İnformasiya təhlükəsizliyi və şəxsi həyatın toxunulmazlığı

Rəhbər dövlət qulluqçuları üçün

İKT-nin Əsasları Akademiyası

ESCAP / APCICT

Rəhbər dövlət qulluqçuları üçün İKT-nin Əsasları Akademiyası

İnformasiya Təhlükəsizliyi və Şəxsi Həyatın Toxunulmazlığı

APCICT - İNKİŞAF NAMİNƏ İNFORMASİYA VƏ KOMMUNİKASİYA TEXNOLOGİYALARI ÜZRƏ ASİYA VƏ SAKİT OKEAN TƏLİM MƏRKƏZİ

Rəhbər dövlət qulluqçuları üçün İKT-nin Əsasları Akademiyası

İnformasiya Təhlükəsizliyi və Şəxsi Həyatın Toxunulmazlığı

onun orqanlarının hüquqi statusu və ya onun hüdudlarının və ya sərhədlərinin delimitasiyasına dair hər hansı bir fikrin ifadə olunmasını ehtiva etmir.

Şirkət adlarının və kommersiya məhsullarının göstərilməsi Birləşmiş Millətlər Təşkilatının dəstəyini ehtiva etmir.

Bu hesabatla bağlı yazışmalar apcict@un.org e-poçt ünvanına göndərilməlidir.

Koreya Respublikasında çap olunmuşdur
ST/ESCAP/2934

Cildin tərtibatı: cənab Ho-Din Liqay

Əlaqə:

İnkişaf Naminə İnformasiya və KommunikasiyaTexnologiyaları üzrə

Asiya və Sakit Okean Təlim Mərkəzi

(APCICT/ESCAP)

5-ci mərtəbə G-Tower, 175 İncəsənət mərkəzi, Daero

Yeonsu-gu, İnçxon, Koreya Respublikası

Tel +82 32 458 6650

E-poçt: apcict@un.org

MODULLAR SERİYASI HAQQINDA

Bugünkü “İnformasiya əsrində” informasiyaya asan çıxış yaşayış, işləmə və oyun tərzimizi dəyişir. “Bilik iqtisadiyyatı”, “şəbəkə iqtisadiyyatı” və ya “yeni iqtisadiyyat” kimi də tanınan “rəqəmsal iqtisadiyyat” malların istehsalından ideyaların yaradılmasına keçidlə xarakterizə olunur. Bu, informasiya kommunikasiya texnologiyalarının (İKT) iqtisadiyyatda, xüsusən də, bütövlükdə cəmiyyətdə artan rolunu vurğulayır.

Nəticədə, bütün dünyada hökumətlər İKTİ üçün (informasiya kommunikasiya texnologiyaları və inkişaf) İKT- yə daha çox diqqət yetirirlər. Bu hökumətlər üçün İKTİ təkcə İKT sənayesini və ya iqtisadiyyat sektorunu inkişaf etdirmək deyil, həm də iqtisadi artımı, eləcə də sosial və siyasi inkişafı stimullaşdırmaq üçün İKT-dən istifadəni əhatə edir.

Bununla belə, hökumətlərin İKT siyasətini formalaşdırmaqda üzləşdiyi çətinliklər arasında sürətlə dəyişən texnoloji mənzərə və milli inkişaf naminə İKT-dən istifadə etmək üçün lazım olan səriştələrə bələd olmamaq da var. Çünki insan ona aydın olmayanı tənzimləyə bilməz, bir çox siyasətçilər İKT siyasətindən çəkiniblər. Lakin İKT siyasətini texnoloqların öhdəsinə buraxmaq da yanlışdır, çünki texnoloqlar çox vaxt inkişaf etdirdikləri və istifadə etdikləri texnologiyaların sosial və siyasi təsirlərindən xəbərsiz olurlar.

Rəhbər dövlət qulluqçuları üçün İKT Əsasları Akademiyasının modullarseriyası Asiya və Sakit Okean Hövzəsi Ölkələri üçün İnkişaf naminə İnformasiya və Kommunikasiya Texnologiyaları üzrə Təlim Mərkəzi (APCİCT) tərəfindən aşağıdakı subyektlər üçün hazırlanmışdır:

1. İKT siyasətinin hazırlanmasına cavabdeh olan milli və yerli hökumət səviyyəsində siyasətçilər ;

2. İKT-yə əsaslanan tətbiqlərin işlənib hazırlanması və həyata keçirilməsinə cavabdeh olan hökumət məmurları ;

3. Layihənin idarə edilməsi üçün İKT alətlərindən istifadə etmək istəyən dövlət sektorunda çalışan rəhbər işçilər.

Modullar seriyası həm siyasət, həm də texnologiya nöqteyi-nəzərindən İKTİ ilə bağlı əsas məsələlərlə tanışlığı inkişaf etdirmək məqsədi daşıyır. Məqsəd texniki İKT təlimatını hazırlamaq deyil. Əksinə, onun məqsədi cari rəqəmsal texnologiyanın nəyə qadir olduğunu və texnologiyanın hara yönəldiyini və bunun siyasətin qurulması üçün nə demək olduğunu yaxşı başa düşməkdir. Modulların əhatə etdiyi mövzular təlim ehtiyaclarının təhlili və dünya üzrə digər təlim materiallarının sorğusu vasitəsilə müəyyən edilmişdir.

Modullar elə tərtib edilmişdir ki, hər bir fərd bu materiallardan öz-özünə təhsildə və ya təlim kursu və ya proqramında mənbə kimi istifadə edə bilər. Modullar həm ayrı-ayrılıqda istifadə oluna bilər, həm də onlar bir-biri ilə əlaqəlidir. Hər bir modulda bu seriyaya aid digər modullardakı Modullar arasında mövzulara və müzakirələrə keçid üçün səy göstərilmişdir. Uzunmüddətli məqsəd modulları sertifikatlaşdırıla bilən ardıcıl kursa çevirməkdir.

Hər bir modul, oxucuların öz irəliləyişlərini qiymətləndirə biləcəyi modul məqsədləri və təlimin hədəf seçilən nəticələrinin bəyan edilməsi ilə başlayır. Modulun məzmunu əsas anlayışı dərinləşdirməyə kömək etmək üçün kazusları və çalışmaları əhatə edən bölmələrə bölünür.

Təlimlər fərdi oxucular və ya təlim iştirakçılarından ibarət qruplar tərəfindən keçirilə bilər. Müzakirənin dəqiq aspektlərini göstərmək üçün rəqəmlər və cədvəllər təqdim olunur.

Oxucuların əlavə perspektivlər əldə etmək üçün axtarması üçün istinadlar və onlayn resurslar siyahıya alınmışdır.

İKTİ-nin istifadəsi o qədər müxtəlifdir ki, bəzən modullar daxilində və modullar arasında nümunələr və kazuslar ziddiyyətli görünə bilər. Bu gözləniləndir. Buna səbəb bu intizamın həyəcanı və çağırışı və onun vədidir, çünki ölkələr inkişaf üçün vasitə kimi İKT potensialından istifadə edirlər.

APCICT Virtual Akademiyası (http://e learning.unapcict.org) təlimçilərin təqdimatlarını video formatda və PowerPoint təqdimatlarında əks etdirən virtual sinif otaqlarından ibarət rəhbər dövlət qulluqçuları üçün İKT Əsasları Akademiyasının çap formatında modullar seriyasını dəstəkləyən onlayn distant təhsil platformasıdır.

Təşəkkürnamə

Rəhbər dövlət qulluqçuları üçün İKT Əsasları Akademiyası: İnformasiya Təhlükəsizliyi və Şəxsi Həyatın Toxunulmazlığı modulu Asiya və Sakit Okean Hövzəsi Ölkələri üçün İnkişaf naminə İnformasiya və Kommunikasiya Texnologiyaları üzrə Tədris Mərkəzinin direktoru Kiyounq Ko-nun ümumi rəhbərliyi altında Freddi Tan tərəfindən hazırlanmışdır. Modul Robert De Cesus tərəfindən koordinasiya edilib.

Modul 27-28 noyabr 2019-cu il tarixlərində İnçonda keçirilən Rəqəmsal İnkişaf naminə Potensialın Gücləndirilməsi üzrə Məşvərət Toplantısının iştirakçılarının məzmunla bağlı şərhlərindən faydalanmışdır. Əlavə rəylər və məlumatlar Beynəlxalq Telekommunikasiya İttifaqı (BTİ) və ESKAP-ın İnformasiya və Kommunikasiya Texnologiyaları və Fəlakət Riskinin Azaldılması Bölməsi tərəfindən də təqdim edilmişdir.

Cildin tərtibatı Ho-Din Liqay tərəfindən hazırlanmışdır, tərtibat isə Ancielika Bartolome və Gyubin Hvang tərəfindən hazırlanmışdır. Sişinq Pon və Sara Bennouna isə mətnlərin korrektəsini aparmışlar. Co Eun Çunq və Ho-Din Liqay bu modulun buraxılması üçün lazım olan bütün inzibati prosesləri öz üzərinə götürüblər.

Modulun məqsədləri

Modulun məqsədləri aşağıdakılardan ibarətdir:

1. İnformasiya təhlükəsizliyi, şəxsi həyatın toxunulmazlığı konsepsiyasını və bununla əlaqədar konsepsiyaları aydınlaşdırmaq;
2. İnformasiya təhlükəsizliyinə qarşı yönələn təhdidlərə və onların qarşısının necə alınmalı olmasına dair məlumat vermək;
3. İnformasiya təhlükəsizliyinə dair siyasətin formalaşdırılması və həyata keçirilməsi tələblərini, habelə informasiya təhlükəsizliyi siyasətinin mərhələlərini müzakirə etmək; və
4. Bəzi ölkələr və beynəlxalq informasiya təhlükəsizliyi təşkilatları tərəfindən istifadə olunan informasiya təhlükəsizliyi və şəxsi həyatın toxunulmazlığının qorunması standartlarına nəzər salmaq.

Təlimin nəticələri

Bu modul üzrə işlədikdən sonra oxucular aşağıdakı imkanlara malik olmalıdırlar:

1. İnformasiya təhlükəsizliyi, şəxsi həyatın toxunulmazlığı və əlaqəli konsepsiyaları müəyyənləşdirmək;
2. İnformasiya təhlükəsizliyinə qarşı təhdidləri müəyyənləşdirmək;
3. İnformasiya təhlükəsizliyi və şəxsi həyatın toxunulmazlığının qorunması üzrə beynəlxalq standartlar baxımından mövcud olan informasiya təhlükəsizliyi siyasətini dəyərləndirmək; və
4. Öz kontekstinə uyğun ola biləcək informasiya təhlükəsizliyi siyasəti ilə bağlı tövsiyələri hazırlamaq və ya təqdim etmək.

Mündəricat

1. İNFORMASİYA TƏHLÜKƏSİZLİYİNİN ZƏRURİLİYİ

Bu bölümün məqsədi aşağıdakılardan ibarətdir:

- **İnformasiya və informasiya təhlükəsizliyi konsepsiyasını izah etmək; və**
- **İnformasiya təhlükəsizliyi tədbirlərinə tətbiq edilən standartlar barədə məlumat vermək**

Bu gün insan həyatı informasiya və kommunikasiya texnologiyalarından (İKT) yüksək dərəcədə asılıdır. Bu, fərdləri, təşkilatları və dövlətləri informasiya sistemlərinə hakerlik, kiberterrorçuluq, kibercinayətkarlıq və sairə bu kimi hücumlara qarşı zəif edir. Çox az insan və təşkilat belə hücumlara qarşı silahlıdır. Hökumətlər informasiya-kommunikasiya infrastrukturunu genişləndirməklə informasiya təhlükəsizliyinin təmin olunmasında və informasiya təhlükəsizliyinə təhdidlərə qarşı müdafiə üçün sistemlərin təsis olunmasında mühüm rol oynayırlar.

Bu modulda kiber təhlükəsizliyin bir hissəsi olan informasiya təhlükəsizliyinə diqqət yetirilir. İnternetdə ifadə azadlığı, onlayn məkanda insan hüquqları, onlayn məkanda qadınlara və qızlara qarşı zorakılıq, rəqəmsal sui-istifadə və onlayn məkanda cinsi qısnama, onlayn məkanda nifaq yaradan nitq, kiber zorakılıq və uşaqların onlayn məkanda müdafiəsi təşəbbüsləri ilə bağlı məsələlər bu modulda əks etdirilməyib və onlar internet/onlayn təhlükəsizlik barədə məlumatlılıq üzrə ayrıca modulun bir hissəsini təşkil edə bilərlər.

1.1 İnformasiya təhlükəsizliyinə dair əsas konsepsiyalar

İnformasiya nədir?

Ümumiyyətlə, informasiya əqli fəaliyyətin nəticəsi kimi qəbul olunur; bu, media vasitəsilə ötürülən qeyri-maddi məhsuldur. İKT sahəsində, informasiya məlumatın emalının, onunla davranmanın və onun təşkilinin nəticəsidir ki, bu da sadəcə faktların toplanmasıdır..

İnformasiya Təhlükəsizliyi sahəsində, informasiya “aktiv” kimi təyin olunur; o, dəyəri olan və buna görə də qorunmalı bir şeydir. İSO / İEC 27001:2005-də informasiya və informasiya təhlükəsizliyinin anlayışı bu modul boyu istifadə olunur.

Bu gün informasiyaya verilən dəyər kənd təsərrüfatı cəmiyyətindən sənaye cəmiyyətinə və nəhayət informasiya-yönümlü cəmiyyətə doğru keçidi əks etdirir. Kənd təsərrüfatı cəmiyyətlərində torpaq ən mühüm aktiv olmuşdur və ən böyük taxıl hasilatı olan ölkə rəqabət üstünlüyünə malik olmuşdur. Sənaye cəmiyyətlərində neft ehtiyatlarına sahib olmaq kimi kapital gücü rəqabət qabiliyyətində mühüm faktordur. Bilik və informasiya yönümlü cəmiyyətdə isə, informasiya çox mühüm aktivdir və informasiyanı toplamaq, onu təhlil etmək və ondan istifadə etmək imkanı hər hansı bir ölkə üçün rəqabət üstünlüyüdür.

Perspektiv təmiz aktiv dəyərindən informasiya aktivi dəyərinə keçid aldığından informasiyanın mühafizə edilməsinə dair konsensus artır. İnformasiyanın özü ona malik olan mediadan daha dəyərlidir. 1-ci Cədvəldə informasiya aktivləri maddi aktivlərə qarşı qoyulur.

İnformasiya aktivləri üçün risklər

İnformasiya aktivlərinin dəyəri artdıqca, əhali arasında onlara çıxış imkanı əldə etmək və onlara nəzarət etmək istəyi də artır. Müxtəlif məqsədlərlə informasiya aktivlərindən istifadə etmək üçün qruplar yaradılır və bəziləri hər hansı bir vasitə ilə informasiyanı əldə etmək üçün səylər göstərirlər. Bura icazəsiz giriş (hakerlik), icazəsiz istifadə (piratlıq), kompüter virusları vasitəsilə informasiya sistemlərini dağıtma və sairə aiddir. İnformasiya texnologiyalarının yayılması ilə bağlı belə risklər bu modulun 2-ci bölümündə müzakirə olunur.

İnformasiya yönümlü mühitlərin neqativ aspektlərinə aşağıdakılar aiddir:

Anonimlikdən yaranan qeyri-etik davranışın artması – Anonimliyi saxlamaq üçün İKT-dən istifadə oluna bilər, bu da bəzi fərdlər üçün qeyri-etik və cinayətkar fəaliyyətlə məşğul olmağı, o cümlədən qanunsuz olaraq informasiyanı əldə etməyi asanlaşdırır.

İnformasiyaya sahiblik və ona nəzarətlə bağlı ziddiyyətlər- İnformasiyalaşdırmanın artması ilə informasiyaya sahiblik və ona nəzarətin doğurduğu ziddiyyətlər də artmışdır. Məsələn, hökumətlər e-hökumət çətiri altında özəl informasiyaya dair məlumat bazasını qurmağa çalışdıqları üçün bəzi sektorlar özəl informasiyanın digər tərəflərə açıqlanması səbəbindən şəxsi həyatın toxunulmazlığının pozulmasının mümkünlüyündən narahatlıqlarını bildirmişlər.

Siniflər və ölkələr arasında informasiya və sərvət fərqləri – Saxlanılan informasiya aktivlərinin ölçüsü bilik / informasiya yönümlü cəmiyyətlərdə zənginliyin barometri ola bilər. İnkişaf etmiş ölkələr daha çox informasiya hasil etmək və informasiyanı məhsul kimi satmaqdan gəlir əldə etmək potensialına malikdirlər. Digər bir tərəfdən, informasiya baxımından yoxsul olan ölkələr yalnız informasiyaya çıxış imkanı əldə etmək üçün böyük yatırımlara ehtiyac duyurlar.

Qabaqcıl şəbəkələr səbəbindən informasiyanın təsirinin artması – Bilik / informasiya yönümlü cəmiyyət şəbəkə cəmiyyətidir. Bütün dünya sanki bir şəbəkə vasitəsilə birləşmişdir, bu da o deməkdir ki, şəbəkənin bir hissəsində zəiflik şəbəkənin digər hissəsinə də mənfi təsir göstərə bilər.

İnformasiya təhlükəsizliyi nədir?

İnformasiya təhlükəsizliyi məlumatın məxfiliyinin, bütövlüyünün və əlçatanlığının qorunması kimi tərif edilir. Bu adətən icazəsiz/uyğun olmayan giriş, istifadə, ifşa olunma, pozulma, silinmə/məhv, korrupsiya, modifikasiya, təftiş, qeyd və ya devalvasiya ehtimalının qarşısının alınmasını və ya ən azı azaldılmasını əhatə edir, baxmayaraq ki, bu, həm də insidentlərin mənfi təsirlərinin azaldılmasını əhatə edə bilər. Məlumat istənilən formada ola bilər, məsələn, elektron və ya fiziki, maddi (məsələn, sənədləşmə işləri) və ya qeyri-maddi (məsələn, bilik).

