“ AZƏRBAYCAN HAVA YOLLARI ”

QAPALI SƏHMDAR CƏMİYYƏTİ

MİLLİ AVİASİYA AKADEMİYASİ



**SƏRBƏST İŞ №2**

Fakültə: “Aerokosmik”

İxtisas: “İnformasiya texnologiyalari”

Fənn: “Veb sistemləri və texnologiyaları”

Mövzu : “Məlumatların şifrələnmə metodları”

Qrup: 2441a

Tələbə: Alqayev Bəxtiyar

Müəllim: Nübar Heydərzadə

BAKI 2024

**Məlumatların Şifrələnməsi**

Şifrələmə şəxsi məlumatların və məxfi təşkilati məlumatların qorunması üçün mühüm vasitədir. Girişə nəzarət, audit və siyasətlər qorunan məlumatların təhlükəsizliyi üçün vacibdir. Bununla belə, bəzi ssenarilərdə əlavə təhlükəsizlik səviyyəsi əlavə etmək üçün şifrələmə tələb olunur. Şifrələmə məlumatların saytlar arasında təhlükəsiz ötürülməsini və ya məlumatın saxlanmasını təmin etməyə kömək edir.

Şifrələmə qərarı asan olsa da, yerləşdirilməsi qeyri-müəyyənliklə dolu ola bilər. Müxtəlif şifrələmə alqoritmləri, şifrələmənin tətbiqi yolları, şifrələmənin tətbiq ediləcəyi səviyyələr və şifrələmə strategiyasını tətbiq etməzdən əvvəl nəzərə alınmalı olan yan təsirlər var.

1. Kripto Dizayn və Tətbiq Mülahizələri

Bir təşkilat üçün şifrələmənin tətbiqi asan məsələ deyil. Ssenaridən, müqavilə razılaşmalarından və ya normativ tələblərdən asılı olaraq müxtəlif şifrələmə növləri tətbiq oluna bilər. Həmçinin, bəzi biznes ehtiyacları istifadə edilən şifrələmə növünə təsir göstərə bilər. Təşkilat daxilində şifrələməni yerləşdirməyə qərar verməzdən əvvəl şifrələmə ölçüsü, şifrələmə performansı və digər məqamlar nəzərə alınmalıdır.

2. Tətbiqin Şifrələnməsi

Bir çox proqramlar daxili şifrələməni təmin edərək, şifrələmə prosedurlarının işlənib hazırlanması ehtiyacını azaldır. Verilənlər bazaları, mətn prosessorları, e-poçt proqramları və kommunikasiya proqramı funksiyalar siyahısının bir hissəsi kimi şifrələmə xidmətləri göstərən proqramlara misaldır. Bu, öz tətbiqləri üçün şifrələmə xüsusiyyətlərini inkişaf etdirmək üçün resursları olmayan təşkilatlar üçün böyük fayda ola bilər. Quraşdırılmış şifrələmədən istifadənin çatışmazlığı, verilənlərə tətbiq oluna bilən şifrələmə növündə çox vaxt seçimin az olmasıdır. Tətbiqdən istifadə etdikdə və köhnəldikdə, proqram tərəfindən istifadə edilən şifrələmə alqoritmi məlumatların zəif qorunmasını təmin edə bilər. Məlumatı paylaşarkən, paylaşmada iştirak edən hər bir şəxsin eyni proqrama girişi olmalıdır və ya məlumatın pozulmasına məruz qalmadan əvvəl məlumatın şifrəsi açılmalıdır.

3. Fayl Şifrələmə

Fayl şifrələməsi faylın bütün məzmununun şifrələnməsini əhatə edir. Fayl bir neçə yolla şifrələnə bilər:

**Parolun qorunması** (**Password protection**) – Bu üsul istifadəçidən parol qəbul edir və adətən faylın şifrələnməsi üçün istifadə edilən şifrələmə açarının yaradılmasına tətbiq edilir. Bu, faylı şifrələmək üçün sadə üsuldur, çünki istifadəçi şifrələmə alqoritmini öyrənməli və ya şifrələmə açarlarını idarə etməli deyil. İstifadəçi parolu fayla daxil olmaq istəyən hər kəslə paylaşmalı olacaq. Parolun sızmasının qarşısını almaq və ya əvvəllər oğurlanmış açarların işləməsinin qarşısını almaq üçün bəzən parolu çevirmək üçün diqqətli olmaq lazımdır. İT mütəxəssisləri parolla qorunan faylların həqiqətən şifrələndiyinə əmin olmalıdırlar.

