MÜƏSSİSƏ İNFORMASİYA TƏHLÜKƏSİZLİYİ SİYASƏTİ

Şəfiyeva Rəhilə
Rəhimova Nazilə
Azərbaycan Dövlət Neft və Sənaye Universiteti

Xülasə
Təşkilatda müəssisənin informasiya sisteminin tətbiqinin vacib tərəfi biznes prosesləri üçün informasiya sistemi daxilində təhlükəsizliklə bağlı məsələlərin işlənib hazırlanmasıdır. Bu yazıda təşkilatlar daxilində müəssisə informasiya sistemlərinin istifadəsi ilə bağlı təhlükəsizlik siyasətindən bəhs edilir. Məqalədə həm təşkilatlar, həm də istifadəçilər üçün işləyən məlumat təhlükəsizliyi siyasətlərinin niyə, nə üçün və necə yaradılması ilə bağlı məlumat verilmişdir.

Açar sözlər - Müəssisə informasiya sistemləri,informasiya təhlükəsizliyi,təhlükəsizlik siyasəti,informasiya texnologiyaları ,informasiya təhlükəsizliyinin idarə edilməsi.

Giriş

Müəssisə informasiya sistemləri şirkətlərin birdən daha çox iş fəaliyyəti məlumatlarını bir məlumat anbarında ümumiləşdirmək üçün istifadə etdiyi şirkət həcmində İnformasiya Texnologiyaları (İT) sistemləridir. Onlar şirkətə bütün təşkilat dairəsində istifadə edilən məlumatları uyğunlaşdırmağa imkan verir. Həmin sistemlərə təşkilatın insan resursları,maliyyə,logistika,satış və marketinq kimi müxtəlif bölmələrdən məlumatlar əlavə edilə bilər. Son bir neçə onillikdə işlənib hazırlanmış və inkişaf etdirilmiş çoxlu informasiya texnologiyaları, məlumat itkisi olması və ya üst-üstə düşməsi qorxusu yaranmadan indi bütün uyğun məlumatı bir giriş ünvanından əldə edən menecerlər üçün prosesi sadələşdirib.

Bu rahatlığa görə aşkarlanmış problem ümumi şirkət məlumatlarının indi bir yerdə cəmləşməsidir. Təhlükəsizlik pozuntuları (ziyanlı və ya qəsdən) fasiləsizlik axının pozulması, informasiyanın zəif etibarlılığı, proseslərin təsirliliyinin və səmərəliliyinin azalması ilə nəticələnər və hətta hüquqi nəticələrə səbəb ola bilər. Bütövlükdə, firmalar öz işçilərinin kredit kartı məlumatları, insan resursları personalı məlumatları, daxili maliyyə hesabatları və inkişaf planlarından tutmuş bir sıra məlumatı qorumalıdır. Məsələn, 2010-cu ildə ABŞ hökumətinin Ümumi Xidmətlər Administrasiyasının əməkdaşı bilmədən özünün 12.000 əməkdaşının sosial təminat nömrələrini şəxsi e-poçt ünvanına ötürdü ki, bu da dövlət qurumunu işçilərinə oğurluq sığortası və kredit monitorinqini təmin etməyə məcbur etdi [1]. Hazırda üzləşdiyimiz paradiqma dəyişikliyi səbəbindən bu mövzuda daha çox araşdırma vacibdir. Son vaxtlara qədər müəssisənin informasiya sistemlərində təhlükəsizliklə bağlı narahatlıqların çoxu daha çox texniki xarakter daşıyırdı (məsələn, viruslar, qurdlar, troyanlar və s.), lakin daha çox araşdırmalar göstərir ki, insanların sistemlərlə qarşılıqlı əlaqəsi onların əksəriyyətinin əsl səbəbidir.