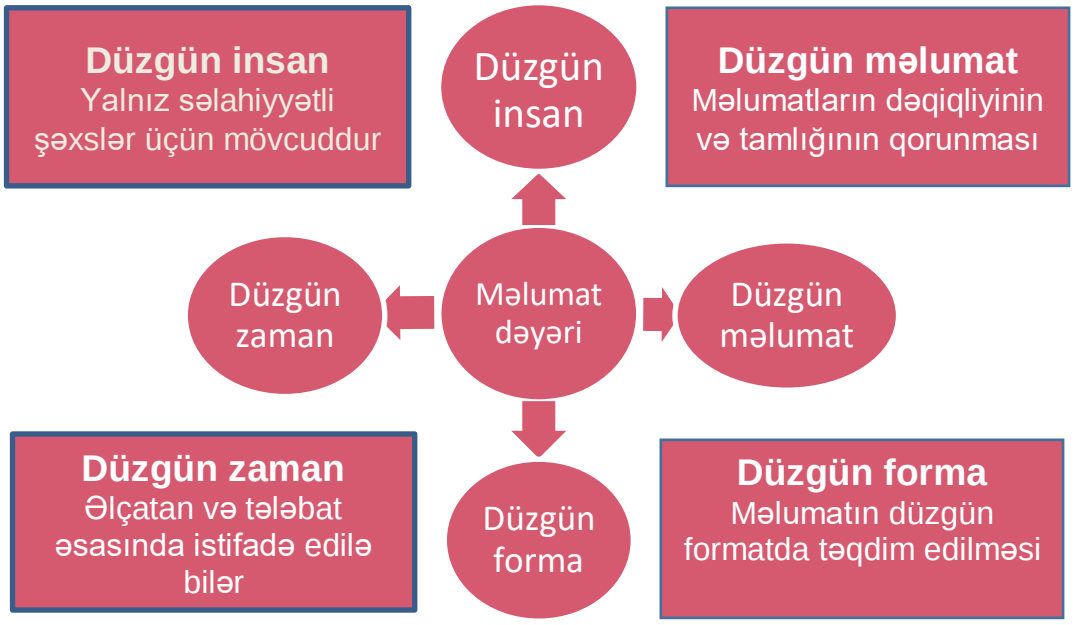
İnformasiya təhlükəsizliyində əsas diqqət, təşkilatın məhsuldarlığına maneçilik törətmədən, səmərəli siyasətin həyata keçirilməsini d diqqətdə saxlamaqla məlumatların məxfiliyinin, bütövlüyünün və əlçatanlığının (CIA – confidentiality, integrity və aviability triadası kimi də tanınır) balanslaşdırılmış şəkildə qorunmasıdır.

Kibertəhlükəsizlik, əksinə, təkcə informasiya təhlükəsizliyini deyil, həm də dəyərli məlumatların mühafizəsindən kənara çıxan SCADA (Supervisory Control and Data Acquisition) Müşahidə Nəzarəti və Məlumatların Alınması sistemləri and Əşyaların İnterneti (Internet of Things - IoT) sistemləri kimi rəqəmsal infrastruktur təhlükəsizliyini də əhatə edir.

İnformasiya təhlükəsizliyində 4R-lər

İnformasiya təhlükəsizliyində 4R-lər düzgün informasiya, düzgün insanlar, düzgün vaxt və düzgün formadır. 4R-lər informasiyanın dəyərini saxlamaq və ona nəzarət etmək üçün ən səmərəli yoldur.

Şəkil 1. İnformasiya təhlükəsizliyində 4R-lər



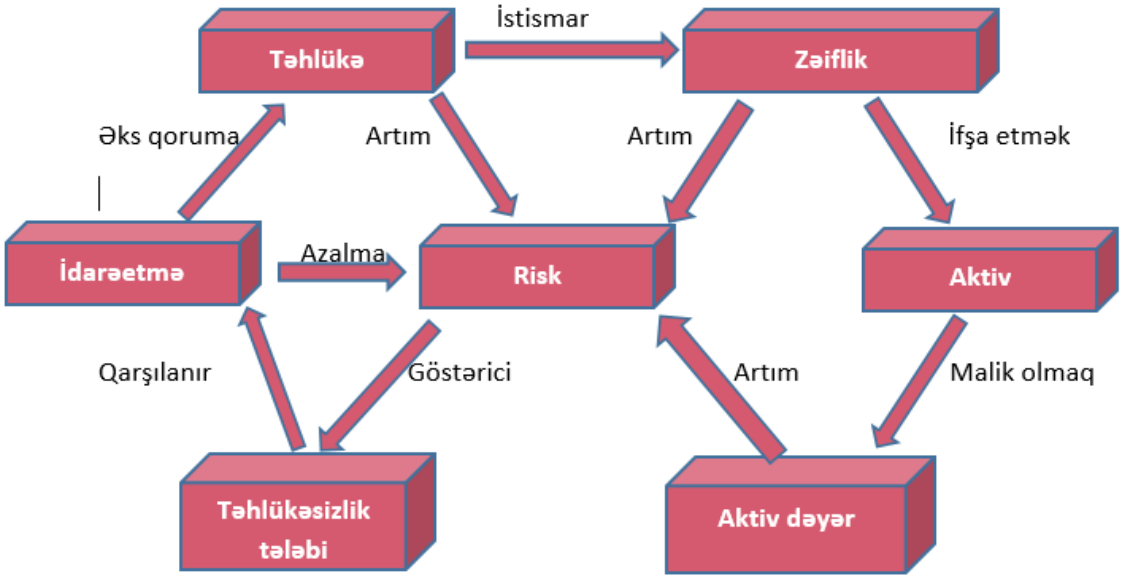
"Düzgün informasiya" dedikdə informasiyanın dəqiqliyi və tamlığı nəzərdə tutulur ki, bu da informasiyanın bütövlüyünə zəmanət verir.

"Düzgün insanlar" dedikdə informasiyanın yalnız səlahiyyətləndirilmiş fərdlər üçün mövcudluğu nəzərdə tutulur ki, bu da məxfiliyə zəmanət verir.

"Düzgün vaxt" dedikdə informasiyanın əlçatanlığı və səlahiyyətləndirilmiş qurumun sorğusu əsasında ondan istifadənin rahatlığı və sadəliyi nəzərdə tutulur. Bu, mövcudluğa zəmanət verir.

"Düzgün forma" dedikdə informasiyanın düzgün formatda təmin olunması nəzərdə tutulur.

İnformasiya təhlükəsizliyini qorumaq üçün 4R-lər lazımi şəkildə tətbiq edilməlidir. Bu, informasiya ilə davranarkən məxfilik, bütövlük və mövcudluq məsələlərinə riayət edilməsi deməkdir.



İnformasiya təhlükəsizliyi, həmçinin, informasiya aktivlərinin dəyərinin, habelə onların zəif tərəflərinin və müvafiq təhlükələrin aydın şəkildə başa düşülməsini tələb edir. Bu, risk idarəetməsi kimi bilinir. 2-ci Şəkildə informasiya aktivləri və risk arasında əlaqə göstərilir.

Risk aktivin dəyəri, təhlükələr və zəif tərəflərlə müəyyən olunur. Düstür belədir: Risk= ∫ (Aktivin dəyəri, təhlükələr və zəif tərəflər)

Risk aktivin dəyəri, təhdidlər və zəifliklərlə birbaşa mütənasibdir. Beləliklə, risk aktivin dəyərinə, təhdidlərə və zəifliklərə təsir göstərməklə artırıla və ya azaldıla bilər. Bu, risk idarəetməsi vasitəsilə edilə bilər.

Risk idarəetmə metodları aşağıdakılardır:

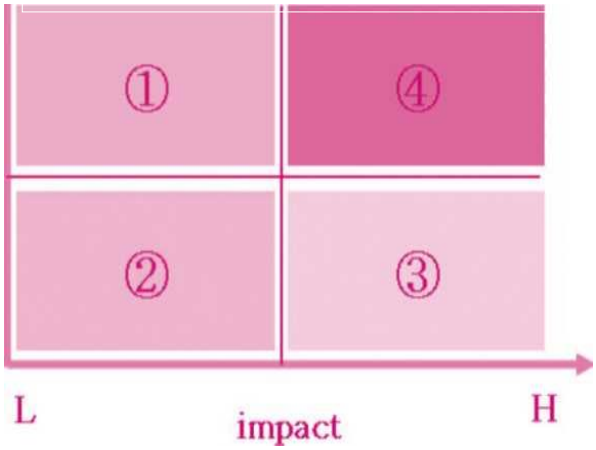
Riskin azaldılması (risk yüngülləşdirmə) - Bu, təhdid / zəiflik riski yüksək olduqda, lakin onların təsiri az olduqda edilir. Burada ilk əvvəl təhlükələrin və zəif tərəflərin nədən ibarət olduğu başa düşülür, onlar dəyişdirilir və ya azaldılır və əks tədbirlər görülür. Lakin, riskin azaldılması rirskin dəyərini "0"-a endirmir.

Riski qəbul etmə - Bu, təhlükə / zəif tərəf ehtimalı az, onların təsiri isə az və ya məqbul olduqda edilir.

Riskin ötürülməsi – Risk həddən artıq yüksək olduqda və ya təşkilat zəruri nəzarət tədbirlərini görmək iqtidarında olmadıqda riks təşkilatdan kənarlaşdırıla bilər. Buna misal kimi sığorta polisinin alınmasını göstərmək olar.

Riskdən qaçma – Əgər həm təhlükələr və zəif tərəflərin olma riski həm də onların təsiri hədsiz yüksəkdirsə, məsələn, məlumatların işlənməsi üçün kənardan avadanlığı və heyəti cəlb etməklə, riskdən qaçmanın ən yaxşı yoludur.

Şəkil 3. Risk idarəetmə metodları



3-cü Şəkildə risk idarəetmənin bu dörd metodu qrafik şəkildə təsvir olunur. Bu şəkildə "1" rəqəmi ilə işarələnmiş kvadrat riskin azaldılması, "2" riskin qəbul edilməsi, "3" riskin ötürülməsi və "4" riskdən qaçmadır.
Müvafiq risk idarəetmə üsulunun seçilməsində əsas məsələ məsrəf baxımından effektivlikdir. Məsrəf baxımından effektivliklə bağlı təhlillər riskin azaldılması, qəbul edilməsi, ötürülməsi və ondan qaçma planı müəyyən edilməmişdən əvvəl aparılmalıdır.

1.2 İnformasiya təhlükəsizliyi tədbirləri üçün standartlar

Vahid inzibati, fiziki və texniki planın mobilizasiyası olmadan informasiya təhlükəsizliyi tədbirlərini effektiv şəkildə həyata keçirmək mümkün deyil.

Bir çox təşkilatlar informasiya təhlükəsizliyi tədbirləri üçün standartlar tövsiyə etmişlər. Buna misal olaraq Beynəlxalq Standartlaşdırma Təşkilatı və Beynəlxalq Elektrotexnika Komissiyası (ISO/IEC), Beynəlxalq Telekommunikasiya İttifaqı (İTU-U), İnformasiya Sistemlərinin Auditi və Onlara Nəzarət Assosiasiyasının (İSACA) İnformasiya Sistemləri üzrə İxtisaslı Auditorunun (CISA) və Beynəlxalq İnformasiya Sisteminin Təhlükəsizlik Sertifikatlaşdırılması Konsorsiumunun İnformasiya Sistemlərinin Təhlükəsizliyi üzrə İxtisaslı Mütəxəssisin (CİSSP) informasiya təhlükəsizliyi tələblərini və qiymətləndirmə bəndlərini göstərmək olar. Bu standartlar informasiya təhlükəsizliyi siyasətinin işlənib hazırlanması, informasiya təhlükəsizliyi təşkilatının qurulması və fəaliyyət göstərməsi, insan resurslarının idarə olunması, fiziki təhlükəsizliyin idarə olunması, texniki təhlükəsizliyin idarə olunması, təhlükəsizlik auditi və işin davamlılığına nəzarət kimi vahid informasiya təhlükəsizlik tədbirlərinin həyata keçirilməsini tövsiyə edir.

2-ci cədvəldə informasiya təhlükəsizliyi domenləri ilə bağlı standartlar sadalanır.

Cədvəl 2. İnformasiya təhlükəsizliyi domenləri və müvafiq standartlar və sertifikatlar

9	**ISO/IEC 27001**	**CISA**	**CISSP**
İnzibati	İnformasiya təhlükəsizliyi siyasəti	İT üzrə Nəzarət və idarəçilik	Təhlükəsizlik sisteminin quruluşu və texnikası
	İnformasiya təhlükəsizliyi təşkilatı		
	Aktivlərin idarə olunması	İnformasiya aktivlərinin qorunması	Təhlükəsizlik və risk idarəçiliyi
	İnsan resurslarının təhlükəsizliyi		
	İnformasiya təhlükəsizliyi ilə hadisələrə nəzarət		
	İşin davamlılığının informasiya təhlükəsizliyi aspektləri		
	Təchizatçı ilə əlaqələr Uyğunluq	İnformasiya sistemləri (İS) üzrə prosesi	Təhlükəsizliyin qiymətləndirilməsi və sınaqdan keçirmə
Fiziki	Fiziki və mühit təhlükəsizliyi		Aktivlərin təhlükəsizliyi
Texniki	Kriptoqrafiya Kommunikasiyanın təhlükəsizliyi Əməliyyatların təhlükəsizliyi		Təhlükəsizliklə bağlı əməliyyatlar Kommunikasiya və şəbəkə təhlükəsizliyi
	Daxil olmaya nəzarət		Şəxsiyyətin təsdiqi və girişin idarə edilməsi
	Sistemlərin əldə olunması, inkişaf etdirilməsi və onlara xidmət	İnformasiya sistemlərinin olunması, inkişaf etdirilməsi və tətbiqi	Proqram təminatının hazırlanması Təhlükəsizlik

ISO/IEC27001 diqqəti inzibati təhlükəsizliyə yönəldir. Xüsusilə, o, inzibati tədbir kimi sənəd və əməliyyatların auditi və siyasətə / rəhbər qaydalara və qanunvericiliyə riayət etmə vurğulanır. İnzibatçı tərəfindən davamlı təsdiqetmə və əks tədbirlər tələb olunur. Beləliklə, ISO/IEC27001 təhlükəsizlik sistemləri, avadanlığın zəif məqamlarını və digər məsələləri inzibati yolla həll etməyə səy göstərir.

Bundan fərqli olaraq, diqqəti audit tədbirlərinə və informasiya sistemləri üzərində nəzarətə yönəldən CİSA-da insan resursları və ya fiziki təhlükəsizlik haqqında heç nə deyilmir. Müvafiq olaraq, auditorların rolu və audit prosesinin

həyata keçirilməsi çox vacib hesab edilir.

CISSP[3] diqqəti texniki təhlükəsizliyə yönəldir. O, proqram təminatının hazırlanması, şəxsiyyət və girişin idarə olunması, kommunikasiya və şəbəkə təhlükəsizliyi və əməliyyatların təhlükəsizliyini vurğulayır.

Çalışma

1. Təşkilatınızdakı heyət üzvləri arasında informasiya təhlükəsizliyinə dair məlumatlılıq səviyyəsini dəyərləndirin.

2. Təşkilatınız informasiya təhlükəsizliyi ilə bağlı hansı tədbirləri həyata keçirir? İnformasiya təhlükəsizliyinin dörd metodu baxımından bu tədbirləri qruplaşdırın.

3. Təşkilatınız çərçivəsində və ya sizin ölkədə və ya yurisdiksiya altında digər təşkilatlarda inzibati, fiziki və texniki domenlərdə informasiya təhlükəsizliyi tədbirlərinə dair misallar gətirin.

4. Təlim iştirakçıları bu çalışmanı kiçik qruplarda edə bilərlər. Əgər iştirakçılar müxtəlif ölkələrdəndirsə, kiçik qruplar ölkələr üzrə ola bilər.

Özünü sına

1. İnformasiya digər aktivlərdən necə fərqlənir?
2. Nə üçün informasiya təhlükəsizliyi siyasətçilər üçün maraq kəsb edir?
3. İnformasiya təhlükəsizliyini təmin etməyin yolları hansılardır? İnformasiya təhlükəsizliyinin təmin olunmasının müxtəlif metodlarını bir-birindən fərqləndirin.
4. Üç informasiya təhlükəsizliyi domeninin (inzibati, fiziki və texniki) hər birini fərqləndirin.

2. İNFORMASİYA TƏHLÜKƏSİZLİYİNİN MEYLLƏRİ VƏ İSTİQAMƏTLƏRİ

Bu bölümün məqsədi aşağıdakılardan ibarətdir:

- **İnformasiya təhlükəsizliyinə təhdidlərin ümumi icmalını vermək və**
- **Belə təhdidlərə qarşı əks tədbirləri təsvir etmək**

2.1 Kiber təhlükələrin növləri

Xarici təhdidlər

Xarici təhdidlər qeyri-işçilər tərəfindən həyata keçirilən hücumlardır və bu hücumlar adətən təşkilatın ofisindən kənarda həyata keçirilir. Belə təhdidlərə hakerlik, xidmətdən imtina və zərərli proqram təminatı nümunə ola bilər.

Daxili təhdidlər

Daxili təhdidlər təşkilatın sistemlərinə, şəbəkələrinə və tətbiqlərinə fiziki girişi olan işçilər və ya podratçılar tərəfindən həyata keçirilən hücumlardır. Bu cür hücumlar adətən narazı işçilər/podratçılar tərəfindən həyata keçirilir. Daxili hücumlar sosial mühəndislikdən istifadə edən işçilər/podratçılar tərəfindən və təhlükəsizlik tədbirlərindən daha az xəbərdar olan işçilər tərəfindən də bilmədən edilə bilər.

2.2 Xarici təhlükələrin növləri

Hakerlik

Hakerlik qanuni icazə olmadan informasiyanı əldə etmək və ya dəyişdirmək üçün kompyuterə və ya kompüter şəbəkəsinə daxil olmaqdır.

Hücumun məqsədindən asılı olaraq, hakerlik əyləncə, cinayət və ya siyasi xarakterli hakerlik kimi təsnif oluna bilər. Əyləncə xarakterli hakerlik sadəcə hakerin öz marağını təmin etməsi üçün proqramları və məlumatları icazəsiz dəyişdirməsidir. Cinayət xarakterli hakerlikdən dələduzluq və casusluqda istifadə olunur. Siyasi xarakterli hakerlik icazəsiz siyasi bildirişləri yaymaq üçün vebsaytlara müdaxilə etməkdir.[1]

Son vaxtlarda hakerlik milli təhlükəsizliyə böyük təhlükə yaratmaqla, kiber terror və kiber müharibə ilə daha çox əlaqələndirilmişdir. Digər bir yeni meyl olaraq milli maraq kəsb edən və yüksək həssas informasiyanın olduğu iri saytları hədəf seçmiş haker qrupları müşahidə olunur.

Çərçivə 1. Cinayət və əyləncə xarakterli hakerliyin bəzi nümunələri

"JPMorgan Chase Bank"ına haker hücumu oldu. 2014-cü ildə 80 milyondan çox istifadəçi hesabı hakerlər tərəfindən ifşa edildi.

Rusiyalı haker qrupu Amerika Birləşmiş Ştatlarının ən böyük banklarından birinə hücum edib. Onlar 76 milyon şəxsi hesabı və 7 milyon kiçik biznes hesabını sındıra biliblər. Onlar "JPMorgan Chase"in bütün 90 server kompyuterinə sızıb və hesab sahiblərinin bütün şəxsi məlumatlarına baxa biliblər.

Hakerlər adlar, telefon nömrələri, e-poçt ünvanları və ev ünvanları kimi əsas məlumatları oğurlayıblar.

Xidmətdən-imtina və paylanmış xidmətdən-imtina növündə hücum

Xidmətdən-imtina (Denial-of-Service- DoS), sistemin lazımi şəkildə cavab verməsini çətinləşdirərək və dayandıraraq, digər proseslər, resurslar və ya tədbirlərlə nəticələnməklə, kompyuter və ya şəbəkədə olan avadanlığın işinin fərqli istiqamətə yönləndirilməsinə səbəb olur. Paylanmış xidmətdən-imtina (Distributed Denial-of-Service-DDoS) hücumlarında isə bu əməl müxtəlif yerlərdən çoxsaylı qurğulardan istifadə olunmaqla edilir.

