya elektron məlumat təhlükəsizliyi kimi də tanınır. Bu termin, biznesdən mobil qurğularla hesabalamalaradək müxtəlif kontekstlərdə tətbiq olunur və bir neçə ümumi kateqoriyaya bölünə bilər.

- **Şəbəkə təhlükəsizliyi -** kompüter şəbəkəsinin hədəflənmiş təcavüzkarların və ya təsadüfi ziyankar proqramların müdaxilələrindən mühafizə edilməsidir.
- **Proqram təhlükəsizliyi** proqram təminatının və qurğuların təhlükələrdən mühafizə edilməsidir. Təhlükəyə məruz qalmış proqram qoruması nəzərdə tutulmuş verilənlərə daxil olmağa imkan verə bilər. Uğurlu təhlükəsizlik layihələndirmə mərhələsində, hər hansı bir proqram və ya qurğu istifadə edilməzdən çox əvvəl başlayır.
- **İnformasiya təhlükəsizliyi** həm saxlanılan, həm də göndərilən verilənlərin bütövlüyünü və məxfiliyini qoruyur.
- **Əməliyyatların təhlükəsizliyi** məlumat aktivlərini idarə etmək və qorumaq üçün proseslərdən və qərarlardan ibarətdir. Şəbəkəyə daxil olduqda istifadəçilərə verilən icazələr və verilənlərin necə və harada

saxlana və ya birgə istifadə edilə biləcəyini müəyyən edən prosedurların hamısı bu anlayışa daxildir.

- **Qəza hallarında bərpa və işin davamlılığı** hər hansı bir təşkilatın kiber təhlükəsizlik hadisəsinə. yaxud əməliyyatların və ya verilənlərin itirilməsinə səbəb olan hər hansı digər hadisəyə necə cavab verdiyini müəyyən edir. Qəza hallarında bərpa strategiyası təşkilatın hadisədən əvvəl olduğu kimi eyni işləmək qabiliyyətinə qayıtması üçün əməliyyatlarını və məlumatlarını necə bərpa etdiyini diktə edir. İşin davamlılığı, müəyyən vəsaitlər olmadan fəaliyyət göstərməyə çalışarkən təşkilatın əl atdığı bir plandır.

- **Son istifadəçilərin təhsili** nə edəcəyi öncədən ən çox bilinməyən kiber təhlükəsizlik amilinə - insanlara - müraciət edir. Hər kəs təsadüfən düzgün təhlükəsizlik təcrübəsinə əməl etməyərək təhlükəsiz sistemə virus sala bilər. İstifadəçilərə şübhəli e-poçt qoşmalarını silməyi, müəyyən olunmayan USB drayverlərini qoşmamağı və digər vacib dərsləri öyrətmək istənilən təşkilatın təhlükəsizliyi üçün çox vacibdir.

Kiber təhlükənin miqyası

ABŞ hökuməti kiber təhlükəsizliyə ildə 19 milyard dollar xərcləyir, lakin xəbərdarlıq edir ki, kiberhücumlar sürətlə inkişaf edir. Ziyankar kodun yayılması ilə mübarizə aparmaq və erkən aşkarlanmasında yardımın göstərmək üçün Milli Standartlar və Texnologiyalar İnstitutu (NİST) bütün elektron resursların davamlı, real vaxt rejimində monitorinqini tövsiyə edir.

Kiber təhlükəsizliyin müqavimət göstərdiyi təhlükələr üç aspektdən ibarətdir:

1. Kibercinayətkarlığa maliyyə qazancı və ya korlamaq üçün sistemləri hədəfə alan tək subyektlər və ya qruplar daxildir.

2. Kiberhücum çox vaxt siyasi məlumatların toplamasından ibarət olur.

3. Kiberterror, çaxnaşma və ya qorxu yaratmaq üçün elektron sistemləri korlamaq məqsədi daşıyır.

Təcavüzkarların kompüterləri və ya şəbəkələri idarə etmək üçün ən çox istifadə etdiyi metodlara viruslar, soxulcan proqramlar (worm), casus proqramlar (spyware), troyanlar və soyğunçu proqramlar (ransomware) daxildir. Viruslar və soxulcan proqramlar özlərini çoxalda və fayllara və ya sistemlərə zərər vura bilir, casus proqramlar və troyanlar isə çox vaxt gizli məlumatların toplanması üçün istifadə olunur. Soyğunçu proqram, istifadəçinin bütün məlumatlarını

şifrələmək üçün bir fürsət gözləyir və istifadəçiyə giriş imkanını geri qaytarmaq üçün ödəniş tələb edir. Ziyankar kod çox vaxt istənilmədən göndərilmiş e-poçt qoşması və ya həqiqətən ziyankar proqramın faydalı verilənlərini daşıyan qanuni görünən bir yükləmə yolu ilə yayılır.

Kiber təhlükəsizlik təhlükələri həcmindən asılı olmayaraq bütün sahələrə təsir göstərir. Son illərdə ən çox kiberhücumların baş verdiyi haqqında məlumat verilən sahələr səhiyyə, istehsal, maliyyə və hökumət sektorlarıdır. Bu sektorların bəziləri maliyyə və tibbi məlumatlar topladıqları üçün kiber cinayətkarlara daha çox müraciət edirlər, lakin şəbəkələrdən istifadə edən bütün təsərrüfat subyektləri müştəri məlumatları, korporativ cəsusluq və ya müştəriləri hücumları üçün hədəf alına bilər.

