AZƏRBAYCAN RESPUBLİKASI ELM VƏ TƏHSİL NAZİRLİYİ

AZƏRBAYCAN TEXNİKİ UNİVERSİTETİ

Əlyazması hüququnda

Vəlizadə Sənan Yusif oğlu

Ələsgərli Kənan Rövşən oğlu

Əhmədli Araz Fikrət oğlu

Eminov Nüsrət Emin oğlu

Əliyev Əhməd Kamil oğlu

ELMİ-TEXNOLOJİ TUTUMLU SƏNAYE MÜƏSSİSƏSİNİN İNFORMASİYA İNFRASTRUKTURUNUN TƏHLÜKƏSİZLİYİ

mövzusunda

MAGİSTRLİK DİSSERTASİYASI

İxtisas: **60632 – "İnformasiya texnologiyaları və sistemləri mühəndisliyi"**

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

Elmi rəhbər: **t.e.f.d Şahverdiyeva Roza Orduxan qızı**

BAKI-2024

AZƏRBAYCAN TEXNİKİ UNİVERSİTETİ

YÜKSƏK TƏHSİL İNSTİTUTU

MAGİSTRANTIN ANDI

"Elmi-texnoloji tutumlu sənaye müəssisəsinin informasiya infrastrukturunun təhlükəsizliyi" 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.

Vəlizadə Sənan Yusif oğlu _____

Ələsgərli Kənan Rövşən oğlu _____

Əhmədli Araz Fikrət oğlu _____

Eminov Nüsrət Emin oğlu _____

Əliyev Əhməd Kamil oğlu _____

3 iyun 2024-cü il

XÜLASƏ

Elm və texnologiyaya yönəlmiş bir sənaye müəssisəsinin informasiya infrastrukturunun təhlükəsizliyi rəqəmsal aktivlərin, şəbəkələrin və sistemlərin kiber təhdidlərdən və risklərdən qorunmasını əhatə edir. Buraya məlumatların qorunması, icazəsiz girişin qarşısını almaq və kritik məlumatların düzgün işləməsini, düzgün şəbəkə seqmentasiyası və topologiyasını təmin etmək daxildir.

İnfrastrukturun təhlükəsizliyinin təmin edilməsinin əsas aspektlərinə risk qiymətləndirmələrinin aparılması, etibarlı təhlükəsizlik siyasətlərinin və prosedurlarının tətbiqi, şəbəkə və son nöqtə təhlükəsizlik tədbirlərinin tətbiqi, hadisələrə cavab planlarının hazırlanması və müvafiq qayda və standartların icrası daxildir.

Bundan başqa infrastrukturlarını təhlükəsizliyini daimi təmin oluna bilməsi üçün 7/24 TƏM xidmətinin təşkil olunması yanaşmaları işlənilmişdir. Kibertəhlükəsizliyə inteqrasiya olunmuş bir yanaşma tətbiq edərək, bu müəssisələr riskləri azalda bilər, əqli mülkiyyəti qoruya bilər və texnoloji sistemlərinin bütövlüyünü və mövcudluğunu qoruya bilər.

SUMMARY

The security of the information infrastructure of an industrial enterprise focused on science and technology involves the protection of digital assets, networks and systems from cyber threats and risks. This includes protecting data, preventing unauthorized access and ensuring the correct operation of critical data, proper network segmentation and topology.

Key aspects of ensuring infrastructure security include conducting risk assessments, implementing reliable security policies and procedures, implementing network and endpoint security measures, developing incident response plans, and implementing relevant rules and standards.

In addition, approaches to organizing 7/24 SOC services have been developed to ensure the security of their infrastructure permanently. By adopting an integrated approach to cybersecurity, these businesses can reduce risks, protect intellectual property, and maintain the integrity and availability of their technological systems.

MÜNDƏRİCAT

GİRİŞ

Mövzunun aktuallığı. 21-ci əsrin digər sektorları kimi, sənaye müəssisələri də texnologiyaların sürətli inkişafına ayaq uydurmağa məcburdurlar. Bu, informasiya texnologiyalarının sənaye proseslərində tətbiqi ilə nəticələnir və elmi-texnoloji tərəfdarlar üçün böyük imkanlar yaradır. Lakin, bu texnologiyaların sənaye müəssisələrinin informasiya infrastrukturunda tətbiq edilməsi, ciddi təhlükələri də özündə əks etdirir. Müxtəlif informasiya sistemi hücumları, məlumatlara müdaxilə, məxfi informasiyanın çıxarılması və ya informasiya bazarlarının parçalanması kimi təhlükələr, sənaye müəssisələrinin informasiya infrastrukturunun zəifliyini və məhv edilməsini ortaya qoyur. Bu təhlükələrə qarşı qorunmaq üçün informasiya təhlükəsizliyi, informasiya infrastrukturunun fəaliyyət sahəsində asılı olmayaraq əhəmiyyətli bir hissəsi olaraq diqqət çəkir. Sənaye müəssisələri, texnologiya tətbiqləri ilə məşğul olarkən informasiya təhlükəsizliyinə diqqət yetirməlidirlər. Bu, informasiya sistemlərinin, şəbəkələrin, və digər informasiya texnologiyalarının mənafelərini artırmaq və təhlükələri azaltmaq üçün strateji tədbirləri əhatə edir.

Elmi-texnoloji tutumlu sənaye müəssisələrinin informasiya infrastrukturunun təhlükəsizliyini araşdırmaq, bu sektorun sürətli inkişafında əhəmiyyətli bir rolu olan informasiya təhlükəsizliyinə diqqətin çəkilməsi baxımından vacibdir. Bütün bunlar bu mövzuda mənbələrin müzakirə edilməsi, mühüm konseptlərin tədqiqi, təhlükəsizlik standartlarının və prinsiplərinin təhlili ilə birgə elmi bir tədbirdir. Bu tədqiqat, elmi-texnoloji tutumlu sənaye müəssisələrinin informasiya təhlükəsizliyinə diqqəti artırmağa və potensial təhlükələrin qarşısını almağa kömək edə biləcək yanaşmaların araşdırılmasına həsr olunmuşdur.

Mövzu ətrafında mühüm bir müzakirə məsələsi, elmi-texnoloji tutumlu sənaye müəssisələrinin informasiya infrastrukturunun təhlükəsizliyinin artırılması və buna qarşı müdafiə strategiyalarının təkmilləşdirilməsidir. Bu, informasiya sistemlərinin qorunması, məlumatların müdafiəsi, kiber təhlükələrə qarşı mübarizə, və informasiya təhlükəsizliyi prinsiplərinin tətbiqi kimi sahələrdə tədbirləri daxil edir.

Tədqiqatın məqsədi və məsələləri. Tədqiqatın elmi-texnoloji tutumlu sənaye müəssisələrinin informasiya infrastrukturunun təhlükəsizliyini artırmağa və müxtəlif

təhlükələrə qarşı müdafiə strategiyalarını inkişaf etdirməyə kömək etməkdir. Bu yolda, tədqiqat, müxtəlif təhlükələrin təyin edilməsi, risklərin qiymətləndirilməsi, təhlükəsizlik prinsiplərinin tətbiqi, təhlükəsizlik standartlarının əsasları və sənaye müəssisələri üçün effektiv təhlükəsizlik strategiyalarının təklif edilməsi ilə əlaqələnir.

Tədqiqatın obyekti və metodikası. Elmi-texnoloji tutumlu sənaye müəssisəsinin informasiya infrastrukturunun təhlükəsizliyi sənaye şirkətlərinin, xüsusən də elm və texnologiyaya əsaslanan şirkətlərin rəqəmsal aktivlərinin və texnoloji sistemlərinin qorunmasına yönəlmişdir. Buraya təşkilat daxilində məlumat saxlayan, işləyən və ötürən bütün rəqəmsal aktivlər, şəbəkələr, verilənlər bazaları, proqram sistemləri, aparat komponentləri, serverlər, kompüterlər sənaye idarəetmə sistemləri, sensorlar və IOT cihazları daxildir. Belə bir müəssisənin metodologiyalarını tətbiq etməklə elmi-texnoloji tutumlu sənaye müəssisəsinin informasiya infrastrukturunun təhlükəsizliyini artıra, riskləri azalda, qiymətli aktivlərini və əqli mülkiyyətini qorumaq mümkündür. Bura risklərin qiymətləndirilməsi, təhlükəsizlik siyasətləri və prosedurları, şəbəkə təhlükəsizliyi və məlumatların qorunması kimi bir neçə əsas metodologiyanı nümunə göstərmək olar.

Tədqiqatın elmi yeniliyi və praktik əhəmiyyəti. Bu dissertasiya, elmi-texnoloji tutumlu sənaye müəssisələrinin informasiya infrastrukturunun təhlükəsizliyini artırmağa dair təcrübələrin və yaxşı praktikaların müzakirəsinə nəzər salmaq üçün çoxsaylı metodologiya tətbiq edir. Bu, sənaye müəssisələrinin informasiya təhlükəsizliyi üzrə mövqeyini mənimsəmələri və fəaliyyətlərini bu istiqamətdə təkmilləşdirmələri üçün tədqiqatın mənasını və önəmini vurğulayır.

Dissertasiya işinin strukturu. Dissertasiya işi giriş, 4 fəsil, nəticə və 43 elmi mənbədən ibarət ədəbiyyat siyahısı da daxil olmaqla 96 səhifədə toplanmışdır.

İlk fəsildə, elmi-texnoloji tutumlu sənaye müəssisəsinin mövcud xüsusiyyətləri nəzərə alınmaqla informasiya təminatı sisteminin təhlükəsizliyinə dair fəaliyyət istiqamətləri işlənmişdir.

İkinci fəsildə, müəssisənin kiberhücumlara qarşı təhlükəsizliyinin təmin olunmasında təhlükəsizlik prinsipləri, qayda və standartlara uyğunluq, məlumatların

sinifləşdirilməsi və həmin məlumatların mühafizəsi üçün məlumat itkisi və məlumat pozuntularının qarşısının alınması yönündə müvafiq işlər həyata keçirilmişdir.

Üçüncü fəsildə, perimetr təhlükəsizliyinin təmin olunması məqsədilə server seqmenti təhlükəsizliyi, korporativ şəbəkə təhlükəsizliyi və onun artırılması üçün Demilitarizə bölgə konsepsiyası barəsində əsaslı işlər görülmüşdür.

Sonuncu fəsildə isə informasiya infrastrukturuna daimi nəzarətin təmin olunması istiqamətində təhlükələrə cavab və loq fayllara nəzarət, Təhlükəsizlik Əməliyyatları Mərkəzinin fəaliyyət mexanizmləri və müəssisə daxilində son istifadəçi təhlükəsizliyinin əsas standart və üstünlükləri xarakterizə olunmuşdur. **Dissertasiya işində qrup üzvlərinin töhfələri.** İlk fəsil müəssisə infrastrukturunun fəaliyyət istiqamətləri və təhlükəsizliyinin ümumi problemləri haqqında olub, **Əliyev Əhməd Kamil oğlu** tərəfindən yazılmışdır.

İkinci fəsil informasiya təhlükəsizliyinin təmin olunması, məlumatların sinifləşdirilməsi və məlumat itkisinin qarşısının alınması barəsindədir, **Əhmədli Araz Fikrət oğlu** tərəfindən işlənilmişdir.

Üçüncü fəsil 2 hissəyə ayrılıb, ilk hissə server təhlükəsizliyinin təmin olunması və informasiya sistemlərində Demilitarizə bölgə adlanan yanaşmalar haqqında olub, **Vəlizadə Sənan Yusif oğlu** tərəfindən hazırlanmışdır. Digər hissə isə korporativ şəbəkə prinsipləri, perimetr təhlükəsizliyi və onun inkişaf strategiyaları haqqında olub, **Eminov Nüsrət Emin oğlu** tərəfindən hazırlanmışdır.

Sonuncu fəsil təhlükəsizlik əməliyyatları mərkəzinin fəaliyyəti, təhlükələrə cavab və loq fayllarının idarə edilməsi, son istifadəçi təhlükəsizliyinin nəzarət mexanizmləri haqqındadır. Bu hissə **Ələsgərli Kənan Rövşən oğlu** tərəfindən ərsəyə gətirilmişdir.

I FƏSİL. ELMİ-TEXNOLOJİ TUTUMLU SƏNAYE MÜƏSSİSƏLƏRİNİN (ETTSM) FƏALİYYƏTİNİN TƏŞKİLİNDƏ İNFORMASİYA TƏMİNATI SİSTEMİNİN VƏ İNFORMASİYA İNFRASTRUKTURUNUN FORMALAŞDIRILMASI XÜSUSİYYƏTLƏRİ

1.1. ETTSM fəaliyyət istiqamətləri və xüsusiyyətləri

Hər bir ölkənin iqtisadi inkişafında elmi-texnoloji innovasiya texnoparkları əhəmiyyətli rola malikdir. Çünki İnformasiya və biliklər iqtisadiyyatının infrastrukturunun əsasını elmi-texnoloji innovasiya texnoparkları təşkil edir. İnnovasiya yönümlü, informasiya və biliyə əsaslanan iqtisadiyyatın qurulmasında yüksək texnologiyalar, innovativ parklarının yaradılması əsas məqsədlərdəndir. Rəqəmsal və ya innovativ iqtisadiyyata keçid üçün yüksək texnologiyalar parkı, elm-texnoloji innovasiya texnoparkları əsas hərəkətverici qüvvədir [Ələvsət Əliyev, Roza Şahverdiyeva, 2015] .

Yeni texnologiyaların texnopark və digər innovativ müəssisələrin idarə etmə sahələrinə tətbiq olunması innovasiya fəaliyyəti ilə xarakterizə olunur. Texnoparklarda innovasiya fəaliyyəti əhatəli və çox istiqamətlidir. Ona görə də belə fəaliyyəti həm ayrı-ayrılıqda olan göstəricilərlə, həm də qrup və istiqamətlərdə birləşən göstəricilərlə xarakterizə edirlər.

Texnoparklarda innovasiya fəaliyyəti üzrə:

- Müəssisənin innovativ aktivliyi;
- Müəssisələrdə elmi-tədqiqat bölməsinin mövcudluğu;
- Daxili və xarici bazarlardakı satışın həcmində innovasiya məhsul və xidmətlərinin strukturu, xüsusi çəkisi;
- İnnovasiya fəaliyyəti nəticələrinin reytinq göstəriciləri;
- Ölkə və regionlar üzrə innovasiya fəaliyyəti ilə məşğul olan innovativ müəssisələrin strukturu;
- Maliyyə mənbələri üzrə innovasiya xərclərinin strukturu;
- İnnovasiya fəaliyyəti növləri üzrə xərclərin strukturu və xüsusi çəkisi;
- İnnovasiya üzrə məlumat mənbələrinin reytinqi;

- Texnoloji innovasiyalara mane olan faktorların reytinqi və s. kimi əsas göstəriciləri təhlil etmək lazımdır.

Göstərilən xüsusiyyətlər, mərhələlər və göstəricilər innovasiyanın formalaşmasına birbaşa təsir etdiyi kimi, onlarla əlaqədə olan informasiya təminatı və təhlükəsizliyi məsələlərinin müəyyənləşdirilməsi və həlli istiqamətlərinin işlənilməsinə də bilavasitə təsir edir [Aliyev A.G., Shahverdieva R.O., Salimkhanova S.A., 2023].

1.2. ETTSM-in informasiya təminatı sistemi və ona qoyulan tələblər

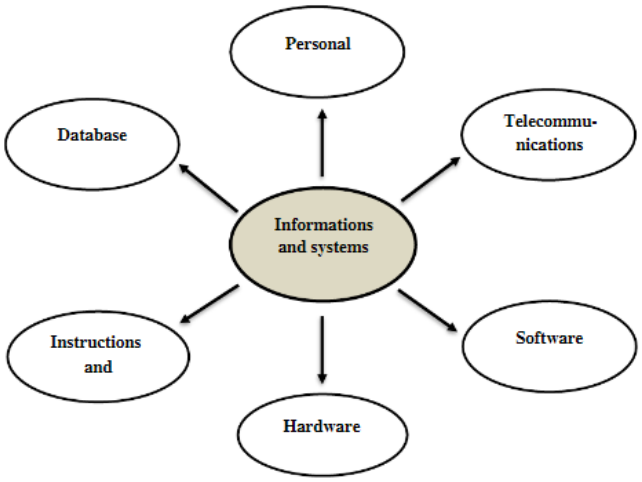
İnformasiya sistemlərini bu gün sənaye müəssisələrində istifadə olunan müasir informasiya texnologiyalarının ən təsirli vasitələrindən biri adlandırmaq olar. Müəssisələrdə informasiya sistemləri həm idarəetmə proseslərinin, həm də fərdi istifadəçilərin informasiya ehtiyaclarını ödəmək üçün geniş istifadə olunur. Yaşadığımız dövr kütləvi kompüterləşmə və İnformasiya Cəmiyyəti dövrüdür. İnformasiya cəmiyyətində müasir bir insanın iş fəaliyyəti, inkişaf etmiş bir müəssisə və təşkilatın idarə edilməsi kompüter və müasir informasiya texnologiyaları olmadan təsəvvür edilə bilməz. Planlaşdırma, istehsal mərhələlərinin idarə edilməsi, malların alqı-satqısı və s.daxil olmaqla sənaye müəssisələrində mühasibat və nəzarət məsələlərini həll edərkən kompüter texnologiyalarından intensiv istifadə olunur. Buna baxmayaraq, müasir sənaye müəssisələrinin idarə edilməsində informasiya texnologiyalarının daha intensiv və sistematik istifadəsinə ehtiyac var [Roza Şahverdiyeva, 2018].

Bazar iqtisadiyyatına uyğun dinamizm, qeyri-müəyyənlik və risklər şəraitində düzgün qərarlar qəbul etmək üçün sənaye müəssisəsinin maliyyə-təsərrüfat fəaliyyətinin müxtəlif sahələrinə (istehsal, kadr, təchizat, satış və s.) daim nəzarət etmək lazımdır. Bu səbəbdən müasir yanaşma idarəetmə digər şeylər arasında informasiya texnologiyalarına kifayət qədər investisiya tələb edir. Əlbəttə ki, müəssisə böyüdükcə investisiya miqdarı müvafiq olaraq artmalıdır. Məlumdur ki, yüksək rəqabət şəraitində informasiya texnologiyalarından daha yaxşı istifadə edən və səmərəli şəkildə təşkil olunan müəssisələr faydalanır. Beləliklə, informasiya texnologiyalarının istifadəsinə sistemli bir yanaşma tətbiq etməklə onlardan istifadənin

səmərəliliyi artırıla bilər. İnkişaf etmiş ölkələrin iqtisadi inkişaf tarixinə diqqət yetirsək, görərik ki, sənaye istehsalında sürətli iqtisadi artım və keyfiyyət dəyişiklikləri bir sıra yeni elmi və praktik vəzifələr qoyur. Bu proseslərin həyata keçirilməsi üçün texniki və texnoloji sistemlərin yaradılması, kompüter texnologiyalarının, kibernetik və riyazi modelləşdirmə metodlarının tətbiqi prioritetdir. Ölkəmizin müasir inkişaf mərhələsi idarəetmənin bütün sahələrində effektiv qərarlar qəbul etmək üçün məlumatların operativliyinə, tamlığına və etibarlılığına kəskin ehtiyac ilə xarakterizə olunur. Texnologiyanın və mühəndisliyin dayandırıla bilməyən bir sürətlə inkişaf etdiyi müasir dövrdə bu, keyfiyyət menecmenti konsepsiyasında yeni və yenilikçi metodlardan istifadə üçün şərait yaradır. Məhsulun xüsusiyyətləri bu texnologiyalardan və yenilikçi metodlardan hansını seçəcəyinizə qərar verərkən həlledicidir [Ələvsət Əliyev, 2013].

Yüksək rəqabətli sənaye məhsullarının istehsalının müxtəlif yolları var. Ancaq bütün yolların kəsişdiyi iki əsas nöqtə məlumatların işlənməsi və istehsal xərclərinin azalmasıdır. İstehsal olunan sənaye məhsullarının elm intensivliyi millətin zəka səviyyəsini təyin edən vacib elementlərdən biridir. Müasir idarəetmə yeni texnologiyalardan istifadə etməklə müxtəlif sahələrdə əldə olunan məlumatların işlənməsi yolu ilə optimal idarəetmə qərarlarının qəbul edilməsinə əsaslanır. Vaxt keçdikcə qərar qəbul etmək üçün işlənəcək məlumatların həcminin və təbiətinin dəyişməsi emal texnologiyasının dəyişməsinə, daim yenilənməsinə və müasir informasiya şəbəkəsinin və informasiya məlumat sisteminin yaradılmasına səbəb oldu. Strateji idarəetmədə bu informasiya sistemlərinin vəzifəsi şirkət rəhbərliyinə uzunmüddətli inkişaf meylləri, ən yaxşı texnologiyalar, məhsullar və idarəetmə metodları barədə məlumat verməkdir. Bu məlumatlar şirkətin uzun müddətdə rəqabət qabiliyyətini qorumasına imkan verən bir strategiya hazırlamaq üçün hazırlanmışdır [Aliyev A.G., Shahverdieva R.O., Salimkhanova S.A., 2023].

Müxtəlif istiqamətli müəssisələrdə informasiya sistemi yeni texnologiyaların və sistemli yanaşmanın köməyi ilə yaradılan və texniki, proqram, məlumat, təşkilati, metodoloji və hüquqi dəstək vasitələrindən ibarət mürəkkəb bir kompleksdir (Şək. 1.2.1.).



Şək. 1.2.1 İnformasiya təminatı sisteminin komponentləri (R.Şahverdiyeva, 2018)

Müəssisədəki informasiya sisteminin ən vacib funksiyası idarəetmə işçilərini və mütəxəssisləri qərar qəbul etmək üçün lazım olan müvafiq məlumatlarla təmin etməkdir. Bu prosesi həyata keçirmək üçün məlumatların avtomatlaşdırılmış toplanması, saxlanması, axtarışı, işlənməsi və nəticələrin istifadəçilərə verilməsini təmin etməlidir. Sənaye müəssisələrində informasiya sistemi bir və ya daha çox kompüter şəbəkəsindən, məlumat bazasından (məlumatdan), verilənlər bazası idarəetmə sistemindən, bir sıra tətbiq proqramlarından, xidmət işçiləri ilə rahat və rahat bir dialoq təmin edən bir interfeysdən ibarətdir [Roza Şahverdiyeva, 2018].

Sənaye müəssisəsində istifadə olunan informasiya ehtiyatlarının təbiətinə görə informasiya sistemlərini aşağıdakı kimi bölmək olar:

- Sənədli sistemlər;
- Faktoqrafik sistemlər;
- Məlumat axtarış motorları;
- Sənəd idarəetmə sistemləri;
- Ofis avtomatlaşdırma sistemləri;
- İnformasiya idarəetmə sistemləri;
- İnformasiya və məsləhət sistemləri.

Sənədli sistemlər təbii dildə yazılmış müxtəlif sənədlərlə (monoqrafiyalar, dövri nəşrlər, normativ hüquqi sənədlər, məqalələr, dissertasiyalar və s.) işləmək üçün

istifadə olunur. Məlumat axtarış motorları ən çox istifadə olunan iş axını sistemlərinə aid edilə bilər. Məlumat axtarış sisteminin əsas vəzifəsi sənədləri təbii dildə toplamaq və müxtəlif meyarlara uyğun axtarışlarını təmin etməkdir. Bu cür sistemlər həm müəssisə daxilində, həm də internetdə müxtəlif növ sənədlərin toplanması, sistemləşdirilməsi və axtarışı üçün istifadə olunur [Aliyev A.G., Shahverdieva R.O., Salimkhanova S.A., 2023].

Müəssisədəki informasiya sistemləri də müəssisənin təşkili metodlarına və ya memarlığına görə təsnif edilə bilər. Qeyd etmək lazımdır ki, informasiya sistemlərinin təsnifatları müəyyən mənada ənənəvidir. Əksər hallarda, böyük informasiya sistemlərində bütün və ya bəzi müvafiq problem sinifləri var. Məsələn, böyük sənaye müəssisələri üçün yaradılan korporativ informasiya sistemləri müxtəlif funksiyaları yerinə yetirən bir neçə alt sistemdən ibarət ola bilər. İnformasiya sistemlərinin yuxarıda göstərilən xüsusiyyətlərini nəzərə alaraq qeyd etmək olar ki, müəssisədə informasiya sisteminin tətbiqinin məqsədi zəruri məlumatların toplanması və sonrakı işlənməsi və çevrilməsi, istər qərar qəbul etmək, istər strateji nəzarət, istərsə də qəbul edilmiş qərarların icrası üçün məlumat tələb edən işçilərə vaxtında çatdırılmasını təmin etməkdir.müəssisə tərəfindən hazırlanmışdır. Buna görə menecerin məhsuldarlığı istənilən nəticəni əldə etmək üçün informasiya sisteminin imkanlarını idarə etmək bacarığından asılıdır. Xülasə etmək üçün bir məlumat sistemi, müəssisənin planlaşdırılmasını, nəzarətini, koordinasiyasını, qərar qəbul edilməsini və idarə edilməsini asanlaşdırmağa yönəlmiş texniki avadanlıq, proqram təminatı, infrastruktur və təlim keçmiş kadrların səmərəli birləşməsi kimi təsvir edilə bilər [Ələvsət Əliyev, 2013].

İnformasiya təminatı sistemləri müəssisələrin biznesdə qalması üçün həyati əhəmiyyətə malikdir. Qərarların qəbul edilməsində müştəri tələblərinin artması, müəssisədəki ayrı qrupların əlaqələndirilməsi informasiya təminatı sistemlərinin qurulmasının vacib səbəblərindən biridir. Xarici ətraf mühit amilləri və daxili institusional amillər, müəssislərin seçdikləri, inkişaf etdirdikləri və istifadə etdikləri informasiya təminatı sistemlərinin növlərinə təsir göstərir. Bəzi xarici ekoloji amillər - əmək xərclərinin və ya digər mənbələrin artması, rəqiblərin hərəkətləri və normativ

hüquqi aktlarda və hökumət qərarlarında olan dəyişikliklərdir. Bunları xarici məhdudiyyətlər hesab etmək olar. Eyni zamanda, ətraf mühit də müəssisələr üçün fürsət yaradır: yeni texnologiyalar, yeni kapital mənbələri, yeni istehsal proseslərinin inkişafı və ya müəyyən məhsullara tələbatı artıran yeni bir hökumət proqramı və.s təşkil edir. İnstitusional amillər İS-nin tətbiqinə və dizaynına təsir göstərir. Bunlara müəssisə üçün strateji əhəmiyyət kəsb edən məsələlərin tənzimlənməsində mühüm rol oynayan dəyərlər, normalar, maraqlar daxildir. Müəssisədə biznes proseslərinin səmərəliliyi və effektivliyində informasiya texnologiyalarının əhəmiyyəti üçün informasiya sisteminin funksional xüsusiyyətlərini qiymətləndirməyə ehtiyac var ki, bu da informasiya sistemindəki mənbələrə tələbatın sürətlə artmasına səbəb olur.İnformasiya sisteminin fəaliyyətini qiymətləndirmək aparat, proqram təminatının, kompüter şəbəkələrinin, informasiya və insan resurslarının fəaliyyətini qiymətləndirmək deməkdir. İnformasiya sisteminin fəaliyyətini qiymətləndirməyin əsas məqsədi xidmətin keyfiyyətini müasirləşdirmək və yaxşılaşdırmaqdır [Roza Şahverdiyeva, 2018].

İnformasiya sistemi çeviklik, etibarlılıq, effektivlik, təhlükəsizlik tələblərinə cavab verməlidir.

Çeviklik. Uyğunlaşma və daha da inkişaf etdirmə qabiliyyəti, informasiya sisteminin yeni şərtlərə, müəssisənin yeni ehtiyaclarına uyğunlaşma qabiliyyətini ifadə edir.

Etibarlılıq. İnformasiya sisteminin etibarlılığı, məlumatları təhrif etmədən itkisiz işləməsini nəzərdə tutur.Etibarlılıq tələbi, saxlanılan informasiyaların ehtiyat nüsxələrini yaratmaq, giriş əməliyyatları aparmaq, rabitə kanallarının və fiziki mühitin keyfiyyətini qorumaq, müasir proqram və avadanlıqlardan istifadə etməklə təmin edilir.

Effektivlik. Sistem ona ayrılmış mənbələri nəzərə alaraq, verilən tapşırıqları ən qısa müddətdə həll etməyə imkan verərsə effektivdir. Sistemin səmərəliliyi informasiyaların və onların işlənməsi metodlarının optimallaşdırılması, orijinal inkişafların, fikirlərin, dizayn metodlarının tətbiqi ilə təmin olunur.

Təhlükəsizlik. Sistemin mülkiyyəti kimi başa düşülür, bunun sayəsində icazəsiz şəxslər, onlar üçün nəzərdə tutulmuşlar istisna olmaqla, müəssisənin informasiya

mənbələrinə daxil ola bilmirlər . İcazəsiz girişdən informasiyanın qorunması sistem mənbələrinə daxil olmağa nəzarət etmək və informasiyanı qorumaq üçün müasir proqramlardan istifadə etməklə təmin edilir.İri müəssisələrdə, informasiya təhlükəsizliyini təmin edən bölmələrin yaradılır, kiçik müəssisələrdə bu sahəyə cavabdeh bir işçi təyin olunur [Ələvsət Əliyev, 2013].

1.3. ETTSM-in informasiya infrastrukturunun formalaşdırılması xüsusiyyətləri

İT infrastrukturu hər hansı bir təşkilatın texnoloji ekosisteminin təməlidir. Bu, təşkilatın informasiya texnologiyalarını dəstəkləmək və idarə etmək üçün tələb olunan aparat, proqram təminatı, şəbəkələr və xidmətlərdən ibarətdir. Dayanıqlı İT infrastrukturunun yaradılması və idarə edilməsi müasir rəqəmsal müəssisələrin düzgün fəaliyyət göstərməsi üçün böyük əhəmiyyət kəsb edir.

İT infrastrukturunun uğurla qurulmasını təmin etmək üçün strukturlaşdırılmış bir layihə planına sahib olmaq lazımdır. İT infrastrukturunun tətbiqi üçün layihə planı, infrastrukturun yerləşdirilməsi və saxlanılması üçün lazım olan vəzifələri, resursları və son tarixləri müəyyən edir. Bu plan, icra prosesinin hər mərhələsində layihə qrupuna rəhbərlik edən bir yol xəritəsi rolunu oynayır.