**Üçüncü tərəf proqramı (Third-party program)**. Bu üsul faylı şifrələmək və deşifrə etmək üçün üçüncü hissə proqramından istifadə etməyi tələb edir. İstifadəçi faylın kriptoqrafik performansına və ölçüsünə seçilmiş şifrələmə növündən təsirlənəcəyini başa düşərək, istədiyiniz qorunma səviyyəsinə əsasən istifadə olunacaq şifrələmə növünü seçə bilər. Hər bir istifadəçi şifrələmə proqramına, eləcə də deşifrə açarına malik olmalıdır.

**Rəqəmsal Hüquqların İdarə Edilməsi (Digital Rights Management)**. Bu mexanizm faylı şifrələyə bilər, həmçinin faylın qəbuledicisinin faylda yerinə yetirə biləcəyi əməliyyatları məhdudlaşdıra bilər. Məsələn, istifadəçi faylı oxuya bilər, lakin onu e-poçt vasitəsilə hər kəslə paylaşa və ya çap edə bilməz. Hüquqların idarə edilməsi sənədlərə daxil olmaq üçün istifadəçilərin hüquqların idarə edilməsi xidmətinə daxil olmalarını tələb edir. Xidmətin fayla giriş imkanı verən şifrələmə açarlarının surətini saxlaması tələbi də ola bilər. Heç bir açar və ya parol mübadiləsi tələb olunmur. Bu xüsusiyyət tez-tez təşkilat sənədlərinə təşkilatdan kənarda daxil olmağın qarşısını almaq üçün istifadə olunur.

4. Disk Şifrələmə

Disk şifrələməsi kompüterdəki bütün sabit diski şifrələmək imkanı verir. Bu, kompüter oğurlandıqda məlumatların qeyri-adekvat şəkildə əldə edilməsi riskini azaltmağın ən sadə yollarından biridir. İnsanların çoxu bilmir ki, bir şəxs kompüterə daxil ola bilməsə də, şifrələnməsə, sabit disk çıxarıla və onun üzərindəki məlumat asanlıqla oxuna bilər. Sürücünün şifrələnməsi güclü paroldan istifadə etməklə kompüterə girişin qorunması ehtiyacını azaltmır, çünki istifadəçi daxil olduqdan və disk sürücüsü quraşdırıldıqdan sonra sürücüdəki məlumatların şifrəsi açılır.

Başqa bir risk, sürücünü şifrələmək üçün istifadə edilən parolun itirilməsidir ki, bu da diskdəki bütün məlumatların itirilməsinə səbəb olur. Bu riski azaltmaq üçün vacib məlumatlar həmişə ehtiyat nüsxəsini çıxarmalıdır, o cümlədən parollar. Ehtiyat nüsxəniz və ya yaddaşınız uğursuz olarsa, etibarlı dostunuz və ya ailə üzvünüz parollarınızın surətinə sahib olmalıdır. Bununla belə, müəssisə ssenarilərində, əgər işçi diskin şifrəsini açmaq üçün parolu itirmiş və ya unutmuşsa, İT administratorunun diski bərpa etməsi mümkündür, eyni şəkildə kompüter üçün parol da bərpa oluna bilər.

5. LUKS Disk Şifrələməsi

Linux Unified Key Setup (LUKS) bütün diski şifrələmək üçün istifadə edilə bilən disk şifrələmə spesifikasiyasıdır. LUKS-şifrələnmiş sürücü üçün açar faylı USB açarında saxlanıla bilər. Bu, kompüterin oğurlanması və ya müsadirə edilməsi halında qoruma təmin edə bilər. Mühafizə olunan kompüterin sahibinin üzərində cihaz yoxdursa, o, cihazın kilidini açmağa məcbur edilə bilməz. Cihazın bir nüsxəsi evdə və ya işdə təhlükəsiz yerdə saxlanıla bilər ki, kompüter tranzit zamanı təhlükəsiz olsun.

6. Şifrələmə Qaydası

Şifrələmə məlumatlarını tənzimləyən bir sıra qaydalar var. Əksər milli məxfilik qanunları şəxsi məlumatların qorunması üçün bir vasitə kimi şifrələmənin istifadəsini təklif edir. Bilin ki, bəzi ölkələrdə senzuranı tətbiq etmək üçün şifrələmə əleyhinə qaydalar var. Aşağıda sənayeyə məxsus şifrələmə qaydalarına dair bəzi nümunələr verilmişdir.

• Basel III – istirahət və tranzit zamanı maliyyə hesabatları və digər əlaqəli həssas məlumatlar üçün məcburi şifrələmə tələb olunur.

• HIPAA – sağlamlıq məlumatının məxfiliyini təmin etmək üçün şifrələmə texnologiyalarından istifadəni təklif edir.

• PCI DSS – açıq, ictimai şəbəkələrdə kart sahibi məlumatlarının şifrələnmiş ötürülməsini tələb edir.