Hədəfləri cavab vermək imkanından məhrum etməklə nəticələnən bu xüsusi hücum və ya zəiflikdən yararlanma səciyyəvi olaraq DDoS və Dos hücumları üçün eynidir. DDoS hücumlarında iştirak edən paylanmış mənbələrin olması çox vaxtı ona qarşı mübarizəni çətinləşdirir və daha iri və sürətli cavab verən hədəflərə qarşı daha uğurlu olur.[2]

Kazus 1: DDoS hücumundan əziyyət çəkən qlobal vebsaytlar

E-poçt spam

Spam e-poçt kimi informasiya kommunikasiya xidməti vasitəsilə çatdırılan kütləvi, istənməyən, ticari elektron mesajdır. Spam reklam üçün ucuz və effektiv vasitədir. Son dövrlərdə spam zərərli kodu yaymaq və ya şəxsi məlumatları ələ keçirmək üçün istifadə olunur. Bəzən bu tip spamlar əksər hallarda zərərli kodlarla yoluxmuş zombi kompyuterlərdən göndərilir.

2016-cı ilin oktyabr ayında kibercinayətkarlar böyük DDoS hücumlarına başladılar və Twitter, Netflix, PayPal, Pinterest və PlayStation Network daxil olmaqla bir sıra vebsaytları sıradan çıxardılar.

Hücum bir dəfə 1 Tbps-yə yaxın olmaqla öz ölçüsünə görə təəccüb doğurur. Bu hücumun arxasında dayanan qrup bunu IoT qurğularının iyirmi min son nöqtəsini ələ keçirməklə, onları botnetə çevirməklə və əsasən də axını DNS-ə malik Dyn provayderinə yönəltməklə bunu edib.

Mənbə (dəyişikliklə): https://www.welivesecurity.com/2016/12/30/biggest-security-incidents-2016/

Kazus 2: Dünyanın ən böyük spam e-poçt mənbəyinin bağlanması

Virusa yoluxmuş kompyuterlərin beynəlxalq şəbəkəsi olan Rustock botneti illərdir, lisenziyasız onlayn aptekləri və aşağı qiymətli iktidarsızlıq dərmanlarını təbliğ edərək, hər gün milyardlarla e-poçt alıb.

2011-ci ilin martında Microsoft şirkəti məhkəmə qərarı əsasında fəaliyyət göstərən ABŞ marşalları tərəfindən dəstəklənərək təxminən bir milyon Windows kompyuterinə gizli nəzarət etdiyi təxmin edilən serverləri ələ keçirdi.

Serverlər görünüşə görə Orta Qərbdəki Rustockdakı rollarından xəbərsiz olan kommersiya məqsədli internet hostinq firmalarından icarəyə götürülmüşdü. Bu "əmr və idarəetmə" serverləri bütün dünyada yoluxmuş ev və iş kompüterlərinə təlimatlar verəcəkdi.

Mənbə (dəyişikliklə): https://www.telegraph.co.uk/technology/news/8391532/Worlds-biggest-source-of spam-email-shut-down.html.

Fişinq

Fişinq etibarlı qurumdan istifadə etməklə istifadəçi adları, parollar və kredit kartı detalları kimi şəxsi məlumatları əldə etmək üçün e-poçt və ya mesajların istifadəsidir. Bu, adətən e-poçt spufinqi və ya ani mesajlaşma yolu ilə həyata keçirilir və o, tez-tez istifadəçiləri qanuni saytın görünüşünə və izləniminə uyğun gələn saxta veb-saytda şəxsi məlumatları daxil etməyə yönəldir.

Kazus 3: Birləşmiş Krallığın ən böyük kiber dələduzluğu

Birləşmiş Krallıqda paytaxt polisinin dələduzluqla mübarizə bölməsi hesab edir ki, 14 ölkədəki bank müştərilərinin hesablarına daxil olmaq üçün mürəkkəb fişinq dələduzluqları törətməkdə günahlandırılan üç nəfərin saxlanılması ilə Böyük Britaniyada 59 milyon funt sterlinq dəyərində dələduzluğun qarşısı alınıb.
Bank saytlarını təqlid edən 2600-ə yaxın fişinq səhifəsi Met polis mərkəzi e-cinayət bölməsi (Met Police Central E-Crime Unit- PCeU), Ağır Mütəşəkkil Cinayətlər Agentliyi və ABŞ-ın məxfi xidməti tərəfindən təhlil edilib.

Dələduzluqların arxasında dayanan adamlar Böyük Britaniyada aşkar edilib və onlar Londonda dəbdəbəli mehmanxanalarda qaldıqları vaxt öz dələduzluq əməllərini davam etdirirdilər.

Daha sonra məmurlar 12500-ü Birləşmiş Krallıqda olan 30000 bank müştərisinin məlumatlarını və fişinq dələduzluqlarında istifadə edilmək üçün 70 milyon müştərinin e-poçt ünvanını ehtiva edən serverləri aşkar ediblər.

Həmin şəxslər 2016-cı ildə ümumilikdə 20 il müddətinə azadlıqdan məhrum ediliblər. İstintaqı aparan zabit Di Ceson Tun, istintaq zamanı bildirib ki, "bu, PCeU-nun bu günə qədər məşğul olduğu ən böyük hadisədir və böyük ehtimalla, Böyük Britaniyada indiyə qədər olan ən böyük kiber fişinq işidir".

Bu, Birləşmiş Krallıqda ən böyük kiber dələduzluq idi. Dələduzluq əməllərinin ən yüksək nöqtəsində həftədə 2 milyon funt-sterlinqə qədər gəlir əldə edilirdi.

Mənbə (dəyişiklik ilə): Böyük Britaniyanın ən böyük kiber dələduzları özlərini BANK işçiləri kimi qələmə verməklə qurbanlarına zəng edərək 113 milyon funt sterlinq oğurlayıblar: Dələduzluqda ittiham olunanlar alış-veriş yarmarkaları üçün nağd pulla dolu zibil çantalarından istifadə edib,dəbdəbəli avtomobillər və Lahorda malikanə alıblar.https://www.dailymail.co.uk/news/article-3792417/Fraud-ring-boss-gang-stole-113million-UK-firms.html

İstifadəçi mandatından istifadə

İstifadəçi mandatından istifadə, adətən istifadəçi adlarının və/və ya e-poçt ünvanlarının siyahılarından və müvafiq parollardan (çox vaxt üçüncü tərəf serverində məlumatların pozulması nəticəsində) ibarət olan oğurlanmış hesab mandatından böyük hesablar vasitəsilə istifadəçi hesablarına icazəsiz giriş əldə etmək üçün istifadə edildiyi kiberhücum növüdür və veb tətbiqinə qarşı yönəlmiş geniş miqyaslı avtomatlaşdırılmış giriş sorğuları vasitəsilə istifadəçi hesablarına icazəsiz giriş əldə etmək üçün istifadə olunur. İstifadəçi mandatından istifadə hücumları

mümkündür, çünki bir çox istifadəçi eyni istifadəçi adı/parol kombinasiyasını bir neçə saytda təkrar istifadə edir. Bir sorğu istifadəçilərin 81 faizinin iki və ya daha çox saytda eyni paroldan təkrar istifadə etdiyini və istifadəçilərin 25 faizinin eyni parolu bir neçə saytda istifadə etdiyini bildirir.

Kazus 4: Amerika Birləşmiş Ştatlarının Dövlət Təsərrüfatı hesablarının istifadəçi mandatına hücumla ələ keçirilməsi

2019-cu ilin avqust ayında Amerika Birləşmiş Ştatlarının sığorta şirkəti "State Farm" istifadəçi mandatına hücum zamanı təcavüzkar tərəfindən onlayn hesaba giriş məlumatları ələ keçirilən istifadəçilərə e-poçt bildirişləri göndərdi. Təcavüzkar digər təşkilatların məlumatlarının pozulması nəticəsində sızan istifadəçi adları və parolları tərtib edib və onlardan Dövlət Təsərrüfatında hesablara giriş əldə etmək üçün istifadə edib. Dövlət Təsərrüfatı həmçinin giriş mandatları təcavüzkar tərəfindən ələ keçirilən hesablar üçün parolları sıfırlamışdı.

Zərərli kod

Zərərli kod dedikdə icra olunduqda sistemə ziyan vuran proqramlar nəzərdə tutulur. Viruslar, zərərvericilər (soxulcanlar) və Troyan atları zərərverici kodun növləridir.
Kompüter **virusu**, digər proqrama, kompyuterin yükləmə sektoruna və ya sənədə köçürülməklə çoxalaraq kompyuter sistemlərinə və məlumata zərər verən proqram və ya proqramlaşdırma kodlarıdır.
Zərərverici (soxulcan) faylları dəyişdirməyən, lakin avtomatik və istifadəçinin görə bilmədiyi əməliyyat sisteminin hissələrindən istifadə edərək aktiv yaddaşda qalır. Onların nəzarətsiz şəkildə çoxalması sistemin resurslarını tələf edərək digər funksiyaları ləngidir və ya azaldır. Bu, adətən, zərərvericilərin (soxulcanların) mövcudluğu aşkar edildikdə baş verir.

Troyan atı faydalı və / və ya zərərsiz görünən, lakin həqiqətdə gizli proqramları və ya komanda skriptlərini yoxa çıxarmaqla sistemi müdaxilələrə qarşı zəifləşdirmə kimi zərərli funksiyaya malik olan proqramdır.

Kazus 5. İran İslam Respublikası: Stuxnet “soxulcanı” kibermüharibənin yeni mərhələsindən xəbər verir

“Stuxnet” soxulcanı Belarusun təhlükəsizlik şirkəti tərəfindən 2010-cu ilin iyun ayında İran İslam Respublikasındakı kompyuterlərdə aşkar edilib. Bu soxulcan, əksəriyyəti İranda olmaqla, dünyada 100,000-dən çox kompyuter sistemini yoluxdurmuşdur.

“Los Angeles Times” məlumat verir: “Stuxnet” nə vaxtsa buraxılan ən mürəkkəb kiber silah adlandırılır, buna səbəb isə onun İranın nüvə proqramında istifadə olunan məxfi şəkildə hədəf seçildiyi deyilən xüsusi avadanlığa gizlicə yaxınlaşma yoludur”.

Hədəf seçilmiş kod Siemens Simatic WinCC SCADA sistemlərinə hücum etmək üçün nəzərdə tutulub. Siemens sistemi boru kəmərlərini, nüvə zavodlarını və müxtəlif xidmət və istehsal avadanlıqlarını idarə etmək üçün fərqli

qurğularda istifadə olunur. “Stuxnet” bir çox sistemlərə təsir göstərsə də, bir çoxları belə bir məlumat yaymışlar ki, bu soxulcan məhz İranın nücə sənayesini hədəf seçmək üçün yaradılmışdır.

“Ransomware” faydalı və/yaxud zərərsiz görünən, lakin fidyə ödənilmədikdə, qurbanın məlumatlarını dərc etməklə və ya ona həmişəlik girişi bloklamaqla hədələmək kimi zərərli funksiyaya malik proqramdır.

Kazus 6: WannaCry kiberhücumları nəticəsində 19.000 görüş ləğv edildiyi üçün, bu, 92 milyon funt-sterlinqə başa gəldi.

Fidyə ödənişi tələb edən hakerlərin mesajları ilə dünyada yüz minlərlə kompyuteri bağlayan WannaCry haker hücumu milli səhiyyə müəssisələrinin üçdə birinə və sahə həkimlərinin 8 faizinə zərər vurdu. Bir həftə ərzində bütün Milli Səhiyyə Xidmətinin fəaliyyətinin 1%-i pozuldu.

Haker hücumu 19.000-dən çox görüşün ləğv edilməsinə səbəb oldu, 12 may və 19 may tarixləri arasında Milli Səhiyyə Xidmətinə 20 milyon funt-sterlinqə və sonrakı təmizləmə və İT sistemlərində aparılan təkmilləşdirmələrə 72 milyon funt-sterlinqə başa gəldi.

Kiberhücum 200.000 kompyuterin Bitkoin kriptovalyutasını tələb edən qırmızı hərfli xəta mesajları ilə istifadəçilər üçün bloklanmasına səbəb oldu. Hücumda bir il davam edən araşdırmadan sonra Şimali Koreyanın elit hakerləri günahlandırıldı.

Müasir davamlı təhdid

Müasir davamlı təhdid (APT) icazəsi olmayan şəxsin şəbəkəyə daxil olmaq üçün çıxış imkanı əldə etdiyi və orada uzun müddət aşkar olunmadan qaldığı şəbəkə hücumudur. APT hücumunun məqsədi şəbəkəyə və ya təşkilata ziyan vurmaqdan daha çox məlumatı oğurlamaqdır.[3]APT hücumları, milli müdafiə, istehsal və maliyyə sahəsi kimi yüksək dəyərli informasiyanın olduğu sektordakı təşkilatları hədəf seçir.

APT üsulu ilə hücum edən şəxs çox vaxtı, qanuni vasitələrlə şəbəkəyə daxil olmaq üçün sosial mühəndisliyin bir növü olan “nizə fişinqdən” istifadə edir. Bir dəfə daxil olduqdan sonra hücum edən şəxs “arxa qapı” yaradır.

Növbəti addım etibarlı istifadəçilərə dair məlumat toplayaraq (xüsusən də inzibati) və şəbəkə boyu yanaki hərəkət edərək daha çox arxa qapı quraşdırmaqdır. Arxa qapılar hücum edən şəxsə saxta xidmətlər quraşdırmaq və açıq nəzərdə gizli qalan zərərverici proqramları yaymaq üçün “xəyali infrastruktur” yaradır.

Kazus 7: RSA-nın müasir davamlı təhlükəli hücumlara məruz qalması

2011-ci ilin mart ayında EMC-nin təhlükəsizlik bölümü RSA bəyan etmişdir ki, o, hücumun hədəfinə çevrilib və RSA-nın SecurID iki-faktorlu autentifikasiya məhsulları ilə bağlı məlumatlar hücum edənlər tərəfindən oğurlanıb.

Araşdırmalar onu göstərib ki, hücum APT kateqoriyasında olub. APT təhdidləri bütün iri korporasiyalar üçün ciddi məsələyə çevrilir. APT-ləri müəyyənləşdirmək üçün təşkilatlar tək davranışın təhlil edilməsi yolu ilə bütün mümkün

[3] SearchSecurity.com, "qabaqcıl davamlı təhdid (APT)", http://searchsecurity.techtarget.com/definition/advanced-persistent-threat-APT.

təhlükələri müəyyənləşdirmək deyil, eyni zamanda virtual mühitdə bütün şübhəli elementləri sınaqdan keçirmək imkanına malik olan texnologiyaları tətbiq etməlidirlər.

İki-faktorlu autentifikasiya tək istifadəçi adı və məxfi sözlə (parol) təmin olunandan daha güclü təhlükəsizliyi təmin etmənin üstünlük verilən metodudur. İki-faktorlu autentifikasiyanın ən geniş yayılmış metodlarından biri autentifikasiya və sayta və ya tətbiqə giriş imkanı əldə etmək üçün istifadəçi adı və məxfi sözdən (paroldan) əlavə istifadəçinin daxil etməli olduğu təsadüfi kodu təmin edən açar asılqan və ya tokendən istifadədir.

RSA iki-faktorlu autentifikasiya həllərinin aparıcı təminatçısıdır və onun açar asılqanları və tokenləri virtual olaraq hər yerdə istifadə olunur. Əlavə təhlükəsizliyi təmin etmək və hesabları icazəsiz girişlərdən qorumaq üçün RSA-ya güvənən milyonlarla müştərinin olduğu bir zamanda indi zərərverici hakerlərin bu qorumanı sındırmaq üçün açarlara malik olması narahatlıq doğurur.

RSA öz müştərilərini əmin edir ki, çıxarılan məlumatlar onların RSA SecurID müştərilərindən hər hansı birinə qarşı uğurlu birbaşa hücum etmək imkanını verməmişdir. Lakin, bu, daha geniş bir hücumun bir hissəsi kimi hazırki iki-faktorlu autentifikasiyanın həyata keçirilməsinin effektivliyini azaltmaq üçün istifadə edilə bilər. RSA-nın müştərisi Lockheed-Martinə qarşı haker hücumu olmuşdur və belə deyilir ki, bu, eyni haker tərəfindən edilmişdir (yuxarıdakı kazusa baxın).

Mənbələr (dəyişikliklə): Toni Bredli “RSA SecurID haker hücumu APT-lərin təhlükəsini göstərir”, *PCWorld,* 19 Mach 2011, http://www.pcworld.com/ businesscenter/article/222555/rsa_securid_hack_shows_danger_of_apts.html; and Warwick Ashford, “RSA hit by advanced persistent threat attacks”, *Computer Weekly,* 18 March 2011, http://www.computerweekly.com/Articles/2011/ 03/18/245974/ RSA-hit-by-advanced-persistent-threatattacks.htm

2.3 Daxili hücumların növləri

Narazı işçilər/podratçılar

Daxili hücumlar məlumat və sistemlərimizin üzləşdiyi ən böyük təhlükələrdən biridir. Şəbəkələr, məlumat mərkəzləri və admin hesabları haqqında biliyi və onlara çıxışı olan qeyri-qanuni işçilər, xüsusən İT komandasının üzvləri təşkilat şəbəkəsinə, sistemlərinə və məlumatlarına ciddi ziyan vura bilər.

İşçilərin təhlükəsizlikdən bixəbər olması

İşçilər üçün təhlükəsizliyə dair maarifləndirmə təlimi potensial kiber pozuntulara səbəb ola biləcək riskli davranışların aradan qaldırılmasına kömək edir. Təlim proqramları təşkilatın üzləşdiyi bəzi təhdidləri, xüsusən də telefon, mətnli mesaj və ya sosial media kanalları vasitəsilə fişinq e-poçtları, məlumatları açıqlamama müqabilində fidyə tələb etmə və sosial mühəndislik dələduzluqları kimi hücumları həll edə bilər.

Sosial mühəndislik

“Sosial mühəndislik” termini məxfi məlumatı yaymaq üçün insanları manipulyasiya etmək üçün istifadə olunan texnikalar toplusuna aiddir. Bu, etibarlılıq hiyləsi və ya sadə fırıldaqçılığa bənzəsə də, bu termin adətən məlumat toplamaq və ya kompüter sisteminə daxil olmaq üçün hiylələrə aiddir. Əksər hallarda təcavüzkar qurbanı ilə heç vaxt üz-üzə gəlmir.