İT infrastrukturunda strukturlaşdırılmış Layihə İdarəetmə metodologiyası da effektiv icra üçün vacibdir. Bu metodologiya layihə fəaliyyətlərinin planlaşdırılması, təşkili və nəzarətinə əsaslanır. Tətbiqin plana uyğun getməsini, təşkilatın tələblərinə cavab verməsini və büdcə və cədvəl çərçivəsində tamamlanmasını təmin edir.

İT infrastrukturunun əhəmiyyətini dəyərləndirmək çətindir. İT, rabitə, əməkdaşlıq, məlumatların saxlanması və kritik tətbiqlərə giriş təmin edərək iş əməliyyatları üçün bir çərçivə təmin edir. Etibarlı və yaxşı xidmət göstərən İT infrastrukturu, bütövlükdə biznesin məhsuldarlığını, səmərəliliyini və effektivliyini artırır.

İT infrastrukturunun düzgün idarə edilməsi onun gələcək uğuru üçün çox vacibdir. Buraya komponentlərin monitorinqi və istismarı, problemlərin operativ həlli və performansın optimallaşdırılması daxildir. İnfrastrukturun səmərəli idarə edilməsi yüksək əlçatanlığı, etibarlılığı və təhlükəsizliyi təmin edir, uğursuzluqları minimuma

endirir və təşkilatın texnologiyaya yatırımını artırır [Aliyev A.G., Shahverdieva R.O., Salimkhanova S.A., 2023].

İT infrastrukturunun komponentləri. İT infrastrukturunun müasir komponentlərinə təşkilatın texnoloji ehtiyaclarını qarşılamaq üçün birlikdə işləyən bir neçə əsas element daxildir. Bu komponentləri anlamaq, İT infrastrukturunun inkişafı üçün hərtərəfli strategiyanın hazırlanması və həyata keçirilməsi baxımından çox vacibdir.

- **Hardware.** Bura serverlər, kompüterlər, şəbəkə cihazları, saxlama sistemləri və ətraf mühit daxildir. Təchizat, İT infrastrukturunun fiziki təməlini təşkil edir;
- **Software**. O, müxtəlif infrastruktur funksionallığını təmin edən əməliyyat sistemləri, proqramlar, verilənlər bazaları, virtualizasiya vasitələri və digər proqram təminatlarını əhatə edir. Hiperkonvergent infrastruktur (HCI) isə bir çox İT infrastruktur liderlərinin uğur qazandığı müasir texnologiyadır;
- **Şəbəkə.** Routerlər, açarlar, təhlükəsizlik duvarları və kabellər kimi şəbəkə komponentləri cihazları birləşdirir və bütün infrastrukturda məlumat ötürülməsini asanlaşdırır;
- **Məlumat mərkəzləri.** Bu mərkəzləşdirilmiş otaqlarda serverlər, saxlama sistemləri və şəbəkə avadanlığı yerləşir. Məlumat mərkəzləri optimal performans və məlumatların qorunması üçün güc, soyutma və təhlükəsizlik xüsusiyyətləri ilə idarə olunan bir mühit təmin edir;
- **Bulud xidmətləri.** Xidmət kimi infrastruktur (IaaS), xidmət kimi platforma (PaaS) və xidmət kimi proqram təminatı (SaaS) daxil olmaqla bulud hesablama xidmətləri, infrastrukturun tələblərinə uyğun olaraq genişlənə bilən və çevik həllər təklif edir;
- **Təhlükəsizlik sistemləri.** Təhlükəsizlik divarları, antivirus proqramları, müdaxilənin aşkarlanması sistemləri və şifrələmə texnologiyaları kimi infrastruktur təhlükəsizlik tədbirləri, icazəsiz giriş, məlumat pozuntuları və kibernetik təhlükələrdən qoruyur.
- **İT xidmətlərinin idarə edilməsi (ITSM).** İTSM platformaları və alətləri, hadisə idarəçiliyi, dəyişikliklər, problemlər və xidmət masası dəstəyi daxil olmaqla İT xidmətlərini effektiv şəkildə idarə etməyə imkan verir. Bu komponentlər

birlikdə işləyir, təşkilatın əməliyyatlarını və strateji hədəflərini dəstəkləyən etibarlı, genişlənə bilən və təhlükəsiz İT infrastrukturunu təmin edir.

İT infrastruktur xidmətlərinə diqqət yetirmək vacibdir. İT infrastruktur xidmətləri, bir təşkilatın informasiya texnologiyaları infrastrukturunun planlaşdırılmasını, yerləşdirilməsini, idarə edilməsini və saxlanmasını dəstəkləyən bir sıra xidmətlər və həllərdir. Bu xidmətlər, infrastruktur komponentlərinin və sistemlərinin səmərəli işləməsini təmin etmək üçün hazırlanmışdır [Roza Şahverdiyeva, 2018].

Bəzi ümumi İT infrastruktur xidmətləri:

Şəbəkə xidmətləri. Bu xidmətlər, yerli şəbəkələr (LAN), qlobal hesablama şəbəkələri, marşrutlaşdırıcılar, açarlar, təhlükəsizlik divarları və şəbəkə təhlükəsizliyi daxil olmaqla şəbəkə infrastrukturunun dizaynı, tətbiqi və idarə edilməsinə yönəldilmişdir. Şəbəkə xidmətləri etibarlı əlaqə, səmərəli məlumat ötürülməsi və təhlükəsiz təşkilati rabitə təmin edir.

Server və saxlama xidmətləri. Bu xidmətlər serverlərin və saxlama sistemlərinin hazırlanması, konfiqurasiyası və idarə edilməsini əhatə edir. Bunlara Server yerləşdirmə, virtualizasiya, saxlama şəbəkəsi (SAN) idarəetməsi, ehtiyat və bərpa həlləri və server performansının optimallaşdırılması daxildir.

Məlumat mərkəzi xidmətləri. Məlumat mərkəzi xidmətlərinə məlumat mərkəzinin fiziki obyektlərinin planlaşdırılması, tikintisi və idarə edilməsi daxildir. Buraya enerji və soyutma idarəetməsi, rafların və şkafların quraşdırılması, fiziki təhlükəsizlik və infrastrukturun yüksək mövcudluğu və etibarlılığı üçün monitorinq sistemləri daxildir.

Bulud xidmətləri. Bulud xidmətləri, təşkilatlara tələb əsasında İnternet vasitəsilə hesablama resurslarına, anbarlara və proqramlara giriş imkanı verir. Xidmət kimi infrastruktur (IaaS), xidmət kimi platforma (PaaS) və xidmət kimi proqram təminatı (SaaS) təşkilatlara geniş yerli avadanlıq və texniki xidmətə ehtiyac olmadan genişlənə bilən və çevik infrastrukturdan istifadə etməyə imkan verən bulud xidmətlərinin nümunələridir.

Təhlükəsizlik xidmətləri. Təhlükəsizlik xidmətləri İT infrastrukturunu potensial təhdidlərdən və zəifliklərdən qorumağı hədəfləyir. Bunlar təhlükəsizlik duvarları, müdaxilənin aşkarlanması və qarşısının alınması sistemləri, antivirus proqramları,

məlumat şifrələməsi və təhlükəsizlik yoxlamalarının tətbiqi kimi həlləri əhatə edir. Təhlükəsizlik xidmətləri məlumatların qorunmasına, icazəsiz girişlərin qarşısının alınmasına və tənzimləmə tələblərinə cavab verməyə yönəlmişdir.

Texniki dəstək. Texniki Dəstək, son istifadəçilərə texniki problemləri həll etməyə, aparat və proqram təminatında problemlərin həllinə kömək edir və İT infrastrukturundan istifadə üçün tövsiyələr verir. Bu xidmətlər, işçiləri infrastrukturdan səmərəli istifadə etmək üçün lazımi dəstək və resurslarla təmin edir.

İT xidmətlərinin idarə edilməsi (ITSM). İnnovasiya texnoparklarının əsas məqsədləri və onların fəaliyyətində mühüm rolu olan informasiya təhlükəsizliyinin və informasiya təminatının əhəmiyyətini dəstəkləyirəm. İnnovasiya texnoparkları, iqtisadiyyatın inkişafına və rəqabət qabiliyyətinin artırılmasına dəstək olmaq məqsədi ilə fəaliyyət göstərir. Bu texnoparkların informasiya təhlükəsizliyi və təminatı, məlumatların qorunması, informasiya sistemlərinin effektiv işləməsi və texnoparkın ümumi fəaliyyətinin səmərəliliyinin təmin edilməsi üçün əhəmiyyətli bir rol oynayır.

İnnovasiya texnoparklarının informasiya təhlükəsizliyi sistemləri, informasiya təhlükəsizliyinin standartlarını və prinsiplərini nəzərə alaraq, texnoparkın fəaliyyətini potensial təhdidlərdən və zəifliklərdən qoruyur. Bu sistemlər, müxtəlif təhlükəsizlik tədbirlərini, həm də informasiya təhlükəsizliyi proseslərinin və texnoparkın əsas texniki infrastrukturunun monitorinqini və idarə olunmasını dəstəkləyir. Bu, texnoparkın fəaliyyətində informasiya təhlükəsizliyinin və təminatının yaxşı idarə olunması və texnoparkın müştərilərinə etibarlı və səmərəli xidmətlər təklif edilməsi üçün əhəmiyyətli bir məsələdir.

Həmçinin, informasiya təminatı sistemi, texnoparkın idarə olunmasına və effektiv işləməsinə dəstək olur. Bu sistem, məlumatların toplanması, analiz edilməsi, idarə olunması və informasiya təhlükəsizliyi tədbirlərinin həyata keçirilməsi üçün lazımi məlumatı təmin edir. Bu, texnoparkın fəaliyyətində informasiya resurslarının effektiv istifadəsini və texnoparkın müştərilərinə səmərəli xidmət təqdim etməsini təmin edir.

Ümumiyyətlə, informasiya təhlükəsizliyi və təminatı ilə birlikdə informasiya təminatı sistemi, innovasiya texnoparklarının müvəffəqiyyətlə fəaliyyət göstərməsi və

onların strateji məqsədlərini həyata keçirməsi üçün əhəmiyyətli bir amildir. Bu sistemlərin mövcudluğu və effektivliyi, texnoparkların inkişafında və onların müştərilərinə dəyərli xidmətlər təklif etməsində kritik bir rol oynayır [Ələvsət Əliyev, 2013]

1.4. ETTSM-in informasiya infrastrukturunun təhlükəsizliyinin ümumi problemləri

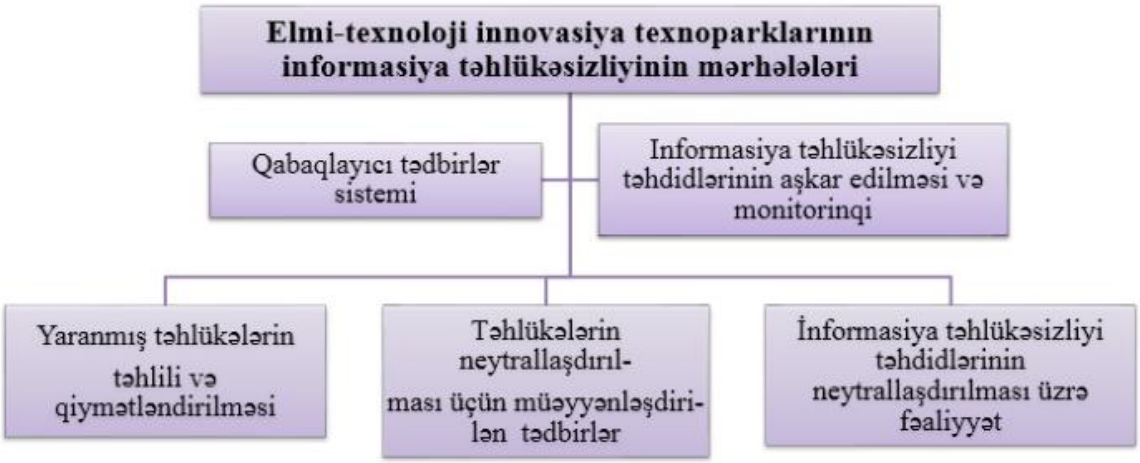
Texnoparklara daha çox təhlükə yaradan hallar arasında yerli informasiya və telekommunikasiya sənayesinin fəaliyyəti və bu sektorun infrastrukturunu formalaşdırması ilə bağlı problemlər, onların müvafiq məhsullarının istehsalı və xidmət göstərilməsi prosesində qarşılaşdıqları çətinliklər göstərilir. Bununla yanaşı, ictimai-zəruri informasiya resurslarına məhdudiyyətlər qoyulması, açıq informasiya fondlarına girişin məhdudlaşdırılması və yenilikçi texnologiyaların tətbiqinin maneələri də bu təhlükələr arasındadır. Həmçinin, informasiya manipulyasiyası, yeni informasiya texnologiyalarından imtina, intellektual mülkiyyətin sərxoşluğu, informasiya emalı texnologiyaları prosedurunun pozulması, şəbəkələrdə informasiyanın ələ keçirilməsi və onun dezinformasiya və digər mənfi məqsədlər üçün istifadəsi kimi fəaliyyətlər də təhlükələr sırasında hesaba alınır.

Texnoparkların təhlükəsizlik siyasətinin reallaşdırması üçün informasiyanın mühafizəsi metodlarına aşağıdakılar daxildir:

- Müdafiə edilən obyektlərdə kompleks müdafiənin reallaşdırılmasına imkan verən texniki vasitələr və təşkilati tədbirlər;
- Müdafiənin əsas vasitələrinin seçimi və yerləşdirilməsi üçün təklif və tövsiyələr;
- Mümkün təhlükələrin qiymətləndirilməsi, itkilərin ölçülərini nəzərə almaqla sistemin effektivliyinin qiymətləndirilməsi;
- İnformasiya təhlükəsizliyi siyasətinin dəstəklənməsi və reallaşdırılması üzrə planın hazırlaması;
- Müəssisədə informasiya təhlükəsizliyi sistemlərinin inkişafı və təkmilləşdirilməsi ilə bağlı təkliflərin hazırlanması;

- Təklif olunan mühafizə tədbirlərinin səmərəliliyini nəzərə alaraq innovasiya struktiurunun səmərəliliyin qiymətləndirilməsi.

Texnoparkların ümumi təhlükəsizlik konsepsiyasına müvafiq olaraq informasiya mühafizəsi xidmətinin praktiki fəaliyyəti nümunəvi sxem, prosedur və fəaliyyətə əsaslanır. Burada ilk növbədə həmin fəaliyyətin müəyyən ardıcıl mərhələlər üzrə həyata keçirildiyini qeyd etmək lazımdır (Şək. 1.4.1.).



Şəkil 1.4.1. Elmi-texnoloji innovasiya texnoparklarının informasiya təhlükəsizliyinin idarə olunması mərhələləri (R.Şahverdiyeva, 2018)

Texnoparkların fəaliyyətində mövcud təhlükələrin struktur təhlili informasiya risklərini müəyyənləşdirməyə və nəticə etibarı ilə həmin strukturun dayanıqlı kompleks fəaliyyət proqramını işləməyə imkan verir. Risklərin idarə olunması üçün daxili və xarici təhlükə mənbələrini müəyyən etmək və həmin təhlükə ilə yaranacaq risk və fəaliyyət nəticələri arasındakı səbəb-nəticə əlaqələrini aşkarlamaq zəruridir. **Texnoparkların fəaliyyətində informasiya təhlükəsizliyinin təkmilləşdirilməsi üçün bir sıra məsələlərə baxılır və həll edilir:**

- Texnoparkın informasiya təhlükəsizliyinin təminatı üçün məqsədli proqramın işlənilməsi;
- Texnoparkın informasiya təhlükəsizliyinin təminatı sisteminin inkişaf etdirilməsi və təkmilləşdirilməsi;

- Vahid dövlət siyasətini həyata keçirməklə informasiya təhlükəsinin proqnozlaşdırılması və qiymətləndirilməsi üzrə üsul və formaların təkmilləşdirilməsi;
- Strukturun informasiya təhlükəsizliyinin təminatı vasitələri və sistemlərinin səmərəliliyinin qiymətləndirilməsi üzrə metod və kriteriyalarının işlənilməsi;
- İnformasiya təhlükəsizliyinin təminatı sahəsində bütün innovativ müəssisə və təşkilatların fəaliyyətinin əlaqələndirilməsi;
- Milli iqtisadiyyatın vacib sahələrində texnoparkların texnoloji müstəqilliyinin təmin olunması;
- Texnoparklarda informasiyanın mühfizə edilməsində müasir üsul, metodların işlənilməsi və yeni texnologyların tətbiqi;
- İnformasiya təhlükəsizliyinin təmin olunmasında elmi-texniki və hüquqi məsələlərin həllində beynəlxalq orqanlarla və təşkilatlarla qarşılıqlı əlaqələrin genişlənləndirilməsi;
- Qlobal informasiya şəbəkələri və sistemlərinin yaradılması proseslərində regional iştirakın təmini;
- Texnoparklar üçün informasiya təhlükəsizliyi və informasiya texnologiyaları sahəsində kadrların hazırlanması üzrə vahid sistemin yaradılması [Əlövsət Əliyev, 2013, Roza Şahverdiyeva, 2018].

II FƏSİL. ETTSM-İN İNFORMASİYA TƏHLÜKƏSİZLİYİNİN TƏMİNİNDƏ MƏLUMATLARIN SİNİFLƏŞDİRİLMƏSİ VƏ MƏLUMAT İTKİSİNİN QARŞISININ ALINMASI

2.1. İnformasiya təhlükəsizliyinin təmin olunması istiqamətləri

İnformasiya sistemi aşkar edilmiş zəifliklər vasitəsilə stimullaşdırılan mövcud əks tədbirləri nəzərdən keçirmək və daha çox işə ehtiyac duyulan sahəni müəyyən etmək deməkdir. Məlumat təhlükəsizliyi menecmentinin məqsədi təhlükəsizlik insidentlərinin qarşısını almaq və təsirini minimuma endirməklə biznesin davamlılığını təmin etmək və dəyən ziyanı azaltmaqdır. İnformasiya təhlükəsizliyi (İT) təşkilatların məlumatı qorumaq üçün istifadə etdiyi alətləri və prosesləri əhatə edir. Buraya icazəsiz şəxslərin biznes və ya şəxsi məlumatlara daxil olmasının qarşısını alan siyasət parametrləri daxildir. İT şəbəkə və infrastruktur təhlükəsizliyindən tutmuş testinq və auditə qədər geniş sahələri əhatə edən böyüyən və inkişaf edən sahədir. İnformasiya təhlükəsizliyi həssas məlumatları icazəsiz fəaliyyətlərdən, o cümlədən yoxlama, dəyişdirmə, qeyd etmə və hər hansı pozulma və ya məhvetmədən qoruyur. Məqsəd müştəri hesabı detalları, maliyyə məlumatları və ya əqli mülkiyyət kimi kritik məlumatların təhlükəsizliyini və məxfiliyini təmin etməkdir. Təhlükəsizlik insidentlərinin nəticələrinə şəxsi məlumatların oğurlanması, məlumatların dəyişdirilməsi və məlumatların silinməsi daxildir. Hücumlar iş proseslərini poza və müəssisənin reputasiyasına xələl gətirə bilər, həmçinin maddi xərclərə də səbəb ola bilər. İnformasiya təhlükəsizliyinin əsas prinsipləri konfidensiallıq, bütövlük və əlçatanlıqdır. Bu prinsiplər birlikdə **CIA triadını** əmələ gətirir (Şək. 2.1.1.) [Schneier, B. 2023].

Şəkil 2.1.1. CIA triadı (Secumantra, 2024)

Konfidensiallıq - Konfidensiallıq tədbirləri məlumatın icazəsiz açıqlanmasının qarşısını almaq üçün nəzərdə tutulmuşdur. Konfidensiallıq prinsipinin məqsədi şəxsi məlumatı məxfi saxlamaq və onun yalnız ona sahib olan və ya təşkilati funksiyalarını yerinə yetirmək üçün ehtiyacı olan şəxslər üçün görünən və əlçatan olmasını təmin etməkdir.

Bütövlük - verilənlərin icazəsiz dəyişikliklərdən (əlavələr, silinmələr, dəyişikliklər və s.) qorunması deməkdir. Bütövlük prinsipi məlumatların dəqiq və etibarlı olmasını, təsadüfən və ya bilərək modifikasiya olunmamasını təmin edir.

Əlçatanlıq - Əlçatanlıq, istifadəçinin ehtiyac duyduğu zaman (və ya müəyyən vaxtda) proqram təminatı sistemlərini və məlumatlarını tam əlçatan etmək üçün sistemin qabiliyyətinin qorunmasıdır. Əlçatanlığın məqsədi texnoloji infrastrukturu, tətbiqləri və məlumatları təşkilati proses və ya müəssisənin müştəriləri üçün lazım olduqda əlçatan etməkdir [5th International conference on Information Engineering for Mechanics and Materials (ICIMM). China, 2015].

Bu prinsiplərdən əlavə İT üçün mühüm əhəmiyyət kəsb edən **inkar edilməzlik** prinsipi də mövcuddur. Bu prinsip hər hansı bir hərəkətin və ya əməliyyatın baş verdiyini və bunun konkret şəxs və ya sistem tərəfindən həyata keçirildiyini sübut etmək qabiliyyətinə istinad edir. "İnkar edilməzlik" termini bir hərəkət və ya əməliyyatın onu həyata keçirən şəxs və ya sistem tərəfindən inkar edilə bilməyəcəyini nəzərdə tutur [Bejtlich, R., 2023].

İnformasiya təhlükəsizliyi kibertəhlükəsizlikdən həm əhatə dairəsinə, həm də məqsədinə görə fərqlənir. Bu iki termin tez-tez bir-birini əvəz edir, lakin daha dəqiq

desək, kibertəhlükəsizlik informasiya təhlükəsizliyinin **alt kateqoriyası**dır. İnformasiya təhlükəsizliyi fiziki təhlükəsizlik, son nöqtə təhlükəsizliyi, məlumatların şifrələnməsi və şəbəkə təhlükəsizliyi kimi bir çox sahələri əhatə edən geniş bir sahədir. O, həmçinin məlumatı təbii fəlakətlər və server xətaları kimi təhlükələrdən qoruyan informasiya təminatı ilə sıx bağlıdır.

İnformasiya Təhlükəsizliyi Siyasəti (İTS). İnformasiya texnologiyaları aktivlərindən istifadə edərkən fərdlərə rəhbərlik edən qaydalar toplusudur. Müəssisələr işçilərin və digər istifadəçilərin təhlükəsizlik protokolları və prosedurlarına əməl etmələrini təmin etmək üçün informasiya təhlükəsizliyi siyasətləri yarada bilərlər. Təhlükəsizlik siyasətləri yalnız səlahiyyətli istifadəçilərin həssas sistemlərə və məlumatlara daxil ola bilməsini təmin etmək məqsədi daşıyır. Effektiv təhlükəsizlik siyasətinin yaradılması və uyğunluğu təmin etmək üçün addımların atılması təhlükəsizlik təhdidlərinin qarşısının alınması və azaldılması istiqamətində mühüm addımdır. Siyasətin effektivliyini artırmaq üçün müəssisədə baş verən dəyişiklikləri, yeni təhdidləri, əvvəlki pozuntulardan əldə edilən nəticələri, təhlükəsizlik sistemləri və alətlərində edilən dəyişiklikləri nəzərə alaraq onu daim yeniləmək lazımdır. Müəssisə daxilində müxtəlif departamentlərin ehtiyaclarını və aktuallığını qarşılamaq üçün, müəyyən hallarda şöbələrə və ya şəxslərə qaydalardan yayınmağa imkan verən təsdiqləmə prosesi ilə istisnalar sistemini tətbiq etmək lazımdır [Chen, L., & Wang, Y., 2022].

İnformasiya təhlükəsizliyi təhdidlərinin yüzlərlə kateqoriyası və milyonlarla məlum təhlükə vektoru var. Müasir müəssisələrdə təhlükəsizlik qrupları üçün prioritet olan əsas təhlükələr olaraq aşağıdakıları sadalaya bilərik:

Təhlükəli və ya qismən təhlükəli sistemlər. Sürət və texnoloji inkişaf çox vaxt təhlükəsizlik tədbirlərində çatışmamazlıqlara gətirib çıxarır. Belə ki, sistemlər təhlükəsizlik nəzərə alınmadan hazırlanır və müəssisədə köhnə sistemlər kimi fəaliyyətdə qalır. Müəssisələr zəif qorunan bu sistemləri müəyyən etməli və onları yamaqlamaq(patching), istismardan çıxarmaq və ya təcrid etməklə təhlükəni azaltmalıdır.

Sosial mühəndislik. Təcavüzkarların istifadəçilərə e-poçt və ya mesajlar göndərərək onların təhlükəsizliyini pozan və ya şəxsi məlumatlarını yayan fəaliyyətlərdə

olmalarına sövq edir. Təcavüzkar arzu, istək və qorxu kimi psixoloji fəndlərdən istifadə edərək istifadəçini manipulyasiya edə bilir.

Sosial mühəndislik mesajının mənbəyi etibarlı göründüyü üçün insanlar cihazlarına zərərli proqram quraşdıran linklərə kliklәməklə və ya şəxsi məlumat, etimadnamə və maliyyə təfərrüatları kimi həssas məlumatlarla təcüvazkarı təmin edirlər. Müəssisələr istifadəçiləri onun təhlükələrindən xəbərdar etməklə, şübhəli sosial mühəndislik mesajlarını müəyyən etmək və onlardan qaçınmaq yollarını öyrətməklə sosial mühəndisliyi azalda bilər. Bundan əlavə, müəssisələr sosial mühəndisliyi mənbəyində bloklamaq və ya istifadəçilərin naməlum linklərə klikləmək ya da naməlum qoşmaları yükləmək kimi təhlükəli hərəkətlər etməsinə mane olmaq üçün texnoloji sistemlərdən istifadə edilə bilər [Park, C., & Lee, H., 2020].

Son istifadəçi cihazlarında zərərli proqramlar. Müəssisədə istifadəçilər stolüstü kompüterlər, noutbuklar, planşetlər və mobil telefonlar kimi çoxlu sayda son istifadəçi cihazları ilə işləyir və bunların bir çoxu şəxsi mülkiyyətdədir, eyni zamanda təşkilatın nəzarəti altında deyil və hamısı müntəzəm olaraq internetə qoşula bilir. Bütün bu son istifadəçi cihazları üçün əsas təhlükə müxtəlif vasitələrlə ötürülə bilən, son nöqtənin özü üçün təhdid olan və həmçinin digər sistemlərdə imtiyazların artmasına(privilege escalation) səbəb ola bilən zərərli proqram təminatıdır. Ənənəvi antivirus proqramı zərərli proqramların bütün müasir formalarını bloklamaq üçün kifayət deyil və son istifadəçi kompüterlərinin təhlükəsizliyini təmin etmək üçün son istifadəçi təhlükəsinin aşkarlanması və ona cavab (EDR) kimi daha təkmil yanaşmalar inkişaf etdirilməkdədir.

Zəif şifrləmə. Şifrləmə prosesi dedikdə məlumatların şifrlənməsi nəzərdə tutulur ki, bununla da həmin məlumatlar yalnız gizli açarları olan istifadəçilər tərəfindən deşifrə oluna bilir. Bu üsul avadanlıqların itirilməsi və ya oğurlanması halında ya da təşkilati sistemlərin təcavüzkarlar tərəfindən ələ keçirildiyi halda məlumat itkisinin və ya korrupsiyanın qarşısını almaqda çox effektivdir. Təəssüf ki, bu tədbir onun mürəkkəbliyi və düzgün həyata keçirilməsi ilə bağlı hüquqi öhdəliklərin olmaması səbəbindən çox vaxt diqqətdən kənarda qalır. Müəssisələr saxlama cihazlarını almaqla, şifrləməni dəstəkləyən bulud xidmətlərindən və ya xüsusi

təhlükəsizlik vasitələrindən istifadə etməklə şifrələməni getdikcə daha çox prioritet olaraq qəbul edirlər.

Düzgün olmayan təhlükəsizlik konfiqurasiyası. Müasir müəssisələr veb aplikasiyalar, verilənlər bazaları və Amazon Veb Servis kimi provayderlərin təmin etdiyi Proqram təminatı Servis kimi (SaaS) və ya İnfrasturuktur Servis kimi və s. aplikasiyaları kimi texnoloji platformalardan və alətlərdən istifadə edirlər. Korporativ səviyyəli platformalar və bulud xidmətləri öz təhlükəsizlik xüsusiyyətlərinə malikdir, lakin bu xüsusiyyətlər müəssisə tərəfindən konfiqurasiya olunmalıdır. Səhlənkarlıq və ya insan səhvi səbəbindən yalnış təhlükəsizlik konfiqurasiyası böyük təhlükəsizlik pozuntusu ilə nəticələnə bilər. Digər problem isə "konfiqurasiya sürüşməsi"dir ki, burada təhlükəsizlik konfiqurasiyası öz aktuallığını itirdiyi zaman İT(informasiya texnologiyaları) və ya təhlükəsizlik işçilərindən xəbərsiz olaraq sistemi həssas hala gətirə bilər.

Hər bir müəssisə sistemi davamlı olaraq izləyən, konfiqurasiya boşluqlarını müəyyən edən və sistemi zəiflədən konfiqurasiya problemləri barədə xəbərdarlıq edən, hətta avtomatik düzəlişlər edən texnoloji platformalardan istifadə edərək yalnış təhlükəsizlik konfiqurasiyasını azalda bilər [Stoneburner, G., Goguen, A., & Feringa, A., 2023].

2.2. İnformasiya təhlükəsizliyində mövcud standartlara və təcrübələrə uyğunluq

Son zamanlarda informasiya sistemlərindən asılılığın artması təşkilatların öz kritik informasiyalarının kiber-cinayətlərə məruz qalmasına yol açmışdır. Nəticədə bugünkü dinamik mühitdə təşkilatın informasiya infrastrukturunun mühafizəsi üçün qabaqlayıcı yanaşmaların qəbul edilməsinə zəmin yaranmışdır. İnformasiya Təhlükəsizliyinin Uyğunluğu(İTU) müəssisələrdə informasiyanın qorunması üçün informasiya təhlükəsizliyi standartlarının və siyasətlərinin həyata keçirilməsini realizə edən qabaqlayıcı yanaşmalardan biridir [Smith, J., & Brown, A., 2021].