Son istifadəçinin qorunması

Beləliklə, kiber təhlükəsizlik tədbirləri istifadəçiləri və sistemləri necə qoruyur? İlk növbədə kiber təhlükəsizlik e-poçtları, faylları və digər vacib məlumatları şifrələmək üçün kriptoqrafik protokollara etibar edir. Bu nəinki yolda olan məlumatları qoruyur, həm də itkidən və ya oğurluqdan qoruyur. Bundan əlavə, son istifadəçinin təhlükəsizliyi proqramı ziyankar kodların hissələrinin olub-olmadığını yoxlamaq üçün kompüterləri skan edir, bu kodu karantinə alır və sonra kompüterdən silir. Təhlükəsizlik proqramları hətta Master Boot Record (MBR) -də gizlədilmiş və kompüterin sərt diskindən məlumatları şifrələmək və ya silmək üçün nəzərdə tutulan ziyankar kodu aşkar edib silə bilər.

Elektron təhlükəsizlik protokolları ziyankar proqramların real vaxt rejimində aşkarlanmasına da diqqət yetirir. Çoxları hər dəfə icra edilərkən şəklini dəyişdirən viruslardan və ya troyanlardan (polimorf və metamorfik ziyankar proqram) qorumaq məqsədilə proqramın davranışına və onun koduna nəzarət etmək üçün evristik və davranış təhlillərindən istifadə edirlər. Təhlükəsizlik proqramları, potensial ziyankar proqramları, davranışlarını təhlil etmək və yeni infeksiyaların daha yaxşı aşkar etmə yollarını öyrənmək üçün istifadəçi şəbəkəsindən ayrı olan virtual qovuqda məhdudlaşdıra bilər.

Kiber təhlükəsizlik üzrə mütəxəssisləri yeni təhlükələr və onlarla mübarizə üçün yeni yollar aşkar etdikləri üçün təhlükəsizlik proqramları inkişaf etməkdədir.

Kiber təhlükəsizlik anlayışı

İnformasiya təhlükəsizliyi də adlandırılan kiber təhlükəsizlik məlumatların bütövlüyünün, məxfiliyinin və əlçatanlığının (İKA) təmin edilməsinə şamil olunur. Kiber təhlükəsizlik, şəbəkələri, qurğuları, proqramları və verilənləri hücumlardan və ya icazəsiz girişlərdən qorumaq üçün nəzərdə tutulmuş inkişaf edən alətlər dəstindən, risklərin idarə olunması yanaşmalarından, texnologiyalardan, təlimlərdən və qabaqcıl təcrübələrdən ibarətdir.

Kiber təhlükəsizlik niyə vacibdir?

Dünya əvvəlkindən daha çox texnologiyalara güvənir. Nəticədə rəqəmsal verilənlərin yaradılması sürətlənmişdir. Bu gün müəssisələr və hökumətlər belə verilənlərin böyük bir hissəsini kompüterlərdə saxlayır və şəbəkələr vasitəsilə digər kompüterlərə ötürürlər. Qurğular və onların əsas sistemləri istismar edildikdə hər hansı bir təşkilatın sağlamlığını və məqsədlərini pozan zəifliklərə malikdir.

Məlumat sızması hər hansı bir müəssisə üçün bir sıra dağıdıcı nəticələrə səbəb ola bilər. Bu, istehlakçıların və ortaqların etimadını itirməklə şirkəti nüfuzdan sala bilər. Mənbə faylları və ya əqli mülkiyyət kimi vacib məlumatların itirilməsi şirkətin rəqabət üstünlüyünə başa gələ bilər. Bundan başqa, məlumat sızması, verilənlərin qorunması qaydalarına əməl edilməməsi səbəbindən korporativ gəlirlərə təsir göstərə bilər. Müəyyən edilmişdir ki, məlumat sızmasına görə orta hesabla təsirə məruz qalan təşkilata 3.6 milyon dollara başa gəlir. Mətbuatda işıqlandırılan çox vacib məlumatların sızmasına görə, təşkilatların güclü kiber təhlükəsizlik yanaşması qəbul edib həyata keçirməsi vacibdir.

Kiber təhlükəsizliyin geniş yayılmış növləri

Şəbəkə təhlükəsizliyi – təhlükələrin şəbəkəyə daxil olmasının və ya şəbəkədə yayılmasının qarşısını almaq üçün daxil olan və çıxan əlaqələri idarə etməklə şəbəkə trafikini qoruyur.

Məlumat itkisinin qarşısının alınması (DLP) – hərəkət etməyən, istifadədə və hərəkətdə olan məlumatların yerləşməsi, təsnifatı və monitorinqinə diqqət yetirərək məlumatları qoruyur.

Bulud təhlükəsizliyi - bulud əsaslı xidmətlərdə və proqramlarda istifadə olunan məlumatların qorunmasını təmin edir.

Müdaxiləni aşkar edən sistemlər (İDS) və ya Müdaxilənin qarşısını alan sistemlər (IPS) - pisniyyətli olması ehtimal edilən kiber fəaliyyəti aşkar etmək üçün nəzərdə tutulur.

Eyniləşdirmə və girişin idarə olunması (İAM) - daxili sistemləri ziyankar obyektlərdən qorumaq üçün işçilərin daxil olma imkanını məhdudlaşdırmaq və izləmək üçün təsdiqləmə (autentifikasiya) xidmətlərindən istifadə edir.

Şifrələmə - verilənləri tanınmaz hala gətirmək üçün kodlaşdırma prosesidir və çox vaxt yolda olarkən oğurlanmasının qarşısını almaq məqsədilə məlumat ötürülməsi zamanı istifadə olunur.

Antivirus / ziyankar proqrama qarşı proqram həlləri - məlum təhlükələrin olub-olmadığını yoxlamaq üçün kompüter sistemlərini skan edir. Müasir həllər hətta davranışlarına görə əvvəllər məlum olmayan təhlükələri də aşkar edə bilir.