Bu o deməkdir ki, yaxşı düşünülmüş, başa düşülən və izlənilməsi asan olan müəssisənin informasiya təhlükəsizliyi siyasətinin (İnformation Security Policy-ISP) olması həmişəkindən daha vacibdir. **İnformasiya təhlükəsizliyi siyasəti** Müəssisənin informasiya təhlükəsizliyi siyasəti təşkilatın məlumatlarına, şəbəkələrinə və digər İT resurslarına çıxışı olan insanların kiber riskə məruz qalmasını azaltmaq üçün riayət etməli olduğu qaydalar toplusudur. Kibertəhlükəsizliyə davamlılığın təməli olan ISP-lər ideal şəkildə müəssisə İT ekosisteminin bütün elementlərini,aparat və proqram təminatından tutmuş işçilərə və şirkətin genişləndirilmiş təchizatçı şəbəkəsinə qədər bütün elementləri əhatə edir.

Başqa sözlə, ISP təşkilatın məlumatlarının zədələnməsinə, itməsinə və ya sui-istifadəsinə qarşı ilk müdafiə xəttidir. İnformasiya təhlükəsizliyi siyasətinin əsas məqsədi kibertəhlükəsizliyə ümumi yanaşmanı müəyyən etmək, istifadəçilərə təhlükəsizliklə bağlı aydın və müvafiq təlimat təklif etmək və effektiv,təhlükəsiz informasiya idarəçiliyi üçün məsuliyyət və rolları bölməkdir. İnformasiya təhlükəsizliyi siyasətinin əsas məqsədi qorumaların tətbiq edilməsini və məlumatların əhatə dairəsini

genişləndirməsini yalnız icazəsi olan şəxslərlə məhdudlaşdırmağdır. Təşkilatların ISP yaratması məqsədləri aşağıdakılardır:

- İnformasiya təhlükəsizliyinə ümumi münasibətin yaradılması
- Sənəd təhlükəsizliyinin təmin olunması və istifadəçinin daxil olmasına nəzarət siyasətləri
- Məlumatların, mobil telefonların, şəbəkələrin, kompüterlərin və proqramların zərərli şəkildə faydalanma kimi təhlükəyə məruz qalmış məlumat aktivlərinin təsirini üzə çıxarmaq və sayını azaltmaq
- Təşkilatın etibarlılığını təmin etmək
- Fişinq, zərərli proqram kimi həqiqi və ya qəbul edilən təhlükəsizliklə bağlı şikayət və sorğulara cavab vermək üçün təsirli mexanizmlər təqdim etmək
- Münasib istifadəyə malik olanların vacib informasiya texnologiyalarına çıxışını sonlandırmaq

Bütün inteqrasiya tələblərinə cavab verən təsirli informasiya təhlükəsizliyi siyasətinin məlumat sızması və məlumat əlçatmazlığı kimi təhlükəsizlik hadisələrinin qarşısının alınmasında əsas, vacib prosesdir. İnformasiya təhlükəsizlik siyasəti yenicə yaradılmış müəssisələr üçün əhəmiyyətlidir. Rəqəmsal dönüşümün artması o deməkdir ki, hər bir işçi yeni məlumat yaradır və bu məlumatların müəyyən hissəsi icazəsiz girişdən müdafiə olunmalıdır. Sənayedən asılı olaraq o, hətta müəyyən nizamlar və şərtlərlə qoruna bilər.