2.4 İnformasiya təhlükəsizliyinə təhdidlərdə meyllər4

İnformasiya təhlükəsizliyinin qorunmasında mühüm bir tədbir təhlükəsizliyə qarşı təhdidlərdə meyllərin təhlil olunmasıdır. Burada təhlükəsiliyə qarşı təhdidlərin formalarının necə dəyişdiyini və inkişaf etdiyini müəyyənləşdirmək, yeni istiqamətlərdən yayınmaq və ya keçmək məqsədilə vaxtaşırı təhlükəsizliyə qarşı təhdid formaları üçün axtarış nəzərdə tutulur. İnformasiyanın toplanması və əlaqələndirilməsi və hadisə nümunələri ilə bağlı modellərin təkmilləşdirilməsi kimi bu təkrarlanan proses ona görə aparılır ki, oxşar və ya mümkün təhdidlərin qarşısını almaq və bu təhdidlərə qarşı müvafiq cavab tədbirlərini hazırlamaq mümkün olsun.

İnformasiya təhlükəsizliyinə təhdidlərdəki meyllərin təhlilini aparan və təhlükəsizliyə təhdidlərdə meyllərə dair hesabatları bölüşən təşkilatlara aşağıdakılar aiddir:

• FireEye (https://www.fireeye.com/current-threats/threat-intelligence- reports.html)
• IBM (https://www.ibm.com/security/data-breach/threat-intelligence/)
• Microsoft (www.microsoft.com/en-us/security/operations/security- intelligence-report)
• Symantec (https://www.symantec.com/security-center/threat-report)
• Verizon (https://enterprise.verizon.com/resources/reports/dbir/)

İnformasiya təhlükəsizliyinə təhdidlərdə məlum olan meyillər aşağıda təsvir olunur.

Hücum vasitələrinin avtomatlaşdırılması[9]

İndi saytlara qanunsuz daxil olanlar minlərlə internet sayt sahibləri barədə informasiyanı cəld və asanlıqla toplamaq imkanı verən avtomatlaşdırılmış vasitələrdən istifadə edirlər. Bu avtomatlaşdırılmış vasitələrdən istifadə etməklə, şəbəkələr uzaq məsafədən skanner vasitəsilə köçürülə və xüsusi zəif məqamları olan sayt sahibləri müəyyən edilə bilər. Saytlara qanunsuz daxil olanlar sonrakı istifadə üçün informasiyanı kataloqlaşdırır, digərləri ilə bölüşür və ya onları satır, yaxud da dərhal hücum edirlər. Bəzi vasitələr (Cain & Abel kimi) ümumi məqsədə doğru kiçik hücumları avtomatlaşdırır. Məsələn, saytlara qanunsuz daxil olanlar şəbəkədə marşrutlaşdırma vasitəsi və ya şəbəkələr-arası ekran (brandmauer) məxfi sözlərini əldə etmək üçün paketlər monitorundan (paket araşdırıcısından) istifadə edirlər, süzgəcləri təsirsiz etmək üçün məxfi sözlərə daxil olurlar və sonra serverdə məlumatı oxumaq üçün şəbəkə fayl xidmətindən istifadə edirlər.

Aşkar edilməsi çətin olan hücum vasitələri

Bəzi hücum vasitələrində mövcud aşkarlama vasitələri ilə aşkar edilməyən yeni hücum modellərindən istifadə edilir. Məsələn, hücum vasitələrinin xüsusiyyətlərini ört-basdır etmək və ya gizlətmək üçün məhkəmə ekspertizası ilə müəyyən edilə bilməyən üsullardan istifadə olunur. Polimorf vasitələr hər dəfə istifadə ediləndə öz formasını dəyişir. Bu vasitələrdən bəzilərində hipermətn ötürmə protokolu (HTTP) kimi ümumi yayılmış protokollardan istifadə olunur, bu da onları qanunu şəbəkə hərəkətindən fərqləndirməyi çətinləşdirir.[5] MSN Messenger zərərvericisi (soxulcanı) buna bir nümunədir. MSN Messenger Ani Yazışma (İM) xidmətindən istifadə edən müştəri məktubu almaq barədə ilk bildiriş verildikdən sonra yoluxmuş istifadəçinin ünvanlar kitabından əlaqədə olduğu şəxslərə sistemləri yoluxdurmaq üçün nəzərdə tutulan fayl göndərir. Həqiqi İM istifadəçisi olan şəxsin belə davranışı təqlid ediləndir, bu isə narahat edicidir.[6]

---

4 Bu bölüm Tim Şimeal və Fil Villiamsdan götürülmüşdür, İnformsiya təhlükəsizliyində meyllərin təhlilinin modelləri (Pitsburq, CERT Təhlil Mərkəzi, 2002-ci il) , http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.11.8034.

5 Sureş Ramazubramanian, Salman Ansari və Fuatai Pursel, "İnternetdən istifadəyə nəzarət", səh. 94 (3-cü haşiyəyə bax).

6 Munir Kotadia, "E-poçt zərərvericisi (soxulcanı) İM-ə daxil olur". *ZDNet.co.uk*, 4 aprel 2005-ci il, http://www.zdnet.co.uk/news/security-management/2005/04/04/email-worm-graduates-to-im-39193674/.

Zəif məqamların daha sürətli şəkildə müəyyənləşdirilməsi

Hər il proqram təminatı məhsullarında yeni aşkar olunan və Kompüterlə bağlı Fövqəladə Hallar Qrupunun Əlaqələndirmə Mərkəzinə (CERT / CC) bildirilən zəif məqamların sayı iki dəfədən çox artaraq inzibatçılar üçün yeniliklərə uyğunlaşmanı çətinləşdirir. Saytlara qanunsuz daxil olanlar bunu bilirlər və bundan yararlanırlar.[7]Saytlara qanunsuz daxil olan bəzi şəxslər sıfır-gün (və ya sıfır-saat) hücumuna başlayırlar hansı ki, bu, inzibatçılar tərəfindən hələ aşkar olunmadığı üçün onlara qarşı düzəlişin və ya müdafiənin olmadığı kompüter avadanlığının zəif məqamlarından yararlanan kompüter təhdididir.[8]

Qeyri-simmetrik təhdidlərin artması və hücum metodlarının konvergensiyası

Qeyri-simmetrik hücum, hücum edən şəxsin müdafiə olunan üzərində üstünlüyə malik olduğu şərtdir. Təhlükə yaratma prosesinin avtomatlaşdırılması və hücum vasitələrinin mürəkkəbləşdirilməsi ilə qeyri-simmetrik təhdidlərin sayı da artır.

Hücum metodlarının konverqensiyası dedikdə əlaqələndirilmiş zərərverici fəaliyyətə dəstək göstərən qlobal şəbəkələr yaratmaq üçün saytlara hücum edənlərin istifadə etdikləri müxtəlif hücum metodlarının birləşməsi nəzərdə tutulur. Məsələn, Zeus kimi də tanınan Zbot gizli forumlarda satılan zərərverici proqram paketidir. Paketdə komanda və nəzarət serveri kimi istifadə üçün icra koduna malik zərərverici və veb server fayllar (PHP, təsvirlər, SQL cədvəllər) yarada bilən qurucu ünsür vardır. Zbot uzaq məsafədə yerləşən icazəsiz istifadəçinin tam nəzarətinə imkan verən ümumi arxa qapı olduğu halda, Zbot-un başlıca funksiyası, FTP, e-poçt, onlayn bank və digər onlayn məxfi sözlər kimi onlayn parolları oğurlamaqla maliyyə vəsait qazanmaqdır.[9]

İnfrastruktura hücumlardan yaranan təhlükənin artması

İnfrastruktura hücumlar internetin əsas ünsürlərinə geniş şəkildə təsir göstərən hücumlardır. İnternetdə təşkilatların və istifadəçilərin sayına və onların gündəlik işi aparmaq üçün İnternetdən asılılığın artmaqda olmasına görə bu hücumlar narahatlıq doğurur. İnfrastruktura hücumlar DoS-lə nəticələnir, həssas informasiyaya müdaxilə edilir, yanlış informasiya yayılır.

“Hakerlik” infrastruktur hücumuna misaldır. "Hakerlik" termini qanuni icazə olmadan məlumat əldə etmək və ya dəyişdirmək üçün kompüterə və ya kompüter şəbəkəsinə giriş əldə etmək əməlinə aiddir.

“Hakerlik” hücumun məqsədindən asılı olaraq əyləncə, cinayət və ya siyasi haker kimi təsnif edilə bilər. Əyləncə məqsədli hakerlik sadəcə olaraq hakerin marağını təmin etmək üçün proqramların və məlumatların icazəsiz dəyişdirilməsidir. Kriminal hakerlik fırıldaqçılıq və ya casusluqda istifadə olunur. Siyasi hakerlik icazəsiz siyasi mesajlar yayımlamaq üçün internet saytlarına müdaxilədir.

Son vaxtlarda, hakerlik kiberterrorizm, kibersiyasət və kibermüharibədə daha çox yayılmağa başladı və o, milli təhlükəsizlik üçün böyük təhlükə yaradır.

---

7 Sureş Ramazubramanian, Salman Ansari və Fuatai Pursel, "İnternetdən istifadəyə nəzarət"

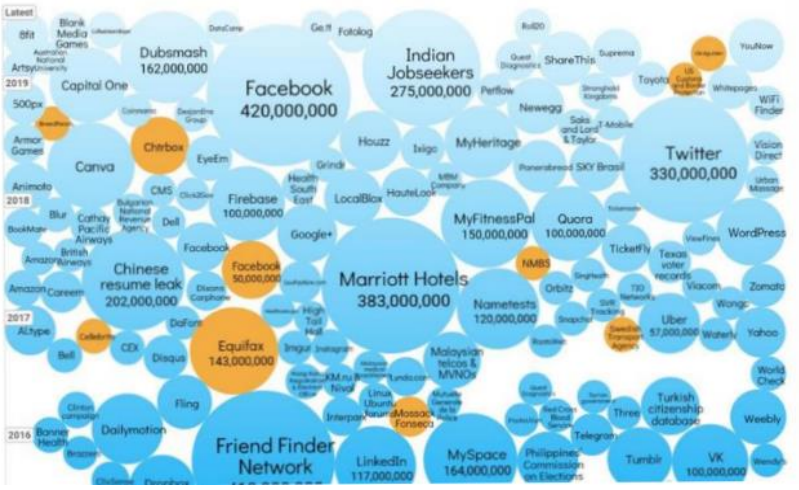
8 Wikipedia, "Sıfır gün hücumu", http://en.wikipedia.org/wiki/Zero_day_attack

9 Nikolas Falliere və Erik Çien, *Zeus: Zərəvericilər kralı, təhlükəsizlik tədbiri* (Cupertino, CA, Symantec, 2009-cu il), səh. 1, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/zeus_king_of_bots.pdf

Başqa bir yeni tendensiya milli maraqları olan və yüksək həssas məlumatları saxlayan əsas saytları hədəf alan haker qruplarını göstərir.

Şəkil 4 məlumatların pozulması həcmlərindəki tendensiyanı göstərir.

Şəkil 4: Məlumatların pozulması statistikası



Mənbə: İnformasiya gözəldir.

Kazus 8: Hakerliklə Mübarizə – Milli kazus

İndoneziya Respublikasının Baş Prokurorluğu xüsusi olaraq kibercinayətkarlıq işlərinə baxılmasında bilik, bacarıq və təcrübəyə malik prokurorlardan ibarət olan Kibercinayətkarlıqla Mübarizə Qrupunu hazırlamaq, layihələndirmək və formalaşdırmaqla qurumu institusional olaraq gücləndirir və canlandırır.

İşçi qrup üç xüsusi bölmədən ibarət olacaq, yəni:

- Birincisi, kompüterlərdən və ya informasiya texnologiyaları vasitələrindən cinayət törətmək vasitəsi kimi istifadə edən cinayət işlərinə baxılması üçün təyin edilmiş Kompüterlə Əlaqədar Cinayətlər Bölməsi,
- İkincisi, kompüterlərə və informasiya texnologiyalarına qarşı cinayətləri idarə etmək üçün təyin edilmiş Kompüterlərə Qarşı Cinayətlər Bölməsi; və
- Üçüncüsü, həm milli, həm də beynəlxalq səviyyədə işlərin və əməkdaşlığın həllində dəstək verən Əməkdaşlıq və Katiblik Bölməsi.

Texniki: Aktiv botnetlər haqqında məlumatı müəyyən etmək və toplamaq üçün alətlər və üsullar

- Botnet fəaliyyətini azaltmaq üçün informasiya təhlükəsizliyi və şəxsi həyatın toxunulmazlığının ən yaxşı təcrübələri
- Botnet fəaliyyətini yumşaltmaq (yüngülləşdirmək) üçün qeydiyyatçı və reyestr üzrə ən yaxşı təcrübələr
- Elektron ticarət və onlayn əməliyyat təminatçıları üçün potensialın yaradılması

Sosial: İnternetin etibarlılığı və təhlükəsizliyi üzrə geniş təhsil layihələri

- İstifadəçilər üçün təhlükəsiz İKT-yə çıxış imkanına kömək edilməsi

PTF ITU SPAM vasitələr toplusu siyasəti planlaşdıranlara, tənzimləyici qurumlara və şirkətlərə siyasəti tənzimləməkdə və e-poçta inamın bərpa olunmasında kömək etmək üçün geniş bir paketdir. Bu vasitələr toplusu, həmçinin, beynəlxalq problemlərin qarşısını almaq üçün ölkələr boyu informasiya mübadiləsini tövsiyə edir.

Hücumların məqsədlərində dəyişikliklər

Əvvəllər kompüter və şəbəkələrə hücumlar maraqdan irəli gələrək və ya özünü məmnun etmə üçün törədilirdi. İndi məqsəd adətən pul, böhtan və məhv etmədir. Bundan əlavə, bu növ hücumlar kibercinayətkarlığın geniş spektrinin yalnız kiçik bir hissəsini təşkil edir.

Kibercinayətkarlıq, siyasi, iqtisadi, dini və ya ideoloji səbəblərdən məqsədli şəkildə rəqəmsal məlumatların və ya informasiyanın məhv edilməsi, kəsilməsi və ya təhrif edilməsidir. Ən çox yayılmış cinayətlər hakerlik, DoS, zərərverici kodlar və sosial mühəndislikdir. Son vaxtlarda kibercinayətkarlıq, milli təhlükəsizliyə mənfi təsirlər göstərməklə, kiber-terrorçuluğun və kiber-müharibənin bir hissəsinə çevrilmişdir.

Aşağıda 3-cü Cədvəldə kibercinayətləri törədənlərin nə qazandıqları göstərilir.

Cədvəl 3. 2017-cu ildə kibercinayətlərdən gəlirlər

Bənd	**Qiymət aralığı (dollarla)**
Ümumi qeyri-maliyyə təşkilatına giriş etimadnamələr	1
Kredit və ya Debit kart	5-110
Sürücülük vəsiqəsi, Sadiqlik hesabları	20
Onlayn ödəniş xidmətlərinin giriş məlumatları, məs. Paypal	20-200
Diplomlar	100-400
Tibbi Qeydlər	1-1000
Pasportlar	1000-2000

Mənbə: Stack, B. (6 dekabr 2017-ci il). Qara veb-səhifədə sizin şəxsi məlumatlarınızın necə satıldığı buradadır. Experian. https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-sellingfor-on-the-dark-web

2.5 Təhlükəsizliyin artırılması

Təhlükəsizliyə təhdidlərə və hücum texnologiyalarına nəzər saldıqda görürük ki, güclü müdafiə üçün dəyişkən mühitə uyğunlaşmaya imkan verən çevik strategiya, düzgün müəyyən edilmiş siyasətlər və prosedurlar, müvafiq təhlükəsizlik texnologiyalarından istifadə və daimi sayıqlıq tələb olunur.

Təhlükəsizliyin hazırki vəziyyətini müəyyənləşdirməklə təhlükəsizliyin artırılması proqramına başlamaq faydalıdır. Təhlükəsizlik proqramı sənədləşdirilmiş siyasətləri və prosedurlar, habelə onların tətbiqinə dəstək göstərən texnologiyanı əhatə edir.

İnzibati təhlükəsizlik

İnzibati təhlükəsizlik informasiya təhlükəsizliyi strategiyasından, siyasətindən və bununla bağlı rəhbər prinsiplərdən ibarətdir.

İnformasiya təhlükəsizliyi strategiyası informasiya təhlükəsizliyi ilə bağlı bütün tədbirlər üçün istiqaməti müəyyən edir.

İnformasiya təhlükəsizliyi siyasəti bütöv təşkilatda informasiya təhlükəsizliyi üçün sənəd qismində qəbul edilmiş yüksək-səviyyəli plandır. O, inzibati və fiziki təhlükəsizliklə planı kimi xüsusi qərarlar üçün çərçivəni təmin edir.

Informasiya təhlükəsizliyi siyasəti uzun-müddətli baxış nöqteyinə malik olduğu üçün, onda texnologiyanı səciyyələndirən məzmun istisna edilməli və işin davamlılığına dair effektiv planlaşdırma aparılmalıdır.

İnformasiya təhlükəsizliyinə dair rəhbər prinsiplər informasiya təhlükəsizliyi strategiyasına və siyasətinə uyğun olaraq müəyyən edilməlidir. Rəhbər prinsiplər informasiya təhlükəsizliyi ilə bağlı hər bir sahə üçün qaydaları dəqiq müəyyən etməlidir. Və rəhbər prinsiplər əhatə dairəsinə görə geniş və milli olduğundan, onlar, təşkilatlar tərəfindən riayət edilməsi üçün hökumət tərəfindən işlənib hazırlanmalı və qəbul edilməlidir.

İnformasiya təhlükəsizliyi standartları elə müəyyən edilməlidir və səciyyəvi olmalıdır ki, onlar informasiya təhlükəsizliyi ilə bağlı bütün sahələrə tətbiq edilə bilsin. Hər bir ölkə üçün bütün dünyada geniş istifadə olunan inzibati, fiziki və texniki təhlükəsizlik standartlarını təhlil etdikdən sonra standartların işlənib hazırlanması məqsədəuyğundur. Standartlar üstünlük təşkil edən İKT mühitinə uyğun olmalıdır.

Ölkənin informasiya təhlükəsizliyi strategiyası, siyasəti və buna dair rəhbər prinsiplər müvafiq qanuna uyğun olmalıdır. Onların əhatə dairəsi milli və beynəlxalq qanunlar çərçivəsində olmalıdır.

İnformasiya təhlükəsizliyi fəaliyyəti və prosesi

Informasiya təhlükəsizliyi strategiyası, siyasəti və buna dair rəhbər prinsiplər müəyyən edildikdən sonra informasiya təhlükəsizliyi üzrə fəaliyyət prosedurları və prosesləri müəyyən edilməlidir. İnformasiyaya hücum və daxili informasiyanın sızması halları insanlar tərəfindən törədildiyindən insan resurslarının idarə olunması informasiya təhlükəsizliyi fəaliyyətində ən mühüm faktordur. Beləliklə aşağıdakılar həyata keçirilməlidir:

1. İnformasiya təhlükəsizliyinə dair təhsil və təlim proqramı – Təşkilatda informasiya təhlükəsizliyi səviyyəsini qaldırmaq üçün bir çox metodlar vardır, lakin təhsil və təlim əsas tədbirlərdir. Təşkilatın heyət üzvləri təhsil və təlim vasitəsilə informasiya təhlükəsizliyinə duyulan ehtiyacı dəyərləndirməli və müvafiq vərdişlər əldə etməlidirlər. Lakin, iştirakı maksimuma çatdırmaq üçün müxtəlif proqramların işlənib hazırlanması vacibdir, belə ki, informasiya təhlükəsizliyinə dair standartlaşdırılmış təhsil və təlim proqramları effektiv olmaya bilər.
2. Müxtəlif tədbirlər vasitəsilə inkişafı gücləndirmək – İnformasiya təhlükəsizliyi strategiyasının, siyasətinin və rəhbər prinsiplərinin uğurla həyata keçirilməsində əməkdaşların iştirakı vacibdir. İnformasiya təhlükəsizliyi müxtəlif gündəlik tədbirlər vasitəsilə əməkdaşlar arasında inkişaf etdirilməlidir..