İnformasiya Təhlükəsizliyinin Uyğunluğu(İTU) etibarlı kibertəhlükəsizlik strategiyasının təməl daşıdır. O, müəssisənin standart və qaydalar əsasında təhdid və zəifliklərə qarşı qorunmasını əhatə edən təhlükəsizlik tədbirlərini ehtiva edir.

Məlumat təhlükəsizliyi və məlumatların məxfiliyi barədə sənaye və məkana xas çoxsaylı qaydalar mövcuddur. Aşağıda ən məşhur məlumatların qorunması qaydalarından bəziləri verilmişdir (Şək. 2.2.1.).

Şəkil 2.2.1. Uyğunluq standartı və qaydaları (Shivam Jha, 2024)

HIPAA – Rəsmi olaraq 1996-cı ildə yaradılan Health Insurance Portability and Accountability Act (Tibbi Sığortanın Daşınması və Cavabdehlik Aktı) olaraq bilinən HIPAA müəssisə və provayderlərin xəstələrin şəxsi sağlamlıq məlumatlarını məxfi və təhlükəsiz saxlamağına dair məlumat təhlükəsizliyi standartlarını müəyyən edir. Ümumi olaraq səhiyyə sahəsində olan hər hansı bir müəssisə HIPAA məlumat təhlükəsizliyi və uyğunluq standartlarına uyğun olmalıdır.

GDPR – General Data Protection Regulation (Ümumi Məlumatların Qorunması Qaydası) Avropa İttifaqı tərəfindən yaradılmış və vətəndaşların məlumatlarının məxfi və təhlükəsiz saxlanılması üçün istifadə olunan qaydadır. Avropa İttifaqında müştəriləri olan bütün müəssisələr GDPR-ə tabedir.

PCI-DSS – 2004-cü ildə yaradılan təhlükəsizlik standartları toplusudur. Payment Card Industry Security Standards Council tərəfindən idarə olunan bu uyğunluq sxemi, məlumat oğurluğu və fırıldaqçılığa qarşı kredit və debit kartlarının tranzaksiyalarının təhlükəsizliyini təmin etmək məqsədi daşıyır.

SOX – ABŞ-ın korporativ saxtakarlığın qarşısını almağa yönəlmiş Sarbanes-Oxley Qanununda (SOX) göstərilən maliyyə hesabatı, informasiya təhlükəsizliyi və audit tələblərinə uyğunluqdur.

İTU tələbləri bunlardır:

Təhlükəsizlik qaydalarını anlamaq - GDPR, SOX, HIPAA, PCI DSS və ya ISO 27001 kimi müvafiq təhlükəsizlik qaydalarını və standartlarını müəyyənləşdirmək.

Qiymətləndirmə - Mövcud uyğunluq statusunu müəyyən etmək üçün hərtərəfli təhlükəsizlik qiymətləndirməsini aparmaq. İnkişaf tələb edən boşluqların və sahələrin müəyyənləşdirilməsi.

Təhlükəsizlik siyasətləri – zəruri qaydaların xüsusi tələblərinə cavab verən təhlükəsizlik siyasəti və prosedurlarını hazırlayıb həyata keçirmək.

Girişə nəzarət – həssas məlumatlara və sistemə girişi yalnız səlahiyyətli işçilərə məhdudlaşdırmaq üçün ciddi giriş nəzarəti yaratmaq.

Məlumatların mühafizəsi - İcazəsiz girişin qarşısını almaq üçün həssas məlumatları şifrələmək.

Mütəmadi auditlər - Uyğunluğa nəzarət etmək və yaranan təhlükələri aradan qaldırmaq üçün müntəzəm təhlükəsizlik auditləri və qiymətləndirmələri aparmaq.

İşçilərin maarifləndirilməsi - Təhlükəsizlik siyasətlərini anlamaları və ona əməl etmələrini üçün işçilərə təhlükəsizlik təlimləri verilməsi.

İnsidentə cavab - Təhlükəsizlik pozuntularını və məlumat insidentlərini effektiv idarə etmək üçün insidentlərə cavab planı yaratmaq.

Sənədləşdirmə - Təhlükəsizlik tədbirləri, insidentlər və uyğunluq fəaliyyətlərinin ətraflı araşdırılması və xüsusi qeydlərin aparılması [David G. Hill, Кучеренко, В. 2020].

2.3. İnformasiya təhlükəsizliyində məlumatların sinifləşdirilməsi

Verilənlərin təsnifatı verilənləri növünə, həssaslığına və dəyərinə (dəyişdirildikdə, oğurlandıqda və ya məhv edildikdə müəssisə üçün kəsb etdiyi əhəmiyyətinə) görə sinifləşdirir. O, müəssisəyə məlumatlarının dəyərini anlamağa, məlumatların risk altında olub-olmadığını müəyyən etməyə və riskləri azaltmaq üçün nəzarətləri həyata keçirməyə kömək edir.

Məlumatların təsnifatı həmçinin müəssisəyə SOX, HIPAA, PCI DSS və GDPR kimi müvafiq sənayeyə xas tənzimləyici mandatlara əməl etməkdə kömək edir.

Məlumat təsnifatının tipləri. Məlumatlar məzmununa, aid olduğu sənayeyə, tətbiq olunan tənzimləmə qaydasına və formatına əsasən çoxsaylı müxtəlif yollarla sinifləndirilə və təhlil edilə bilər, lakin bütün məlumatlar arasında ardıcıllıq yaratmaq üçün məlumatların bir neçə əsas növü mövcuddur (Şək. 2.3.1.):

- İctimai məlumatlar - iş elanları və press-relizlər kimi ictimaiyyətlə paylaşıla bilən məlumatlardır;
- Daxili məlumatlar - bəzi məqamlarda fərdlərin e-poçt və əlaqə məlumatlarını ehtiva edən, ictimai məlumatlarla müqayisədə daha həssas, lakin sui-istifadə edildikdə konfidensial məlumatlardan daha az zərər verən məlumatlar hesab edilir. Bu tip məlumatlar adətən böyük qismdə səlahiyyətli işçilər qrupu və podratçılar kimi üçüncü tərəflər arasında paylaşılır;
- Konfidensial məlumatlar - şəbəkə və infrastruktur məlumatları kimi müəssisənin əməliyyatları üçün daxili məlumatlardan daha vacib və yaxud daha həssas olan məlumatlar sayılır. Sui-istifadəsi zamanı təşkilatın rəqabət mövqeyinə və nüfuzuna orta dərəcədə ziyan vura və ya fərdlər üçün orta dərəcədə risklər yarada bilər. Konfidensial məlumatlara daxil olma səlahiyyətinə malik işçilər qrupu və üçüncü tərəflər daxili məlumatlara nisbətdə daha kiçik miqyası əhatə edir;

1. Məhdudlaşdırılmış məlumatlar - fərdlərin sağlamlıq və ya maliyyə məlumatları ya da məxfilik müqaviləsi ilə təmin olunan strateji biznes məlumatları kimi yüksək həssaslıqda elementlərdən ibarətdir. Bu cür məlumatların icazəsiz əldə edilməsi və istifadəsi tənzimləyici və ya müqavilə tələblərini poza, müəssisə və fərdlər üçün ciddi nəticələrə səbəb ola, təşkilatın rəqabət mövqeyinə və ya nüfuzuna geri dönüşü olmayan şəkildə təsir edə və fərdlər üçün yüksək risklər yarada bilər. Məhdudlaşdırılmış məlumatlar, məlumat əldə etmək üçün strateji biznesi olan səlahiyyətli işçilər, podratçılar və biznes tərəfdaşlarından ibarət daha kiçik qrupla məhdudlaşır [Harold F. Tipton, Micki Krause].

Şəkil 2.3.1. Məlumatların növləri (UCSF Data Resources, 2024)

Məlumatların daxili, konfidensial və ya məhdudlaşdırılmış kimi təsnif edilə biləcəyini müəyyən etmək üçün müəssisələr üç yanaşma tətbiq edə bilər:

Məzmun əsaslı təsnifat - faylların və ya sənədlərin məzmunu əsasında həssas məlumatları müəyyən edir. (məsələn, şəxsi müəyyən edə bilən informasiya (PII)). Məzmun əsaslı təsnifat "faylda/sənəddə nə var?" sualına cavab verir;

Kontekst əsaslı təsnifat - faylı yaradan proqram (məsələn, mühasibat proqramı), sənədi yaradan şəxs (məsələn, maliyyə işçisi) və ya faylların yaradıldığı və ya dəyişdirildiyi məkan (məsələn, maliyyə və ya hüquq şöbəsinin binaları) kimi meta verilənlər əsasında faylların təsnifatını nəzərdə tutur;

İstifadəçi əsaslı təsnifat - məlumatlı istifadəçinin şəxsi mühakiməsi əsasında məlumatları təsnifatlandırır. Sənədlərlə işləyən şəxslər məlumatların nə qədər həssas olduqlarını müəyyən edə bilərlər - onlar bunu sənədi yaratdıqda, əhəmiyyətli redaktə və ya nəzərdən keçirmədən sonra və yaxud sənəd buraxılmazdan əvvəl edə bilər [Charu C. Aggarwal].

Məlumatları təsnifatlandırmaq üçün daha 2 yanaşma istifadə oluna bilər ki, bunlar məlumat vəziyyəti və məlumat formatıdır. Məlumat vəziyyətləri arasındakı xüsusiyyətləri və fərqləri anlamaq təşkilatlara həssas məlumatları daha təhlükəsiz idarə etməyə kömək edə bilər. Məlumat **üç** vəziyyətdən birində mövcuddur - saxlanılan halda, hərəkət halında və istifadədə.

Saxlanılan halda olan məlumatlar kompüterin yaddaşında olan heç ya da nadir halda girişi olan və ya mübadilə edilməyən bütün məlumatları əhatə edir. İşçinin kompüterinin hard diskində saxlanılan mühüm korporativ faylları, xarici hard diskdə olan faylları, yaddaş sahəsi şəbəkəsində (SAN) qalan məlumatları və ya saytdan kənar ehtiyat nüsxə xidməti göstərən təminatçının serverlərindəki faylları misal olaraq

göstərə bilərik. Saxlanılan halda olan məlumatlar digər vəziyyətdə olan məlumatlarla müqayisədə sabit hesab olunur. Sistemlər və ya cihazlar arasında hərəkət etmir və CPU tərəfindən emal edilmir.

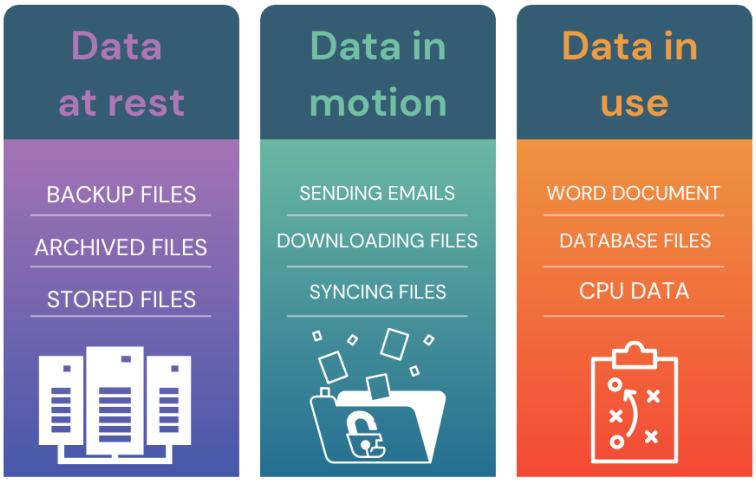
Müəssisələr, dövlət qurumları və digər qurumlar hərəkətsiz halda olan məlumatlara qarşı təcavüzkarlar tərəfindən törədilən təhlükələrin qarşısını almaq məqsədilə məlumatların şifrələnməsi, iyerarxik parolla qorunması, təhlükəsiz server otaqları və kənar məlumatların mühafizəsi xidmətləri kimi qorunma üsulları ilə xüsusi tədbirlər görürlər. Bundan əlavə, çoxfaktorlu autentifikasiya və işçilər üçün ciddi məlumat təhlükəsizliyi protokolları hərəkətsiz halda olan məlumatları qorumağa kömək edir.

Hərəkət halında olan məlumatlar kompüter sistemləri arasında və ya sistemdaxili ötürülən məlumatlardır. Bulud yaddaşı və lokal fayl saxlama nöqtəsi arasında hərəkət edən və ya bir şəbəkədən digərinə keçən məlumatlar da hərəkət halında olan məlumatlar hesab olunur. Buraya hətta, kompüterin əməli yaddaşından emal edilməyə, yenilənməyə və ya sadəcə oxunmağa hazır olan məlumatlar daxildir. Hərəkət halında olan məlumatlar sistem daxilində simsiz və ya kabellə ötürülə bilər. Bundan əlavə, bir FTP saytı və ya e-poçt daxilində bir qovluqdan digərinə atılan fayllar hərəkətdə olan məlumatlar hesab olunur.

Digər vəziyyətlərdəki məlumatlar kimi, hərəkətdə olan məlumatların da təcavüzkarlar tərəfindən ələ keçirilməsinin qarşısını almaq üçün şifrələmək lazımdır. Hərəkətdə olan məlumat üçün ümumi şifrələmə formalarına məlumatın ötürülməzdən əvvəl (məlumatın hərəkətsiz halında) və ya verilənlərin göndərildiyi kanalın şifrələnməsi daxildir [Park, C., & Lee, H., 2020].

İstifadədə olan məlumatlar sistem tərəfindən hazırda yenilənən, emal edilən, əldə edilən və oxunan verilənlərdir. Bu halda olan məlumatlar bir və ya bir neçə istifadəçi tərəfindən birbaşa əlçatan olduğundan, məlumatların hücumlara ən həssas olduğu və şifrələmənin ən vacib olduğu vəziyyət budur. Şifrələmə ilə yanaşı, istifadə olunan məlumatların qorunmasının bəzi mühüm üsullarına bütün mərhələlərdə istifadəçilərin autentifikasiyası, yüksək səviyyədə kimlik menecmenti və müəssisə daxilində profillər üçün verilən icazələr daxildir. Rəqəmsal qorunma formalarından

başqa, müəssisələrin işçilərinin əldə etdikləri məlumatların mühafizəsi ilə bağlı gizlilik müqavilələrini imzalaması lazımi addımlardan biridir (Şək 2.3.2.) [38].

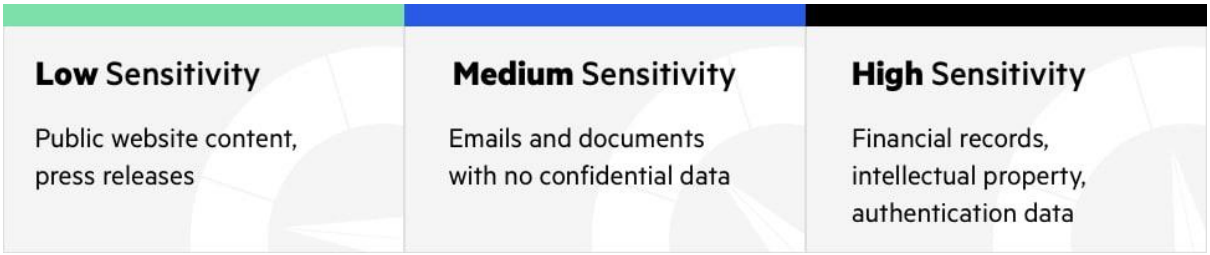


Şəkil 2.3.2. Məlumat vəziyyətləri (Nader Elmansi, 2024)

Göstərilən məlumat vəziyyətlərindən asılı olmayaraq, konfidensial olaraq təsnif edilən məlumatlar həmişə konfidensial olaraq da qalmalıdır.

Məlumatlar formatına əsasən strukturlaşdırılmış və strukturlaşdırılmamış olaraq iki yerə bölünür. Strukturlaşdırılmış məlumatlar adətən insanlar tərəfindən oxuna və indeksləşdirilə bilər. Strukturlaşdırılmış verilənlərə nümunələr verilənlər bazası obyektləri və elektron cədvəllərdir. StrukturlaŞdırılmamış məlumatlar adətən insan tərəfindən oxuna və indeksləşdirilə bilməz. Strukturlaşdırılmamış verilənlərə misal olaraq mənbə kodu, sənədlər və binar faylları göstərmək olar [Charu C. Aggarwal].

Məlumatın həssaslıq səviyyələri. Məlumatlar həssaslıq səviyyəsinə görə aşağıdakı kimi təsnif edilir (Şək. 2.3.3.):



Şəkil 2.3.3. Məlumatın həssaslıq dərəcələri (Donia Fadil, 2022)

Aşağı həssaslıqda məlumatlar - ümumi istifadə üçün nəzərdə tutulub. Buna görə də ictimai vebsaytlar, press-relizlər və xəritələr aşağı həssaslıq kateqoriyasına aid edilə bilər.

Orta həssaslıqda məlumatlar - Orta həssaslıqda məlumatlar adətən müəssisə daxili saxlanmalıdır və icazəsiz əldə olunarsa orta dərəcədə zərər verə bilir. Şirkətlərin sözləşmə müqavilələri, müştəri adı və əlaqə məlumatları kimi şəxsi məlumatlarla əlaqəli müəyyən atributlar, e-poçt və konfidensial məlumatları olmayan sənədlər orta həssaslıq kateqoriyasına daxildir.

Yüksək həssaslıqda məlumatlar - ümumiyyətlə qayda və ya tənzimləmə ilə qorunan, təhlükəyə məruz qaldıqda ciddi nəticələrə səbəb ola bilən məlumatlar aiddir. Həssas şəxsi və qorunan tibbi məlumatlar, maliyyə qeydləri, əqli mülkiyyət, autentifikasiya məlumatları və s. yüksək həssaslıq kateqoriyasına uyğun gəlir.

Kiberhücumlar müəssisə və fərdlər üçün əhəmiyyətli risklər yaradır. Bu hücumların yaratdığı risklərdən bəziləri bunlardır:

Reputasiyaya dəyən zərər - Kiberhücumlar təşkilatın reputasiyasına və etibarına xələl gətirə bilər ki, bunun da həlli çətin və uzun müddət tələb edə bilər.

Məlumat itkisi - Kiberhücumlar həssas məlumatların oğurlanması və ya məhv edilməsi ilə nəticələnə və məlumat itkisinə səbəb ola bilər [Stoneburner, G., Goguen, A., & Feringa, A., 2023].

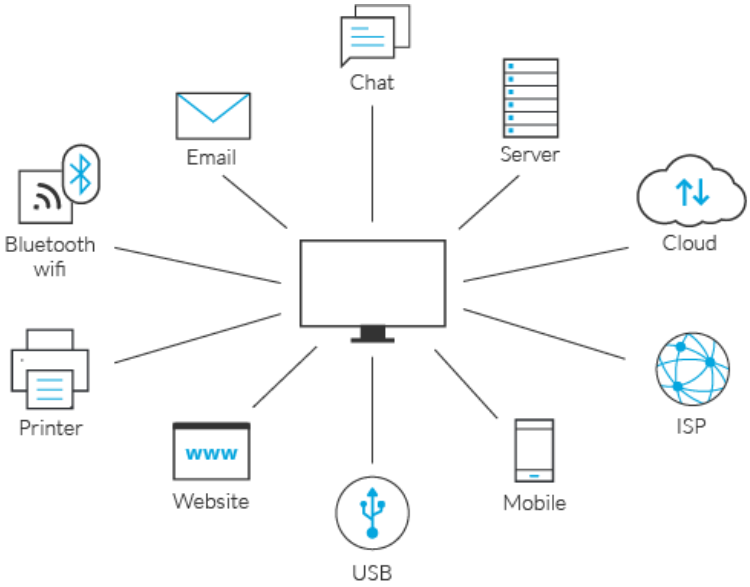
2.4. Məlumat itkisinin qarşısının alınması üçün yanaşmalar (Data Loss Preventing(DLP))

Məlumat İtkisinin Qarşısının Alınması (DLP) məlumat pozuntularının, məxfi məlumatların xaric edilməsinin və ya arzuolunmaz məhvinin aşkar edilməsi və qarşısının alınması təcrübəsidir. Müəssisələr öz məlumatlarını qorumaq və təhlükəsizliyini təmin etmək, həmçinin qaydalara riayət etmək üçün DLP-dən istifadə edirlər. “DLP” termini müəssisələri həm məlumat itkisinə, həm də məlumat sızmasının qarşısının alınmasına qarşı müdafiə etməni istinad edir. Məlumat itkisinin qarşısının alınması(DLP) məlumatların müəssisənin sərhədlərindən kənarda qeyri-qanuni ötürülməsinin qarşısını almağa yönəlmişdir. DLP həlli antivirus, süni intellekt və maşın öyrənməsi kimi vasitələrdən istifadə edərək müəssisənin icazəsiz istifadəçilərə məruz qalmadan məlumatları necə sinifləşdirilməsi, bölüşülməsi və qorunmasını

müəyyən edən DLP siyasətinə əsasən məzmunu müqayisə etməklə şübhəli fəaliyyətləri aşkarlamağı nəzərdə tutur (Şək 2.4.1.).

Müəssisələr adətən DLP-dən istifadə edir:

- Şəxsi müəyyənləşdirə bilən informasiyanı(PII) qorumaq və müvafiq qaydalara əməl etmək üçün;
- Müəssisə üçün vacib olan əqli mülkiyyəti qorumaq üçün;
- Böyük müəssisələrdə məlumatların görünməsinə nail olmaq üçün;
- Öz Cihazını Gətir (BYOD) mühitlərində işçi qüvvəsinin təhlükəsizliyini təmin etmək üçün;
- Uzaqdan bulud sistemlərində məlumatların təhlükəsiz saxlanması üçün;



Şəkil 2.4.1. Müxtəlif mənbələrdə DLP (Technoveraco, 2024)

Məlumat itkisinin səbəbləri. Məlumat sızmasının 3 təməl səbəbi vardır:

- Daxili təhdidlər - bədniyyətli insayder və ya imtiyazlı istifadəçi hesabını ələ keçirmiş təcavüzkar onun icazələrindən sui-istifadə edir və məlumatları müəssisədən kənara çıxarmağa cəhd göstərir;
- Hücumçular tərəfindən xaricdən təsir - bir çox kiber hücumun əsas hədəfi həssas məlumatlardır. Təcavüzkarlar fişinq, zərərli proqram təminatı və ya kod inyeksiyası kimi üsullardan istifadə edərək təhlükəsizlik perimetrinə nüfuz edir və həssas məlumatlara giriş əldə edə bilir;

- Qəsdən və ya ehtiyatsızlıqdan məlumatların ifşası - məlumat sızması adətən, həssas məlumatları ictimai yerlərdə itirən, məlumatlara açıq İnternet çıxışı təmin edən və ya müəssisənin siyasətlərinə uyğun olaraq girişi məhdudlaşdırmayan işçilər ucbatından baş verir;

2. **Məlumat itkisinin qarşısının alınması üsulları.** Məlumatların itkisi və sızmasının qarşısını almaq üçün standart təhlükəsizlik vasitələrindən istifadə oluna bilər. Məsələn, Intrusion Detection System (Hücumun Aşkarlanması Sistemi) təcavüzkarın həssas məlumatlara daxil olmaq cəhdləri barədə xəbərdarlıq etmə qabiliyyətinə malikdir. Antivirus proqramı həssas sistemlərə zərər verilməsinin qarşısını ala bilir. Firewall hər hansı icazəsiz şəxslərin həssas məlumatları saxlayan sistemlərə girişini bloklaya bilər [Harold F. Tipton and Micki Krause].
3. Məlumat itkisinin qarşısının alınması prosesində, həmçinin Security Operations Center (Təhlükəsizlik Əməliyyatları Mərkəzi) alətlərindən istifadə oluna bilər. Məlumat sızmasını təşkil edə biləcək hadisələri aşkar etmək və əlaqələndirmək üçün Security Information and Event Management (Təhlükəsizlik Məlumatları və Hadisələrin İdarə Edilməsi (SIEM)) sistemindən istifadə etmək mümkündür [Larry J. Whiteside Jr. and Kim-Kwang Raymond Choo].

III FƏSİL. ELMİ-TEXNOLOJİ TUTUMLU SƏNAYE MÜƏSSİSƏLƏRİNİN İNFORMASİYA İNFRASTRUKTURUNDA SERVER SEQMENTİ VƏ PERİMETR TƏHLÜKƏSİZLİYİ

3.1. Server seqmentinin təhlükəsizliyinin təmin olunmasına yanaşmalar

Bu fəsildə biz server seqmentinin təhlükəsizliyinin əsas əhəmiyyətini və rəqəmsal dünyada onun təkamülünü araşdıracağıq. İnternetin əlaqələrinin, məlumat mübadiləsini artan tendensiyaları özüylə birlikdə kibertəhlükələri də gətirir. Serverlər biznes prosesin əsasını təşkil etdiyindən şəbəkəmizin digər komponentlərindən daha çox serverlərin təhlükəsizliyinə önəm verməliyik. Server təhlükəsizliyinin üzləşdiyi çoxşaxəli problemləri həll etmək üçün tələb olunan bəzi yanaşmalar haqqında aşağıda daha geniş məlumat verilib. Müasir informasiya texnologiyalarının dinamik mənzərəsində serverlərin rolu təşkilati şəbəkələr daxilində problemsiz kommunikasiya, məlumatların saxlanması, biznes prosesinin davamlılığı və proqramların çatdırılmasını asanlaşdırmaqda böyük əhəmiyyət kəsb edir. Müəssisələr öz əməliyyatlarını idarə etmək üçün getdikcə və bir-biri ilə əlaqəli sistemlərə etibar etdikcə, server seqmentlərinin təhlükəsizliyi kritik bir problemə çevrilir. Həssas məlumatları, əqli mülkiyyəti və təşkilati infrastrukturların bütövlüyünü qorumaq üçün möhkəm tədbirlər tələb edən kiber təhlükələr inkişaf etməyə davam edir. Bu fəsildə server seqmentinin təhlükəsizliyinin mürəkkəb sahəsini araşdırır, şəbəkə daxilində serverlərin perimetrlərini gücləndirməyə yönəlmiş metodologiyaları, texnologiyaları və ən yaxşı təcrübələri araşdırır. Əsas məqsəd müasir kibertəhlükələrin yaratdığı problemləri araşdırmaq və proaktiv müdafiə mexanizmi kimi server seqmentasiyasının strateji həyata keçirilməsinə dair hərtərəfli fikirləri təmin etməkdir.

Bir-birinə bağlı sistemlərin və rəqəmsal asılılığın müasir mənzərəsində server təhlükəsizliyi təşkilati aktivlərin və həssas məlumatların qorunmasında, işlənməsində təməl daşı kimi dayanır. Bu fəsil təşkilatların üzləşdiyi çətinlikləri, yaranan tendensiyaları və inkişaf edən təhlükə mənzərəsini əhatə edən server təhlükəsizliyinin cari vəziyyətinin dərin təhlilini təqdim edir. Hazırkı ssenarini hərtərəfli başa düşməklə, bu tədqiqat effektiv server təhlükəsizlik strategiyalarının sonrakı tədqiqi üçün əsas

yaratmaq məqsədi daşıyır. Kiber təhdidlər serverlərin bütövlüyü, məxfiliyi və əlçatanlığı (CIA) üçün əhəmiyyətli risklər yaradaraq inkişaf etməkdə davam edir. Zərərli aktorların zəifliklərdən istifadə etmək üçün amansız axtarışları və yeni hücum vektorlarının yaranması server təhlükəsizliyinə ayıq və adaptiv yanaşma tələb edir. Bu bölmə təşkilatların hal-hazırda üzləşdiyi müxtəlif təhdidlər spektrini araşdırır və aşağıdakı bölmələrdə müzakirə olunan problemlər üçün kontekstual fon təqdim edir.

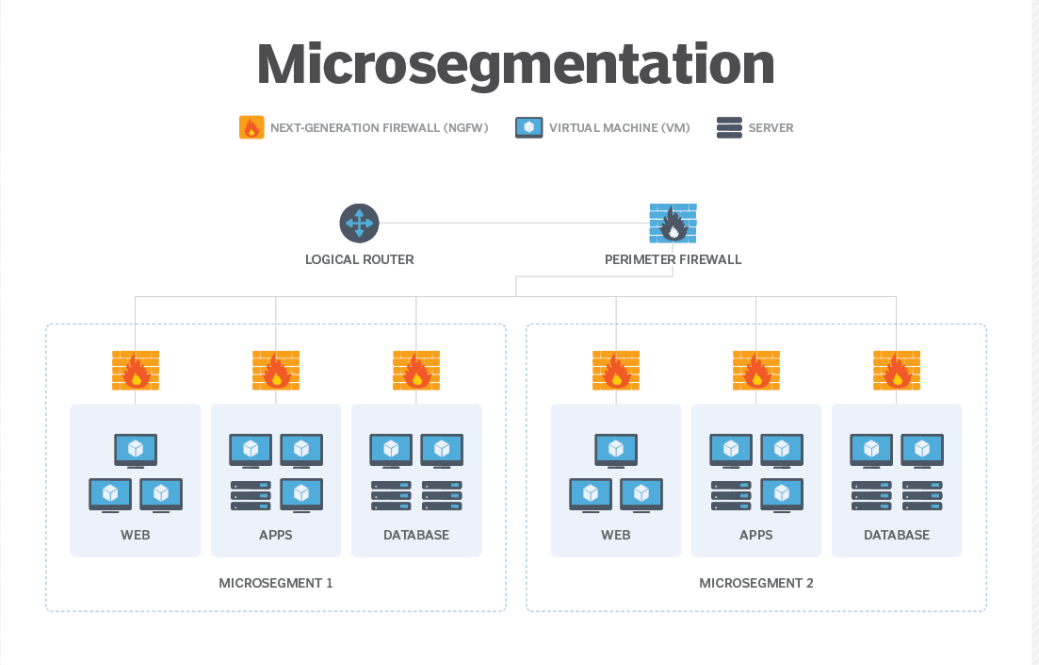
Təşkilatlar serverlərinin təhlükəsizliyini təmin etmək üçün çoxşaxəli çətinliklərlə mübarizə aparırlar. Sürətlə inkişaf edən sıfır gün zəifliklərindən tutmuş daxili fəaliyyətlərin davamlı təhlükəsinə qədər mürəkkəbliklər genişdir. Bundan başqa bulud təhlükəsizliyi ilə bağlı narahatlıqlar, artan hücum səthləri və təhlükəsizlik və istifadəçi əlçatanlığı arasında mürəkkəb tarazlıq kimi məsələlərə işıq salmaqla problemlərin təfərrüatlı tədqiqini aparılması vacibdir [Al-Serhani, M., & Chatterjee, S., 2021].