İnformasiya təhlükəsizliyinin üç əsas prinsipi. Hər şey güclü korporativ informasiya təhlükəsizliyi modelinin üç prinsipi ilə bağlıdır,yəni, məxfilik, bütövlük və əlçatanlıq. Məxfilik-təşkilatın məlumatı, elektron dinləmə kimi açıqlama hücumlarından qorumaq qabiliyyətinə aiddir. Məxfilik tədbirləri, məsələn, şifrələmə, səlahiyyətli istifadəçilərin xüsusi aktivlərə daxil olmaq üçün lazımi imtiyazlara malik olmasını təmin etmək üçün tətbiq edilir.Eyni zamanda bu tədbirlər sayəsində icazəsiz istifadəçilərin onlara daxil olmasının qarşısı fəal şəkildə alınır. Dürüstlük-məlumatın təqdim edilməsi zamanı və ya sonrasında saxtalaşdırılmamasını təmin etməkdir. Məlumatların bütövlüyü təsadüfən, insan səhvi, səhv məlumat ötürülməsi və ya cihaz nasazlığı,məqsədli şəkildə müdaxilənin aşkarlanmasından yayınmaqla və ya istənməyən girişə icazə vermək üçün fayl konfiqurasiyalarını dəyişdirməklə pozula bilər. Məlumatların bütövlüyünü qorumaq üsullarına şifrələmə həmçinin rəqəmsal sertifikatlar və imzalar daxildir. Əlçatanlıq-təşkilatlardan səlahiyyətli istifadəçilərin heç bir fasilə və ya gözləmə olmadan məlumat əldə etməsinə zəmanət vermək üçün işlək sistemlərə, şəbəkələrə və proqramlara malik olmasını tələb edir. Bu, kiber təhdidlər, insan səhvləri, aparat və proqram təminatının nasazlıqları, təbii fəlakətlər və elektrik enerjisinin kəsilməsi daxil olmaqla, məlumatların əlçatanlığının bütün növlərinə qarşı dayanıqlılıq deməkdir. Qarşı tədbirlər müntəzəm sistem təkmilləşdirmələri və ehtiyat nüsxələrindən tutmuş xidmətdən imtinaya qarşı qorunma həllərinə qədər ola bilər.

Səlahiyyət və girişə nəzarət siyasəti

Girişə nəzarət siyasəti təşkilatın hər pilləsi üçün məlumat və İT sistemləri üzərində icazə dərəcəsini müəyyən etməyə kömək edir. O, həssas məlumatların (şəxsi,sağlamlıq,məxfi,təhsil qeydləri və s. kimi informasiya) necə idarə olunacağını, təhlükəsizlik idarəsinin kimin məsuliyyətində olduğunu, hansı giriş nəzarətinin mövcud olduğunu və hansı təhlükəsizlik normalarının uyğun olduğunu göstərməlidir O, həmçinin şirkət şəbəkələrinə və serverlərinə kimin daxil ola biləcəyini, eləcə də güclü parol tələbləri, biometrik məlumatlar, şəxsiyyət vəsiqələri daxil olmaqla hansı autentifikasiya tələblərinin lazım olduğunu göstərən şəbəkə təhlükəsizliyi siyasətini əhatə edə bilər .Bəzi hallarda əməkdaşlar hər hansı informasiya sistemlərinə və məlumat mərkəzlərinə giriş icazəsi verilməzdən əvvəl müqavilə əsasında informasiya təhlükəsizliyi siyasətinə əməl etməyə borcludurlar.

Məlumatların qruplaşdırılması İnformasiya təhlükəsizliyi siyasəti məlumatları əsas qruplara bölməlidir. Məlumatları mühafizəyə ehtiyacının artma dərəcəsinə görə beş səviyyəyə qruplaşdırmağın yaxşı yolu:

Səviyyə 1. İctimai məlumat.

Səviyyə 2. Təşkilatın məxfi saxlamağı seçdiyi məlumat, lakin,açıqlama maddi ziyana səbəb olmur.
Səviyyə 3. Məlumat izah olunduğda, fərdlərə və ya təşkilata maddi zərər vurma riski var.
Səviyyə 4. Məlumat izah olunduğu təqdirdə şəxslərə və təşkilata ciddi zərər vurma riski çoxdur.
Səviyyə 5. Məlumat izah olunsa, şəxslər və təşkilata ciddi zərər vurulacaq.

Məlumatlar toplusu və əməliyyatlar Verilənlər qruplaşdırıldıqdan sonra hər bir mərhələnin hansı dərəcədə idarə olunacağını təsvir etmək lazımdır. İnformasiya təhlükəsizliyi siyasətinin bu bölməsi üçün əsasən üç element var:

Məlumatların qorunması qaydaları. Şəxsi müəyyən edilə bilən məlumatları və ya həssas məlumatları saxlayan təşkilatlar təşkilati normalara, ən yaxşı praktikaya, sənaye uyğunluq normalarına və şərtlərə uyğun olaraq qorunmalıdır.