3. Təhlükəsizliyə dəstək – Əməkdaşlar arasında informasiya təhlükəsizliyinə dair məlumatlılıq yüksək səviyyələrdə olsa da və onlar informasiya təhlükəsizliyini qorumaq üçün güclü iradəyə malik olsalar da, təşkilatın ən yüksək dairələrinin dəstəyi olmadan informasiya təhlükəsizliyini təmin etmək çətindir. Baş İcraçı Rəhbərin və Baş İnformasiya Rəhbrərinin dəstəyi olmalıdır.

Texnoloji təhlükəsizlik

Öz informasiya sistemlərini qanunsuz müdaxilələrdən qorumaqda təşkilatlara kömək etmək üçün müxtəlif texnologiyalar işlənib hazırlanmışdır. Bu texnologiyalar sistemləri və informasiyanı hücumlara qarşı qorumağa, qeyri-adi və ya şübhəli fəaliyyəti aşkar etməyə və təhlükəsizliyə təsir göstərən tədbirlərə cavab verməyə kömək edir.

Bu günkü təhlükəsizlik sistemləri istifadədə olan texnologiyalara vahid nəzarətə gətirib çıxaran Dərindən-Müdafiə (DİD) modeli əsasında qurulmuşdur və inkişaf etdirilmişdir. Bu model bütün təhlükələrə qarşı yalnız bir müdafiə qatının olduğu perimeter müdafiəsindən fərqlənir. DİD modeli, hər bir mərhələdə təhlükələri azaltmaqla, qarşısını alma, aşkar etmə və dözümlülükdən ibarətdir. (bax, 5-ci Təsvir).

Şəkil 5. Dərindən-Müdafiə modeli

Mənbə: Müdafiə Elmi Şurasının İşçi Qrupu, *Vətəni müdafiə: müdafiə informasiya əməliyyatları 2000-ci il yay təlimi, II Tom* (Vaşinqton, K.D.), səh. 5, http://www.carlisle.army.mil/DIME/documents/dio.pdf

Qarşısını alma texnologiyası

Qarşısını alma texnologiyaları saxlama və ya sistem səviyyəsində qanunsuz müdaxilələrə və təhlükələrə qarşı qoruyur. Bu texnologiyalara aşağıdakılar aiddir:

1. Kriptoqrafiya – Kodlaşdırma kimi də nəzərdə tutulan kriptoqrafiya informasiyanın ilkin formadan (açıq mətn adlanan) kodlaşdırılmış, oxuna bilməyən (şifrlənmiş mətn adlanan) formaya çevirilməsidir. Kodsuzlaşdırma isə şifrələnmiş mətnin açılması və onun yenidən əvvəlki açıq mətn formasına qaytarılmasıdır. Kriptoqrafiya müxtəlif tətbiqi proqramları qorumaq üçün istifadə edilir. Kriptoqrafiya və müvafiq texnologiyalarla (IPSec, SSH, SSL, VPN, OTP, etc.) bağlı daha geniş informasiyanı aşağıdakı veb səhifələrdən əldə etmək olar:

- IETF RFC (http://www.ietf.org/rfc.html)
- RSA Laboratoriyalarının bu günkü kriptoqrafiya ilə bağlı tez-tez soruşulan sualları (http://www.rsa.com/rsalabs/node.asp?id=2152)

2. Bir-dəfəlik məxfi sözlər (OTP-lər) – Addan göründüyü kimi, OTP-lər yalnız bir dəfə istifadə edilə bilər. Sabit məxfi sözlərlə müdafiəni məxfi sözün itməsi, məxfi sözün tapılması, güc hesabına məxfi sözün sındırılması və bu kimi yollarla asanlıqla açmaq olar. OTP ilə edildiyi kimi, daima dəyişdirilən məxfi sözlə bu risk xeyli azaldıla bilər. Bu səbəbdən, onlayn bank əməliyyatları kimi elektron şəkildə aparılan maliyyə əməliyyatlarının təhlükəsizliyini təmin etmək üçün OTP-dən istifadə olunur.

3. Təhlükəsizlik divarı (firewall) – Təhlükəsizlik divarı (firewall) inamın olmadığı zona – İnternet və yüksək səviyyədə inamın olduğu zona – daxili şəbəkə arasında olduğu kimi müxtəlif kompüter şəbəkələri arasında bəzi hərəkət axınını tənzimləyir. İnternet və inamın olduğu daxili şəbəkə arasında yerləşən aralıq inam səviyyəsinə malik zonaya çox vaxtı “perimeter şəbəkəsi” və ya hərbsizləşdirilmiş zona kimi istinad olunur.

4.Zəif tərəflərin təhlil edilmə vasitəsi - hücum metodlarının artması və ümumi istifadədə olan tətbiqi proqramlarda zəif tərəflərin olması səbəbindən, mütəmadi olaraq sistemin zəif tərəflərinin mütəmadi olaraq dəyərləndirilməsi zəruridir. Kompüter təhlükəsizliyində zəif tərəf hücum edən şəxsə sistemi sındırmağa imkan verən zəiflikdir. Zəif tərəflər zəif məxfi sözlər, proqram təminatında səhvlər, kompüter virusu, yazıda şrift kodların çıxması, SQL-in

çıxması və ya zərərli proqram təminatlarının nəticəsi ola bilər. Zəif tərəflərin təhlil vasitələri bu zəifliklər üzə çıxarır. Onları asanlıqla onlayn şəkildə əldə etmək olar və təhlil xidmətləri göstərən şirkətlər mövcuddur. Lakin, ödənişsiz şəkildə İnternet istifadəçiləri üçün açıq olan bu xidmətlərdən müdaxilə edən şəxslər tərəfindən sui-istifadə edilə bilər. Ətraflı məlumat üçün bax:

- Secunia zəif tərəflər arxivi (http://secunia.com/advisories)
- Təhülkəsizliklə bağlı zəif tərəflər arxivi (http://www.securityfocus.com/bid)
- 100 ən yüksək şəbəkə təhlükəsizlik vasitəsi (http://sectools.org)

Şəbəkə zəifliyinin təhlil vasitələri marşurtlaşdırma qurğusu (router), şəbəkələrarası ekran (brandmauer) və serverlər kimi şəbəkə resurslarının zəifliyini təhlil edir.

Serverin zəifliyi ilə bağlı təhlil vasitəsi zəif məxfi söz, zəif konfiqurasiya və daxili sistemdə fayl icazə səhvi kimi zəif tərəfləri təhlil edir. Serverin zəifliyi ilə bağlı təhlil vasitəsi şəbəkənin zəifliyi ilə bağlı təhlil vasitəsinə nisbətən daha dəqiq nəticələr verir, belə ki, bu vasitə, daxili sistemdə daha çox zəifllikləri təhlil edir.

Veb zəifliklə bağlı təhlil vasitələri XSS və veb üzərindən SQL daxiletmə kimi veb tətbiqi proqramlarının zəif tərəflərini təhlil edir. Daha geniş informasiya üçün http://www.owasp.org/index.php/Top_Ten_2010 ünvanda Açıq Veb Tətbiqetmə Təhlükəsizlik Layihəsinə nəzər salın.

5.Hava boşluğu aləti – Hava divarı və ya hava boşluğu təhlükəsiz kompüter şəbəkəsinin ictimai İnternet və ya təhlükəli yerli şəbəkə kimi təhlükəli şəbəkələrdən fiziki olaraq təcrid olunmasını təmin etmək üçün bir və ya bir neçə kompüterdə tətbiq edilən şəbəkə təhlükəsizlik tədbiridir. İllərdir kibertəhlükəsizlik üzrə mütəxəssislərin əksəriyyətinin məsləhəti, təhlükəsizliyə hava boşluğu strategiyası ilə deyil, dərin müdafiə strategiyası (yəni, çoxlu mühafizə) ilə yanaşmaq olub. İllərdir kibertəhlükəsizlik üzrə mütəxəssislərin əksəriyyətinin məsləhəti, təhlükəsizliyə hava boşluğu strategiyası ilə deyil, dərin müdafiə strategiyası (yəni, çoxlu mühafizə) ilə yanaşmaq olub.

6. Brauzer izolyasiyası – Bu, internet istifadəçisinin yerli şəbəkələrindən və infrastrukturundan uzaqda gəzən fəaliyyətini (və əlaqəli kiber riskləri) fiziki olaraq təcrid etmək məqsədi daşıyan kibertəhlükəsizlik modelidir. Brauzer izolyasiya texnologiyaları bu modelə müxtəlif yollarla yanaşır, lakin onların hamısı eyni məqsədə nail olmağa çalışır. Bu, təhlükəsizlik divarları, müdaxilənin qarşısının alınması sistemləri (IDS) və zərərli proqram sandbox sistemləri kimi ənənəvi təhlükə idarəetmə tədbirlərindən fərqlidir, hansıki potensial təhlükə barədə xəbərdarlıq edildikdən sonra adətən sübuta əsaslanan məlumatların araşdırılmasını nəzərdə tutur.

Aşkaretmə texnologiyası

Aşkaretnə texnologiyası qeyri-normal vəziyyətləri və şəbəkələrə və ya mühüm sistemlərə müdaxilələri aşkar etmək və izləmək üçün istifadə edilir. Aşkaretmə texnologiyasına aşağıdakılar aiddir:

1. Antivirus – antivirus proqram təminatı zərərvericilər (soxulcanlar), fişinq hücumları, rutkit proqramlar, Troyan atları və digər zərərli proqram təminatlarını daxil olmaqla, zərərli kodları (proqram təminatlarını) müəyyən etmək, zərərsizləşdirmək və ya aradan qaldırmaq üçün kompüter proqramıdır.[10]

2. Müdaxilələri aşkarlama sistemi (İDS) – İDS təhlükəsizliyin mümkün pozulması hallarını müəyyən etmək üçün kompüter və ya şəbəkə daxilində müxtəlif sahələrdən informasiyanı toplayır və təhlil edir. Müdaxilələri aşkarlama funksiyalarına qeyri-normal fəaliyyət nümunələrinin təhlili və hücum nümunələrini tanıma imkanı aiddir.

3. Müdaxilələrin qarşısını alınması sistemi (IPS) – Müdaxilələrin qarşısını alma işində mümkün təhlükələri müəyyən etməyə və hücumlarda onlardan istifadə olunanadək onlara qarşı cavab tədbilər görməyə cəhd edilir. İPS şəbəkədəki hərəkətə nəzarət edir və şəbəkə inzibatçısı tərəfindən müəyyən edilmiş qaydalara uyğun olaraq mümkün təhlükələrə qarşı dərhal tədbir görür. Məsələn, İPS şübhəli İP ünvandan gələn göndərişlərə blok qoya bilər.[11]

4. Zərərli proqram qum qutusu sistemi – "Zərərli proqram sandbox" adətən zərərli proqramların yayılmasının qarşısını almaq məqsədilə proqramların icrasını ayıran təhlükəsizlik sistemidir. O, tez-tez sınanmamış və ya etibarsız proqramları və ya kodu, ola bilsin ki, yoxlanılmamış və ya etibarsız üçüncü tərəflərdən,

[10] Wikipedia, "Antivirus proqram təminatı", http://en.wikipedia.org/wiki/Antivirus_software.

[11] SearchSecurity.com, "Müdaxilələrin qarşısının alınması", TechTarget, http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci1032147,00. html.

təchizatçılardan, istifadəçilərdən və ya vebsaytlardan “qum qutusunda” ana maşına və ya əməliyyat sisteminə zərər vermədən icra etmək üçün istifadə olunur.

5. Şəbəkə Trafik Təhlili (Network Traffic Analysis- NTA) – Şəbəkə trafikinin təhlili aktiv kibermüdafiə fəaliyyətidir. Bu, “mövcud təhlükəsizlik həllərindən yayınan qabaqcıl təhdidləri aşkar etmək və təcrid etmək üçün şəbəkələr vasitəsilə proaktiv və iterativ axtarış prosesidir”.

İnteqrasiya texnologiyası

İnteqrasiya texnologiyası əsas aktivlərin informasiya təhlükəsizliyi üçün mühüm funksiyaları, yəni müdaxilələrin əvvəlcədən ehtimal edilməsi, aşkarlanması və izlənməsi kimi funksiyaları birləşdirir. İnterqasiya texnologiyasına aşağıdakılar aiddir.

1. Müəssisədə təhlükəsizliyin idarəedilməsi (ESM) – ESM uyğun siyasət əsasında İDS və İPS kimi informasiya təhlükəsizliyini idarə edir, ona nəzarət edir və bu istiqamətdə işi qurur. O, informasiya təhlükəsizliyi ilə bağlı hər bir həll yolunun üstünlüklərindən yararlanmaqla və uyğun siyasət əsasında informasiya təhlükəsizliyinin səmərəliliyini maksimuma çatdırmaqla digər həll yollarının zəif tərəflərini aradan qaldırmaq üçün strategiya kimi istifadə edilir.

Mövcud təhlükəsizlik texnologiyalarını idarə edə bilən ESM-lər, bu təhlükəsizlik texnologiyalarını işlədən insan resurslarının çatışmazlığı, hücum metodlarının cəmləşməsi kimi daha təkmil hücumların artması və aşkar etmək çətin olan hücum vasitələrinin meydana çıxması səbəbindən son vaxtlarda üzə çıxmışdır. ESM-lə nəzarəti səmərəliliyi artır və əks tədbirlər müəyyən edilir.

2. Müəssisədə risk idarəetmə (ERM) – ERM, təşkilatla bağlı, o cümlədən informasiya təhlükəsizliyindən kənar sahələrdə bütün riskləri əvvəlcədən müəyyən etməyə və avtomatik şəkildə əks tədbirlər görməyə kömək edən sistemdir. İnformasiyanı qorumaq üçün ERM-dən istifadə risk idarəetmənin dəqiq məqsədinin və sistemin inkişafı üçün quruluşun müəyyənləşdirilməsini tələb edir. Əksər təşkilatlar, öz ERM-lərini qurmaq və optimallaşdırmaq üçün, bunu özləri etmək əvəzinə, informasiya təhlükəsizliyi üzrə peşəkar məsləhətverici agentliklər vasitəsilə edirlər.

Düşündürücü suallar

1. Sizin təşkilatınız informasiya təhlükəsizliyinə yönələn hansı təhdidlərə qarşı zəifdir? Nə üçün?

2. Sizin təşkilatınızda informasiya təhlükəsizliyinin təmin olunması üçün hansı texnoloji üsullar vardır?

3. Sizin təşkilatınızda informasiya təhlükəsizliyinə dair siyasət, strategiya və rəhbər prinsiplər vardırmı? Əgər vardırsa, Sizin təşkilatınızın kifayət qədər müdafiə oluna bilmədiyi təhlükələri nəzərə alsaq, bunlar nə qədər uyğundur? Əgər yoxdursa, Siz öz təşkilatınız üçün informasiya təhlükəsizliyinə dair siyasət, strategiya və rəhbər prinsiplərlə bağlı nə tövsiyə edərdiniz?

Özünü sına

1. Nə üçün informasiya təhlükəsiliyinə təhdidlərdəki meyllərə dair təhlil aparmaq vacibdir?

2. Nə üçün informasiya təhlükəsizliyinin təmin olunmasında insan resurslarının idarə olunması ən vacib faktordur? İnformasiya təhlükəsizliyi üçün insan resurslarının idarə olunmasında əsas tədbirlər hansılardır?

3. Texniki təhlükəsizliyin Dərindən-Müdafiə modelini izah edin. O, necə işləyir?

3.İNFORMASİYA TƏHLÜKƏSİZLİYİ TƏDBİRLƏRİ

Bu bölümün məqsədi aşağıdakılardan ibarətdir:

- **İnformasiya təhlükəsizliyi üzrə siyasətin işlənib hazırlanmasında bələdci kimi istifadə edilə bilən müxtəlif ölkələrdə informasiya təhlükəsizliyi tədbirlərinə dair nümunələri göstərmək; və**
- **İnformasiya təhlükəsizliyi siyasətinin həyata keçirilməsində beynəlxalq əməkdaşlığı vurğulamaq.**

3.1 Milli İnformasiya Təhlükəsizliyi Strategiyasının hazırlanması

İnformasiya təhlükəsizliyi strategiyası

Milli İnformasiya Təhlükəsizliyi Strategiyasına (NISS) ehtiyac bugünkü bir-biri ilə əlaqəli kompüter şəbəkələrinin mürəkkəbliyi ilə diktə olunur. Dövlət qurumları öz informasiya və İnformasiya Kommunikasiya Texnologiyaları (İKT) sistemlərinin təhlükəsizliyinə cavabdeh olmalıdırlar. Əslində, milli agentliklər də getdikcə daha çox öz milli hüdudlarından kənara çıxa bilən biznes qurumları tərəfindən idarə olunan üçüncü tərəf İKT sistemlərinə etibar edirlər.

Əksər ölkələr informasiya təhlükəsizliyini öz ölkələrinin məqsədlərinə daha yaxşı uyğunlaşdırmaq zərurətini dərk etsə də, bir çoxları hələ də bu etirafı konkret fəaliyyət planlarına çevirmək üçün mübarizə aparır.

Milli İnformasiya Təhlükəsizliyi Strategiyasının (NISS) inkişafında öz baxışını ifadə etmək adi haldır. Bəzi ümumi məqsədlərə aşağıdakılar daxildir:

- Təhlükəsiz, Etibarlı və Davamlı Milli İKT İnfrastruktur Mühiti
- Yüksək İxtisaslı Kibertəhlükəsizlik İşçi Qüvvəsi
- Milli Kibertəhlükəsizlik Maarifləndirmə və Təlim Proqramı
- Kibercinayətkarlıqla mübarizə üçün milli qanunvericiliyin qəbulu
- Milli və Beynəlxalq Təhlükəsizlik Əməkdaşlığı

Daha təkmil Milli İnformasiya Təhlükəsizliyi Strategiyası (NISS) /strategiyalarına aşağıdakı kimi məqsədlər də daxildir:

- Milli Kiber Təhlükələrin Təhlili və Cavab Proqramı
- Milli Kibertəhlükəsizliyə Uyğunluq və İzləmə Proqramı
- Milli Kibertəhlükəsizlik Tədqiqatları, İnnovasiyalar və Sahibkarlıq Proqramı

Milli İnformasiya Təhlükəsizliyi Strategiyasının inkişafı zamanı ya beynəlxalq standartların, ya da təcrübə məcəllələrinin qəbul edilməsi adi haldır.