Şəbəkə təhlükəsizliyində seqmentasiyanın rolu. Şəbəkə seqmentasiya strategiyaları, günümüzdə artan kiber təhlükələr və məlumatların təhlükəsizliyi ilə bağlı artan narahatlıqlar nəticəsində əhəmiyyət qazanır. Şəbəkə seqmentasiyası şəbəkəni funksional domenlərə bölmək və bu domenlər arasında əlaqəni məhdudlaşdırmaq təcrübəsidir.

Məsələn, müəssisə mühasibat uçotu, HR, məhsulun inkişafı, istehsal, müştəri xidməti, marketinq, satış və binanın avtomatlaşdırılması üçün ayrıca seqmentlər yarada bilər. Şəbəkənin heç bir hissəsi istisna edilmir. Seqmentasiya bulud hesablamaları, eləcə də SaaS proqramları üçün işləyir. Bu strategiyalar, şəbəkə infrastrukturunu məntiqi bölgələrə bölərək təhlükəsizliyi və performansı artırmağı məqsədləyir.

Seqmentlər arasında əlaqə təhlükəsizlik təcrübələrinin şəbəkəni təhlükəsiz saxlaya biləcəyi xüsusi yerlərdə idarə olunur. Şəbəkə təhlükəsizliyi qrupları müdaxilənin aşkarlanması, müdaxilədən mühafizə və təhlükəsizlik divarı ilə dərin paket yoxlaması kimi vasitələrdən istifadə edə bilər.

Mikroseqmentasiya, hər cihaz və ya tətbiq üçün ayrı bir təhlükəsizlik sahəsi yaradaraq daha effektiv bir təhlükəsizlik təmin edir (Şək. 3.1.1.) [Новиков, С., 2021, Красильников, А., 2023].



Şəkil 3.1.1. Mikroseqmentasiya (Techtarget, 2020)

Ancaq, mikroseqmentasiyanın tətbiqi bəzi çətinliklərlə üzləşə bilər. Bu çətinliklər arasında aşağıdakılar ola bilər:

1. Tətbiq Kompleksliyi: Şəbəkə infrastrukturunu mikro-seqmentləmək mürəkkəb bir proses ola bilər. Fərqli cihazlar, tətbiqlər və istifadəçi qrupları arasında doğru quruluşu tapmaq və ehtiyacları anlamaq əhəmiyyətli rol oynayır.

2. İdarəetmə Çətinlikləri: Mikro-seqmentasiya, idarəetmə tələblərini artırabilir. Hər bir seqmentin müstəqil idarə olunması və nəzarət olunması tələb oluna bilər, bu da əməkdaşlığın əlavə resurs və vaxt tələb edə bilər.

3. Performans Təsiri: Mikro-seqmentasiyanın şəbəkə performansı üzərindəki təsiri nəzərə alınmalıdır. Hər bir seqment arasındakı trafiki yönləndirmək və nəzarət etmək, şəbəkə performansını təsir edə bilər.

Lakin, bu çətinliklərə baxmayaraq, mikroseqmentasiyanın bir sıra faydaları var:

1. Daha Yaxşı Təhlükəsizlik: Mikro-seqmentasiya, kiber hücumların yayılmasını məhdudlaşdıraraq şəbəkə təhlükəsizliyini artırır. Bir hücum bir seqmentdə məhdudlaşır və digər seqmentlərə yayılma imkanı azalır.

2. Daha Yaxşı Uyğunluq və Nəzarət: Fərqli istifadəçi qrupları və ya tətbiqlər üçün müxtəlif seqmentlər yaradaraq uyğunluq tələblərini qarşılayaraq və nəzarətləri asanlaşdıraraq daha da rahatlaşır.

3. Daha Yaxşı Sürət və Effektivlik: Mikro-seqmentasiya, bəzi istifadə halları üçün optimizasiya edilmiş trafikin daha sürətli və effektiv şəkildə ötürülməsini təmin edə bilər.

Reallığa uyğun senariləri tədqiq edərək uğurlu seqmentasiya memarlıqlarını göstərmək, təşkilatların şəbəkə infrastrukturunu gücləndirmək məqsədilə əhəmiyyətlidir. Bu senarilər, xüsusilə sənayenin tələblərini, biznesin məqsədlərini və mövcud infrastruktur strukturlarını nəzərə alaraq tənzimlənə bilər. Tətbiq nümunələri digər şirkətlərin oxşar strategiyalardan istifadə etmələrinə və tətbiqlərini uğurla apararaq təmin etmələrinə kömək edə bilər. Nəticədə, mikro-seqmentasiya strategiyalarının teorik prinsipləri ilə praktiki tətbiqləri arasındakı qarşılıqlı tarazlıq, güclü və təhlükəsiz bir şəbəkə infrastrukturu yaratmağın əhəmiyyətli bir hissəsidir.

İstifadəçi Autentifikasiyası və Giriş Nəzarəti. İstifadəçi kimlik doğrulama ve girişə nəzarət informasiya sistemlerinin təhlükəsizliyini təmin etmək üçün əsas bir tələbdir. Bu konseptlər, yetkilendirilməmiş girişlərin qarşısını almaq və həssas məlumatlara yalnızca səlahiyyətli şəxslərin girişini təmin etmək üçün istifadə olunur. Burada, əsas elementlər, çox faktorlu kimlik doğrulama və adaptiv giriş nəzarəti kimi daha müasir texnikalarla gücləndirilir.

Çox faktorlu kimlik doğrulama, istifadəçilərin kimliklərini doğrulamaq üçün bir neçə doğrulama metodundan istifadə edilməsini tələb edir. Ənənəvi olaraq, bu metodlar aşağıdakıları əhatə edir:

Bir şifrə və ya PIN ilə birlikdə, SMS ilə göndərilən doğrulama kodu və ya bir biometrik doğrulama kimi fiziki bir cihazın istifadə edilməsi. Bu yanaşma, bir tək kimlik doğrulama metodu ilə müqayisədə daha yüksək bir təhlükəsizlik səviyyəsi təmin edir, çünki hücumçunun birdən çox doğrulama metodunu ələ keçirməsi daha çətindir [С.С.Козунова., 2016, Сидоров, К., 2021].

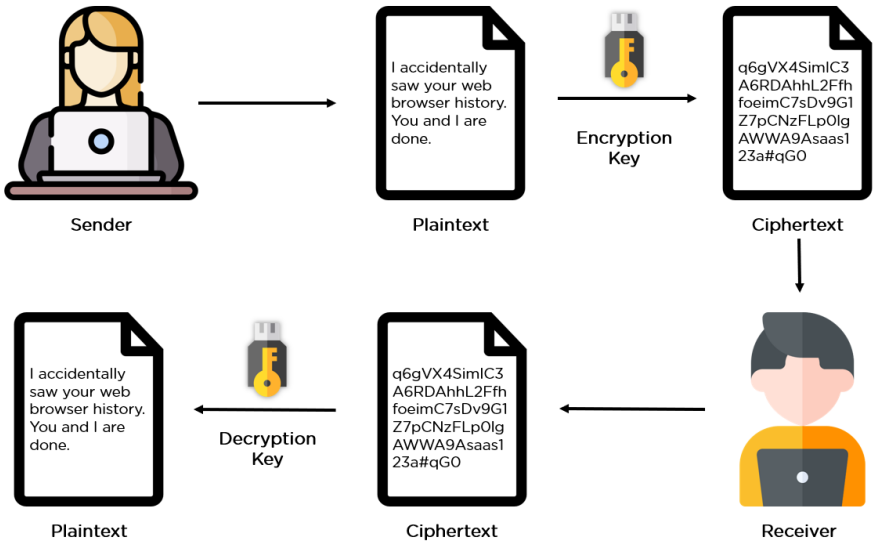
Adaptiv giriş nəzarəti isə istifadəçilərin giriş hüquqlarını dinamik şəkildə idarə edən və qiymətləndirən bir yanaşmadır. Bu, istifadəçilərin davranışlarını və giriş alışqanlıqlarını izləyərək, qeyri-adi və ya potensial olaraq təhlükəli fəaliyyətləri aşkar edə bilər və buna görə də giriş siyasətlərini avtomatik olaraq adaptasiya edə bilər. Məsələn, bir istifadəçinin normal iş saatlarının xaricində sistemə giriş etməyə çalışması

və ya normaldan fərqli bir yerə giriş etməsi halında, adaptiv giriş nəzarəti, əlavə doğrulama addımları və ya girişi məhdudlaşdırma kimi tədbirlər ala bilər.

Giriş nəzarəti çərçivələrinə biometrik və davranış analitikası inteqrasiyası, istifadəçilərin fiziki xüsusiyyətlərini (biometrik məlumatlar) və istifadəçi davranışlarını (davranış analitikası) istifadə edərək kimlik doğrulamasını və giriş nəzarətini gücləndirir. Biometrik məlumatlar, barmaq izi, retina skanı, üz tanıma kimi unikal fiziki xüsusiyyətləri istifadə edərək kimlik doğrulamasını təmin edir. Davranış analitikası isə istifadəçilərin normal həyat tərzi və fəaliyyətlərini öyrənərək, qeyri-adi davranışları aşkar edə bilər və buna görə də giriş siyasətlərini tənzimləyə bilər.

Son olaraq, kimlik və giriş idarəetməsi, istifadəçi mərkəzli təhlükəsizlik tədbirlərinin təşkilat məqsədləri ilə uyğunlaşdırılmasını təmin etmək üçün kritik bir rol oynayır. Bu sistem istifadəçilərin kimliklərini idarə edir, giriş hüquqlarını təyin edir və nəzarət edir, beləliklə də təşkilatların həssas məlumatlara təhlükəsiz bir şəkildə girişini idarə edə və nəzarət edə bilər. Bu, təhlükəsizliyin gücləndirilməsində kritik bir rol oynayır və təşkilatların uyğun təhlükəsizlik siyasətlərini həyata keçirməsinə kömək edir.

Şəbəkə təhlükəsizliyində şifrələmənin rolu. Məlumat təhlükəsizliyi gündəlik olaraq böyük həcmdə məlumatların mübadiləsi və saxlandığı getdikcə rəqəmsallaşan dünyamızın kritik aspektidir. Kiber təhdidlərin və məlumatların pozulması hallarının artması ilə həm fərdlər, həm də təşkilatlar öz həssas məlumatlarını icazəsiz girişdən və potensial sui-istifadədən qorumaq məcburiyyətindədirlər. Burada şifrələmə əsas rol oynayır (Şəkil 3.1.2.).



Şəkil 3.1.2. Məlumat şifrlənməsi (Omprakash, 2024)

Şifrələmə məlumatı oxunmaz formata çevirməklə onları qorumaq üçün güclü və etibarlı üsul təqdim edir və yalnız müvafiq şifrə açma açarı olan səlahiyyətli şəxslərin məlumatı əldə edə və anlaya bilməsini təmin edir. Bugünkü rəqəmsal aləmdə həyatımız data ətrafında fırlanır. Bank məlumatlarından tutmuş şəxsi söhbətlərə qədər məlumatımız böyük rəqəmsal kainatda saxlanılır və ötürülür. Məlumatlarımızı qorumaq təkcə şəxsiyyət oğurluğundan və ya maliyyə itkisindən qaçmaq deyil, məxfiliyimizi qorumaq və rəqəmsal dünyaya inamı qorumaqdır [Bejtlich, R., 2023, Evan Gilman, Doug Barth 2021].

Kompüter şəbəkələri vasitəsilə ötürülən informasiya maliyyə, elm təhsili, hərbi və digər sahələri, o cümlədən nəhəng iqtisadi və ya milli maraqları əhatə edə bilər. Bu məlumatların şəbəkə üzərində CIA üçbucağının tələblərinə uyğun daşınması kibertəhlükəsilik mütəxəssislərinin ən ali məqsədləri olmalıdır. Bu məlumatlar kritik və həssas olduğundan, hücumçuların diqqətini daha çox cəlb edir. Şəbəkə hücumlarının təzahürləri də müxtəlifdir, məsələn, virusa yoluxma, məlumatların oğurlanması, məlumatın dəyişdirilməsi, silinməsi və s.

Məlumatların şifrələnməsi şifrələmə alqoritmləri ilə həyata keçirilir. Onlar məlumatlarınızın necə şifrələndiyini və açıldığını müəyyənləşdirirlər. Klassik simmetrik şifrələmədən (eyni açar həm şifrələmə, həm də deşifrə üçün istifadə olunur) asimmetrik şifrələməyə (şifrələmə və şifrənin açılması üçün müxtəlif açarlardan

istifadə edir və tez-tez təhlükəsiz rabitə üçün istifadə olunur) müxtəlif şifrələmə alqoritmləri mövcuddur.

Bütün məlumatlarınızı şifrələmək əla ideya kimi görünə bilər, lakin bütün məlumatlar bizim üçün kritiklik daşımır. Şifrələmə tətbiq edilməmişdən əvvəl biz hansı məlumatın bizim üçün xüsusi əhəmiyyət daşıdığını müəyyənləşdirməliyik.

Şəbəkə təhlükəsizliyi şəraitə uyğun bir termin olaraq təsnif olunur, bu termin şəbəkənin qorunmasına dair bir neçə şəbəkə strategiyası tətbiq edərək, məlumata icazəsiz girişi, istismarı, dəyişikliyi, silməni və ya kompüter şəbəkəsinin əlçatmazlığından qorumaq məqsədilə istifadə olunur. Bu, həm geniş kompüter şəbəkələrini, həm də hər gün müxtəlif fəaliyyətlər üçün istifadə olunan, şəxsi, publik şəbəkələri əhatə edə bilər.

Hər hansı bir təşkilatın şəbəkə infrastrukturuna baxdıqda, həm "hardware", həm də "software" texnologiyalarının mövcudluğunu görürük. Bu, təşkilat şəbəkəsini və həssas məlumatları təhdidlərdən qorumaq və hücumçuların şəbəkəyə daxil olmasını dayandırmaq və ya şəbəkədə səlahiyyətlərin yüksəldilməsi prosesini dayandırmaq üçün təyin edilmiş bir prosesdir. Bu tip şəbəkə təhlükəsizliyi yanaşmaları daha yaxşı şəbəkə əlçatanlığına kömək edir, bu isə şəbəkəyə effektiv şəkildə məxfilik və bütövlüyü təmin edir.

3.2. İnformasiya Sistemlərində Demilitarizə Bölgə(Demilitarized Zone(DMZ)) yanaşması

Bu günlərdə texnologiya və hesablama gücündə sürətli artım nəticəsində, haqqında danışdığımız ənənəvi şəbəkə təhlükəsizliyi tədbirləri effektivliyini itirir, çünki etibarlı şəbəkələrə istənməyən şəxslərin daxil olması asanlaşıb. Bu da informasiya təhlükəsizliyi mütəxəssislərinin məsuliyyətini xeyli artırır. Bu mütəxəssislərin məqsədi, şəbəkə və məlumat resurslarını təhlükəsiz hala gətirməkdir. Bir çox sənaye müəssisələri öz biznes prosesi daxilində rəqəmsal dünyada var olmaq və ictimaiyyət ilə əlaqədə olmağa ehtiyac duyurlar. Bu da bəzi informasiya resurslarının publik şəbəkədə əlçatanlığını təmin etməklə baş tutur. Hesab etsək ki müəssisə daxili informasiya resurslarının arasında müəyyən kommunikasiyalar var bu proses şəbəkəni digər hissəsini də icazəsiz giriş, ələ keçirmə riskləri ilə üz-üzə qoya

bilər. Bu məqsədlə mütəxəssislər həm rəqəmsal dünyada “qapanmaq”dan həmçinin də təhlükəsizliyin təmin olunması üçün müstəqil bir şəbəkə seqmenti inkişaf etdirirlər. Bu şəbəkə segmentinə "Demilitarizə Bölgə" (DMZ) deyilir.

Məlumat texnologiyaları dünyasında, Demilitarizə Bölgə (DMZ), şəbəkə təhlükəsizliyini artırmaq üçün istifadə olunan əhəmiyyətli bir konsepsiyadır. Bir şəbəkədəki DMZ, xarici dünya ilə daxili şəbəkə arasında bir keçid bölgə yaradır və kritik sistemlərin təhlükəsizliyini təmin etmək üçün dizayn edilmiş bir strukturdur.

DMZ ümumiyyətlə bir şirkətin daxili şəbəkəsi ilə xarici dünya arasındakı məlumat mübadiləsini idarə etmək üçün istifadə olunur. Daxili şəbəkə, təşkilatın həssas məlumatlarını və kritik sistemlərini saxlayarkən, xarici şəbəkə isə ümumi internet daxil olunanı təmin edir. DMZ, bu iki sahə arasında bir ara bölgə yaradaraq təhlükəsizlik risklərini minimuma endirir [Sourabh Shrimali].

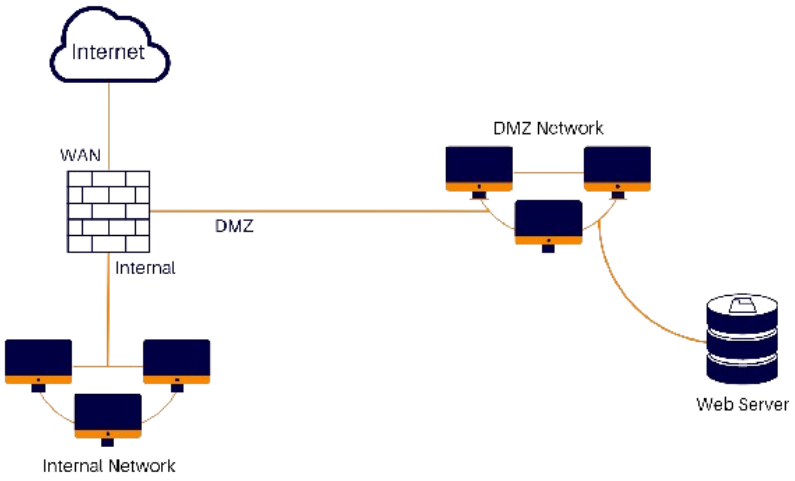
DMZ, korporativ İntranet və İnternet arasında olan korporativ şəbəkə hissələrindən ibarətdir. DMZ sadəcə bir seqment (LAN) və ya müxtəlif seqmentlərə (LAN, WAN, MAN) bölünə bilər. Onun əsas məqsədi istifadəçi girişinin (Daxili/Xarici) növü əsasında tətbiqə girişi məhdudlaşdırmaqdır. Əgər düzgün quraşdırılmış və tətbiq olunmuş bir DMZ haqqında təhlükəsizlik pozuntusu haqqında danışsaq, bu zaman əminliklə deyə bilərik ki, yalnız DMZ daxilində olan ərazi potensial zərərə məruz qalır və hər zaman korporativ daxili şəbəkə qorunur. DMZ üçün bütün yanaşmalarda demək olar ki, ictimai serverlərin bu hissəyə yerləşdirilməsidir. Beləliklə, şəxsi, etibarlı şəbəkə etibarsız şəbəkədən ayrılır. Əgər kənar bir şəxs təsadüfi və ya məqsədli şəkildə DMZ daxilində işləyən serverinizə daxil olursa və ya ələ keçirirsə, bu yalnız DMZ şəbəkəsindəki xidmətləri təsir edər, gizli şəbəkədə işləyən serverlərin xidmətləri təsirə məruz qalmayacaqdır [Joseph M. Adams].

Demilitarizə bölgə, korporativ şəxsi şəbəkə (LAN) kimi daxili şəbəkə olan etibarlı şəbəkələr və ictimai şəbəkə olan xarici şəbəkə olan etibarsız şəbəkə arasında təhlükəsiz keçid kimi işləyən kiçik bir fiziki şəbəkə və ya məntiqi alt-şəbəkədir. Bu, korporativ lokal şəbəkə (LAN) kimi daxili şəbəkələr və xarici, ümumi şəbəkə kimi fərdi şəbəkələri arasında təhlükəsiz körpü funksiyası icra edir. DMZ, daxili şəbəkənin xarici qurğular və şəbəkələr tərəfindən birbaşa istifadə edilməsindən qoruyan əlavə bir

təhlükəsizlik səviyyəsi təmin edir. Həmçinin, DMZ şəbəkəsi, daxili şəbəkəyə məhdud girişə malik olduğundan, hücumçunun bir təşkilatın daxili təhlükəsizliyini pozmaq kimi imkanı olmur. DMZ-nin tətbiqi təhlükəsizlik divarının tətbiqindən daha təhlükəsizdir və həmçinin o şəbəkə "Proxy" server kimi də çalışa bilər. DMZ-də əsasən Web, FTP, SMTP, DNS server kimi serverlər yer alır.

DMZ şəbəkəsini qurmaq üçün bir çox metod mövcuddur. Bu metodlar arasında, ən geniş istifadə olunan iki metod vardır. Bunlardan biri DMZ-nin bir təhlükəsizlik divarı ilə qurulan digəri isə iki təhlükəsizlik divarı ilə qurulan modelidir. Bu şəbəkə arxitekturası, təşkilatın daxili şəbəkə tələblərinə əsaslanaraq daha da mürəkkəbləşdirilə bilər.

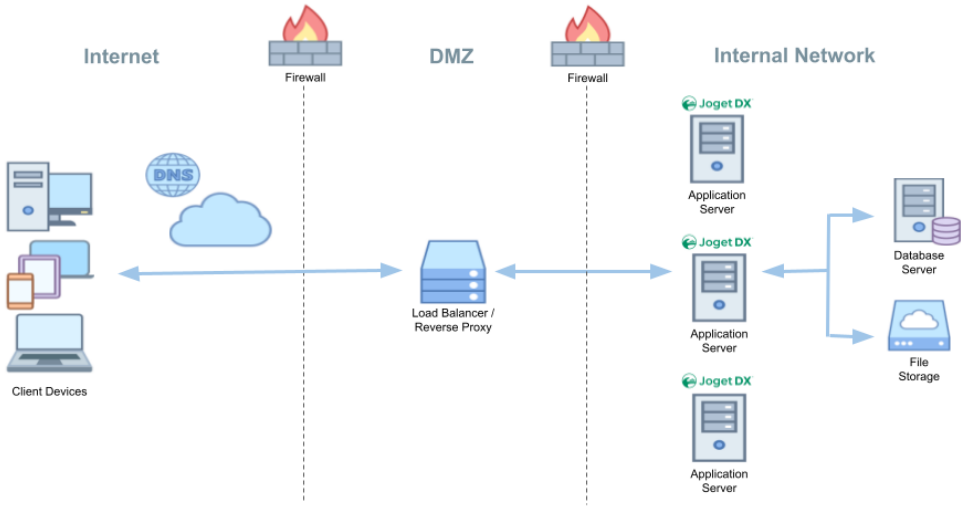
Tək təhlükəsizlik divarı ilə qurulan DMZ arxitekturası həmçinin üçayaq modeli kimi tanınır və özündə üç şəbəkə interfeysi saxlayır. İlk interfeys provayderdən (İnternet Xidmət Provayderləri (İXP)) divara qədər yaradılan xarici şəbəkədir, ikinci şəbəkə interfeysi təşkilatın daxili şəbəkəsidir, üçüncüsü isə müxtəlif növ serverləri olan DMZ şəbəkəsidir. Bu növ arxitekturanın ən böyük problemlərindən biri odur ki, əgər hər hansı bir yolla təhlükəsizlik divarı hücumçu tərəfindən ələ keçirilsə, bütün bu DMZ arxitekturası uğursuz olacaqdır. (Şəkil 3.2.1.)



Şəkil 3.2.1 Tək təhlükəsizlik divarı ilə qurulan DMZ arxitekturası (David Richardson, 2024)

İki təhlükəsizlik divarı ilə qurulan DMZ modeli tək divarlıq modeldən daha təhlükəsizdir, çünki DMZ arxitekturası iki divardan istifadə edərək yaradılır, burada

arxa uc (*ing. back-end*) divarı və ön uc (*ing. front-end*) divarı olmaqla iki divardan



istifadə olunur. Ön uc divarı yalnız DMZ-ə gedən trafikə icazə verir. Arxa uc divarı isə yalnız DMZ-dən daxili şəbəkəyə gələn trafikə icazə verir. Bu növ arxitektura daha güvənlidir və daha çox xərc tələb edir. Bu tip arxitekturada bütün şəbəkəni güzəştə getməsi üçün iki cihaz da ələ keçirilməlidir. Həmçinin çoxsaylı təhlükəsizlik divarı sxemlərindən istifadə yüksək səviyyəli dayanıqlılıq təmin edir ki, aktiv təhlükəsizlik divarı uğursuz olarsa, qarşıdan gələn trafik ehtiyat mühafizə divarına keçirilə bilər. Bu yanaşmanı sistemlərdə istifadə etmək məsələsinə "dərin müdafiə tədbiri təhlükəsizlik strategiyası" (*ing. Defense in depth)* deyilir. Həmçinin DMZ ilə bağlı təhlükəsizlik tövsiyələrindən biri də təhlükəsizlik divarlarının istifadəsində fərqli istehsalçılara məxsus olan məhsulların istifadəsidir. Çünki əgər hər iki divar eyni istehsalçının məhsuludursa, hər hansı bir cihazın ələ keçirilməsi üçün istifadə olunan metodla digər cihazı da ələ keçirilə bilər. Bu da bütün şəbəkə infrastrukturunun ələ keçirilməsi ilə nəticələnə bilər. (Şəkil 3.2.2.)

Şəkil 3.2.2. İki təhlükəsizlik divarı ilə qurulmuş DMZ arxitekturası

(Aadrian Zarin, 2024)

Aşağıdakı cədvəldə tək və iki təhlükəsizlik divarı ilə qurulan DMZ-nin müqayisəli tədqiqi verilmişdir. (Cəd. 3.2.1.)

Cədvəl 3.2.1 DMZ-nin müqayisəli tədqiqi

DMZ növləri	Şəbəkə mürəkkəbliyi	Etibarlılıq	Səmərəlilik
Tək "Firewall"	Tək "firewall" sayəsində daha az mürəkkəbdir.	Daha az etibarlı	Tək "firewall" tək uğursuzluq nöqtəsinə çevrildiyi üçün daha az effektivdir.
İki "Firewall"	İki "firewall" sayəsində daha çox mürəkkəbdir	Daha çox etibarlı	İkili "firewall"dan istifadə sayəsində daha effektivdir.

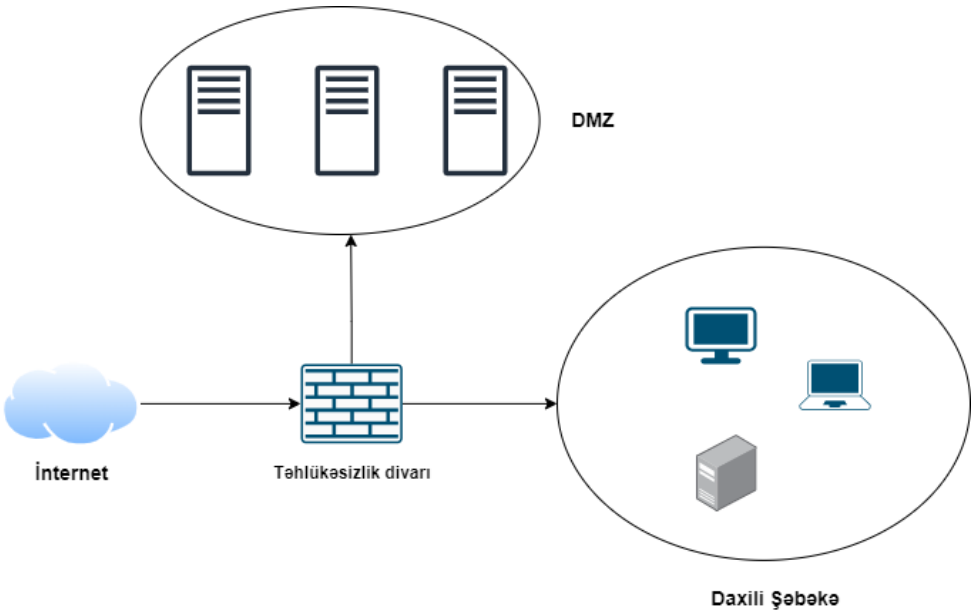
DMZ-nin mövcudluğu, xarici təhlükələrin daxili şəbəkəyə sızmasının qarşısını alır və kritik sistemlərin qorunmasını təmin edir. Həmçinin, DMZ, təhlükəsizlik divarları, hücum aşkar etmə sistemləri və təhlükəsizlik siyasətləri kimi müxtəlif təhlükəsizlik tədbirləri ilə dəstəklənir.

Nəticə olaraq, məlumat sistemlərindəki DMZ-lər, şəbəkə təhlükəsizliyinin əsas dayaqlarından biridir və təşkilatların həssas məlumatlarını qorumaq üçün əhəmiyyətli bir rol oynayır. Təhlükəsizlik baxımından kritik olan bu struktur, şəbəkələrin kiber hücumlarına qarşı müqavimətini artırır və məlumatları qoruyur.

DMZ şəbəkəsi təhlükəsizlik divarı, marşrutlaşdırıcı, şəbəkə açarı və serverlər kimi müxtəlif cihazlardan qurulur. Bu cihazlar, DMZ-nin müxtəlif səviyyələrini və performansını təşkil etmək üçün müxtəlif yollarla istifadə oluna bilər. Bu səviyyələr tamamilə hər hansı bir təşkilatın maliyyəsi, təhlükəsizliyi və performans tələblərinə əsaslanır.

Müxtəlif mənbələrdə DMZ müxtəlif səviyyələrlə izah olunur. Burada biz DMZ - ni dörd səviyyədə izahına baxacağıq.