1. Verilənlərin ehtiyat çoxalması tələbləri. Verilənlərin necə çoxaldığını, hansı dərəcədə şifrələmənin istifadə edildiyini və hansı üçüncü tərəf dəstək təminat verənlərinin istifadə edildiyini izah edir.
2. Verilənlərin hərəkəti. Verilənlərin necə ötürüldüyünü təsvir edir. Məlumat təsnifatında təsnif edilmiş hesab edilən məlumatlar şifrələmə ilə təhlükəsiz şəkildə ötürülməlidir və ortadakı adam hücumlarının qarşısını almaq üçün ictimai şəbəkələr arasında ötürülməməlidir.

Təhlükəsizlik izah etmə təlimi

İnformasiya təhlükəsizliyi siyasətindən nə lazım olunduğunu anlamaq üçün işçilərə ehtiyac var. İşçilərə məlumatların mühafizə olunması, məlumatların qruplaşdırılması, girişə nəzarət və ümumi təhlükəsizlik təhdidləri daxil olmaqla təhlükəsizlik icazələri barədə məlumat vermək üçün təlim keçirilməlidir.

Təhlükəsizlik təlimi aşağıdakıları əhatə etməlidir:

- Sosial mühəndislik. İşçilərə fişinq və digər bütün sosial mühəndislik kiberhücumları barədə məlumat vermək lazımdır.
- Təmiz masa siyasəti. Noutbukları özünüzlə evə aparmaq və iş günü bitdikdə sənədləri masaların üzərində buraxmamaq lazımdır.
- Uyğun istifadə. İşçilər öz şəxsi iş cihazlarından və internetdən nələrdən faydalanmaq üçün istifadə edə bilərlər və nələr limitlənir?

İşçilərin səlahiyyətləri və vəzifələri

İnformasiya təhlükəsizliyi siyasətində aşağıdakı sahələrin sahibləri olmalıdır:

- Təhlükəsizlik proqramları
- Münasib istifadə qaydaları
- Şəbəkə təhlükəsizliyi
- Fiziki təhlükəsizlik
- Biznesin davamlılığı
- Girişin idarə edilməsi
- Təhlükəsizlik məlumatlılığı
- Risk qiymətləndirmələri
- Məlumat təhlükəsizliyi
- Fəlakətin bərpası
- Hadisələrin idarə edilməsi

İnformasiya təhlükəsizliyinin idarə edilməsi üçün ən yaxşı təcrübələr

Yetkin, son informasiya təhlükəsizliyi siyasəti aşağıdakı siyasətləri əhatə və ya onlara istinad edir:

- Münasib istifadə siyasəti. İşçinin şirkətə məxsus kompüter və ya şəbəkədən istifadə etməyə icazə verməli olduğu məhdudiyyətləri ifadə edir.
- Girişin idarə edilməsi siyasəti. Təşkilatın məlumat və informasiya sistemlərinə giriş məhdudiyyətlərini əhatə edir.
- Dəyişikliklərə nəzarət olunması siyasəti. İT, proqram təminatının yaradılması və təhlükəsizliyinə dəyişikliklərin edilməsi üçün qanuni prosesi təsvir edir.
- İnformasiya təhlükəsizliyi siyasəti. Çoxlu sayda təhlükəsizlik idarə edilməsini əhatə edən üstün səviyyəli siyasət.
- Hadisələrə cavab siyasəti. Təşkilatın hadisəni necə idarə edəcəyi və aradan qaldıracağı barədə təşkil olunmuş yanaşma.
- Uzaqdan daxil olma siyasəti. Daxili şəbəkələrə uzaqdan daxil olmanın münasib üsullarını ifadə edir.
- E-poçt, kommunikasiya siyasəti. İşçilərin e-poçt, boşluq və ya sosial media kimi biznesin seçilmiş elektron kommunikasiya kanalından necə istifadə edə biləcəyini təsvir edir.
- Fəlakətin bərpası siyasəti. Təşkilatın kibertəhlükəsizlik və İT komandalarının ümumi iş davamlılığı planına daxil edilməsidir.
- Biznesin Davamlılığı Planı. Təşkilat üzrə səyləri əlaqələndirir və fəlakət zamanı biznesi işlək vəziyyətə gətirmək üçün istifadə olunur.
- Məlumatların təsnifatı siyasəti. Təşkilatın məlumatlarını necə təsnif etdiyini təsvir edir.
- İT prosesləri və idarəetmə siyasəti. Uyğunluq və təhlükəsizlik normalarına cavab vermək üçün bütün sektorların və İT-nin necə birlikdə işlədiyini ifadə edir.
- Şəxsiyyətə giriş və idarəetmə siyasəti. İT rəhbərlərinin sistemləri və tətbiqləri uyğun işçilərə necə icazə verdiyini və işçilərin təhlükəsizlik qaydalarına uyğun olmaq üçün parolları hansı üsulla yaratdıqlarını ifadə edir.
- Məlumat təhlükəsizliyi siyasəti. Müvafiq qanun və qaydalara uyğun olması üçün məlumat təhlükəsizliyi üçün texniki tələbləri və münasib minimum standartları təsvir edir.
- Fərdi və mobil cihazlar siyasəti. İşçilərə şirkət infrastrukturuna daxil olmaq üçün şəxsi cihazlardan istifadə etməyə icazə verilib-verilmədiyini və işçilərə məxsus aktivlərdən məruz qalma riskini necə azaltmaq mümkün olduğunu təsvir edir.