Texniki standartlara misal olaraq ISO 27001 və UN/EDIFACT (Birləşmiş Millətlər/İdarəetmə, Ticarət və Nəqliyyat üçün Elektron Məlumat Mübadiləsi) daxildir.

Davranış Qaydalarına (Code of conduct) nümunə olaraq Avropa Şurası və İƏİT (İqtisadi Əməkdaşlıq və İnkişaf Təşkilatı) daxildir.

Sənaye Təcrübələri və Tələblərinə nümunə olaraq Avropa Təhlükəsizlik Forumu (ESF), Milli Standartlar və Texnologiya İnstitutu (NIST) və Böyük Britaniyanın Ticarət və Sənaye Departamenti (DTI) daxildir.

3.2 Milli İnformasiya Təhlükəsizliyi Strategiyalarının nümunələri

Amerika Birləşmiş Ştatlarının informasiya təhlükəsizliyi strategiyası

9 sentyabr 2001-ci il (9/11) tarixdə törədilən terror hücumlarından sonra, ABŞ hökuməti, yalnız fiziki təhlükələrə qarşı deyil, eyni zamanda kiber-təhlükələrə qarşı milli təhlükəsizliyi möhkəmləndirmək üçün Daxili Təhlükəsizlik Departamentini təsis etmişdir.

Onun informasiya təhlükəsizliyi strategiyasına Daxili Təhlükəsizlik üzrə Milli Strategiya, Mühüm İnfrastrukturların və Əsas Aktivlərin Fiziki Təhlükəsizliyi üzrə Milli Strategiya və Təhlükəsiz Kibermәkan üzrə Milli Strategiya daxildir.

Təhlükəsiz Kibermәkan üzrə Milli Strategiya[12] kibertəhlükəsizlik və mühüm infrastruktur və aktivlərin qorunması üzrə baxışları əks etdirir. O, mühüm infrastruktura və aktivlərə yönələn kiber hücumların qarşısını almaq üçün xüsusi məqsədləri və tədbirləri müəyyən edir. Təhlükəsiz Kibermәkan üzrə Milli Strategiyada müəyyən edilmiş beş milli prioritet aşağıdakılardır:

- Kibermәkanın Təhlükəsizliyi üzrə Milli Tədbirlər Sistemi
- Kibermәkanın Təhlükəsizliyinə Təhdidlərin və Zəifliyin Azaldılması üzrə Milli Proqram
- Kibermәkanın Təhlükəsizliyinə dair Milli Məlumatlandırma və Təlim Proqramı
- Hökumətin Kibermәkanında Təhlükəsizliyin Təmin Olunması
- Milli Təhlükəsizlik və Beynəlxalq Kibermәkan Təhlükəsizliyi Əməkdaşlığı

Ən son Milli Kiber Strategiya 2018-ci ilin sentyabrında dərc edilib. Müəyyən edilmiş dörd əsas sütun bunlardır:

- Amerika xalqı, vətən və Amerika həyat tərzinin qorunması
    - Təhlükəsiz Federal Şəbəkələr və Məlumatlar
    - Təhlükəsiz Kritik İnfrastruktur
    - Kibercinayətkarlıqla Mübarizə edin və Hadisə Hesabatını Təkmilləşdirilməsi
- Amerikanın rifahının dəstəklənməsi
    - Canlı və Dayanıqlı Rəqəmsal İqtisadiyyatın təşviq edilməsi
    - ABŞ-ın Yaradıcılığının dəstəklənməsi və qorunması

12 Ağ Ev, "Təhlükəsiz Kibermәkan üzrə Milli Strategiya" (Vaşinqton, K.D., 2003-cü il), http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf.

- Üstün kibertəhlükəsizlik işçi qüvvəsinin inkişaf etdirilməsi

- Sülhün güc yolu ilə qorunması

  - Məsuliyyətli Hökumət Davranışı Normları vasitəsilə Kiber Sabitliyin Artırılması
  - Kiberməkanda keyfiyyət və qəbuledilməz davranışın qarşısının alınması

- Gücləndirilmiş Amerika təsiri

  - Açıq, Birgə işləyə bilən, Etibarlı və Təhlükəsiz İnterneti təşviq edin
  - Beynəlxalq Kiber Potensial Yaradın

İnformasiya təhlükəsizliyi qanununun sərtləşdirilməsi

2014-cü il Kiber təhlükəsizliyin gücləndirilməsi haqqında Qanun (CSEA) ilk dəfə 2002-ci ildə və ən son versiyası 2014-cü ildə qəbul edilmişdir. O, Daxili Təhlükəsizlik Qanununun ikinci fəslindən ibarətdir. O, bəzi kompyuter cinayətlərinə görə cəza təyin etmə qaydalarına düzəlişlər, fövqəladə hallarda açıqlanma istisnası, vicdanlı istisna, qeyri-qanuni İnternet reklamının qadağan edilməsi və şəxsi həyatın toxunulmazlığının qorunması və digər şeyləri nəzərdə tutur. Qanun layihəsi, həmçinin, "kibertəhlükəsizliyi təkmilləşdirmək, kibertəhlükəsizliyə dair tədqiqat və təkmilləşdirməni, işçi qüvvəsinin inkişafı və təhsilini, ictimai məlumatlılığı və hazırlığı gücləndirmək və digər məqsədlər üçün davamlı, könüllü dövlət-özəl tərəfdaşlığı" nəzərdə tutur.

Böyük Britaniyanın informasiya təhlükəsizliyi strategiyası

Böyük Britaniya hökuməti 2016-2021-ci illər üçün son Milli Kibertəhlükəsizlik Strategiyasını dərc edib. 2021-ci il perspektivi Böyük Britaniyanın kibertəhlükələrə qarşı etibarlı və davamlı olması, rəqəmsal biznesdə uğurlu və inamlı olmasıdır.

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_dat a/file/567242/national_cyber_security_strategy_2016.pdf

Bu perspektivə nail olmaq üçün o, aşağıdakı məqsədləri bəyan edir:

- Müdafiə etmək

  - Böyük Britaniyanı inkişaf edən kibertəhlükələrdən müdafiə etmək, baş verən hadisələrə effektiv cavab vermək və Birləşmiş Krallıq şəbəkələrinin, məlumatlarının və sistemlərinin mühafizəsini və davamlı olmasını təmin etmək üçün vasitələrimiz var.

- Qarşısını almaq

  - Birləşmiş Krallıq kiberməkanda təcavüzün bütün formaları üçün sərt hədəf olacaq. Biz cinayətkarları təqib edərək və mühakimə edərək, bizə qarşı düşməncəsinə hərəkətləri aşkar edir, başa düşür, araşdırır və pozuruq. Kiberməkanda hücum hərəkətləri etmək üçün imkanlarımız var, bunu seçməliyik.

- İnkişaf etmək

- Bizdə dünyada aparıcı elmi tədqiqat və inkişaflarla dəstəklənən yenilikci, inkişaf edən kibertəhlükəsizlik sənayemiz var. Bizim dövlət və özəl sektorda milli ehtiyaclarımızı ödəmək üçün bacarıqları təmin edən öz-özünə davam edən istedad xəttimiz var. Bizim qabaqcıl təhlilimiz və təcrübəmiz Birləşmiş Krallığa gələcək təhdid və çağırışlarla qarşılaşmağa və onların öhdəsindən gəlməyə imkan verəcək.

Avropa İttifaqının informasiya təhlükəsizliyi strategiyası

Hazırda Avropa İttifaqı ölkələrində kiberməkandan iqtisadi və sosial faydaların əldə edilməsinə xələl gətirə biləcək risklərin öhdəsindən gəlməyə kömək edən əsas siyasət xüsusiyyəti kimi Milli Kibertəhlükəsizlik Strategiyası (NCSS) mövcuddur.

2006-cı ilin may ayında verilən məlumatda[13], Avropa Komissiyası, Avropa İttifaqının, bir çox maraqlı tərəflərin iştirakı ilə, bir sıra qarşılıqlı əlaqəli tədbirlərdən ibarət olan informasiya təhlükəsizliyi strategiyasına dair məlumat verir. Bu tədbirlərə 2002-ci ildə Elektron Kommunikasiya üzrə Tənzimləyici Çərçivənin təsis olunması, Avropa İnformasiya Cəmiyyətinin yaradılması üçün i2010 layihəsinin birləşdirilməsi və 2004-cü ildə Avropa Şəbəkə və İnformasiya Təhlükəsizliyi Agentliyinin (ENİSA) təsis olunması aiddir. Məlumata əsasən, bu tədbirlər, xüsusi şəbəkə və informasiya təhlükəsizliyi tədbirləri (NİS), elektron kommunikasiya üçün tənzimləyici çərçivə (hansı ki, bura Şəxsi həyatın toxunulmazlığı və məlumat təhlükəsizlik məsələləri daxildir) və kibercinayətkarlığa qarşı mübarizəni əhatə edən İnformasiya Cəmiyyətində təhlükəsizlik məsələlərinə üç-tərəfli yanaşmanı əks etdirir.

2006-cı il dekabr tarixli Kommunikasiyada Avropa Komissiyası kritik infrastrukturların zəifliklərini azaltmaq üçün Kritik İnfrastrukturun Mühafizəsi üzrə Avropa Proqramını (EPCIP) işə saldı. Bu, Avropada, bütün Avropa İttifaqı dövlətlərində və iqtisadi fəaliyyətin bütün müvafiq sektorlarında kritik infrastrukturun qorunmasının yaxşılaşdırılmasına yönəlmiş tədbirlər paketidir. Avropa İttifaqının Kritik İnformasiya İnfrastrukturunun Mühafizəsi (CIIP) təşəbbüsü mühim İnformasiya və Kommunikasiya Texnologiyaları (İKT) infrastrukturlarının təhlükəsizliyini və dayanıqlığını gücləndirmək məqsədi daşıyır.

(https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:EN:PDF)

Məlumatda informasiya sistemlərinə hücumlar, mobil qurğuların tətbiqinin artması, “kənar məlumatın” daxil olması və istifadəçilərin maarifləndirilməsi Avropa Komissiyası tərəfindən dialoq, tərəfdaşlıq və səlahiyyətlərin verilməsi yolu ilə həll edilməli məqsəd kimi qarşıya qoyulan əsas təhlükəsizlik məsələləri qismində qeyd olunur. Bu strategiyalara müvafiq Məlumatda nəzər salmaq olar (bax, Çərçivə 2).

Çərçivə 2. Avropa Komissiyasının çoxtərəfli dialoqu

Komissiya açıq, əhatəli və çoxtərəfli dialoq təsis etmək üçün bir sıra tədbirlər təklif etmişdir:

- Aİ boyu daha geniş məkanda tətbiq edilə bilməsi üçün ən effektiv təcrübələrin müəyyənləşdirilməsinə kömək etmək üçün şəbəkə və informasiya təhlükəsizliyi ilə bağlı milli siyasətlər üzrə modelləşdirmə işi. Xüsusilə də, bu tapşırıq, kiçik və orta müəssisələri və vətəndaşları şəbəkə və informasiya təhlükəsizliyi ilə bağlı risklər və problemlər barədə maarifləndirmək üçün qabaqcıl təcrübələri müəyyən edəcəkdir; və

13 Avropa "Təhlükəsiz informasiya cəmiyyəti üçün strategiya (2006-cı il məlumatı)", Avropa Komissiyası, http://europa.eu/legislation_summaries/information_society/internet/l24153a_en.htm.

- Mövcud tənzimləyici sənədlərin ən yaxşı halda necə tətbiq edilməsinə dair çoxtərəfli müzakirə. Bu müzakirə konfranslar və seminarlar kontekstində təşkil olunacaqdır.

Tərəfdaşlıq

Effektiv siyasətin işlənib hazırlanması üçün həll edilməli olan problemlərin mahiyyətini aydın şəkildə qavrama, habelə etibarlı, yeni statistic və iqtisadi məlumatlar tələb olunur. Müvafiq olaraq, Komissiya ENİSA-dan aşağıdakıları xahiş edəcəkdir:

- Məlumatların toplanması üçün müvafiq çərçivəni inkişaf etdirmək məqsədilə, üzv-dövlətlərlə və maraqlı tərəflərlə inama söykənən tərəfdaşlığın qurulması; və
- Təhdidlərə effektiv şəkildə cavab verilməsinə şərait yaratmaq üçün Avropa informasiya mübadilə və həyəcan sisteminin tətbiqinin mümkünlüyünü araşdırmaq. Bu sistem təhdidlərə, risklərə və xəbərdarlıqlara dair uyğunlaşdırılmış informasiyanı təmin etmək üçün çoxdilli Avropa portalı da əhatə edir.

Paralel olaraq, Komissiya, İKT təhlükəsizliyi sahəsinə aid məlumatın mövcudluğunu təmin etmək məqsədilə tərəfdaşlıq qurmaq üçün üzv-dövlətləri, özəl sektoru və tədqiqatçıları dəvət edəcəkdir.

2009-cu ilin martında, Komissiya, Mühüm İnformasiya İnfrastrukturunun Mühafizəsinə dair Məlumatı (CİİP) - "Avropanı iri miqyaslı kiber hücumlardan və pozuntulardan qoruma: hazırlığı, təhlükəsizliyi və davamlılığı artırma" başlıqlı məlumatı qəbul etmişdir.[14] O, mühüm İKT infrastrukturlarının təhlükəsizliyini və davamlılığını artırmaq üçün planı müəyyən edir (CİİP fəaliyyət planı). Məqsəd həm milli, həm də Avropa səviyyələrində yüksək səviyyədə hazırlığın, təhlükəsizliyin və davamlılığın inkişaf etdirilməsini həvəsləndirmək və buna dəstək göstərməkdir. Bu yanaşma 2009-cu ildə geniş şəkildə qəbul olunmuşdur.[15]CİİP planı dörd istiqamət üzərində qurulur: (1) hazırlıq və qarşısını alma; (2) aşkar etmə və cavab tədbirləri; (3) yüngülləşdirmə və bərpa; (4) beynəlxalq əməkdaşlıq; və (5) İKT sahəsində Avropanın mühüm infrastrukturları üçün meyarlar. CİİP fəaliyyət planı, hər bir istiqamət üzrə, ENİSA-nın dəstəyi ilə, Komissiya tərəfindən görülməli olan işi müəyyən edir.

Avropa üçün Rəqəmsal Gündəlik[16] (DAE) 2010-cu ilin may ayında qəbul edilmişdir və bununla əlaqədar Şuranın yekun qərarlarında[17] belə bir ümumi məqam vurğulanır ki, İKT-nin geniş şəkildə qəbul olunması və beləliklə də Avropanın 2020-ci il Strategiyasının "planlaşdırılan artım" ölçüsünün məqsədlərinə nail olmaq üçün inam və təhlükəsizlik basilica şərtlərdir.[18] DAE, İKT infrastrukturlarının təhlükəsizliyini və davamlılığını təmin etmək üçün vahid səylərdə bütün maraqlı tərəflərin öz qüvvələrini birləşdirməli olduqlarını vurğulayır. Buna nail olmaq üçün, DAE, həmin neqativ halların qarşısını alma, hazırlıq və maarifləndirməyə diqqət yetirmə, habelə kiber hücumların və kibercinayətkarlığın yeni və daha mürəkkəb formalarına qarşı tədbir görmək üçün effektiv və əlaqələndirilmiş mexanizmləri inkişaf etdirmə tələbini vurğulamışdır. Bu yanaşma, məsələnin həm preventiv, həm də cavab ölçülərinin lazımi şəkildə nəzərə alınmasını təmin edir.

Rəqəmsal Gündəlikdə bəyan edilmiş aşağıdakı tədbirlər görülmüşdür:

---

14 Avropa Cəmiyyətlərinin Komissiyası, " Mühüm İnformasiya İnfrastrukturunun Mühafizəsinə dair Məlumatı (CİİP) - Avropanı iri miqyaslı kiber hücumlardan və pozuntulardan qoruma: hazırlığı, təhlükəsizliyi və davamlılığı artırma" başlıqlı məlumat", Məlumat COM (2009) 149 inal, 30 mart 2009-cu il, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF.

15 Şəbəkə və informasiya təhlükəsizliyinə ümumi Avropa yanaşmasına dair Şuranın 18 dekabr 2009-cu il tarixli qərarı (2009/C321/01).

16 Avropa Komissiyası, "Avropa üçün Rəqəmsal Gündəlik" , Communication COM (2010) 245, 19 may 2010-cu il, http://ec.europa.eu/ information_society/digital-agenda/documents/digital-agenda-communication-en.pdf.

17 Avropanın Rəqəmsal Proqramına dair Şuranın 31 may 2010-cu il tarixli yekun qərarları (10130/10).

18 COM(2010) 2020 və Avropa Şurasının 25/26 mart 2010-cu il tarixli yekun qərarları (EUCO 7/10).

- Komissiya 2010-cu ilin sentyabr ayında İnformasiya sistemlərinə qarşı hücumlara dair Direktiv üçün təklifi qəbul etmişdir.[19]Onun məqsədi, üzv-dövlətlərin cinayət hüququ sistemlərini yaxınlaşdırmaqla və məhkəmə və digər səlahiyyətli orqanlar arasında əməkdaşlığı yaxşılaşdırmaqla kibercinayətkarlığa qarşı mübarizəni gücləndirməkdir. O, həmçinin, kiberhücumların yeni formaları, xüsusilə də botnetlərlə mübarizə üzrə müddəalara da malikdir.

- Bunun davamı olaraq, Komissiya, inamı və şəbəkə təhlükəsizliyini artırmaq məqsədilə, ENİSA-nı gücləndirmək və yeniləşdirmək üçün yeni mandatla da bağlı təklif[20] irəli sürmüşdür. ENİSA-nı gücləndirmə və yeniləşdirmə, kibertəhlükəsizliklə bağlı problemlərin qarşısını almaq, onları aşkar etmək və onlara qarşı cavab tədbirləri görmək üçün Aİ, üzv-dövlətlərə və özəl sektor tərəfdaşlarına kömək edəcəkdir.

Avropa Şurasının Kibercinayətkarlıq haqqında Konvensiyası

2001-ci ildə, Aİ, Avropa Şurasının "kibercinayətkarlığa qarşı qanunvericiliyini inkişaf etdirmək istəyində olan bütün hökumətlər üçün rəhbər prinsipləri müəyyən edən" və "bu sahədə beynəlxalq əməkdaşlıq üçün çərçivəni təmin edən" Kibercinayətkarlıq haqqında Konvensiyasını (CECC) bəyan etmişdir. Otuz doqquz Avropa ölkəsi, bundan əlavə Kanada, Yaponiya, Cənubi Afrika və ABŞ bu müqaviləni imzalamışlar. Bu, 2004-cü ilin iyul ayında qüvvəyə minən Konevnsiyanı "bu mövzu üzrə bu gün qüvvədə olmaqla öhdəlik yaradan yeganə beynəlxalq müqavilə" edir.[21]

Avropa Şəbəkə və İnformasiya Təhlükəsizliyi Agentliyi

ENİSA (Avropa İttifaqı) "Birlik çərçivəsində şəbəkə və informasiya təhlükəsizliyinin artırılmasına kömək etmək və vətəndaşların, istehlakçıların, biznes və ictimai sektor təşklilatlarının faydalanması üçün şəbəkə və informasiya təhlükəsizliyi mədəniyyətini inkişaf etdirmək üçün" 10 mart 2004-cü ildə Avropa Parlamenti və Aİ Şurası tərəfindən təsis olunmuşdur.