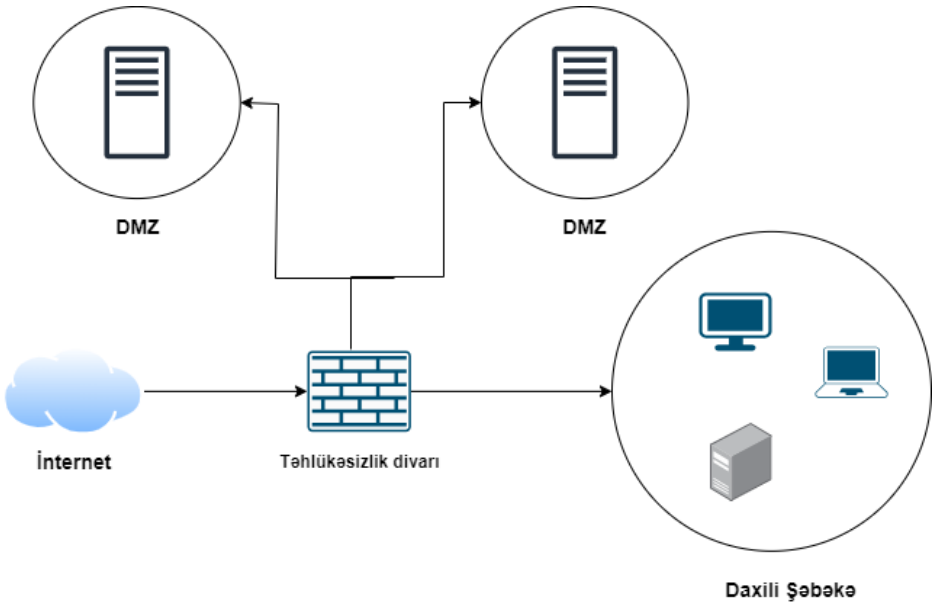
Birinci səviyyə DMZ:1-ci səviyyəli DMZ-ni qurmaq asandır və digər dizayn səviyyələrinə nisbətən ən aşağı səviyyədə təhlükəsizliyə malikdir. Şəkil 3.2.3-də



Şəkil 3.2.3. 1-ci səviyyə DMZ (Vəlizadə Sənan, 2024)

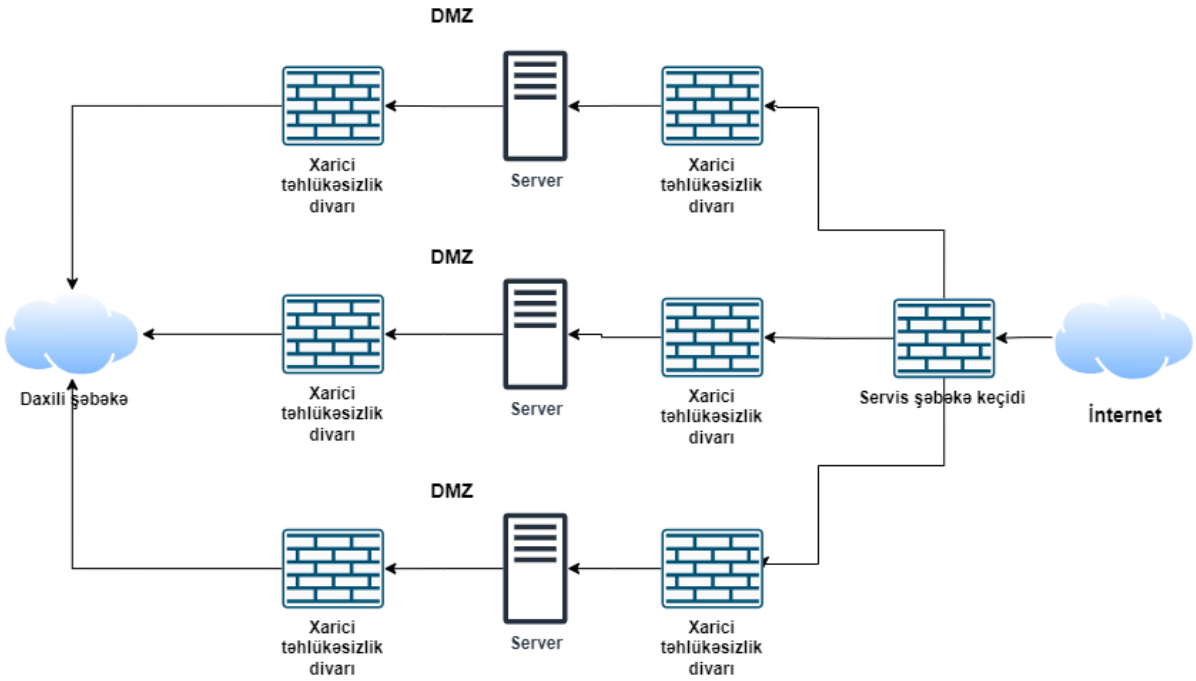
göstərildiyi kimi tək təhlükəsizlik divarlı DMZ modelinə bənzəyir. Bu dizaynda DMZ sərhəd təhlükəsizlik divarından xüsusi portda əlaqə saxlayan fərqli bir şəbəkədədir. Bu həm filtrləmə, həm də qorunma məqsədinə xidmət edir. Bu dizayn veb-serverlər kimi bir neçə ictimai əlçatan resursu olan təşkilatlar üçün yaxşı seçim ola bilər.

İkinci səviyyə DMZ. 2-ci səviyyəli dizaynda, şəbəkəni birləşdirmək üçün tək təhlükəsizlik divarından istifadə edildiyi üçün hələ də "single point of failure" mövcuddur. Bu dizayn səviyyəsini əvvəlki ilə müqayisə etdiyimizdə, bu dizayn yanaşmasının tək fərqi, müxtəlif portlar vasitəsilə bağlanmış müxtəlif DMZ-lərdən istifadə edilməsidir. Bu dizayn yanaşması, təsbit olunan serverlərə trafiki yönəltmək üçün müxtəlif portlardan istifadə edərək resursların ayrılmasına imkan verir və beləliklə təhlükəsizliyi artırır. Həmçinin, bu dizaynda, filtrləmə və trafik qaydalarını tətbiq etmək daha asandır. Bu dizayn, etibarlı şəbəkənin xaricində yerləşən verilənlər bazasının təhlükəsizliyini təmin etmək qabiliyyətini də özündə birləşdirir.



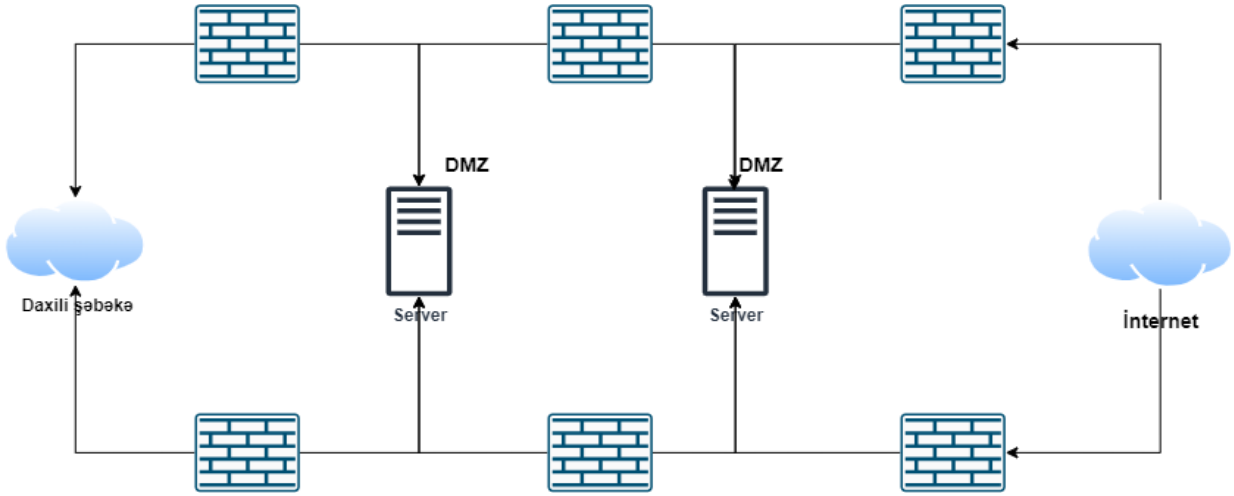
Şəkil 3.2.4. 2-ci səviyyə DMZ (Vəlizadə Sənan, 2024)

Üçüncü səviyyə DMZ. 3-cü səviyyəli DMZ dizaynı təhlükəsizliyin və mürəkkəbliklərin artması nəticəsində mövcud olmuşdur. Bu dizayn hər bir DMZ-də daxili və xarici sərhədləri qurmaq üçün bir sıra divarlıqlardan istifadə edir, Şəkil 3.2.5-də göstərildiyi kimi. Həmçinin, xidmət qapısı divarlığı kimi tanınan əlavə bir divarlıqdan istifadə edir, bu da gələn internet trafikinə gəlmədən əvvəl bir təhlükəsizlik nöqtəsi kimi işləyir. Bu ikili sərhəd mekanizmı serverləri və digər resursları daha da təhlükəsiz edir, çünki yalnız bu resurslar üçün təyin edilmiş trafik, IP ünvanları və port nömrələrinə əsaslanan müvafiq divarlıqdan keçməyə icazə verilir.



Şəkil 3.2.5. 3-cü səviyyə DMZ (Vəlizadə Sənan, 2024)

Dördüncü səviyyə DMZ. Son dizayn yanaşması ən mürəkkəb və ən bahalı dizayndır. Bu DMZ arxitekturası ikili sərhəd konsepsiyasından istifadə edir. Üçüncü səviyyə dizaydan yeganə fərqi, 4-cü səviyyənin müxtəlif DMZ-lər arasında sərhədlər yaratmaq üçün çoxsaylı təhlükəsizlik divarlarının birləşdirilməsidir, bu da bir təşkilatın resurslarını hər bir sərhəd təhlükəsizlik divarları arasında cütlüyü arasında yaymağı mümkün edir.



Şəkil 3.2.6. 4-cü səviyyə DMZ (Vəlizadə Sənan, 2024)

Yuxarıda göstərilən DMZ dizayn səviyyələrinə əsasən, müqayisəli təhlili aşağıdakı cədvəldə göstərilmişdir (Cəd. 3.2.2.) [Vural, H., Dahi, B., & Tuncer, S., 2023].

Cədvəl 3.2.2. DMZ dizayn səviyyələrinə əsasən müqayisəli təhlili

DMZ növləri	Ortalama xərc	Şəbəkə mürəkkəbliyi	Etibarlılıq	Təhlükəsizlik	Effektivlik
1	Aşağı	Tək firewall istifadəsinə görə daha az mürəkkəbdir.	Aşağı etibarlılıq	Daha az təhlükəsiz	Çox aşağı effektivlik
2	Aşağı	1-ci səviyyə ilə müqayisədə nisbətən mürəkkəbdir	Aşağı etibarlılıq	Səviyyə 1 ilə müqayisədə nisbətən təhlükəsizlik timin olunur.	Normal effektivlik
3	Yuxarı	Mürəkkəb	Yuxarı etibarlılıq	Təhlükəsiz	Effektiv
4	Çox yuxarı	Çox mürəkkəb	Çox yuxarı etibarlılıq	Yüksək səviyyədə təhlükəsiz	Çox yüksək effektivlik

3.3. Korporativ şəbəkə təhlükəsizliyi prinsipləri və perimetr təhlükəsizliyi

Korporativ şəbəkə təhlükəsizliyinə, təşkilatların şəbəkələrini potensial təhdid və hücumlardan qorumaq üçün istifadə etdikləri tədbirlər və strategiyalar aiddir. Təşkilatlar günü-gündən rəqəmsal platformalara və internetə inteqrasiya olunur və müxtəlif şəbəkə təhlükəsizliyi təhdidlərinə qarşı daha həssas olurlar. Bu təhdidlərə mübarizə aparmaq üçün davamlı şəbəkə təhlükəsizliyi siyasətləri və strategiyaları hazırlamalı və tətbiq etməlidirlər və ya əhəmiyyətli maliyyə itkisi, marka nüfuzuna xələl gətirmək və həssas iş məlumatlarını güzəştə getmək riskini qəbul etməlidirlər.

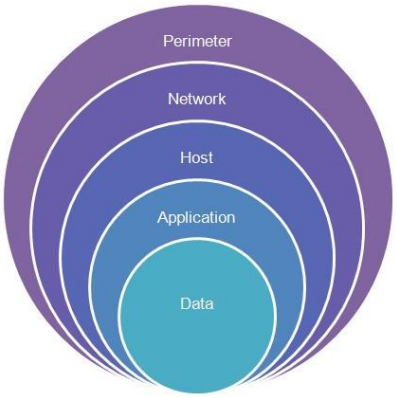
Rəqəmsallaşma kontekstində korporativ şəbəkə təhlükəsizliyinin əhəmiyyətini kənara atmaq olmaz. Etibarlı bir təhlükəsizlik sistemi həssas məlumatlarınızı qorumaqla yanaşı, infrastrukturu rəqəmsal hücumlardan da qoruyur.

Korporativ şəbəkə təhlükəsizliyinin üstünlükləri:

1. Şəbəkə təhlükəsizliyi təhdidlərindən qorunma

Kibercinayətkarlar həmişə istifadə üçün şəbəkəfə zəifliklər axtarırlar. Düzgün qurulmuş şəbəkə təhlükəsizliyi strategiyaları ilə təşkilatlar bu cəhdlərin qarşısını ala bilər. Şəbəkə təhlükəsizliyi siyasəti bu qoruma üçün əsasdır. Şəbəkə təhlükəsizliyinin qorunmasında ardıcıllıq və səmərəliliyi təmin etmək üçün işçilərinizin və şöbələrinizin riayət etməli olduqları qaydalar özündə birləşdirir. Düzgün siyasətlərin tətbiqi ilə riskləri minimuma endirə və hücumlara qarşı müqaviməti artıra bilərik.

2. Həssas korporativ məlumatlarının qorunması
3. Məlumatlar müəssisələrin ən dəyərli mənbələri arasındadır. Belə ki, data "Dərinlikdə müdafiə" startegiyasının da ən dərin nöqtəsində yer alır (Şək. 3.3.1)



Şəkil 3.3.1. Dərinlikdə müdafiə layları (Cohesive Networks, 2015)

Həssas iş məlumatlarınız icazəsiz girişdən və ya məlumatların pozulmasından qorunmalıdır. Ciddi şəkildə şəbəkə təhlükəsizliyi standartlarını tətbiq etmək və müntəzəm risk qiymətləndirmələrini aparmaq, təşkilatınızın təhlükəsizlik infrastrukturundakı boşluqları müəyyənləşdirməyə və həll etməyə kömək edə bilər.

Üstəlik, korporativ şəbəkələrin təhlükəsizlik həlləri təhlükəsizlik təhdidlərini izləmək, aşkar etmək və onlara cavab vermək üçün sistematik bir çərçivə təmin edir. Monitorinq xidmətləri şəbəkənizi qeyri-adi fəaliyyət üçün daim yoxlayır və təhdidləri

zərərsizləşdirmək üçün tez cavab verir. Bu proaktiv yanaşma məlumatların qorunması üçün çox vacibdir.

Şəbəkə təhlükəsizliyini formalaşdıran əsas texnologiyalar:

1. Süni intellekt və maşın öyrənməsi

Süni intellekt və maşın öyrənməsi şəbəkə təhlükəsizliyində inqilab dəyişikliklər gətirmişdir. Suni intellekt insanın imkanlarını genişləndirərək, təhdidləri əvvəlcədən aşkar etmək və onlara vaxtında cavab vermək kimi imkanlar yaratdı. Bu texnologiyalar böyük miqdarda məlumatları təhlil edir, nümunələri müəyyənləşdirir və potensial təhdidləri real vaxtda müəyyənləşdirmək və azaltmaq üçün keçmiş hadisələri analiz edir. Süni intellektə əsaslanan həllər normal şəbəkə davranışını başa düşə, anomaliyaları aşkar edə və təhlükəsizlik hadisələrinə tez cavab verə bilər.

2. Bulud hesablama

Bulud hesablama ölçüləbilən, çevik və səmərəli təhlükəsizlik həlləri təmin edir. Təşkilatınızın təhlükəsizlik infrastrukturunu buluda köçürmək yerli avadanlıqdan asılılığı və əlaqədar texniki xidmət xərclərini azaldır. Bulud təhlükəsizlik xidmətləri ayrıca mərkəzləşdirilmiş idarəetmə, real vaxt yeniləmələri və ən son təhdidlərə qarşı avtomatik qorunma təmin edir.

3. IoT təhlükəsizliyi

IoT cihazlarının yayılması kiberhücumlar üçün yeni imkanlar açdı və IOT təhlükəsizliyini şəbəkə təhlükəsizliyinin ən vacib aspektinə çevirdi. IoT cihazlarını qorumaq və icazəsiz girişin və ya icazəsiz müdaxilənin qarşısını almaq üçün qabaqcıl kriptoqrafik metodlar, cihaz identifikasiyası protokolları və etibarlı rabitə kanalları hazırlanır. Bundan əlavə, şəbəkə seqmentasiyası və ciddi giriş nəzarəti bu cihazlarla əlaqəli riskləri azaltmağa kömək edir.

4. Proqram tərəfindən müəyyən edilmiş şəbəkələr (SDN)

SDN şəbəkə idarəetməsini əsas aparat infrastrukturundan ayırır, mərkəzləşdirilmiş idarəetmə və proqramlaşdırmanı təmin edir. Bu texnologiya, səmərəli şəbəkə təhlükəsizliyi üçün vacib olan şəbəkənizə daha çox rahatlıq, çeviklik və ətraflı nəzarət təmin edir. SDN ayrıca təhlükəsizlik siyasətlərini

dinamik şəkildə tətbiq etməyə, şübhəli trafik sxemlərini müəyyənləşdirməyə və güzəştə getmiş cihazları avtomatik olaraq təcrid etməyə imkan verir və bununla da şəbəkə təhlükəsizliyini artırır.

5. Blockchain texnologiyası

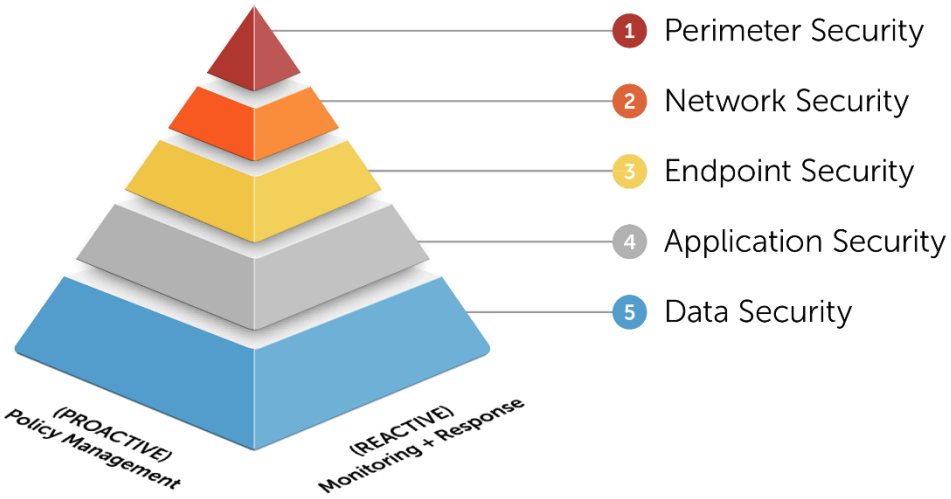
Mərkəzləşdirilməmiş və dəyişməz təbiəti ilə tanınan blockchain texnologiyası şəbəkə təhlükəsizliyini təmin etmək üçün imkanlar təqdim edir. Paylanmış ledger texnologiyası əməliyyatların təhlükəsizliyini, istifadəçi identifikasiyasını və həssas məlumatların qorunmasını təmin etmək üçün istifadə edilə bilər. Qeydlərin icazəsiz girişdən qorunmasını təmin edir və şəbəkə əməliyyatlarının bütövlüyünü artırır, kiber cinayətkarların məlumatları manipulyasiya etməsini və ya güzəştə getməsini çətinləşdirir.

6. Biometriya və çox faktorlu identifikasiya

Barmaq izləri, üz tanıma və iris skan kimi biometrik məlumatlar ənənəvi parolları unikal fiziki xüsusiyyətlərlə əvəz edərək əlavə təhlükəsizlik qatını təmin edir. Çox faktorlu identifikasiya bildiklərinizi (parol), sahib olduğunuz şeylər (ağıllı kart) və kim olduğunuz (biometrik məlumatlarınız) kimi bir çox amilləri birləşdirir ki, bu da şəbəkəyə icazəsiz giriş riskini xeyli azaldır [E. Dart, L. Rotman, B. Tierney, M. Hester and J. Zurawski, 2013].

Müəssisənin informasiya təhlükəsizliyinin qorunması və informasiyaya icazəsiz girişin, kiberhücumların, informasiyanın icazəsiz yayılmasının qarşısının alınması üçün şəbəkə təhlükəsizliyi vacib amildir. Digər vacib məqam isə müəssisənin çərçivəsində müəssisəyə edilən hücumların aşkarlanması və qarşısının alınması üçün qabaqcıl tədbirlərin görülməsidir. Bu cür qabaqcıl tədbirlərin görülməsində lazım olacaq təhlükəsizlik növlərindən biri də Perimetr təhlükəsizliyidir. İndi isə Perimetr təhlükəsizliyinin bu qorunmalar zamanı necə əhəmiyyətli rol oynadığı görüləcəkdir.

Perimetr təhlükəsizliyi aktivlərinizi, məlumatlarınızı və insanları qabaqcıl texnologiya ilə qorumaq üçün ilk müdafiə xəttidir. Bu “Dərinlikdə müdafiə” pirmaidasının ən uc nöqtəsidir (Şəkil 3.3.2).



Şəkil 3.3.2. Dərinlikdə müdafiə piramidası (Entro Security, 2024)

İnsan dərisi bədəni xarici mühitdən və infeksiyalardan qoruduğu kimi, perimetr təhlükəsizlik sistemi də əmlakınıza icazəsiz daxil olmağın qarşısını almaq üçün olan yanaşmadır. Müəssisələr hazırda etibarlı təhlükəsizlik sisteminin yaradılmasına böyük sərmayə qoyur. Çox səviyyəli təhlükəsizlik sisteminin yaradılması əmlakın qorunması üçün vacibdir. Müdaxilənin aşkarlanması, Girişə nəzarət, Bina İdarəetmə Sistemi və daha çox kimi həllərin tətbiqi bu kimi məsələlərdəndir.

Bir şəbəkəni və ya sistemi xarici dünyadan, o cümlədən İnternetdən ayıran sərhəd təhlükəsizlik perimetri adlanır. Təhlükəsizlik perimetri fiziki və ya məntiqi ola bilər. Fiziki təhlükəsizlik perimetri, girişi fiziki olaraq maneə törədən divarlar və qapılar kimi maneələr aiddir. Məntiqi təhlükəsizlik perimetrləri şəbəkəyə və onun mənbələrinə girişə nəzarət etmək üçün təhlükəsizlik protokollarından, giriş nəzarətlərindən və təhlükəsizlik divarlarından istifadə edir.

Üstəlik, məntiqi təhlükəsizlik perimetri ümumiyyətlə aparat, proqram təminatı və insan elementlərini əhatə edir. Aparat təminatı perimetr qorumasına təhlükəsizlik divarları, müdaxilənin aşkarlanması sistemləri, marşrutlaşdırıcılar və açarlar kimi şəbəkə cihazları daxildir. Proqram perimetri qorunması şəbəkələri qorumaq üçün hazırlanmışdır. Buraya girişə nəzarət proqramı, identifikasiya, şifrələmə texnologiyası və antiviruslar daxildir.

Bundan əlavə, insan amilinə parollar, istifadəçi identifikatorları, fiziki giriş kartları, CCTV sistemləri, təhlükəsizlik sistemləri və siqnalizasiya sistemləri kimi elementlər daxil ola bilər. Əksər şirkətlər möhkəm bir qoruma sistemi yaratmaq üçün bir-biri ilə birlikdə bir neçə aparat və proqram məhsullarından istifadə edirlər.

Hər hansı bir təşkilatın kibertəhlükəsizlik strategiyası xarici təhdidlərə qarşı ilk müdafiə xəttini təmin etdiyi üçün təhlükəsizlik perimetrini təmin etməlidir. Beləliklə, məlumat aktivlərinin məxfiliyini, bütövlüyünü və mövcudluğunu təmin etməyə kömək edir.

Effektiv təhlükəsizlik perimetri bu vacib elementlərin bəzilərini və ya hamısını ehtiva edir:

Təhlükəsizlik protokolları: Secure sockets Layer (SSL) və Transport Layer Security (TLS) məlumatları şəbəkə üzərindən keçərkən şifrələyir. Şifrələnmiş məlumatlar onların təcavüzkarlardan təhlükəsizliyini təmin edir.

Giriş nəzarəti: Effektiv Parollar, biometrik identifikasiya və ağıllı kartlar daxil olmaqla giriş nəzarəti yalnız səlahiyyətli istifadəçilərə giriş imkanı verir. RBAC kimi digər giriş nəzarətləri də istifadə edilə bilər.

Təhlükəsizlik divarları: Təhlükəsizlik divarları şəbəkə trafikini izləmək və idarə etmək üçün istifadə olunur. Yalnız icazəsiz trafikin qarşısını alaraq Səlahiyyətli trafikdən keçirlər. Onlar həm aparat, həm də proqram təminatı ola bilər. Bunlar müəyyən trafik növlərini bloklamaq üçün konfiqurasiya edilə bilər. Məsələn, müəyyən portları və ya protokolları blok edə bilərlər [Oh, J., & Lee, S., 2019].

3.4 Perimetr təhlükəsizliyinin inkişaf strategiyaları

Müəssisələr üçün təhlükəsizlik, günümüzdə artan digər bir çox məsələlərlə birlikdə daim inkişaf edən bir sahədir. Bu, müəssisənin məlumatlarını qorumaq və fiziki səlahiyyətlərin təhlükəsizliyini təmin etmək məqsədi ilə digər təhlükəsizlik tədbirləri ilə birlikdə, əsas məsələlərdən biridir. Əvvəlcə, müəssisələr əsasən fiziki sərhədləri müdafiə etməyə çalışırdılar, lakin texnologiya inkişafı ilə birlikdə, perimetr təhlükəsizliyi dair strategiyalar da dəyişdi. Bu məqalədə, perimetr təhlükəsizliyinin inkişafında əsas məsələləri və bu məsələlərin tətbiqatını müzakirə edəcəyik.

Əvvəlcə, perimetr təhlükəsizliyi, müəssisənin fiziki sərhədlərinin qorunması ilə əlaqədar idi. Buna nümunə olaraq, qoruyucu qapılar, hərəkət sensorları və kamera sistemləri ilə mühafizə olunurdu. Lakin, texnologiya inkişafı ilə birlikdə, bu təhlükəsizlik anlayışı dəyişdi. İnternetin və məlumatların əhatəsi artıq fiziki bir sərhədlə məhdudlaşmadığı üçün, perimetr təhlükəsizliyi yeni bir anlayışa doğru inkişaf etdi.

Perimetr təhlükəsizliyinin əvvəlki dövrləri, müəssisələrin təhlükəsizliyi üçün əsasən fiziki mühafizəyə əsaslanan bir dövrü ifadə edir. Bu dövrdə, müəssisələr öz ərazilərini çitlə, qapılarla, hərəkət sensorları ilə və kamera sistemləri ilə müdafiə etməyə çalışırdılar. Fiziki sərhədlər, gəlinir ki, müəssisənin ətrafında bir perimetr yaradır və bu, müəyyən bir təhlükəsizlik səviyyəsinin təmin edilməsini nəzərdə tuturdu.

Əvvəllər müəssisə təhlükəsizliyi, əsasən inzibati tədbirlər, müdafiə strukturları və fiziki gözləmələr əsasında idarə olunurdu. Həmçinin, bu dövrdə məlumat təhlükəsizliyi daha az narahat edici idi, çünki informasiya texnologiyalarının əhəmiyyəti və yayılması hələ də çox məhdudiyyətlər altında idi.

Fiziki təhlükəsizlik tədbirləri müəssisənin ətrafındakı perimetrin güclü mühafizəsi ilə məhdudlaşdırıldığı üçün, bu dövr perimetr təhlükəsizliyinin əsasən maddi və fiziki resurslarla əlaqəli olduğu bir dövrdü. Bununla birlikdə, texnologiya inkişafı ilə birlikdə, perimetr təhlükəsizliyi də dəyişdi və daha kompleks hala gəldi.

Bu dövrdə, təhlükəsizlik çox dəyişik təhlükələrə qarşı mübarizə üçün daha çox mühafizə texnologiyaları və protokolları tələb edir. Günümüzdə, perimetr təhlükəsizliyi daha çox məlumat təhlükəsizliyi, siber təhlükəsizlik və müxtəlif monitorinq sistemləri ilə bağlıdır. Bu, müəssisələrin daha geniş məhdudiyyətlər və daha kompleks təhlükələr nəticəsində daha çox mühafizə tədbirləri almağını tələb edir [Roesch, M., 2020].

Məlumat qorunması və şifrləmə, perimetr təhlükəsizliyinin əsas məsələlərindən biridir. Bu, müəssisələrin məlumatlarını qorumaq və müdafiə etmək üçün ən əsas tədbirlərdən biridir. Məlumat qorunması və şifrləmə, müəssisə məlumatlarının müxtəlif səviyyələrdə müdafiə olunması üçün lazımi tədbirləri əhatə edir.

1. Məlumat Qorunmasının Əsasları: Məlumat qorunmasının əsas məqsədi, müəssisənin daxilindəki məlumatların gizliliyini, bütövlüyünü və məsuliyyətini təmin etməkdir. Bu, müəssisə məlumatlarının müəyyən bir səviyyədə təhlükəsiz saxlanması və yetkin olmayanların məlumata çatmasının qarşısının alınması deməkdir.

2. End-to-End Şifrləmənin Əhəmiyyəti: Məlumatların məhz məlumatı göndərən və alan tərəflər arasında şifrlənərək təhlükəsiz bir şəkildə ötürülməsi, end-to-end şifrləmənin əsasını təşkil edir. Bu, məlumatların üçüncü tərəflər tərəfindən nəzarət edilməsinin və müdaxilə edilməsinin qarşısını alır.