İnformasiya təhlükəsizliyi siyasətində nə olmalıdır? Quruluş və əhatə dairəsi üzrə məsləhətlər

İnformasiya təhlükəsizliyinə gəldikdə, heç bir iki müəssisənin eyni ehtiyacları və problemləri yoxdur. Bu o deməkdir ki, hər kəsə uyğun vahid informasiya təhlükəsizliyi siyasəti şablonu yoxdur. Lakin demək olar ki,yuxarıda göstərilən əsas elementlərə toxunulur. Həmişə məlumat istər müştəri hüquqlarını, istərsə də şirkətin etik və hüquqi məsuliyyətlər statusunu qorumaq baxımından təhlükəsizliyi siyasətinin məqsədini təsvir etməklə başlanılır. Beləliklə, auditoriya siyasətin məqsədinin nə olduğu və onun nəyi müdafiə etdiyi barədə aydın təsəvvürə malik olacaq.

Təhlükəsizlik məqsədləri çərçivəsində siyasətin qısa, orta və uzunmüddətli perspektivdə gətirmək niyyətində olduğu son nəticə müəyyənləşdirilir. Nəzərə alınmalıdır ki, bu vizyon, eləcə də onu həyata keçirmək üçün istifadə olunan strategiyalar siyasət sənədinə daxil edilməzdən əvvəl şirkət rəhbərliyi tərəfindən razılaşdırılmalıdır. Əks halda,siyasət və informasiya təhlükəsizliyi səylərini mənasız hala gətirmək riski daşınılır. Necə başlayacağınızdan əmin olunmadığı halda məqsədlərin və onların təmin edilməsində istifadəçilərin rol və məsuliyyətlərini izah etmək üçün yuxarıda qeyd etdiyimiz üç əsas prinsipdən informasiya təhlükəsizliyi siyasəti çərçivəsi kimi istifadə edilə bilər. Girişə nəzarət siyasəti təşkilati iyerarxiyalara və tənzimləmə tələblərinə uyğun olaraq, həssas məlumatlara xüsusi diqqət yetirməklə, hansı məlumatların paylaşıla biləcəyi və paylaşıla bilməyəcəyinə kimin qərar verdiyinə müraciət edir. Bu, məlumatların təsnifatına, yəni məlumatın tələb olunan məxfilik və qorunma

səviyyəsinə əsasən təsnifatına gətirir. Bunu etmək üçün müəyyən bir yol yoxdur, lakin dörd səviyyəli ISO 27001 məlumat təsnifatı yaxşı bir başlanğıc nöqtəsi ola bilər. Sonra, hər bir məlumat növünün məlumatların qorunması, ehtiyat nüsxəsi və şifrələməsi və ötürülməsi baxımından necə işlənəcəyi təsvir edilir.