2006-cı ilin may ayında ifadə olunmuş Maraqlı Tərəflərin Daimi Qrupunun (PSG) ENİSA ilə bağlı Baxışında[22] ENİSA-ya şəbəkə və informasiya təhlükəsizliyi mərkəzi, NİS maraqlı tərəfləri üçün bir forum və bütün Aİ vətəndaşları üçün informasiya təhlükəsizliyinə dair maarifləndirmə qüvvəsi kimi nəzər salınır. Bu məqsədlə, ENİSA üçün PSG Baxışında aşağıdakı uzun-müddətli tədbirlər nəzərdə tutulmuşdur (bax, Şəkil 6):

---

19 Avropa Komissiyası, "İnformasiya sistemlərinə qarşı hücumlara dair Avropa Parlamentinin və Şuranın Direktivi və Şuranın Çərçivə Qərarının ləğvi üçün təklif", Brüssel, 20 sentyabr 2010-cu il, http://www.statewatch.org/news/2010/sep/ceu-com-atacks-on-info-systems-com-517-10.pdf.

20 Avropa Komissiyası, "Avropa Şəbəkə və İnformasiya Təhlükəsizlik Agentliyi (ENİSA) ilə bağlı Avropa Parlamentinin və Şuranın Qərarı üçün Təklif", Brüssel, 30 sentyabr 2010-cu il, http://www.coe.int/t/dghl/standardsetting/t-cy/Proposal%20new%20regulation%20ENISA.pdf.

21 Avropa Şurası, "Kibercinayətkarlıq: demokratiyaya, insan hüquqlarına və qanunun aliliyinə təhlükə", http://www.coe.int/t/dc/files/themes/cybercrime/default_en.asp.

22 Paul Dorey və Simon Perri, eds., PSG-nin ENİSA ilə bağlı Baxışı" (Maraqlı Tərəflərin Daimi Qrupu, 2006-cı il), http://www.enisa.europa. eu/about-enisa/structure-organization/psg/files/psg-vision.

Şəkil 6. ENİSA üçün uzun-müddətli fəaliyyət

Mənbə: Paul Dorey və Simon Perri, eds., PSG-nin ENİSA ilə bağlı Baxış" (Maraqlı Tərəflərin Daimi Qrupu, 2006-cı il), http://www.enisa.europa. eu/about-enisa/structure-organization/psg/files/psg-vision.

1. Üzv-dövlətlərin milli şəbəkə və informasiya təhlükəsizliyi orqanlarının əməkdaşlığı və əlaqələndirilməsi

Hazırda milli orqanlar arasında əməkdaşlıq çox aşağı səviyyədədir. Milli orqanlar arasında artmaqda olan əlaqə və əməkdaşlığa, xüsusilə də qabaqcıl orqanların yenicə başlamış orqanlarla qabaqcıl təcrübəni bölüşmələrinə şərait yaratmaqla xeyli faydalı iş görmək olar.

2. Tədqiqat institutları ilə əməkdaşlıq

ENİSA-nın məqsədi real-dünya sistemlərində həqiqi təhlükəsizlik risklərinin idarə olunması üçün ən çox faydalı olan sahələrə diqqət yetirmək məqsədilə, əsas tədqiqat və hədəf seçilmiş texniki inkişafı istiqamətləndirməkdir. ENİSA özü tədqiqat proqramını dəstəkləməməlidir, bunun əvəzinə mövcud prosesləri və mövcud proqramların prioritetlərini uyğunlaşdırmaq istiqamətində fəaliyyət göstərməlidir.

3. Proqram təminatı və kompüter avadanlığını satanlarla əməkdaşlıq

Proqram təminatı və avadanlıq satanlar rəqabət aparan tərəflərdir və onların qarşılıqlı təcrübələr üzrə açıq şəkildə razılığa gəlmələri çətin ola bilər. ENİSA obyektiv rəy və həssas mövzularda müzakirələr üçün bir forum təmin edə, eyni zamanda antirəqabət davranışa qarşı zəruri olan mühiti saxlaya bilər.

ENİSA-nın uzun-müddətli baxışında, hazırda tədricən artmaqda olan təhlükəsizlik meyllərinin genişləndirilməsi əvəzinə, zərərvericilərə (soxulcanlara) və digər problemlərə qarşı dayanıqlı olan daha etibarlı şəbəkə və informasiya texnologiyalarının yaradılmasına yönəldilməlidir. Buna, düzgün, təhlükəsiz və etibarlı quruluşları və proqram təminatlarını inkişaf etdirmək üçün üsulları təşviq etməklə nail olmaq olar.

4. Standartları müəyyən edən qurumlarda iştirak

Ən böyük dəyərə malik təşəbbüslərin müəyyənləşdirilməsinə və yayılmasına diqqət yetirməklə, ENİSA standartları müəyyənləşdirən qurumlarda NİS-lə bağlı mövzuları izləməyi və onları nəzarətdə saxlamalı, o cümlədən təhlükəsizliklə bağlı mövcud olan müxtəlif təsdiqetmə və akkreditasiya qurumlarının işini izləməlidir.

5. Lobbiçilik və rəylərin verilməsi ilə qanunvericilik prosesində iştirak

ENİSA, NİS-lə bağlı məsələlər üzrə direktivlərin və digər qanunvericilik aktlarının layihələrinin hazırlanması və təklif olunması prosesində ilk əvvəl dinlənilməli olan etibarlı məsləhətverici quruma çevrilmək üçün çalışmalıdır.

6. İstifadəçi təşkilatlarla işləmə

Çox vaxtı proqram təminatı və avadanlıq satan tərəflərdən fərqli olaraq, istifadəçi təşkilatlar qanunvericilik və standartları müəyyənləşdirən qurumlarda təmsil olunmurlar. ENİSA son istifadəçi qruplarının standarlartlaşdırma işi barədə xəbərdar olmalarını və onların bu işə təsir göstərmə imkanına malik olmalarını təmin edə bilər.

7. Son istifadəçilər üçün üzv-dövlətlərin qabaqcıl təcrübələrinin müəyyənləşdirilməsi və təşviq olunması

ENISA yalnız biznes maraqlarını qorumamalı, eyni zamanda son istifadəçilərin İnternetdən və rəqəmsal mediadan istifadəyə inamını artırmalıdır.

8. Eyniləşdirmə məlumatlarını idarə etmək üçün texniki və siyasi həll yollarının tapılması istiqamətində fəaliyyət göstərmə

İnternetə inamın olmaması geniş-miqyaslı istehlakçı-yönümlü e-biznes üçün əsas maneədir. Saytın sahibinin şəxsiyyətini, e-poçt ünvanını və bəzi onlayn xidmətləri dəqiq şəkildə yoxlamaq imkanına malik olma ümumi istifadəçinin İnternetə inamının yenidən bərpa olunması və artırılması istiqamətində iri bir addım olardı. Sənayenin öndə dayandığı proseslər vasitəsilə bu sahədə texniki həll yolları axtarılmalıdır, lakin ENİSA onlayn qurumların eyniləşdirilməsi üçün bütün Aİ məkanı üçün siyasətlərin işlənib hazırlanması istiqamətində iş apara bilər.

9. Həm "informasiya", həm də "şəbəkə" təhlükəsizliyi məsələləri üçün səylərin tarazlaşdırılması

ENİSA, bütün Avropa boyu biznes müəssisələrinin və istehlakçılarının faydalanması üçün qabaqcıl təcrübələrin müəyyənləşdirilməsində ən iri İnternet və şəbəkə xidmət təminatçılarına (İSP-lər/NSP-lər) kömək etmək üçün onlarla əlaqədə olmalıdır. İSP-lərin/NSP-lərin bütövlükdə İnternetdə təhlükəsizliyin artırılmasında mühüm rol oynaya biləcəyinə görə, bu, vacibdir. Hazırda İSP-lər tərəfindən görülən tədbirlərlə bağlı əməkdaşlıq və əlaqələndirmə lazımi səviyyədə deyildir.

Mənbə: Paul Dorey və Simon Perri, eds., PSG-nin ENİSA ilə bağlı Baxışı" (Maraqlı Tərəflərin Daimi Qrupu, 2006-cı il), http://www.enisa.europa. eu/about-enisa/structure-organization/psg/files/psg-vision.

ENİSA, "Avropa Birlik Agentliyi" qismində fəaliyyət göstərməklə, informasiya təhlükəsizliyi sahəsində xüsusi texniki, elmi vəzifələri həyata keçirmək üçün Aİ tərəfindən təsis olunmuş ekpertiza qurumudur. Agentlik, həmçinin, NİS sahəsində Birliyin qanunvericiliyini yenilmək və inkişaf etdirmək üçün texniki hazırlı işində Avropa Komissiyasına yardım edir.

ENİSA-nın əsas vəzifələri aşağıdakılara yönəlmişdir:

- Komissiyaya və üzv-dövlətlərə, informasiya təhlükəsizliyi üzrə və onların avadanlıq və proqram təminatı məhsullarında təhlükəsizliklə bağlı problemlərin həlli üçün sənaye ilə dialoqunda məsləhətlərin verilməsi və yardım etmə.
- Avropada təhlükəsizliklə bağlı hadisələrə və meydana çıxan risklərə dair məlumat toplama və onları təhlil etmə.
- İnformasiya təhlükəsizliyinə təhdidlərin qarşısını alma potensialını artırmaq üçün risk dəyərləndirmə və risk idarəetmə metodlarını təşviq etmə.
- İnformasiya təhlükəsizliyi sahəsində müxtəlif iştirakçılar arasında, xüsusən də bu sahədə sənaye ilə dövlət – özəl sektor tərəfdaşlığını inkişaf etdirməklə maarifləndirmə və əməkdaşlıq.

Koreya Respublikasının informasiya təhlükəsizliyi strategiyası

2006-cı ilin dekabrında Koreya hökuməti "Hər yerdə informasiya təhlükəsizliyi üzrə Əsas Strategiya" adlı hərtərəfli strategiya yaratdı. Strategiyanın əsas məqsədləri koreyalıların maliyyə, təhsil və tibbi xidmətlər də daxil olmaqla bütün sahələrdə İKT xidmətlərindən təhlükəsiz istifadə edə bilmələrini təmin etməkdir; və şəxsi toxunulmazlığın qorunması və yaxşı məlumat istifadəsi mühitinin həyata keçirilməsi. Hər yerdə İnformasiya Təhlükəsizliyi üzrə Əsas Strategiya u-Təhlükəsizlik, u-Toxunulmazlıq, u-İnam və u-Təmizi əhatə etmək üçün informasiyanın mühafizəsi konsepsiyasını genişləndirir.

1980-ci illərin ortalarından Koreya Respublikası milli informasiyalaşdırma planını həyata keçirməyə başlamışdır və indi görünür ki, artıq stabilləşmə mərhələsinə çatmışdır, lakin bir milli məqsəd kimi, informasiya təhlükəsizliyi, 2000-ci ilin ortalarından başlayaraq nisbətən yeni diqqət yetirilən məsələdir. Həmin vaxtı aparılan araşdırmalar onu göstərmişdir ki, İKT sistemi / maliyyə tərəzisi və müvafiq infrastruktur və tədqiqat və inkişafla bağlı səylər hamısı çox zəifdir. Beləliklə, Koreya hökuməti, geniş plan əsasında hərəkət etməklə addım-addım əsas İKT infrastrukturu yaratmağa qərar vermişdir. 2008-ci ilin iyul ayında, hökumət, İnformasiya təhlükəsizliyi üzrə aralıq-müddət üçün geniş planı həyata keçirməyə başlamışdır. Bu plan aşağıda göstərilən altı proqramı özündə birləşdirir:

1. Kiber-hücumları dəf etmək üçün ölkənin potensialını artırma
2. Mühüm milli informasiya infrastrukturlarının mühafizəsini gücləndirmə
3. Fərdi informasiyanın mühafizə sistemini gücləndirmə
4. İnformasiya təhlükəsizliyi infrastrukturlarını genişləndirmə
5. İnformasiya təhlükəsizliyi sənayesinin rəqabət qabiliyyətini artırma
6. İnformasiya təhlükəsizliyi mədəniyyətini yaratma

2019-cu ilin aprel ayında Milli Təhlükəsizlik İdarəsi 18 əsas vəzifəyə və 73 ətraflı vəzifəyə bölünmüş altı strateji vəzifəni təmin edən Milli Kibertəhlükəsizlik Strategiyasını nəşr etdi. Bu plan çərçivəsində hökumət elektron dövlət xidmətlərinin etibarlılığını təmin etmək, vətəndaşların narahatlığını azaltmaq və biznes fəaliyyətində dürüstlüyün təmin edilməsi yolu ilə təhlükəsiz və hər yerdə mövcud cəmiyyət yaratmaq məqsədini açıqlayıb.

Altı strateji missiya və 18 əsas missiya aşağıdakılardır:

1. Milli əsas infrastrukturun təhlükəsizliyini artırın

    a. Milli informasiya və kommunikasiya şəbəkələrinin təhlükəsizliyinin gücləndirilməsi

    b. Kritik infrastruktur üçün kibertəhlükəsizlik mühitinin təkmilləşdirilməsi

    c. Yeni nəsil kibertəhlükəsizlik infrastrukturunun inkişaf etdirilməsi

2. Kiber hücumlara cavab bacarıqlarını təkmilləşdirin

    a. Kiberhücumların qarşısının alınmasını təmin etmək

    b. Genişmiqyaslı kiberhücumlara hazırlığı gücləndirmək

    c. Kiberhücumlara qarşı hərtərəfli və aktiv əks-tədbirlər aparmaq

    d. Kibercinayətkarlıqla mübarizə imkanlarını təkmilləşdirmək

3. Güvən və əməkdaşlığa əsaslanan idarəçilik qurun

    a. Dövlət-özəl hərbi əməkdaşlıq sistemini asanlaşdırmaq

    b. Ümummilli məlumat mübadiləsi sisteminin yaradılması və asanlaşdırılması

    c. Kibertəhlükəsizlik üçün hüquqi bazanın gücləndirilməsi

4. Kibertəhlükəsizlik sənayesinin inkişafı üçün təməllər qurun

    a. Kibertəhlükəsizlik investisiyalarını genişləndirin

    b. Kibertəhlükəsizlik işçi qüvvəsinin rəqabət qabiliyyətini gücləndirmək və texnologiya

    c. Kibertəhlükəsizlik şirkətləri üçün artımı təşviq edin

    d. Kibertəhlükəsizlik bazarında ədalətli rəqabət prinsipinin yaradılması

5. Kibertəhlükəsizlik mədəniyyətini inkişaf etdirin

    a. Kibertəhlükəsizlik üzrə məlumatlılığın artırılması və kibertəhlükəsizlik təcrübələrinin gücləndirilməsi

    b. Əsas hüquqları kibertəhlükəsizliklə balanslaşdırın

6. Kibertəhlükəsizlik üzrə Beynəlxalq Əməkdaşlığa rəhbərlik edin

a. İkitərəfli və çoxtərəfli əməkdaşlıq sistemlərinin zənginləşdirilməsi

b. Beynəlxalq əməkdaşlıqda inamlı liderlik

Koreya Respublikası Hökuməti hesab edir ki, kibertəhlükəsizlik təkcə hökumətin deyil, həm də fiziki şəxslərin və müəssisələrin iştirakını tələb edir və hökumət bu məqsədlə əməkdaşlığı gücləndirəcək və qapıları açacaqdır və ictimai etimada əsaslanan kibertəhlükəsizlik siyasətini davamlı şəkildə həyata keçirmək məqsədi ilə siyasətin şəffaflığını artıracaqdır.

Yaponiyanın informasiya təhlükəsizliyi strategiyası[23]

Yaponiyanın cari kibertəhlükəsizlik strategiyası 2018-ci ilin iyulunda dərc edilib. Kibertəhlükəsizlik üzrə Strateji Qərargah 2014-cü ilin noyabrında kibertəhlükəsizlik siyasətini effektiv və hərtərəfli təşviq etmək məqsədilə yaradılıb və Nazirlər Kabinetinin Baş Katibi rəhbərlik edir. 2005-ci ildə yaradılan Milli İnformasiya Təhlükəsizliyi Mərkəzi (NISC) Kibertəhlükəsizlik üzrə Milli İnsidentlərə (Hadisələrə) Hazırlıq və Strategiya Mərkəzinə (NISC-National Centre for Incident readiness and Strategy for Cybersecurity) çevrildi və müxtəlif sahələrdə dövlət və özəl sektorlarla əməkdaşlıq edərək "Azad, ədalətli və təhlükəsiz kiberməkan" yaratmaq üçün Kibertəhlükəsizlik Strategiyası Qərargahının katibliyi kimi fəaliyyət göstərir. NİSC Yaponiyada informasiya təhlükəsizliyi ilə bağlı fəaliyyətə nəzarət edən əsas təşkilatdır.

NİSC hökumət CERT və NISC və JPCERT/CC rolunu öz üzərinə götürür, özəl qurumları əhatə edən CERT qismində milli CERT kimi birgə fəaliyyət göstərir. Milli İnformasiya Təhlükəsizliyi Mərkəzi yeddi qrupdan ibarətdir. Hər birindən öz rollarını və planlarını qurmaq və onları idarə etmək tələb olunur (cədvəl 4-ə bax).

Cədvəl 4: Kibertəhlükəsizlik üzrə Milli Strategiyaya əsaslanan rollar və cavabdeh Qrup

Rollar	Qrup
Kibertəhlükəsizlik siyasəti üzrə orta və uzunmüddətli planın formalaşdırılması və kibertəhlükəsizlik texnologiyası tendensiyalarının tədqiqi və təhlilinin aparılması və s	Strategiya və siyasət planlaması
Kibertəhlükəsizlik siyasəti üzrə beynəlxalq əməkdaşlığın təşviqi	Beynəlxalq strategiya
Auditin əsasını təşkil edən dövlət orqanlarının informasiya təhlükəsizliyi tədbirlərinin təşviqi üçün vahid standartların formalaşdırılması və fəaliyyət göstərməsi	Dövlət qurumları üçün hərtərəfli tədbirlər
Kiberhücumlar və Hökumət Təhlükəsizliyi Əməliyyatlarının Koordinasiya Qrupunun (GSOC) fəaliyyəti haqqında ən son məlumatların toplanması	Kibertəhlükəsizlik məlumatının inteqrasiyası və uyğunlaşdırılması
Kritik İnfrastrukturun Mühafizəsi üçün Kibertəhlükəsizlik Siyasəti əsasında kibertəhlükəsizlik tədbirlərində dövlət-özəl tərəfdaşlığının yaradılması	Kritik infrastrukturun mühafizəsi

[23] Bu bölüm NİSC-dən götürülmüşdür, "Yaponiya hökumətinin informasiya təhlükəsizliyi məsələlərini həll etmək üçün səyləri: Kabinetin Katibliyinin səylərinə diqqət yetirmə". təqdimat, 2007-ci ilin noyabr ayı, http://www.nisc.go.jp/eng/.