3. Məlumat Qorunma Texnologiyaları: Məlumat qorunması üçün bir çox texnologiyalar mövcuddur. Bu texnologiyalar arasında şifrləmə alqoritmləri, faylları və şəbəkə əlaqələrini qoruyan proqramlar, məlumat bazalarını müdafiə edən sistemlər və s. yer alır.

4. Məlumat Qorunma Standartları və Qanunvericilik: Bir çox sektorlar özünəməxsus məlumat qorunma standartlarına və qanunvericiliyinə malikdir. Bu standartlar və qanunvericiliklər, müəssisələrin məlumat qorunması tədbirlərini hazırlamaq, icra etmək və yaxşılaşdırmaq üçün əsas təşkil edir.

5. Təhlükəsizliyin Tənzimlənməsi: Məlumat qorunması, müəssisələrin təhlükəsizlik strateji və texnologiyalarını tənzimləməsinin də bir hissəsidir. Bu, müəssisənin məlumat qorunma siyasəti, prosedurları və təlimatları daxilində məlumatların necə qorunacağına dair qaydaları əhatə edir.

Məlumat qorunması və şifrələmə, perimetr təhlükəsizliyinin ən vacib yanaşmalarından biridir. Bu yanaşmalar müəssisələr üçün məlumatların müdafiəsini təmin etmək üçün əsas məsələlərdir [Е.Г.Горшков., 2013].

IV FƏSİL. İNFORMASİYA İNFRASTRUKTURUNUN DAİMİ NƏZARƏTİNİN TƏMİN OLUNMASINDA TƏHLÜKƏSİZLİK ƏMƏLİYYATLARI MƏRKƏZİNİN (SECURITY OPERATIONS CENTER(TƏM)) FƏALİYYƏT MEXANİZMLƏRİ

4.1. Daimi nəzarətin təminində təhlükəsizlik əməliyyatları mərkəzi və onun fəaliyyəti

Təhlükəsizlik Əməliyyat Mərkəzi, qısaca TƏM adlanan, bir təşkilatın məsuliyyətli olduğu kibertəhlükəsizlik hadisələrini və təhlükələri izləmək, aşkar etmək və cavab vermək üçün olan bir mərkəzdir. Bu, bir təşkilatın təhlükəsizlik əməliyyatları üçün sinir mərkəzi kimi xidmət edir, daimi olaraq bir çox təhlükəsizlik sistemlərini, şəbəkələrini və proqramları izləyir.

TƏM, bir təşkilatın təhlükəsizlik vəziyyətini daimi olaraq izləmək və yaxşılaşdırmaq üçün insanlardan, proseslərdən və texnologiyalardan istifadə edən, eyni zamanda kiber təhlükəsizlik hadisələrinə qarşı qoruma, aşkar etmə, təhlil etmə və cavab vermək məqsədi daşıyan mərkəzi bir funksiyadır.

TƏM, bir təşkilatın bütün IT infrastrukturunda baş verən kibertəhlükəsizlik hadisələrini aşkar etmək və onlara mümkün qədər tez və effektiv şəkildə cavab vermək üçün şəbəkəni və sistemləri 24/7 rejimdə izləyən və bu məqsədlə IT təhlükəsizliyi sahəsində işləyən daxili və ya xarici komandadır.

TƏM-in funksiyası, kiber təhlükələri periodik olaraq izləmək, onlardan qorunmaq, aşkar etmək, araşdırmaq və onlara cavab verməkdir. TƏM komandaları, məxfi məlumatlar, əməliyyat sistemləri və brend əhəmiyyətli məxfi informasiyalar daxil olmaqla təşkilatın aktivlərini izləmək və qorumaqla vəzifələndirilmişdir. TƏM komandası, təşkilatın ümumi kiber təhlükəsizlik strategiyasını həyata keçirir və kiber hücumlarla mübarizə üçün koordinasiyalı əməkdaşlıq edərək monitorinq, qiymətləndirmə və müdafiə etmə əməliyyatlarının mərkəzi nöqtəsi kimi fəaliyyət göstərir.

TƏM və informasiya təhlükəsizliyi idarəetmə sistemi. TƏM ümumi müəssisə miqyasında informasiya təhlükəsizliyi proqramının yalnız bir hissəsi olsa da, TƏM-un

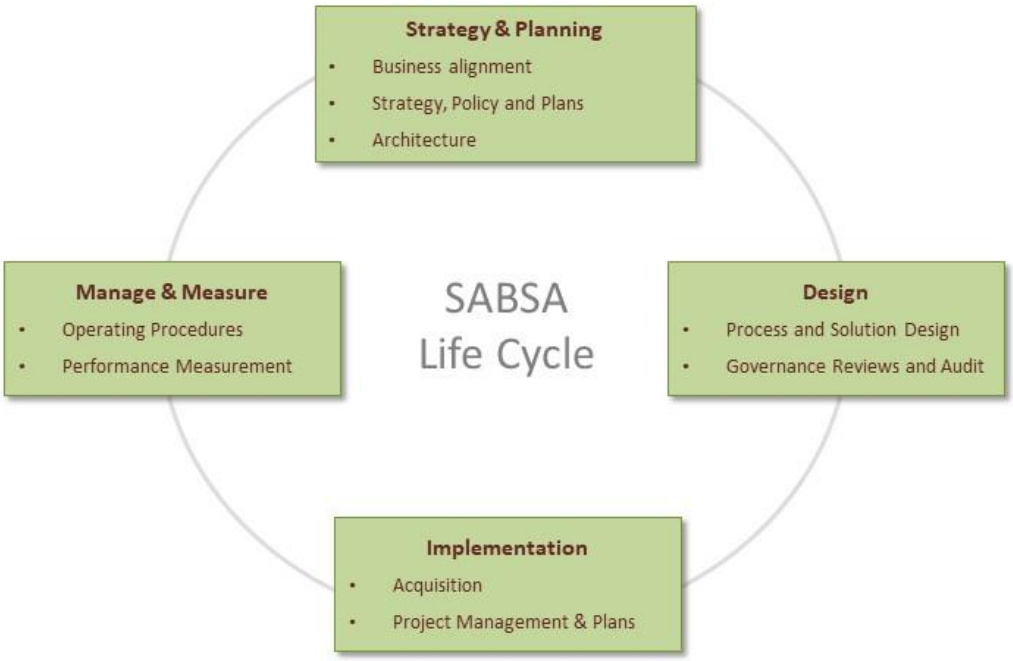
özünün informasiya təhlükəsizliyi idarəetmə sisteminə necə uyğunlaşdığını başa düşmək vacibdir. TƏM üçün standart təşkilati strukturlar və ya fəaliyyət dairələri yoxdur, buna görə də hər bir müəssisə əməliyyat təhlükəsizliyinə yanaşmasını bir qədər fərqli şəkildə təşkil edir.

İnformasiya təhlükəsizliyi haqqında danışarkən, adətən ya Beynəlxalq Standartlaşdırma Təşkilatı ISO 27001: İnformasiya Təhlükəsizliyi İdarəetmə Sistemi və ya NIST Kiber Təhlükəsizlik Framework-nə istinad edilir.

Beynəlxalq Standartlaşdırma Təşkilatı ISO 27001 audit və akkreditasiya üçün uyğun olan nəzarətə əsaslanan yanaşma tətbiq edir, NIST Kiber Təhlükəsizlik Framework isə kiberhücumların qarşısının alınması və onlara reaksiya verilməsinə diqqət yetirir. NIST çərçivəsi beş mərhələli həyat dövrünə malikdir. Hər iki yanaşma təhlükəsizlik nəzarəti və təhlükəsizlik idarəetmə proseslərinin birləşməsini əhatə edir [Chen, H., & Liu, Y., 2023].

Həm ISO 27002, həm də NIST Kibertəhlükəsizlik Çərçivəsi hansı əməliyyat təhlükəsizlik prosedurlarının yerinə yetirilməli olduğunu göstərir, lakin heç biri TƏM yaratmaq üçün xüsusi tələb irəli sürmür.

İnformasiya təhlükəsizliyi çox vaxt təhlükəsizlik strategiyası, edilə biləcək işlərin dizaynı, həyata keçirilməsi və əməliyyatlardan ibarət dörd mərhələli dövr kimi təqdim olunur. Bu davamlı bir dövrdür, çünki həmişə yeni biznes tələbləri və daha çox planlaşdırma tələb edən yeni təhlükələr yaranır. Deming modeli bunun dörd mərhələdən ibarət erkən təqdimatı idi: planlaşdır, et, yoxla və hərəkət et. Bu yaxınlarda Sherwood Applied Business Security Architecture (SABSA) Framework burada təsvir olunduğu kimi strategiya və planlaşdırma, dizayn, həyata keçirmə, idarəetmə və ölçmə mərhələlərini göstərən belə bir təsvir dərc etdi (Şək. 4.1.1.) [Горбунов, А., 2020].



Şəkil 4.1.1 SABSA-nın təsviri (McCarthy, 2022)

Bu model yalnız müəssisə səviyyəsində təhlükəsizliyin mərhələlərini göstərmək üçün istifadə edilmir, o, həmdə təhlükəsizlik proqramının hər bir aspekti üçün aktualdır. Bu, informasiya təhlükəsizliyi proqramının bütün elementlərinin öz strateji komponentinə malik olmasının vacibliyini vurğulayır. Bu komponent ömürboyu qurulmalı, işlədilməli və saxlanmalıdır. Bu, informasiya təhlükəsizliyi proqramının hər hansı digər elementi kimi TƏM-a da aiddir. Başqa sözlə desək, TƏM bütün varlığı boyunca strategiya və planı saxlamalı, öz imkanlarını və proseslərini tərtib etməli, onları həyata keçirməli, həm operativ, həm də performans baxımından onları idarə etməlidir.

Nüfuzetmə testi nöqteyi-nəzərindən bilmək istədiyimiz şey, aşkarlanmanın qarşısını almaq üçün TƏM-un gündəlik əməliyyat fəaliyyətidir və kibertəhlükələrə cavabdeh nöqteyi-nəzərindən, effektiv qabiliyyətin mövcud olmasını təmin etmək üçün TƏM-un bütün varlığı boyunca olan mərhələlərə baxışına malik olmalıyıq.

TƏM üçün planlaşdırma. Hər hansı yeni fəaliyyət üçün ənənəvi başlanğıc nöqtəsi, fəaliyyətlərin gözlənilən əməliyyat mühitində necə işləyəcəyini göstərən Əməliyyatlar Konsepsiyasını (Concept of Operations - Conops) hazırlamaqdır. TƏM Conops üçün TƏM-un biznes üçün dəyərini müəyyən edən və bir sıra əməliyyat təhlükəsizlik

prinsiplərini təsvir edən biznes əsaslandırması ilə başlayaq. Məsələn: Öz müqəddəratını təyinetmə, biznes mülkiyyətinə sahib olmaq və ümumi əməliyyat fəaliyyətləri ilə bağlı qərar qəbul etmək üçün daxili TƏM-un fəaliyyət göstərməsi.
Əməliyyatda Əminlik, təhlükəsizlik əməliyyat prosedurlarının işlənib hazırlanması, əməliyyat mühafizə xidmətinin səviyyələrinin monitorinqi və hesabatının təqdim edilməsi və əməliyyat heyətinin davamlı təlimi.
İnteqrasiya, ardıcıllığı və qənaətcilliyi təmin etmək üçün təhlükəsizlik əməliyyatlarının İT əməliyyatları ilə inteqrasiyası.
Müxtəlif Situasiyalarda fərqindəlik, hər yerdə olan giriş, monitorinq və təhlükəsizlik analitikasının strukturlaşdırılmış prosesi vasitəsilə TƏM-un gündəlik fəaliyyətlərinin analizi.
Dözümlülük, erkən xəbərdarlıq və hücumlara vaxtında cavab verməklə TƏM biznes imkanlarını tez bir zamanda bərpa edə bilər.
Aktiv cavab, aşkarlama imkanlarını aşa bilən (evation) və müəssisə aktivlərinə sızmış zərərli proqramları axtarır və məhv edir [Chen, L., & Wang, Y., 2022].

Kiçik biznes və əməliyyat təhlükəsizliyini kənardan təmin edənlər üçün yerli əməliyyat təhlükəsizliyi fəaliyyətləri virtual ola bilər. Bununla belə, istənilən əhəmiyyətli ölçüdə İT infrastrukturu olan bir təşkilat üçün adətən əməliyyat analitiklərinin işləyə biləcəyi və insidentlə bağlı cavab tədbirlərinin əlaqələndiriləcəyi mərkəzi yer olması əsas məqamlardan biridir.

Conops TƏM-un fiziki mövcudluğunu təsvir edir - onun harada yerləşəcəyini, infrastruktura necə qoşulacağını və TƏM əməliyyatları baxımından necə görünəcəyini - konsol, divara quraşdırılmış ekranlar, insident koordinasiya mərkəzləri, hadisə müşahidəçiləri üçün baxış sahələri və s.

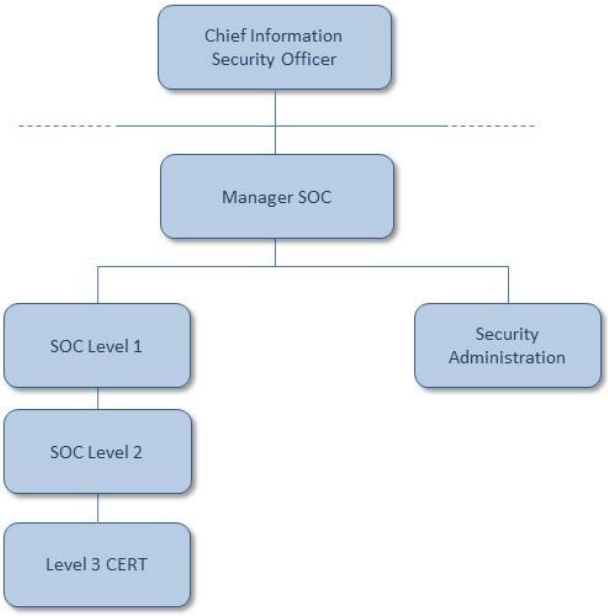
TƏM-un ümumi məqsədi monitorinq və insidentlərə cavab verməklə texnologiya infrastrukturu və əməliyyatları üçün təhlükəsizliyi təmin etməkdir. Bəzi TƏM-ların təhlükəsiz xidməti inkişafını təmin etmək üçün inkişaf qrupları ilə əlaqə saxlamaq üçün daha geniş səlahiyyətləri ola bilər. Bunun, biznes üçün yüksək effektivliyi ola bilər, çünki o, təhlükəsizliyin ən erkən fürsətdə yeni layihələrdə həyata

keçirilməsini təmin edir. TƏM-un bu sonuncu forması inkişafla güclü inteqrasiyasına görə bəzən İnteqral TƏM kimi tanınır.

TƏM adətən dörd komandada qurulur:

- TƏM Level 1 - xəbərdarlığın monitorinqini, triajını və kiçik problemlərin həllini və Level 2 araşdırmasını tələb edən hadisələr üçün ticket-lərin yaradılmasını təmin edir.
- TƏM Level 2, incidentlərə cavab (İnsident Response - IR) playbook kimi tanınan əvvəlcədən hazırlanmış cavabla idarə oluna bilən adi hadisələrin təhlilini, saxlanmasını və həllini təmin edir. Səviyyə 2 komandası təhlükəsizlik hadisəsi reyestrinə sahib olacaq və onu idarə edəcək. Təhlükəsizlik sistemlərinin konfiqurasiyasına və saxlanmasına, o cümlədən təhdid kəşfiyyatı əməliyyatlarının idarə edilməsinə, təhdid imzalarının saxlanmasına, sensorların tənzimlənməsinə cavabdeh olacaq. O, həmçinin təhlükəsizlik divarı qaydalarının idarə edilməsinə də cavabdeh ola bilər, baxmayaraq ki, hər hansı bir şəbəkə konfiqurasiyası dəyişikliyi adətən dəyişikliklərin nəzarəti prosesi əsasında olur və İT şəbəkə komandası tərəfindən idarə olunur.
- Bəzən CERT/CIRT kimi tanınan TƏM Level 3 zərərə nəzarət, daha dərin araşdırma və kriminalistika və ya playbook olmayan insidentlərə cavab tələb edən hadisələr üçün cavabdehdir. Kiçik təşkilatlarda, bu, yalnız lazım olduqda və nadir hallarda çağırılan, kənar xidmətdir.
- Sonuncu komanda olan Təhlükəsizlik administrasiyası giriş kartı problemləri, hesabların təmin edilməsi, giriş icazələrinin nəzərdən keçirilməsi, müntəzəm təhlükəsizlik hesabatları və digər proaktiv təhlükəsizlik prosedurları kimi gündəlik, insidentlə əlaqəli olmayan prosedurlara cavabdehdir.

TƏM-un standart təşkilati sxemi (Şək. 4.1.2.):



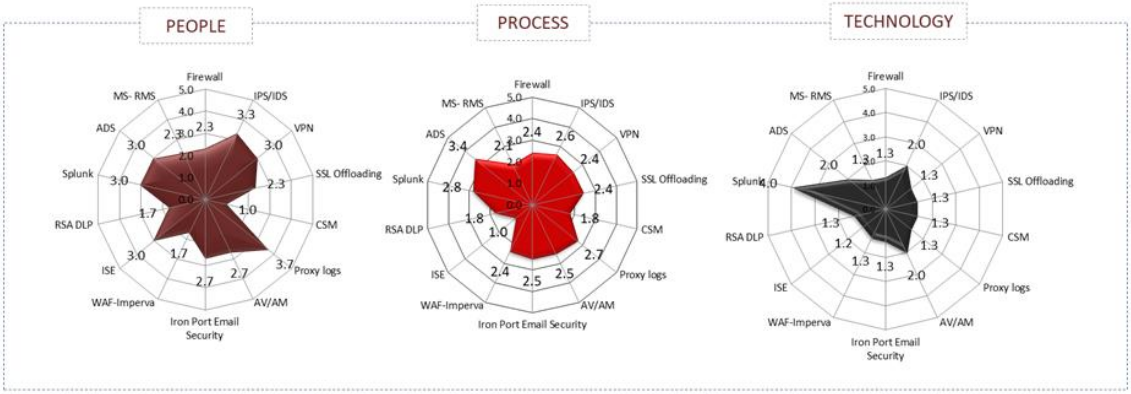
Şəkil 4.1.2. TƏM-in sxemi (Allan S., 2022)

2 və ya 3-cü səviyyələrdə baş verən hər hansı insident, hadisələrin idarə edilməsinə əsas reaksiya daxil olmaqla, eskalasiyaya səbəb ola bilər.

TƏM işlərinin çoxu normal iş saatları ərzində yerinə yetirilə bilər, lakin əsas qərar Level 1 monitorinq xidmətinin 24x7 olaraq qeyri-iş saatları işləməsidir. Rəqiblərin və qırmızı komandaların iş saatları xaricində hücum etmək vərdişləri var və əslində, sistem administratorlarının onlayn olmadığı sakit vaxtları tapmaq çox asandır.

Komandaların gündəlik əməliyyat işi mütəmadi olaraq planlaşdırılan standart əməliyyat prosedurları, habelə Hadisələrə Cavab kimi reaktiv prosedurlar daxil olmaqla, Conops-da təsvir edilməlidir [Crowley, Chris., 2019].

TƏM bir gecədə qurulmur və TƏM texnologiyasından nə dərəcədə istifadə edildiyini, heyətin səlahiyyətlərini və proseslərin yetkinliyini izləmək faydalıdır. Aşağıda bu üç ölçüsün hər biri üçün xüsusi qrafiklərin nümunəsi verilmişdir və hər birinin əsas elementləri göstərilir (Şək. 4.1.3.):



Şəkil 4.1.3. TƏM-in təhlükəsizliyi nümunəsi (McCarthy, 2022)

Bu qrafiklər TƏM-un təkcə biznesi təhlükəsiz saxlamamasını, həm də biznesi kibertəhlükələrdən müdafiə etmək üçün konfiqurasiya edilməsini təmin etmək üçün davam edən inkişafı ən vacib sahələrə yönəltməyə kömək edir.

TƏM-nin yaradılması və davamlı inkişafı texnologiyanın mərhələli yüksəlişini təmin etsə də və dövri baxışlar prosesin təkmilləşdirmələrini müəyyən etsə də, kadrların bacarıqlarının artırılması üçün müəssisə davamlı inkişaf proqramına malik olmalıdır. Bu, 1-ci Səviyyə TƏM monitorinq qrupu üçün xüsusilə vacibdir. Bu komanda hücumları aşkar etmək və onlara cavab vermək bacarıqlarını həyata keçirmək və qiymətləndirmək üçün kiber təlimlər keçirməlidir. Bu təlimlər müəssisənin öz və ya müqavilə bağladığı nüfuzetmə testçiləri qrupu tərəfindən qurula və idarə oluna bilər. Onlar daxili infrastrukturda qurulmuş simulyasiya edilmiş hədəfə qarşı canlı hücumun qurulmasını təmin edirlər. TƏM komandası daha sonra gələn hücumları aşkar etməli və canlı hücumda olduğu kimi hadisəyə cavab verməlidir [Jones, R., & Kim, S., 2019].

TƏM-nin gündəlik olaraq nə edəcəyini başa düşmək üçün biz ucdan-uca informasiya təhlükəsizliyi proqramının icrası ilə bağlı prosesləri başa düşməliyik. Bu proseslər birlikdə Təhlükəsizlik İdarəetmə Çərçivəsini təşkil edir. Mövcud və inkişaf etməkdə olan standart sənədlərdən rəhbər tuta bilərik:

Beynəlxalq Standartlar Təşkilatı (ISO) ISO 27000 - on iki idarəetmə prosesi və dörd dəstək prosesinin modelini təsvir edir.

The Open Group artıq öz İnformasiya Təhlükəsizliyi İdarəetmə Yetkinlik Modeli-ni (ISM3) dərc etmişdir ki, bu da prosesləri SABSA dövrü modelinin həm dizayn, həm də həyata keçirmə mərhələlərinə uyğunlaşdırmışdır.

NIST Kiber Təhlükəsizlik Çərçivəsi müəyyən et, qoru, aşkar et, cavab ver və bərpa et hücum mərhələlərində qruplaşdırılmış iyirmi üç kateqoriyada təhlükəsizlik tələblərinə malikdir. Bunlar siyasətlərin, imkanların və proseslərin qarışığıdır.

Bu təlimatı nəzərdən keçirərək, daxil etməklə biz aşağıda göstərildiyi kimi strateji, taktiki və əməliyyat informasiya təhlükəsizliyinin idarə edilməsi fəaliyyətlərini əhatə edən 36 prosesdən ibarət hərtərəfli informasiya təhlükəsizliyi idarəetmə çərçivəsini əldə edərik (Şək. 4.1.4.):

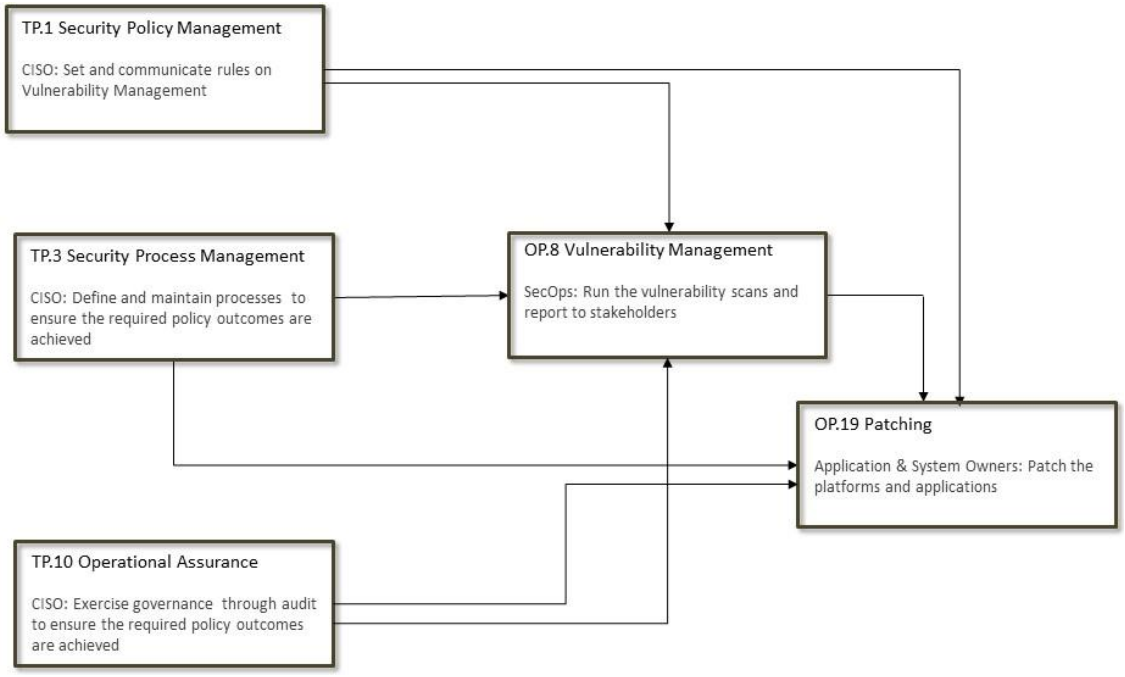
Şəkil 4.1.4. İnformasiya təhlükəsizliyi idarəetməsi (Bejtlich, 2022)

Bu proseslərin qarşılıqlı əlaqəsini başa düşmək üçün zəifliyin idarə edilməsi nümunəsini nəzərdən keçirək.

Strateji səviyyədə zəifliyin skan edilməsi qabiliyyəti SP.4 Müəssisə Təhlükəsizlik Arxitekturasında (ESA) müəyyən edilir və sənədləşdirilir və zəifliyin skan edilməsi və yamaqlanması alətlərinin və ya idarə olunan xidmətlərin əldə edilməsi və yerləşdirilməsinin planlaşdırılması SP.2 Təhlükəsizlik Planlaşdırılması vasitəsilə həyata keçirilir.

Taktiki səviyyədə zəifliklərin skan edilməsi və yamaqlanması siyasəti TP.1 Təhlükəsizlik Siyasətinin İdarəedilməsi vasitəsilə tərtib edilir və ötürülür. Əlaqədar

proseslərin və prosedurların müəyyən edilməsi TP.2 Təhlükəsizlik Proseslərinin İdarə edilməsi vasitəsilə həyata keçirilir. Fəaliyyətə başladıqdan sonra CISO komandası proseslərin və prosedurların effektiv olmasını və onlara əməl olunmasını təmin etmək üçün nəzarəti həyata keçirəcək. Bu, TP.10 Əməliyyat Təminatı Auditi prosesinin məqsədidir. Bütün bu taktiki proseslər CISO-nun səlahiyyətlərinə daxildir. Proseslərin qarşılıqlı əlaqəsi aşağıdakı diaqramda göstərilmişdir (Şək. 4.1.5.):



Şəkil 4.1.5. Zəifliyin idarə edilməsi prosesləri (David G. Hill, 2024)

Əməliyyat səviyyəsində TƏM komandası OP.8 Zəifliyin İdarə edilməsində müəyyən edildiyi kimi zəifliyin idarə edilməsi prosesini və prosedurlarını izləyir. TƏM analitikləri bunun üçün Tenable.io və ya Qualys kimi bir vasitədən istifadə edəcəklər. Onların prosesinin bir hissəsi proqram və sistem sahiblərinə aktivlərində olan zəifliklər barədə məsləhət vermək olacaq.

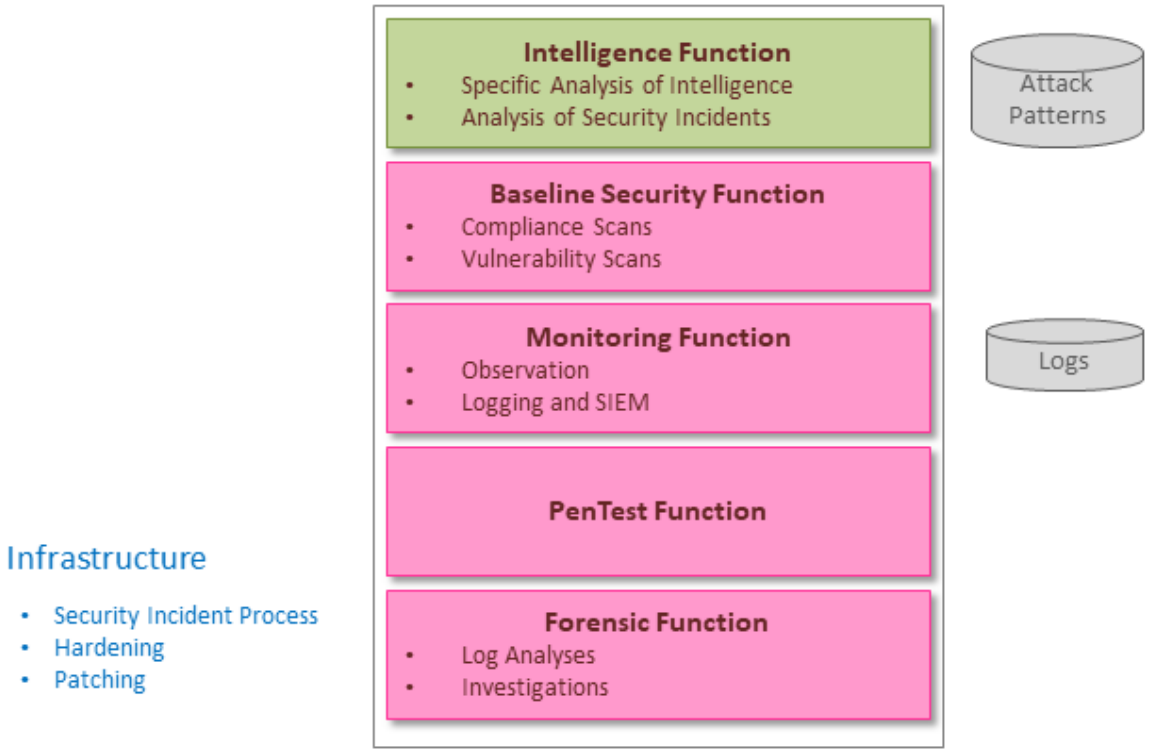
Tətbiq və sistem sahibləri daha sonra yamaq siyasətinə əməl edir və OP.19 Yamaqlama əməliyyat prosesində müəyyən edilmiş prosedurlara uyğun olaraq yamaqları tətbiq edirlər.