İnformasiya təhlükəsizlik siyasəti yazmaq hekayənin yalnız yarısıdır. Ən çox yayılmış kibertəhlükəsizlik təhdidlərinə, şirkətin təmiz masa prinsiplərinə, İT resurslarından məqbul istifadəyə və təhlükəsizlik pozuntusu zamanı atılacaq addımlara diqqət yetirən məlumatların mühafizəsi protokolları üzrə təlim sessiyaları təşkiledilməlidir.

Sonra, şəbəkə, cihaz və məlumat təhlükəsizliyi, siyasətin həyata keçirilməsi, təhsil, habelə insidentlərin hesabatı və cavab tədbirləri ilə bağlı gündəlik işçilərin vəzifələrini müəyyənləşdirilir.

Nəticə

Son yarım əsr ərzində təşkilatlar öz biznes proseslərini idarə etmək üçün informasiya sistemlərini tətbiq ediblər. Bu informasiya sistemləri indi daha çox müəssisə informasiya sistemləri kimi tanınan sistemlərə çevrilmişdir. Təşkilatda müəssisənin informasiya sisteminin tətbiqinin vacib tərəfi biznes prosesləri üçün informasiya sistemi daxilində təhlükəsizliklə bağlı məsələlərin işlənib hazırlanmasıdır. İnformasiya təhlükəsizlik siyasəti mühüm prosesdir. Budur ki, məlumatların icazəsiz girişdən qorunması, müəssisənin təhlükəsizliyinin təmin edilməsi baxımından təhlükəsizlik siyasəti mükəmməl vasitədir. İnformasiya təhlükəsizliyi siyasəti vasitəsi ilə kibertəhlükəsizliyə ümumi yanaşmanı müəyyən etmək, istifadəçilərə təhlükəsizliklə bağlı aydın və müvafiq təlimat təklif etmək və effektiv,təhlükəsiz informasiya idarəçiliyi üçün məsuliyyət,vəzifə və rolları bölmək mümkündür.

Ədəbiyyat

[1] https://tresorit.com/blog/how-to-create-an-enterprise-information-security-policy-and-make-it-stick-the-2022
[2] https://www.upguard.com/blog/information-security-policy#toc-0
[3] https://blog.rsisecurity.com/what-is-the-purpose-of-an-enterprise-information-security-policy/
[4] https://itsecurity.uiowa.edu/policies-standards-guidelines/compliance/enterprise-information-security-program
[5] https://www.ekransystem.com/en/blog/information-security-policies
[6] https://www.caiso.com/NewEmployeeDocuments/EnterpriseInfoSecurityPolicy.pdf
[7] https://www.coskunoz.com.tr/yonetim-sistemleri/politikalar/bilgi-guvenligi-politikasi.html
[8] https://www.elsisan.com/sites/default/files/page/2021-03/BILGI%20GUVENLIGI%20POLITIKASI.pdf
[9] https://www.domainhizmetleri.com/bilgi-guvenligi-politikasi/
[10] https://www.celebiaviation.com/tr/bilgi-guvenligi-politikasi

ŞƏXSİYYƏT İDARƏÇİLİYİNİN GƏLƏCƏYİ: ÜZ TANIMA SİSTEMLƏRİNİN TƏDQİQİ

Rəhimova Nazilə, Əsgərov Nihad
Azərbaycan Dövlət Neft və Sənaye Universiteti

Xülasə:

Üz tanıma sistemləri təhlükəsizlik, şəxsiyyətin yoxlanılması və fərdiləşdirilmiş xidmətlərin mənzərəsini yenidən formalaşdıran təməlqoyma texnologiyası kimi ortaya çıxdı. Süni intellekt (AI) və maşın öyrənməsi (ML) ilə təchiz edilmiş mürəkkəb alqoritmlərdən istifadə etməklə, bu sistemlər üz xüsusiyyətlərini əlamətdar dəqiqliklə aşkarlaya, təhlil edə və müqayisə edə bilər. Onların tətbiqləri səmərəlilik və istifadəçi rahatlığı üçün innovativ həllər təklif edərək hüquq-mühafizə orqanları,