Başdan sona informasiya təhlükəsizliyini həyata keçirmək komanda işidir və ayrı-ayrı müəssisələr xüsusi komandaların strukturunu və məsuliyyətini diktə edən müxtəlif təşkilati modellərə malik olacaqlar. Yuxarıdakı misalda zəifliyin skan edilməsi üçün istifadə edilən texnologiyanın müəyyən edilməsi üçün məsuliyyət

müəssisənin təhlükəsizlik arxitektorunun üzərində olacaq, lakin TƏM seçimdə söz sahibi olacaq. TƏM və ya təhlükəsizlikdən kənar İT Çatdırılma komandası texnologiya həllinin əldə edilməsini və tətbiqini idarə edə bilər. Scanlama siyasəti CISO tərəfindən müəyyən edilir, baxmayaraq ki, TƏM ətraflı təhlükəsizlik əməliyyat prosedurları hazırlaya bilər.

Bu, zəifliyin idarə olunması prosesinin yüksək səviyyəli icmalı idi və biz öyrəndik ki, o, təcrid olunmuş proses kimi mövcud deyil, digər proseslərdən asılılıqları var. Proses çərçivəsində çoxsaylı əməliyyat prosedurları olacaq: zəifliyi skan edən agentlərin yerləşdirilməsini təmin etmək, skan nəticələrinin cavabdeh tərəflərə təqdim edilməsi, zərərli proqram imzalarının yenilənməsini təmin etmək və s. OP.8 üçün proses xəritəsində müəyyən edilmişdir [Kim, D., & Park, S., 2022].

TƏM modeli. TƏM-nin 19 əməliyyat təhlükəsizlik prosesində hansı rol oynadığını araşdıraq. TƏM üçün standart idarəetmə modeli yoxdur, lakin Stef Şinaql və onun komandasının işi TƏM fəaliyyətlərinin beş funksiyaya birləşməsini təklif edir: Kəşfiyyat, Əsas Təhlükəsizlik, Monitorinq, PenTest və Rəqəmsal ekspertiza (Şək. 4.1.6.).



Şəkil 4.1.6. TƏM səviyyəsinim infrastrukturu (Chen L., 2022)

Bu beş funksiya hər üç TƏM səviyyəsini əhatə edir, lakin İnsidentlərə Cavab, Sərtləşdirmə və Yamaq kimi əsas təhlükəsizlik proseslərini istisna edir, çünki onlar TƏM komandasının fəaliyyətinə deyil, İnfrastrukturun altına düşür. Bulud xidmətləri tez-tez bu paylaşılan modeldən istifadə edir.

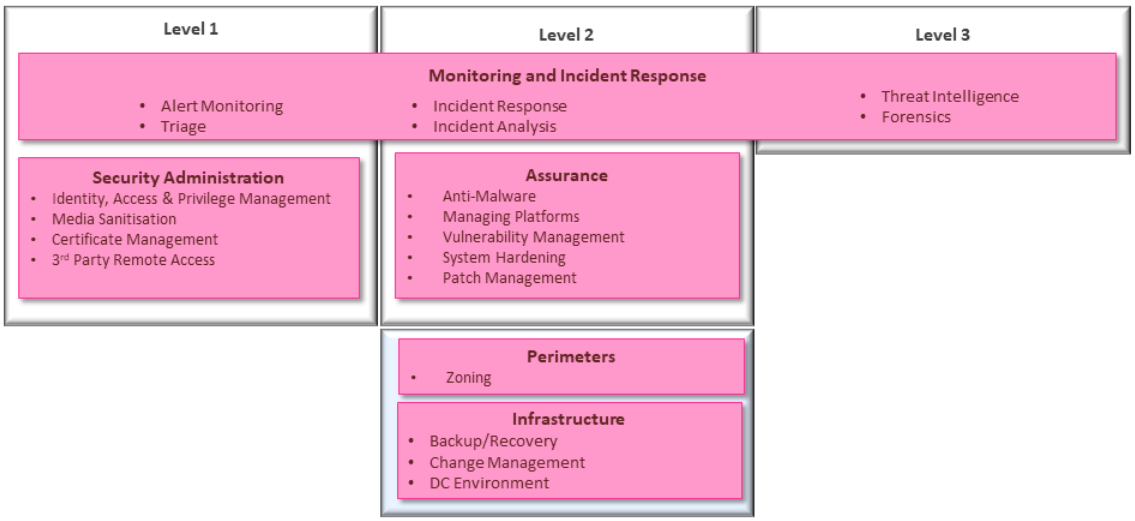
Öz TƏM-ni idarə edən bir təşkilat üçün minimum gözlənti, TƏM-in təhlükəsizlik insidentlərini aşkar etmək və onlara cavab vermək üçün təşkilatın təhlükəsizlik vəziyyətinə davamlı olaraq nəzarət etməsidir. Bu ümumi tərif həm TƏM Səviyyə 1, həm də 2 fəaliyyətlərinin bir çoxunu əhatə edir.

ISMF baxımından, TƏM yalnız Monitorinq və Hadisələrə Cavab verməklə məhdudlaşa bilər, lakin on doqquz əməliyyat təhlükəsizliyinin idarə edilməsi prosesinin əksəriyyətində daha geniş əhatə dairəsinə malik ola bilər.

Bütün modeli Schinagl-ın nəticələrinə əsaslanaq tamamlayaq və bütün on doqquz əməliyyat prosesini nəzərdən keçirək. Gəlin onları prioritet qaydada beş fəaliyyət qrupuna ayıraq:

- Monitorinq və insidentlərə cavab tədbirləri (OP.1, OP.11, OP.12)
- Təminat (OP.2, OP.7, OP.8, OP.10, OP.19)
- Təhlükəsizlik Alətlərinin administrasiyası (OP.3, OP.4, OP.5, OP.9, OP.13, OP.14, OP.15)
- Perimetrlər (OP.6)
- İnfrastruktur (OP.16, OP.17, OP.18)

Nəticə model, aşağıda göstərildiyi kimi, TƏM-un istismarı üçün seçimlər sırasını nəzərdən keçirmək üçün plan kimi istifadə edilə bilər. Bu layihə hansı TƏM modelindən istifadə olunmasından asılı olmayaraq, müəssisə təhlükəsizliyinin effektiv idarə edilməsi üçün yerinə yetirilməli olan proseslərin aydın ifadə olunmasını təmin edir [McMillan, D., 2021].



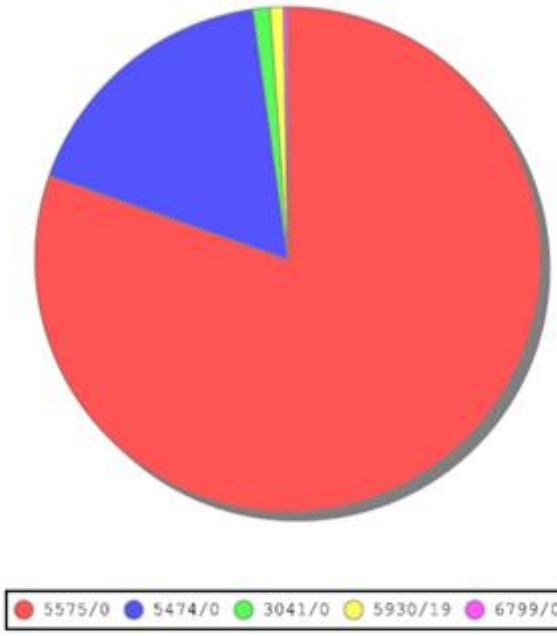
Şəkil 4.1.7. TƏM-in son modeli (Chen L., 2022)

TƏM Hesabatı. TƏM-un işi haqqında hesabat tələbi mütləq olacaq. Bu hesabata əməliyyat səviyyəli razılaşmalara (bəzən daxili xidmət səviyyəsi müqavilələri də deyilir), TƏM Səviyyə 1 tərəfindən açılan ticket-lərin statistikası, TƏM Səviyyə 2 tərəfindən bağlanan ticket-lərin statistikası və hazırda açıq olan ticket-lər daxil olacaq. Tipik TƏM Hadisəsi hesabatı aşağıda göstərilmişdir (Şək. 4.1.8.).

Ticket No.	Date & Time	Description	Severity	Status
SOC-000042	September 24, 2020 10:30:00	**Device Alarm ID / Alarm Description** 7212/1 Web Application Security Test/Attack 106001 Inbound TCP connection denied 106023 Deny IP by ACL 710003 TCP|UDP access denied by ACL **Source IP / Hostname / Domain** 174.143.169.191 Slicehost, US, United States **Destination IP / Hostname / Domain** DC1 192.168.83.16 ACME Website 10.18.66.8 ACME Forefront 10.18.68.27 ACME PKI 10.18.66.31 ACME Website DC2 192.168.146.151 ACME Website 10.10.68.3 ACME PKI 10.10.66.18 ACME Website XX.0.12.X ACME **Destination Port :** 80(http) **Date &Time Range of Incident :** IPS : 09/24/2020 3:13:49 to 3:14:06 AM ASA : 09/24/2020 02:00:00 to 02:51:00 AM	High	Open
Status Summary	Incident template sent to Brian.			

Şəkil 4.1.8. TƏM hadisəsi hesabatı (Wang Y., 2022)

Hadisə ticket-lərinə əlavə olaraq, TƏM infrastruktur dəyişiklikləri tələb etmək üçün ticket-ləri də yarada bilər, məsələn, alt şəbəkələrin skanlardan xaric edilməsi, imzaların tənzimlənməsi və s. Hesabata həmçinin şlüzlərdə işə salınan IDS imzalarının növlərini göstərən diaqramlar daxil ola bilər. Aşağıda aylıq IDS hesabatının nümunəsi verilmişdir (Şək. 4.1.9.):



Signature ID	Signature Description	Count	Percentage
5575/0	NBT NetBIOS Session Service Failed Login	8872	80.39%
5474/0	SQL Query in HTTP Request	1920	17.40%
3041/0	TCP SYN/FIN Packet	120	1.09%
5930/19	Generic SQL Injection	95	0.86%
6799/0	CUCM CTI DoS	29	0.26%

Şəkil 4.1.9. IDS hesabatı

Bu hesabat 2014-cü ilin canlı məlumatlarını əks etdirir. 24 saat ərzində işə salınan təxminən 10.000 imzanın sayına diqqət yetirin. Bu hesabat həm də hücumun mənbəyi tərəfindən və/yaxud zaman periodu üzrə təqdim edilə bilər.

4.2 Təhlükələrə cavab və loq faylların idarə edilməsi

Təhlükəyə Cavab - Bir hadisə təsdiqlənəndə, TƏM ilk müdafiə təşkil edir, endpointi sonlandırır və ya izolyasiya edərək mərkəzləşdirir, zərərli prosesləri sonlandırır (və ya icra edilməsinin qarşısını alır), faylları silir və s. Məqsəd, hücum cəhdinin davam etdirilməməsinə nail olmaq və ya mümkün qədər kiçik bir təsir etməklə lazımi dərəcədə cavab verməkdir.

Bərpa və Düzəltmə - Hadisənin ardından, TƏM sistemləri bərpa etmək və itirilmiş və ya təhlükə altında olan məlumatları bərpa etmək üçün işləyəcəkdir. Bu, endpointləri silib yenidən başlatmaq, sistemləri yenidən konfiqurasiya etmək və ya ransomware hücumları halında, ransom ödəməkdən yayınmaq üçün faydalı ehtimal yedəklər etməkdir. Uğurlu alınarsa, bu addım şəbəkəni hadisədən əvvəlki halına qaytaracaqdır.

Logların İdarəedilməsi - TƏM, təşkilatın bütün şəbəkə fəaliyyəti və kommunikasiyalarının loglarını toplamaq, saxlamaq və düzgün şəkildə nəzarət etmək üçün məsuliyyət daşıyır. Bu məlumat, "normal" şəbəkə fəaliyyəti üçün bir xəritə təyin etməyə kömək edir, təhlükələrin mövcudluğunu açıqlaya bilər və hadisənin ardından bərpa və rəqəmsal istintaq üçün istifadə edilə bilər. Bir çox TƏM-lar, tətbiqlərin, firewall-ların, əməliyyat sistemlərinin və endpointlərin məlumatlarını birləşdirərək və korrelasiya edərək istifadə edən bir SIEM-dən istifadə edirlər.

Əsas Səbəb İncələməsi - Hadisənin ardından, TƏM baş verən hadisənin tam olaraq nə vaxt, necə və niyə baş verdiyini anlamaqdan məsuldur. Bu araşdırma zamanı, TƏM qeyd məlumatlarını və digər məlumatları istifadə edərək problemin mənbəyinə qədər iz sürəcəkdir ki, bu da onlara gələcəkdə oxşar problemlərin qarşısını almağa kömək edəcəkdir.

Təkmilləşdirmə - Kiber cinayətkarlar daimi olaraq alətlərini və taktikalarını təkmilləşdirirlər və onlardan öndə olmaq üçün, TƏM-nun davamlı əsasda təkmilləşdirmələr həyata keçirməsi lazımdır. Bu addımda, Təhlükəsizlik Yol Xəritəsində nəzərdə tutulan planlar həyata keçirilir, amma bu təkmilləşdirmə əsasən red-teaming və purple-teaming kimi praktikaları da əhatə edə bilər.

Uyğunluq İdarəetməsi - Audit Uyğunluğu. TƏM-un bir çox prosesi müəyyən edilmiş ən yaxşı təcrübələrə əsaslanır, amma bəziləri uyğunluq tələbləri tərəfindən idarə olunur. TƏM, sistemlərini düzgün şəkildə təhlil etmək üçün məsuliyyət daşıyır ki, bununla uyğunluğu təmin etsinlər. Bu da onların təşkilatı, sənayesi və ya idarə organları tərəfindən tətbiq edilə bilər. Bu təhlükəsizlik siyasətləri arasında GDPR, HIPAA və PCI DSS kimi nümunələri verə bilərik. Bu tənzimləmələrə əməl etmək, yalnız şirkətin etibarına ziyan vurmasına deyil, ona etibarlı olan cəmiyyətə etibarlı olan cəmiyyətə daxil olmuş məxfi məlumatları qorumağa kömək edir, eyni zamanda ciddi təhlükəsizlik pozuntularından doğan rəqabəti və hüquqi mübahisələrdən də qoruyur.

Mövcud Resursları Qiymətləndirmək. TƏM iki növ aktivləri qoruyur – qorumağa məcbur olduqları cihazlar, proseslər və tətbiqlər və bu qorunmanı təmin etməyə kömək edən müdafiə alətləri.

TƏM-un qoruduğu mövhumlar. TƏM, görmədiyi cihazlar və məlumatları qoruya bilməz. Cihazdan buluda görünürlük(visibility) və nəzarət olmadan, şəbəkə təhlükəsizlik mövqeyində kor nöqtələr olacaqdır ki, onlar tapıla və istismar edilə bilər. Beləliklə, TƏM-un məqsədi işin təhlükə landşaftında tam bir görünüşünü əldə etməkdir, ki, bu, yalnız lokal cihazlar, serverlər və proqramlarla deyil, həmçinin bu aktivlər arasında axışan üçüncü tərəf xidmətləri və trafiki də əhatə edir.

TƏM qoruması anlayışı. TƏM-da olan bütün kiber təhlükəsizlik alətlərinin və TƏM-dakı istifadə olunan bütün iş axınlarının tam bir anlayışı olmalıdır. Bu agile-ı artırır və TƏM-un sürətli effektivlikdə fəaliyyət göstərməsinə imkan verir.

Hazırlıq və Preventiv Dəstək. Ən yaxşı təchiz olunmuş və çevik reaksiya proseslərinə malik olan TƏM belə bəzən problemlərin ilk dəfədən qarşısının alınmasına cavab verə bilmir. Hücumçuların qarşısını almaq üçün, TƏM preventiv tədbirləri həyata keçirir, ki, bunlar iki əsas kateqoriyaya bölünə bilər.

Hazırlıq. Komanda üzvləri, ən yeni təhlükəsizlik inovasiyaları, kibercinayətlərin son trendləri və ətrafındakı yeni təhlükələrin inkişafı barədə məlumatlı olmalıdır. Bu araşdırma, şirkətin kiber təhlükəsizlik üçün istiqamət göstərən bir təhlükəsizlik yol xəritəsi yaratmağa kömək edə bilər, və ən pis hadisələrdə hazır məsləhətləşməni təmin edən bir fəlakət bərpa planı kimi hazır məsləhətləşməni təmin edə bilər.

Preventiv Dəstək. Bu addım, uğurlu hücum cəhdlərini daha çətin edən bütün tədbirləri əhatə edir, bu da mövcud sistemlərin düzgün saxlanılması və yenilənməsi; firewall siyasətlərinin yenilənməsi; zəifliklərin yamalanması; və tətbiqlərin ağ siyahısı, qara siyahısı və təhlükəsizliyin təmin edilməsi daxilində işlənilməsidir.

Davamlı Proaktiv İzləmə. TƏM tərəfindən istifadə olunan alətlər, şəbəkədə hər hansı bir anormallığı və ya şübhəli fəaliyyəti işarələmək üçün 24/7 skan edirlər. Şəbəkəni daimi olaraq izləmək, TƏM-un yeni təhlükələrdən dərhal xəbərdar olmasına imkan verir və onlara ziyanı qarşılamaq və ya azaltmaq üçün ən yaxşı şansı verir. İzləmə alətləri SIEM və ya EDR kimi ola bilər, hətta SOAR və ya XDR kimi, ən mükəmməli olanı isə davranış analizi istifadə edə bilən alətlərdir ki, bu, sistemlərin hər günki hərəkətləri ilə həqiqi təhlükə davranışı arasındakı fərqini "öyrətməyə" imkan verir və insanlar tərəfindən görülməli olan triaj və analiz miqdarını minimuma endirir.

Xəbərdarlıq Sıralaması və İdarəetmə. İzləmə alətləri xəbərdarlıqlar verdiyində, TƏM xəbərdarlıqların hər birinə yaxından baxmalı, yalnız false-positive nəticələri silməli və həqiqi təhlükələrin nə səviyyədə olduğunu və onların məqsədinin nə olduğunu müəyyənləşdirməlidir.

Bu, onlara yeni təhlükələri uyğun şəkildə triyaj etməyə imkan verir və ən təcili məsələləri əvvəlcə həll etmələrinə imkan verir [McCarthy, J., & Allan, S., 2022].

4.3 Son istifadəçi təhlükəsizliyi, ona yanaşmalar və həllər

Son istifadəçi təhlükəsizliyi dedikdə şəbəkədəki müxtəlif son nöqtələrin, məsələn, masaüstü kompüterlər, noutbuklar, smartfonlar, planşetlər, serverlər və digər qurğuların təhlükəsizliyini təmin etmək başa düşülür. Bu son nöqtələr şəbəkəyə giriş nöqtələri kimi xidmət edir və çox vaxt həssas məlumatlara icazəsiz giriş əldə etmək, əməliyyatları pozmaq və ya digər zərərli fəaliyyətlər həyata keçirmək istəyən kiber hücumçuların hədəfinə çevrilir. Son nöqtə təhlükəsizliyi bu son nöqtələri zərərli proqram, ransomware, fişinq hücumları, daxili təhdidlər və digər kiberhücum formaları daxil olmaqla müxtəlif təhlükələrdən qorumaq məqsədi daşıyır. Bu, son nöqtə səviyyəsində təhlükəsizlik insidentlərini aşkar etmək, qarşısını almaq və onlara cavab vermək üçün bir sıra təhlükəsizlik tədbirləri və texnologiyalarının həyata keçirilməsini əhatə edir.

Son nöqtə təhlükəsizliyinin əsas komponentlərinə aşağıdakılar daxildir:

- Antivirus və Antimalware: Viruslar, qurdlar, troyanlar və casus proqramlar kimi zərərli proqramları skan edən və son nöqtələrdən silən proqram.
- Hücumun Aşkarlanması və Qarşısının Alınması Sistemləri (IDS/IPS): Şəbəkə və sistem fəaliyyətlərini zərərli davranış və ya siyasət pozuntuları əlamətləri üçün izləyən və potensial təhlükələrin qarşısını almaq və ya azaltmaq üçün tədbirlər görən alətlər.
- Data Loss Prevention (DLP): Həssas məlumatların qeyri-düzgün və ya icazəsiz əldə edilməsinin, istifadə edilməsinin və ya paylaşılmasının qarşısını almaq üçün nəzərdə tutulmuş texnologiyalar və siyasətlər.

- Endpoint Detection and Response (EDR): Qabaqcıl təhdidlər və sıfır gün hücumları da daxil olmaqla təhlükəsizlik təhdidlərini aşkar etmək və onlara cavab vermək üçün real vaxt rejimində son nöqtə fəaliyyətlərini izləyən həllər.
- Patch Management: Təhlükəsizlik zəifliklərini aradan qaldırmaq və onların ən son təhlükəsizlik düzəlişləri ilə yenilənməsini təmin etmək üçün son nöqtələrə yamaqların və yeniləmələrin müəyyən edilməsi, əldə edilməsi, sınaqdan keçirilməsi və tətbiqi prosesi.
- Cihazın Şifrələnməsi: Cihazın itirilməsi və ya oğurlanması halında icazəsiz girişin qarşısını almaq üçün son nöqtələrdə saxlanılan məlumatların kodlaşdırılması prosesi.
- Endpoint Security Policies: Ən yaxşı təhlükəsizlik təcrübələrini və uyğunluq tələblərini tətbiq etmək üçün son nöqtələrin istifadəsini, konfiqurasiyasını və idarə edilməsini tənzimləyən müəyyən edilmiş qaydalar və təlimatlar.

Həssas məlumatlarını, əqli mülkiyyətini və reputasiyasını kibertəhlükələrdən qorumaq üçün bütün ölçülü və sənaye təşkilatları üçün son nöqtə təhlükəsizliyi vacibdir. Bu, bütün şəbəkə infrastrukturunun potensial hücumlardan qorunmasına yönəlmiş hərtərəfli kibertəhlükəsizlik strategiyasının tərkib hissəsidir [Nguyen, T., & Tran, A., 2020].

Son nöqtə təhlükəsizliyinin tarixi və təkamülü müstəqil kompüterlərin ilkin olaraq istifadə edildiyi hesablamaların ilk günlərinə qədər gedib çıxa bilər. Texnologiya inkişaf etdikcə və şəbəkələr daha çox yayıldıqca, son nöqtələrin təhlükəsizliyinə ehtiyac getdikcə daha aydın oldu. Son nöqtə təhlükəsizliyi tarixindəki əsas mərhələlər və inkişafların qısa icmalı:

Antivirus Proqramı: 1980-ci illərdə kompüter viruslarının artan təhlükəsi ilə mübarizə aparmaq üçün ilk antivirus proqramı ortaya çıxdı. Norton Antivirus və McAfee VirusScan kimi proqramlar məlum zərərli proqram təhdidlərinə qarşı əsas müdafiəni təklif edən bu sahədə ilk qabaqcıllardan idi.

Firewall Texnologiyası: 1990-cı illərdə şəbəkə mühitlərinin və internetin yüksəlişi ilə firewall texnologiyası son nöqtələri icazəsiz giriş və şəbəkə əsaslı hücumlardan qorumaq üçün vacib hala gəldi. Firewalllar daxili şəbəkələrlə xarici

dünya arasında maneə rolunu oynayaraq, əvvəlcədən müəyyən edilmiş təhlükəsizlik qaydaları əsasında trafikə nəzarət edirdi.

Intrusion Detection Systems (IDS): Kiber təhdidlər daha mürəkkəbləşdikcə, şəbəkə trafikinə nəzarət etmək və şübhəli və ya zərərli fəaliyyət əlamətlərini aşkar etmək üçün IDS həlləri hazırlanmışdır. Bu sistemlər potensial təhlükəsizlik pozuntularının erkən aşkarlanmasını təmin edərək, təşkilatlara təhdidlərə operativ reaksiya verməyə imkan verirdi.

Endpoint Protection Platforms (EPP): 2000-ci illərin əvvəllərində son nöqtə təhlükəsizliyi konsepsiyası Endpoint Protection Platforms kimi tanınan daha əhatəli həllərə çevrilməyə başladı. EPP həlləri antivirus, firewall, müdaxilənin qarşısının alınması və cihaza nəzarət kimi müxtəlif təhlükəsizlik texnologiyalarını mərkəzləşdirilmiş idarəetmə və nəzarət üçün vahid platformaya birləşdirdi.

Qabaqcıl Son Nöqtə Mühafizəsi (AEP): Sıfır gün istismarları və hədəflənmiş hücumlar kimi qabaqcıl təhdidlərin ortaya çıxması ilə ənənəvi antivirus və EPP həlləri adekvat qorunmanın təmin edilməsində qeyri-adekvat olduğunu sübut etdi. Next-Generation Endpoint Security kimi də tanınan AEP həlləri real vaxtda mürəkkəb təhdidləri aşkar etmək və onlara cavab vermək üçün davranış analizi, maşın öyrənməsi və süni intellekt kimi qabaqcıl üsullardan istifadə edir.

Endpoint Detection and Response (EDR/XDR): EDR həlləri son nöqtə səviyyəsində proaktiv təhlükənin aşkarlanması və insidentlərə reaksiya imkanlarına artan ehtiyaca cavab olaraq ortaya çıxdı. Bu həllər son nöqtə fəaliyyətlərinin görünməsini təmin edir, şübhəli davranışları aşkar edir və təhlükəsizlik insidentlərinə sürətli reaksiya və düzəlişləri asanlaşdırır.

Bulud əsaslı son nöqtə təhlükəsizliyi(XDR): Bulud hesablama və uzaqdan işləməyə doğru keçidlə son nöqtə təhlükəsizlik həlləri dəyişən təhlükə mənzərəsinə uyğunlaşmaq üçün təkamül etdi. Bulud əsaslı son nöqtə təhlükəsizlik platformaları genişlənmə, çeviklik və mərkəzləşdirilmiş idarəetmə təklif edir ki, bu da onları müasir mühitlərdə paylanmış son nöqtələri qorumaq üçün yaxşı uyğunlaşdırır.

Ümumilikdə, son nöqtə təhlükəsizliyinin tarixi yaranan təhdidləri həll etmək və təşkilatların rəqəmsal aktivlərini effektiv şəkildə qorumaq üçün kibertəhlükəsizlik

texnologiyalarının və strategiyalarının davamlı təkamülünü əks etdirir. Kibertəhlükəsizliklər inkişaf etməyə davam etdikcə, son nöqtənin təhlükəsizliyi hərtərəfli kibertəhlükəsizlik proqramlarının kritik komponenti olaraq qalacaq və rəqibləri qabaqlamaq üçün davamlı innovasiya və uyğunlaşma tələb edir [Li, J., & Zhang, S., 2021].

4.4. Son istifadəçi təhülkəsizliyində əsas standartlar və nəzarət mexanizimləri

Son nöqtə təhlükəsizliyinin müxtəlif aspektlərini həll etmək üçün bir sıra tədqiqat işləri, nəzəriyyələr və çərçivələr hazırlanmışdır. Bunlardan bəziləri aşağıdakılardır:

MITRE ATT&CK Çərçivəsi: MITRE ATT&CK (Düşmən Taktikaları, Texnikaları və Ümumi Bilik) real dünyadaki kiberhücumlarda müşahidə olunan düşmən taktika və texnikalarının əhatəli matrisini təmin edən geniş istifadə olunan çərçivədir. O, son nöqtələri və şəbəkənin digər hissələrini güzəştə getmək üçün rəqiblərin istifadə etdiyi davranışları və üsulları başa düşmək və təsnif etmək üçün strukturlaşdırılmış bir yol təklif edir.

NIST Kibertəhlükəsizlik Çərçivəsi: Milli Standartlar və Texnologiya İnstitutu (NIST) tərəfindən hazırlanmış Kibertəhlükəsizlik Çərçivəsi təşkilatların öz kibertəhlükəsizlik mövqeyini necə idarə edə və təkmilləşdirə biləcəyinə dair təlimat verir. Son nöqtə təhlükəsizliyinə xas olmasa da, son nöqtə təhlükəsizliyi təcrübələrinə tətbiq oluna bilən kibertəhlükəsizlik təhdidlərinin müəyyən edilməsi, qorunması, aşkarlanması, cavablandırılması və bərpası üçün strukturlaşdırılmış yanaşma təklif edir.

Sıfır Güvən Təhlükəsizlik Modeli: Sıfır Güvən modeli güman edir ki, şəbəkə perimetri daxilində və ya xaricində heç bir qurum standart olaraq etibar edilməməlidir. Bu yanaşma, son nöqtələr də daxil olmaqla, şəbəkə daxilində təcavüzkarlar tərəfindən icazəsiz giriş və yan hərəkət riskini azaltmaq üçün şəxsiyyətlərin davamlı yoxlanılmasını, ciddi giriş nəzarətlərini və ən az imtiyazlı giriş prinsiplərini vurğulayır.

Dərin Müdafiə: Dərin müdafiə strategiyası son nöqtələri və digər aktivləri müxtəlif hücum vektorlarından qorumaq üçün çox səviyyəli təhlükəsizlik nəzarəti və əks

tədbirlərin həyata keçirilməsini müdafiə edir. Bu yanaşma qəbul edir ki, heç bir tək təhlükəsizlik tədbiri bütün təhdidlərin qarşısını almaq üçün kifayət deyil, ona görə də möhkəm müdafiə mexanizmləri yaratmaq üçün qabaqlayıcı, əməliyyatçı və cavabdeh nəzarətlərin birləşməsindən istifadə edilməlidir.

Son Nöqtə Təhlükəsizlik Riskinin Qiymətləndirilməsi Çərçivələri: Təşkilatlar daxilində son nöqtə təhlükəsizlik risklərinin qiymətləndirilməsi və idarə edilməsi üçün müxtəlif çərçivələr və metodologiyalar mövcuddur. Bu çərçivələr adətən son nöqtə təhlükəsizlik risklərinin müəyyən edilməsini və qiymətləndirilməsini, bu risklərin potensial təsirinin müəyyən edilməsini və riskə məruz qalmanın effektiv şəkildə azaldılması üçün nəzarət və təsir azaltma strategiyalarının həyata keçirilməsini əhatə edir.

Davranış Analitikası və Təhdid Kəşfiyyatı: Davranış analitikası və təhdid kəşfiyyatı sahəsində tədqiqatlar son nöqtə səviyyəsində təhlükəsizlik təhdidlərinin göstəricisi olan anomal və ya şübhəli davranışı müəyyən etmək üçün məlumat analitikasından və kəşfiyyat toplama üsullarından istifadə etməyə yönəlib. Bu yanaşmalar təşkilatlara davranış nümunələrini təhlil etməklə və onları məlum kompromis göstəriciləri (IOCs) və təhlükə kəşfiyyatı xəbərləri ilə əlaqələndirməklə qabaqcıl təhdidləri daha effektiv aşkar etməyə və onlara cavab verməyə imkan verir.

Endpoint Detection and Response (EDR) Araşdırması: EDR həlləri son nöqtə səviyyəsində təhlükəsizlik insidentlərini aşkar etmək, təhlil etmək və onlara cavab vermək üçün imkanlarını təkmilləşdirməyə yönəlmiş geniş tədqiqatın mövzusu olmuşdur. Bu sahədə tədqiqatlar tez-tez qabaqcıl aşkarlama alqoritmlərinin işlənib hazırlanmasına, məhkəmə-tibbi imkanların artırılmasına və digər təhlükəsizlik texnologiyaları və platformaları ilə inteqrasiyanın təkmilləşdirilməsinə yönəlir.

Bu tədqiqat tədqiqatları, nəzəriyyələr və çərçivələr son nöqtə təhlükəsizlik mövqeyini artırmaq və müasir kibertəhlükələrlə bağlı riskləri azaltmaq istəyən təşkilatlar üçün dəyərli anlayışlar və təlimatlar təqdim edir. Bu resurslardan istifadə etməklə təşkilatlar öz xüsusi ehtiyaclarına və çağırışlarına uyğunlaşdırılmış daha möhkəm və effektiv son nöqtə təhlükəsizlik strategiyaları hazırlaya bilərlər [Chen, H., & Liu, Y., 2023].

XDR və ya Genişləndirilmiş Aşkarlama və Cavab platformaları müxtəlif İT mühitlərində təhdidlərin aşkarlanması, cavablandırılması və aradan qaldırılması üçün nəzərdə tutulmuş hərtərəfli kibertəhlükəsizlik həlləridir. Kiber təhdidlər getdikcə təkmilləşdikcə və geniş yayıldıqca, firewall və antivirus proqramı kimi ənənəvi təhlükəsizlik tədbirləri təşkilatları qabaqcıl hücumlardan qorumaq üçün artıq kifayət etmir. XDR platformaları potensial təhdidlərin vahid görünüşünü təmin etmək üçün çoxsaylı təhlükəsizlik mənbələrindən məlumatların inteqrasiyası və əlaqələndirilməsi ilə daha vahid yanaşma təklif edir.

XDR platformalarının əsas xüsusiyyətləri və imkanlarına adətən aşağıdakılar daxildir:

Məlumat İnteqrasiyası: XDR platformaları son nöqtənin aşkarlanması və cavablandırılması (EDR), şəbəkə trafikinin təhlili (NTA), bulud təhlükəsizliyi, e-poçt təhlükəsizliyi və s. kimi müxtəlif təhlükəsizlik alətləri və mənbələrindən məlumatları birləşdirir. Bu mərkəzləşdirilmiş məlumatların toplanması təşkilatın təhlükəsizlik vəziyyətinin hərtərəfli görünməsinə imkan verir.

Qabaqcıl Analitika: XDR platformaları potensial təhlükəsizlik təhdidlərini göstərən nümunələri müəyyən etmək üçün maşın öyrənməsi və davranış analitikası kimi qabaqcıl analitika üsullarından istifadə edir. Böyük həcmli məlumatları real vaxt rejimində təhlil edərək, bu platformalar həm məlum, həm də naməlum təhlükələri daha effektiv aşkarlaya bilir.

Korrelyasiya və Kontekstuallaşdırma: XDR platformalarının əsas güclü tərəflərindən biri onların İT mühitinin müxtəlif təbəqələrində təhlükəsizlik hadisələrini əlaqələndirmək qabiliyyətidir. Hadisələri və davranışları kontekstləşdirərək, XDR platformaları normal fəaliyyətlər ilə şübhəli və ya zərərli davranışları ayırd edə, yalan pozitivləri azalda və təhlükənin aşkarlanması dəqiqliyini yaxşılaşdıra bilər.

Avtomatlaşdırılmış Cavab: XDR platformaları tez-tez təşkilatlara təhlükəsizlik insidentlərinə sürətlə reaksiya verməyə imkan verən avtomatlaşdırılmış cavab imkanlarını ehtiva edir. Avtomatlaşdırılmış tədbirlərə yoluxmuş son nöqtələrin karantin edilməsi, zərərli IP ünvanlarının bloklanması və ya təhlükəsizlik analitikləri tərəfindən əlavə araşdırma üçün xəbərdarlıqların işə salınması daxil ola bilər.

Qrup əlaqələndirilməsi və İş axını: XDR platformaları mərkəzləşdirilmiş tablolar, oyun kitabları və işin idarə edilməsi funksiyalarını təmin etməklə əməkdaşlığı asanlaşdırır və insidentlərə cavab iş axınlarını sadələşdirir. Bu imkanlar təhlükəsizlik qruplarına səylərini daha effektiv əlaqələndirməyə və ardıcıl cavab prosedurlarını təmin etməyə kömək edir.

Çeviklik: XDR platformaları son nöqtələri, şəbəkələri, bulud infrastrukturunu və IoT cihazlarını əhatə edən müxtəlif İT mühitlərini dəstəkləyərək təşkilatların inkişaf edən ehtiyacları ilə miqyaslaşdırmaq üçün nəzərdə tutulub. Onlar həmçinin mövcud iş axınının pozulmasını minimuma endirərək, mövcud təhlükəsizlik alətləri və texnologiyaları ilə inteqrasiya etmək üçün kifayət qədər çevikdirlər.

Təhlükə Kəşfiyyatının İnteqrasiyası: Təhdid kəşfiyyatı lentləri və xidmətləri ilə inteqrasiya XDR platformalarına təhlükəsizlik məlumatlarını məlum təhdidlər, kompromis göstəriciləri (IOCs) və yeni yaranan hücum üsulları haqqında müasir məlumatla zənginləşdirməyə imkan verir. Bu inteqrasiya təhlükənin aşkarlanmasının dəqiqliyini artırır və inkişaf edən təhdidlərə qarşı proaktiv müdafiəyə imkan verir.

Uyğunluq və Hesabatlılıq: XDR platformaları tez-tez tənzimləyicilərə uyğunluğun monitorinqi və hesabatı üçün funksiyaları ehtiva edir, təşkilatlara sənaye qaydalarına və GDPR, HIPAA, PCI DSS və digərləri kimi standartlara riayət olunmasını nümayiş etdirməyə kömək edir. Avtomatlaşdırılmış hesabat imkanları uyğunluq yoxlamaları və hesabatlarda vaxt və səylərə qənaət edir.

Ümumilikdə, XDR platformaları inkişaf etmiş təhdidlərin aşkarlanması, sürətli reaksiya imkanları və mürəkkəb İT mühitlərində təkmilləşdirilmiş görünürlük təmin etməklə təşkilatların kibertəhlükəsizlik mövqeyinin gücləndirilməsində mühüm rol oynayır. Kiber təhdidlər inkişaf etməyə davam etdikcə, XDR platformaları, çox güman ki, rəqibləri qabaqlamaq və onların qiymətli aktivlərini və məlumatlarını qorumaq istəyən təşkilatlar üçün getdikcə əvəzolunmaz olacaq.

4.5.Son istifadəçi təhlükəsizliyinin vacibliyi və müəssisə təhlükəsizliyinə onun faydaları

XDR (Genişləndirilmiş Aşkarlama və Cavab) və ənənəvi antivirus həlləri kibertəhlükəsizliyə müxtəlif yanaşmaları təmsil edir, hər birinin öz güclü tərəfləri və məhdudiyyətləri var. Budur ikisi arasında bir müqayisə:

Ənənəvi Antivirus: Ənənəvi antivirus proqramı ilk növbədə imza əsaslı aşkarlama metodları əsasında məlum zərərli proqram təminatının aşkarlanmasına və bloklanmasına diqqət yetirir. O, adətən son nöqtə səviyyəsində işləyir, məlum zərərli nümunələr üçün faylları və prosesləri skan edir.

XDR: XDR platformaları şəbəkələr, bulud xidmətləri, e-poçt və s. daxil olmaqla, ənənəvi son nöqtələrdən kənarda çoxsaylı təhlükəsizlik mənbələrindən məlumatları inteqrasiya etməklə daha geniş əhatə dairəsi təklif edir. XDR həlləri həm məlum, həm də naməlum təhdidləri aşkar etmək üçün qabaqcıl analitika və maşın öyrənməsindən istifadə edərək mürəkkəb hücumlara qarşı daha əhatəli müdafiə təmin edir.

Aşkarlama Texnikaları

- Ənənəvi Antivirus - Ənənəvi antivirus əsasən faylları və prosesləri məlum zərərli proqram imzalarının verilənlər bazası ilə müqayisə edən imza əsaslı aşkarlamaya əsaslanır. Məlum təhlükələrə qarşı effektiv olsa da, ənənəvi antivirus həlləri yeni və ya əvvəllər görünməmiş zərərli proqram variantlarını aşkar etməkdə çətinlik çəkə bilər.
- XDR - XDR platformaları sıfır gün hücumları və qabaqcıl davamlı təhdidlər (APT) daxil olmaqla geniş spektrli təhdidləri aşkar etmək üçün imza əsaslı aşkarlama, davranış analitikası, maşın öyrənməsi və təhdid kəşfiyyatının birləşməsindən istifadə edir. XDR platformaları bir çox mənbədən alınan məlumatları əlaqələndirməklə, potensial təhlükələri göstərən şübhəli nümunələri və anomaliyaları müəyyən edə bilər.

Reaksiya Bacarıqları

- Ənənəvi Antivirus: Ənənəvi antivirus həlləri adətən müəyyən edilmiş zərərli proqramların bloklanmasına və ya karantinə qoyulmasına diqqət yetirir. Onlar yoluxmuş faylları silmək və ya karantin etmək kimi bəzi əsas remediasiya

imkanlarını təklif etsələr də, XDR platformalarının hərtərəfli cavab imkanlarından məhrumdurlar.

- XDR: XDR platformaları avtomatlaşdırılmış remediasiya tədbirləri, təhlükə ovlanması və insidentlərə cavab tədbirlərinin təşkili daxil olmaqla qabaqcıl cavab imkanları təklif edir. Cavab prosedurlarını avtomatlaşdırmaq və mərkəzləşdirilmiş insidentlərin idarə edilməsi funksiyalarını təmin etməklə, XDR platformaları təşkilatlara təhlükəsizlik insidentlərinə sürətlə reaksiya verməyə və pozuntuların təsirini minimuma endirməyə imkan verir.

Kontekstuallaşdırma və Korrelyasiya

- Ənənəvi Antivirus: Ənənəvi antivirus həlləri daha geniş kontekstual məlumatları nəzərə almadan və ya İT mühitinin müxtəlif təbəqələrində təhlükəsizlik hadisələrini əlaqələndirmədən yalnız son nöqtənin qorunmasına diqqət yetirərək, təcrid olunmuş şəkildə fəaliyyət göstərir.
- XDR: XDR platformaları son nöqtələr, şəbəkələr və bulud xidmətləri kimi çoxsaylı təhlükəsizlik mənbələrindən məlumatları inteqrasiya edərək kontekstuallaşdırma və korrelyasiya imkanlarını təmin edir. Bütün İT mühitində hadisələri və davranışları əlaqələndirməklə, XDR platformaları normal fəaliyyətlər və şübhəli davranışlar arasında fərq yarada, yalan pozitivləri azalda və təhlükənin aşkarlanması dəqiqliyini yaxşılaşdıra bilər.

Ölçəklənmə və Çeviklik

- Ənənəvi Antivirus: Ənənəvi antivirus həlləri, ümumiyyətlə, fərdi son nöqtələri qorumaq üçün nəzərdə tutulub və müxtəlif infrastruktur və cihazlara malik mürəkkəb İT mühitlərinə uyğunlaşmaq üçün genişlənmə və ya çevikliyə malik olmaya bilər.
- XDR: XDR platformaları son nöqtələri, şəbəkələri, bulud infrastrukturunu və IoT cihazlarını əhatə edən müxtəlif İT mühitlərini dəstəkləyərək təşkilatların inkişaf edən ehtiyaclarına uyğun miqyas almaq üçün nəzərdə tutulub. Onlar mövcud iş axınlarının pozulmasını minimuma endirərək, mövcud təhlükəsizlik alətləri və texnologiyaları ilə inteqrasiya etmək üçün çeviklik təklif edir.

XDR hərtərəfli qorunma, aşkarlama və cavab imkanları təklif edən Genişləndirilmiş Aşkarlama və Cavab (XDR) həllərində yeni standart müəyyən edir. XDR son nöqtəsindən və müxtəlif üçüncü tərəf mənbələrindən məlumatları təhlil edərək, kibertəhlükəsizlik mənzərəsində inkişaf edən təhdidlərə effektiv şəkildə qarşı çıxır. XDR ənənəvi son nöqtə təhlükəsizliyindən kənara çıxır, şəbəkə, son nöqtə, bulud, üçüncü tərəf və identifikasiya mənbələri arasında tam görünürlük təmin edir.

Əsas Xüsusiyyətlər

- Gücləndirilmiş effektivlik üçün avtomatlaşdırma: XDR sadələşdirilmiş avtomatlaşdırma hərəkətlərini özündə birləşdirir, təhlükəsizlik analitikləri üçün araşdırma proseslərini sadələşdirir və onları təhdidlərə cavab verməkdə daha səmərəli edir.
- Hərtərəfli görünmə: Adi həllərdən fərqli olaraq, XDR son nöqtə ilə məhdudlaşmır, tam görünməni təmin edir. O, şəbəkə, bulud, üçüncü tərəf və şəxsiyyət mənbələrini əhatə edir və təhlükənin aşkarlanmasına vahid yanaşma təklif edir.
- Aşkarlamaq və cavab vermək üçün azaldılmış vaxt: XDR, ümumi insidentlərə reaksiya imkanlarını artıraraq, aşkarlama üçün Orta Vaxtı (MTTD) və Cavab Vermək üçün Orta Vaxtı (MTTR) əhəmiyyətli dərəcədə azaldır.
- Şəxsiyyət yönümlü təhlükənin aşkarlanması: Qutudan kənar şəxsiyyət yönümlü təhlükənin aşkarlanması ilkin giriş taktikaları, texnikaları və prosedurlarına (TTP) müraciət edir. Əlavə əlavələr daxili təhdidlər kimi təkmil şəxsiyyətə əsaslanan təhdid aşkarlama analitikası üçün əlçatandır.
- Sübut edilmiş effektivlik: XDR MITER ATT&CK Raund 4 Qiymətləndirməsindən təsirli nəticələrə malikdir və 97% aşkarlama dərəcəsinə nail olur.
- Məlumat elminə əsaslanan aşkarlamalar: Maşın öyrənmə alqoritmlərindən istifadə edərək, XDR, xüsusən aşkarlanması çətin olan təhdidlər üçün səs-küyü minimuma endirən və effektivliyi yaxşılaşdıran həqiqi məlumat elminə əsaslanan aşkarlamaları təmin edir.

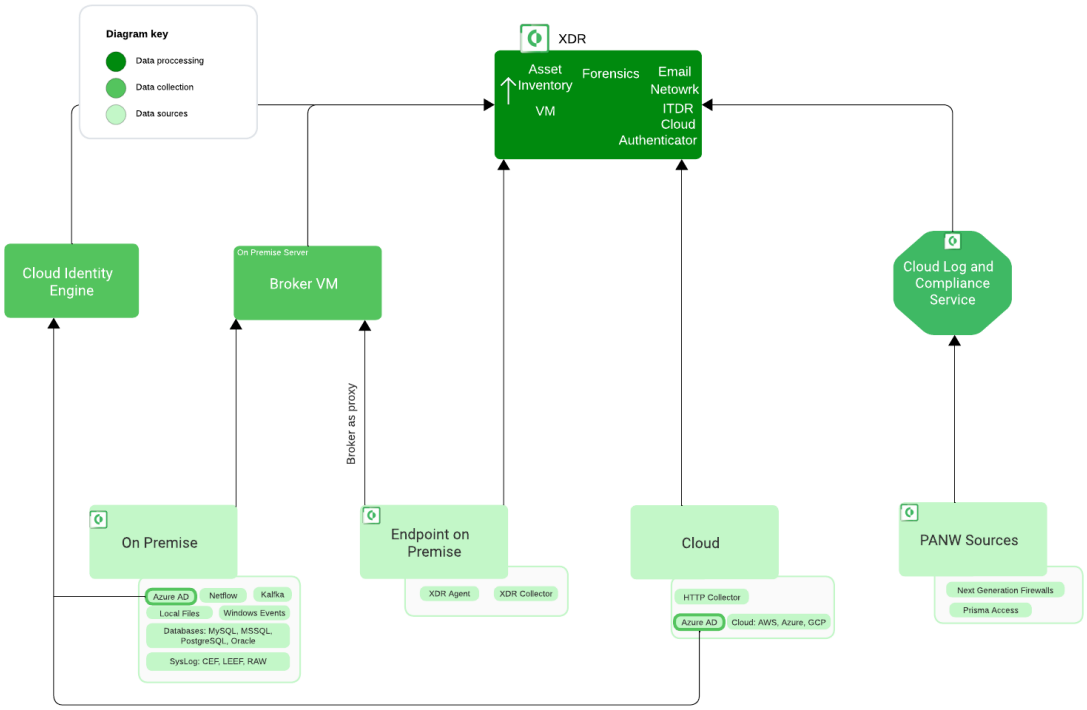
- Buludla işləyən miqyaslanma: XDR, yerli həll tələbləri olmadan buludun gücündən istifadə edərək, müəssisə ehtiyaclarına uyğun miqyas vermək üçün nəzərdə tutulmuşdur.
- Vahid son nöqtə agenti: Yeni Nəsil Antivirus (NGAV), Son Nöqtənin Aşkarlanması və Cavab (EDR), host təhlükəsizlik divarı, cihaz nəzarəti, disk şifrələməsi və məhkəmə ekspertizasının toplanması və host anlayışları üçün əlavə əlavələri təmin edən vahid son nöqtə agenti daxildir [Kim, D., & Park, S., 2022].

XDR tərəfindən həll edilən təhlükəsizlik problemləri

XDR bu gün təşkilatların üzləşdiyi bir neçə təhlükəsizlik problemini effektiv şəkildə həll edir:

- Siloların parçalanması: Son nöqtə agenti, təhlükənin aşkarlanması analitikası, avtomatlaşdırma, şəxsiyyət təhlükəsinin aşkarlanması və məhkəmə-tibbi imkanları əhatə edən inteqrasiya olunmuş həlli təqdim etməklə, XDR təhlükəsizlik həlli siloslarını sıradan çıxarır.
- Davamlı təhdid kəşfiyyatının inteqrasiyası: XDR, müştərilərə ən müasir anlayışlar təqdim edərək, seçilmiş Unit 42 və təhdid tədqiqatını davamlı şəkildə inteqrasiya edərək köhnəlmiş və parçalanmış təhdid kəşfiyyatı problemini həll edir.
- Təhlükənin aşkarlanmasının balanslaşdırılması: XDR, üçüncü tərəfin sınaqları ilə nümayiş etdirildiyi kimi, həm məlum, həm də naməlum təhlükələri qaçırma riskini azaldır. O, aşağı siqnal-səs nisbətini qoruyur, yalan pozitivləri azaldır və təhlükəsizlik analitiklərini yalançı bayraqları təqib etməkdən azad edir.
- Artan ROI: XDR dar konsentrasiyalı Son Nöqtə Təsbiti və Cavab (EDR) həlləri və Təhlükəsizlik Məlumatı və Hadisə İdarəetmə (SIEM) həlləri ilə müqayisədə artan investisiya gəliri (ROI) təklif edir. Müştərilər üzərində idarəetmə yükünü minimuma endirməklə yanaşı, təkmilləşdirilmiş aşkarlama effektivliyini təmin edir.
- Şəxsiyyətə əsaslanan təhdidlərin aşkarlanması: XDR şəxsiyyətə əsaslanan təhdidlərin artan narahatlığını həll etməklə, şəxsiyyət təhlükəsinin

aşkarlanması və cavablandırılması (ITDR) modulu ilə daxili təhdidləri, yanal hərəkəti və anormal istifadəçi və qurum davranışını əhatə etməklə fərqlənir (Şək. 4.5.1) [Nguyen, T., & Tran, A., 2020].



Şəkil 4.5.1. XDR modeli (Paloalto, 2024)

Məlumat mənbələri zəncirin aşağı hissəsində toplanır və yerli serverlər və mühərriklər tərəfindən işlənir. Məlumatlar ilkin olaraq Cortex Data Model (XDM) və XQL istifadə edərək işlənir və təhlil edilir, sorğular və təhlillərə imkan verir. İşlənmiş məlumatlar Virtual Maşınlar, Məhkəmə və AI analitikası, ML modelləri ilə inteqrasiya olunur. Bu, XDR-ə xəbərdarlıqları və təhlükəsizliyi avtomatlaşdırmağa imkan verir.

NƏTİCƏ

Bu dissertasiyada müasir İT infrastrukturlarının təhlükəsizliyinin təmin edilməsində çətinlikləri, strategiyaları və irəliləyişləri aydınlaşdırmaq məqsədi daşıyan son nöqtə təhlükəsizliyi, server təhlükəsizliyi, perimetr təhlükəsizliyi, TƏM və DLP-nin kritik sahələri araşdırılmışdır. Ədəbiyyatın geniş nəzərdən keçirilməsi, nümunə araşdırmalarının təhlili və yaranan tendensiyaların nəzərdən keçirilməsi nəticəsində bir neçə əsas nəticə ortaya çıxmışdır:

Son İstifadəçi Kompüteri Təhlükəsizliyi: Son nöqtələrin hər yerdə mövcud olması və onların güzəştə meyilli olması nəzərə alınmaqla, son nöqtə təhlükəsizliyi təşkilatın təhlükəsizlik mövqeyinin təməli kimi xidmət edir. Son nöqtənin aşkarlanması və cavablandırılması (EDR), davranış analitikası və sıfır etibar çərçivələri daxil olmaqla qabaqcıl son nöqtə mühafizə mexanizmləri son nöqtə ilə əlaqəli riskləri effektiv şəkildə azaltmaq üçün vacibdir.

Server Təhlükəsizliyi və Perimetr Müdafiəsi: Serverlərin təhlükəsizliyi və şəbəkə perimetrlərinin gücləndirilməsi kritik aktivlərin və məlumatların xarici təhdidlərdən qorunması üçün çox vacibdir. Güclü server sərtləşdirmə təcrübələri, müntəzəm yamaq idarəetməsi və yeni nəsil təhlükəsizlik divarlarının tətbiqi təşkilatın müdafiəsini gücləndirir, müdaxilənin aşkarlanması sistemləri (IDS) və müdaxilənin qarşısının alınması sistemləri (IPS) kimi perimetr təhlükəsizlik tədbirlərini artırır.

TƏM vasitəsilə əməliyyat səmərəliliyi: Təhlükəsizlik Əməliyyatları Mərkəzinin (TƏM) yaradılması təşkilatın təhlükəsizlik insidentlərini vaxtında aşkar etmək, onlara cavab vermək və onları azaltmaq qabiliyyətini artırır. Qabaqcıl SIEM (Təhlükəsizlik Məlumatı və Hadisələrin İdarə Edilməsi) həllərindən, təhdid kəşfiyyatı lentlərindən və avtomatlaşdırma imkanlarından istifadə TƏM komandalarına yaranan təhdidləri fəal şəkildə müəyyən etmək və zərərsizləşdirmək imkanı verir və bununla da təşkilatın kiber rəqiblərə qarşı dayanıqlığını gücləndirir.

İSTİFADƏ OLUNMUŞ ƏDƏBİYYATLARIN SİYAHISI

An innovative structure of information security equipment for remote control. 5th International conference on Information Engineering for Mechanics and Materials (ICIMM). China, Jul. 25-26, 2015. Book Series: AER-Advances in Engineering Research, volume 21, pp.1002-1006

Aliyev A.G., Shahverdieva R.O., Salimkhanova S.A. Issues of development of the information support system of innovative enterprises based on modern digital platforms. Information Technologies (Информационные технологии), 2023, No.7, vol.29, pp.374-381

Al-Serhani, M., & Chatterjee, S. (2021). Network Segmentation with VMware NSX. Packt Publishing.

Bejtlich, R. (2023). Network Security Monitoring: Detection and Analysis Using Zeek, Wireshark, and More. No Starch Press.

Chen, H., & Liu, Y. (2023). "Evaluating the Effectiveness of Endpoint Security Solutions: A Comparative Study." Journal of Computer Security, 20(2), 145-158.

Chen, L., & Wang, Y. (2022). "The Role of Security Operations Centers (SOCs) in Cyber Threat Intelligence Sharing: A Case Study of Large Enterprises." Journal of Information Security, 11(2), 85-97.

Crowley, Chris., SANS Institute: Common and Best Practices for Security Operations Centers: Results of the2019 SOC Survey (2019). https://www.sans.org/media/analyst-program/common-practices-security-Page 16/18operations-centers-results-2019-soc-survey-39060.pdf

“Data Classification: Algorithms and Applications” by Charu C. Aggarwal

"Data Loss Prevention: The Insider Threat" by Larry J. Whiteside Jr. and Kim-Kwang Raymond Choo

David G. Hill "Data Protection: Governance, Risk Management, and Compliance"

E. Dart, L. Rotman, B. Tierney, M. Hester and J. Zurawski, "The Science DMZ: A network design pattern for data-intensivescience," 2013 SC - International Conference for High Performance

Evan Gilman, Doug Barth "Zero Trust Networks: Building Secure Systems in Untrusted Networks" (2021)

Ələvsət Əliyev. İnformasiya sistemlərinin təhlükəsizliyinə vurulan ziyanların kompleks qiymətləndirilməsi məsələləri. Azərbaycan xalqının ümummilli lideri Heydər Əliyevin 90 illik yubileyinə həsr olunmuş "İnformasiya təhlükəsizliyi problemləri üzrə I respublika elmi-praktiki konfransı", 17-18 may, 2013, səh.71-74.

Ələvsət Əliyev, Roza Şahverdiyeva. İnnovativ struktur və proseslərin idarə olunmasında informasiya təhlükəsizliyi məsələləri. İnformasiya təhlükəsizliyinin multidistiplinar problemləri üzrə II respublika elmi-praktiki konfransı. 14 may 2015, səh.66- 69

"Information Security Management Handbook" edited by Harold F. Tipton and Micki Krause

Hinson, G., & Berlin, D. (2021). Implementing and Managing Information Protection in Microsoft 365. Apress.

Jones, R., & Kim, S. (2019). "Integration of Machine Learning Algorithms in Security Systems: A Review of Recent Advances." IEEE Security & Privacy, 17(3), 29-38.

Joseph M. Adams "FTP Server Security Strategy for DMZ".

Kim, D., & Park, S. (2022). "Enhancing Endpoint Security through Application of Zero Trust Principles: A Case Study Analysis." International Journal of Information Security, 18(3), 201-214.

Li, J., & Zhang, S. (2021). "The Role of Endpoint Detection and Response (EDR) Systems in Strengthening Enterprise Security Posture." Journal of Cybersecurity, 14(4), 321-335.

McMillan, D. (2021). Beyond Cybersecurity: Protecting Your Digital Business. Wiley.

McCarthy, J., & Allan, S. (2022). Cybersecurity Operations Handbook. Wiley.

Nguyen, T., & Tran, A. (2020). "Analyzing the Impact of Insider Threats on Endpoint Security: A Longitudinal Study." Computers & Security, 25(1), 45-58.

Oh, J., & Lee, S. (2019). "A Review of Endpoint Security Solutions and Emerging Trends." International Journal of Network Security, 15(2), 89-102.

Park, C., & Lee, H. (2020). "The Impact of Social Engineering Attacks on Enterprise Security: A Study of Spear Phishing Incidents." International Journal of Information Security, 17(1), 45-56.

Roesch, M. (2020). Intrusion Detection and Prevention with Snort 3.0. Cisco Press.

Roza Şahverdiyeva. Elmi-texnoloji innovasiya parklarının informasiya təhlükəsizliyi problemləri. "İnformasiya təhlükəsizliyinin aktual multidissiplinar elmi-praktiki problemləri" IV respublika konfransı, 14 dekabr 2018-ci il, səh. 199-203.

Smith, J., & Brown, A. (2021). "Compliance with Cybersecurity Standards: A Review of Practices in the Financial Sector." Journal of Cybersecurity, 8(4), 321-335.

Stoneburner, G., Goguen, A., & Feringa, A. (2023). NIST Special Publication 800-53 Revision 5: Security and Privacy Controls for Information Systems and Organizations.

Schneier, B. (2023). Click Here to Kill Everybody: Security and Survival in a Hyper-connected World. W. W. Norton & Company.

Sourabh Shrimali. "DeMilitarized Zone: Network Architecture for Information Security" Internet:

Vural, H., Dahi, B., & Tuncer, S. (2023). "Network Security Measures in Establishing DMZ for Enterprise Systems." International Journal of Computer Applications, 192(3), 7-13.

Горбунов, А. (2020). Защита информации от утечки: современные методы и технологии. Питер.

Е.Г.Горшков. Информационная безопасность управления интеллектуально-промышленными комплексами – технопарками в Российской Федерации. Вестник ОУ. Серия «Экономика», 2007, № 2, с. 127–131. Computing, Networking, Storage and Analysis (SC), Denver, CO, 2013,pp. 1-10.

Жуков, Д. (2023). Профессиональная кибербезопасность: методы защиты сетей, программ и данных. БХВ-Петербург.

С.С.Козунова. Система управления информационной безопасностью предприятия. Евразийский Союз Ученых (ЕСУ), Технические Науки , 2016, №7(28), pp.22-23.

Сидоров, К. (2021). Управление информационной безопасностью организации. Питер.

Лебедев, А. (2022). Разработка и внедрение систем защиты информации. БХВ-Петербург.

Новиков, С. (2021). Сетевая безопасность: полный курс. Питер.

Кучеренко, В. (2020). Кибербезопасность: угрозы и защита информации. Питер.

Красильников, А. (2023). Сегментация сетей: практическое руководство. БХВ-Петербург.