Məqsədli e-poçtların və zərərli proqramların təhlili və digər kiberhücum hallarının araşdırılması	Hadisənin tədqiqi və təhlili
2020-ci il Tokio Olimpiya və Paralimpiya Oyunları üçün kibertəhlükəsizlik tədbirlərinin təşviqi	Tokio 2020

Mənbə (dəyişiklik ilə): NISC, http://www.nisc.go.jp/eng/.

Mövcud Kibertəhlükəsizlik Strategiyası 2018-ci ilin iyul ayında dərc edilmiş Kibertəhlükəsizlik üzrə Əsas Akt çərçivəsində ikincidir. Kibertəhlükəsizlik siyasətini təşviq etmək üçün 2015-ci ildən etibarən Kibertəhlükəsizlik üzrə Əsas Akt həyata keçirilir:

• Kibertəhlükəsizlik siyasətinin əsas prinsiplərinin müəyyən edilməsi;

• Hökumətin, özəl qurumların və vətəndaşların öhdəliklərinin aydınlaşdırılması;

• Kibertəhlükəsizlik strategiyasının formalaşdırılması və Kibertəhlükəsizlik üzrə Strateji Qərargahın yaradılması kimi kibertəhlükəsizlik siyasəti üçün çərçivənin müəyyən edilməsi

Cari Kibertəhlükəsizlik Strategiyasının icmalı aşağıdakı kimidir (strategiyanın xülasəsi üçün Şəkil 7-yə baxın).

Şəkil 7

Məqsədlər, prinsiplər, fəlsəfə və yanaşmalar
-Azad, ədalətli və təhlükəsiz kiberməkanın inkişaf etdirilməsi
1. Sosial-iqtisadi canlanma və davamlı inkişafa töhfə verilməsi
2. Təhlükəsiz Cəmiyyət
3. Beynəlxalq Sülh və Milli Təhlükəsizlik

-Aşağıdakı prinsiplərə əsaslanır
1. Sərbəst məlumat axını
2. Qanunun aliliyi
3. Açıqlıq
4. İnternetin muxtariyyəti
5. Müxtəlif Maraqlı Tərəflərin Əməkdaşlığı

-Kibertəhlükəsizlik Ekosistemini təşviq etmək fəlsəfəsi ilə aşağıdakı yanaşmalarla kibertəhlükəsizliyin təşviq edilməsi
1. Missiyanın Təminatı
2. Risklərin idarə edilməsi
3. İştirak, Koordinasiya və Əməkdaşlıq

Şəkil 7. Milli Kibertəhlükəsizlik strategiyasının konturları

- **Məqsədlərə çatmaq üçün tədbirlər**

Sosial-İqtisadi Canlılıq və Davamlı İnkişaf
1. Kibertəhlükəsizlik Dəyər Yaradıcısı kimi
2. Müxtəlif Əlaqələrdən Dəyər Yaradan Təchizat Zəncirinin həyata keçirilməsi
3. Təhlükəsiz IoT Sistemlərinin yaradılması

İnsanlar üçün etibarlı və təhlükəsiz cəmiyyət
1. Proaktiv Kibermüdafiə və Kibercinayətkarlıqla Mübarizə səyləri
2. PPP vasitəsilə Kritik İnfrastrukturun Mühafizəsi
3. Beynəlxalq Hökumətin Təhlükəsizlik Tədbirlərinin Gücləndirilməsi
4. Akademiya və Tədqiqat İnstitutlarında kibertəhlükəsizlik
5. "2020-ci ildən sonra" nəzərdə tutulan Tokio 2020 üçün CS
6. Yeni Məlumat Paylaşımı və Əməkdaşlıq Çərçivəsi
7. Kütləvi Kiberhücum Böhranına Hazırlığın Artırılması

Sülh və beynəlxalq cəmiyyətin stabillliyi və milli təhlükəsizlik
1. Azad, Ədalətli və Təhlükəsiz Kiberməkana sadiqlik
2. Müdafiə, Çəkindirmə və Situasiya Məlumatlılığının Gücləndirilməsi
3. Beynəlxalq əməkdaşlıq və əlaqələr

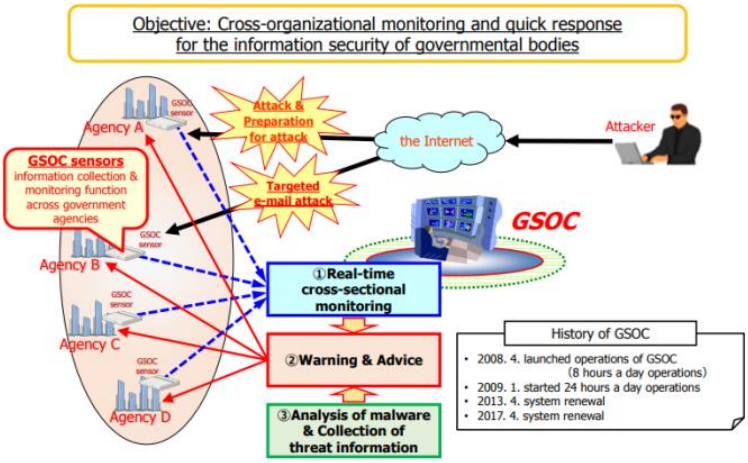
Ümumi kəsişən tədbirlər

İnsan resurslarının inkişafı
R&D Təşviqi
Kiber Gigiyena Bütün Maraqlı Tərəflərin Tam İştirakı

Hökumət Şəbəkəsi

Milli Informasiya Təhlükəsizlik Mərkəzi, Hökumət Təhlükəsizliyi Əməliyyatlarının Koordinasiya qrupu (GSOC) adlı real vaxt rejimində hökumət səviyyəsində monitorinq qrupunu idarə edir. Hökümət Təhlükəsizliyi Əməliyyatlarının Koordinasiya Qrupu (GSOC) təkcə hökumətə məxsus sistemlərə daxil olan və ya onlardan çıxan zərərli rabitələrə nəzarət etmir, həm də dövlət qurumları arasında məlumat mübadiləsi çərçivəsi kimi işləyir. Hökümət Təhlükəsizliyi Əməliyyatlarının Koordinasiya Qrupu (GSOC) şübhəli siqnallar və ya zərərli proqramlar aşkar etdikdə dövlət qurumları üçün xəbərdarlıqlar və məsləhətlər verir.

Şəkil 8: Hökumət Təhlükəsizliyi Əməliyyatlarının Koordinasiya qrupu (GSOC)



Kritik İnfrastruktur

2005-ci ildən etibarən "Kritik infrastrukturun qorunması üçün kibertəhlükəsizlik siyasəti" kritik infrastrukturun mühafizəsi üçün məsuliyyət daşıyan hökumət və müvafiq qoruyucu tədbirləri müstəqil həyata keçirən mühüm infrastruktur operatorları tərəfindən paylaşılan ümumi fəaliyyət planı kimi müəyyən edilmişdir və 4-cü nəşr 2017-ci ildə nəşr edilmişdir.

Bu sənəd 14 sektoru kritik infrastruktur kimi müəyyən edir və maraqlı tərəflərdən aşağıdakı beş tədbiri həyata keçirmələrini gözləyir.

• Təhlükəsizlik prinsiplərinin inkişafı və nüfuzu

• Məlumat mübadiləsi sisteminin təkmilləşdirilməsi

• Hadisəyə cavab vermək qabiliyyətinin gücləndirilməsi

• Risklərin idarə edilməsi və hadisəyə hazırlığın hazırlanması

• Kritik infrastrukturun mühafizəsi üçün əsasların yaradılması

Düşünməli suallar

1. Ölkənizdəki informasiya təhlükəsizliyi tədbirləri yuxarıda təsvir edilənlərdən nə dərəcədə fərqlənir?

2. Bu bölmədə qeyd olunan ölkələrdə sizin ölkənizdə tətbiq olunmayan və ya ona aid edilməyən informasiya təhlükəsizliyi tədbirləri həyata keçirilirmi? Əgər belədirsə, hansıları və nə üçün tətbiq oluna bilməz və ya uyğun deyil.

3.3 Beynəlxalq səviyyədə informasiya təhlükəsizliyi tədbirləri

Birləşmiş Millətlər Təşkilatının informasiya təhlükəsizliyi ilə bağlı həyata keçirdiyi tədbirlər

BMT tərəfindən maliyyələşdirilən **İnformasiya Cəmiyyəti üzrə Ümumdünya Zirvə Toplantısında** (İCÜS)[24]informasiya cəmiyyətinin effektiv inkişafı və "informasiya bərabərsizliyinin" aradan qaldırılması üçün prinsiplər bəyannaməsi və fəaliyyət planı qəbul edilmişdir. Fəaliyyət planında aşağıdakı fəaliyyət istiqamətləri müəyyən edilir:

- İnkişaf naminə İKT-lərin təşviqində hökumətlərin və bütün maraqlı tərəflərin rolu
- Əhatəli informasiya cəmiyyəti üçün informasiya və kommunikasiya infrastrukturu mühüm əsas kimi
- Informasiya və biliklərə çıxış imkanı
- Potensialın inkişaf etdirilməsi
- İKT-lərdən istifadədə inam və təhlükəsizlik yaratma
- Əlverişli mühit yaratma

- Həyatın bütün aspektlərində İKT-nin tətbiqi
- Mədəni müxtəliflik, şəxsiyyət, dil müxtəlifliyi və yerli məzmun
- Media
- İnformasiya Cəmiyyətinin etik ölçüləri
- Beynəlxalq və regional əməkdaşlıq[25]

İnternet İdarəçilik Forumu (İİF)[26]İnternet idarəçilik məsələləri üzrə BMT-nin yardımçı qurumudur. O, İnternet idarəçiliyi ilə bağlı problemləri müəyyən etmək və həll etmək üçün Tunisdə İCÜS-nin ikinci mərhələsindən sonra təsis edilmişdir. 12 – 15 noyabr 2007-ci il tarixlərdə Braziliyanın Rio-de-Janeyro şəhərində ikinci İİF forumunda diqqət kiberterrorçuluq, kibercinayətkarlıq və İnternetdə uşaqların təhlükəsizliyi kimi informasiya təhlükəsizliyi məsələlərinə yönəldilmişdir.

OECD-nin informasiya təhlükəsizliyi tədbirləri[27]

İqtisadi Əməkdaşlıq və İnkişaf Təşkilatı (OECD) 30 bazar demokratiyasının hökumətlərinin qloballaşan dünya iqtisadiyyatında üzləşilən iqtisadi, sosial, ekoloji və idarəçiliklə bağlı problemləri həll etmək üçün biznes və vətəndaş cəmiyyəti ilə birgə işlədiyi yeganə forumdur. OECD çərçivəsində, İKT-nin informasiya təhlükəsizliyinə və Şəxsi həyatın toxunulmazlığına təsirini təhlil etmək və İnternet iqtisadiyyatına inamın saxlanması üçün siyasətlə bağlı tövsiyələr hazırlamaq məqsədilə İnformasiya, Kompyuter və Kommunikasiya Siyasəti üzrə

---

24 İnformasiya Cəmiyyəti üzrə Ümumdünya Sammiti, "Əsas informasiya: İCÜS haqqında", http://www.itu.int/wsis/basic/about.html

25 İnformasiya Cəmiyyəti üzrə Ümumdünya Sammiti, "Fəaliyyət planı", 12 dekabr 2003-cü il, http://www.itu.int/wsis/docs/geneva/official/poa.html.

26 İnternet İdarəçilik Forumu, http://www.intgovforum.org.

27 Bu bölüm WPISP-dən götürülmüşdür, "İnformasiya Təhlükəsizliyi və Şəxsi həyatın toxunulmazlığı üzrə İşçi Qrup" (may 2007-ci il)

Komitənin nəzdində İnformasiya Təhlükəsizliyi və Şəxsi həyatın toxunulmazlığı üzrə İşçi Qrup (WPISP) fəaliyyət göstərir.

WPISP-nin informasiya təhlükəsizliyi üzrə fəaliyyəti: 2002-ci ildə, OECD, "informasiya sistemlərinin və şəbəkələrinin inkişaf etdirilməsində təhlükəsizlik və informasiya sistemlərindən və şəbəkələrindən istifadə edərkən və onlarla qarşılıqlı əlaqədə olarkən yeni düşüncə tərzinin və davranışın qəbul edilməsini" təşviq etmək üçün "İnformasiya Təhlükəsizliyinin və Şəbəkələrinin Təhlükəsizliyi üzrə Rəhbər Prinsiplər: Təhlükəsizlik Mədəniyyətinə Doğru"[28] adlı sənədi qəbul etmişdir.[29]

İnformasiya cəmiyyətində qabaqcıl təcrübələri bölüşmək məqsədilə, 2003-cü ildə İnformasiya Sistemlərinin və Şəbəkəsinin Təhlükəsizliyi üzrə Qlobal Forum və 2005-ci ildə İnformasiya Sistemlərinin və Şəbəkələrinin Təhlükəsizliyinə dair OECD-APEC Seminarı keçirilmişdir.

2010-cu ildə, informasiya təhlükəsizliyi və Şəxsi həyatın toxunulmazlığı perspektivlərindən irəli gələrək, botnetlərlə mübarizə metodlarını araşdırmaq üçün layihə təklif olunmuşdur. Layihə üzrə fəaliyyəti davam etdirmək üçün könüllülərdən ibarət qrup təsis olunmuşdur. Bu könüllülər qrupu Avstraliyadan, Kanadadan, Almaniyadan, Yaponiyadan, Koreya Respublikasından, Niderlanddan, İsveçdən, Türkiyədən, BK-dən, ABŞ, və Avropa İttifaqından və OECD-nin Komitələrindən (o cümlədən Biznes və Sənaye üzrə Məşvərət Komitəsindən, Vətəndaş Cəmiyyəti İnformasiya Cəmiyyəti üzrə Məşvərət Komitəsindən və İnternet Texniki Məşvərət Komitəsindən) olan nümayəndələrdən ibarətdir. Koreya Respublikası bu layihədə iştirak edəcəkdir və ona maliyyə dəstəyi göstərəcəkdir.

WPISP-nin şəxsi həyatın toxunulmazlığı ilə bağlı fəaliyyəti: 1980-ci ildə qəbul edilmiş "Şəxsi həyatın toxunulmazlığının və Şəxsi Məlumatların Transsərhəd Axınları üzrə Rəhbər Prinsiplər" ictimai və özəl sektorlarda şəxsi informasiya ilə davranma üzrə beynəlxalq konsensusdur. 2002-ci ildə qəbul edilmiş "Şəxsi həyatın toxunulmazlığı onlayn şəbəkədə: OECD-nin Siyasət və Təcrübə üzrə Rəhbər Qaydaları"nda əsas diqqət e-kommersiya ilə bağlı Şəxsi həyatın toxunulmazlığını -gücləndirən texnologiyalara, onlayn Şəxsi həyatın toxunulmazlığı siyasətlərinə, tətbiqetmə və bərpa və digər məsələlərə yönəldilmişdir.

2011-ci ildə OECD-yə üzv-ölkələr arasında etibarlı və müqayisə edilə bilən statistik məlumatlar üçün informasiya təhlükəsizliyinə və Şəxsi həyatın toxunulmazlığına dair göstəricilərin işlənib hazırlanması ilə bağlı layihə təklif olunmuşdur. Koreya Respublikası aktiv iştirak və maliyyə dəstəyi ilə bu layihəyə kömək edəcəkdir.

Digər fəaliyyət: 1998-ci ildə OECD-nin "Kriptoqrafiya Siyasəti üzrə Rəhbər Prinsipləri" və Elektron Kommersiya üçün Autentikləşdirmə üzrə Ottava Nazirlər Bəyannaməsi" qəbul edilmişdir. 2002-ci ildən 2003-cü ilə kimi "OECD-yə üzv-ölkələrdə e-autentikləşdirmə və e-imzalar üzrə hüquqi və siyasət çərçivələrinin icmalı" aparılmışdır. 2005-ci ildə "OECD ölkələrində sərhədlər boyu autentikləşdirmədən istifadə" bəyan edilmişdir.

2004-cü ildə "Biometrik texnologiyalar" yazılmışdır və 2005-ci ildə reklam xarakterli sui-istifadə halları üzrə işçi qrup yaradılmışdır. Digər cari fəaliyyət rəqəmsal eyniləşdirmə məlumatlarını idarəetmə, zərərli proqram

---

28 OECD, *OECD İnformasiya Təhlükəsizliyinin və Şəbəkələrinin Təhlükəsizliyi üzrə Rəhbər Prinsiplər: Təhlükəsizlik Mədəniyyətinə Doğru (Paris, 2002-ci il)*, http://www.oecd.org/dataoecd/16/22/15582260.pdf.

29 Eyni mənbə, səh.8

təminatları, nüfuz edən radio tezlik eyniləşdirməsi (RFİD), sensorlar və şəbəkələr və informasiya təhlükəsizliyinin və Şəxsi həyatın toxunulmazlığının həyata keçirilməsi üçün ümumi çərçivə ilə bağlıdır.

APEC-in informasiya təhlükəsizliyi tədbirlər[30]

Asiya və Sakit Okean Hövzəsi üzrə İqtisadi Əməkdaşlıq (APEC) qurumu, üç rəhbər qrupdan (Liberallaşdırma üzrə Rəhbər Qrup, İKT-nin İnkişafı üzrə Rəhbər Qrup və Təhlükəsizlik və Tərəqqi üzrə Rəhbər Qrup) ibarət olan Telekommunikasiya və İnformasiya üzrə İşçi Qrup (TEL) vasitəsilə, Asiya və Sakit Okean Hövzəsi regionunda informasiya təhlükəsizliyi tədbirlərini həyata keçirir.

Xüsusən də 2005-ci ilin iyun ayında Perunun Lima şəhərində keçirilmiş APEC-in Telekommunikasiya və İnformasiya Sənayesi üzrə Altıncı Nazirlər Toplantısından bəri, Təhlükəsizlik və Tərəqqi üzrə Rəhbər Qrup kibertəhlükəsizlik və kibercinayətkarlıq üzrə müzakirələri önə çəkmişdir. İstehlakçının e-kommersiyadan istifadəyə inamını artırmağa yönələn APEC-in Kiber-Təhlükəsizlik Strategiyası müxtəlif iqtisadiyyatların səylərini birləşdirməyə xidmət edir. Bu səylərə BMT-nin Baş Assambleyasının 55/63 nömrəli Qətnaməsinə [31] və Kibercinayətkarlıq haqqında Konvensiyaya[32] uyğun olan kibertəhlükəsizlik haqqında qanunların qəbul edilməsi və tətbiqi aiddir. TEL Kibercinayətkarlıq üzrə Qanunvericilik Təşəbbüsü və Tətbiqetmə Potensialını İnkişaf Etdirmə Layihəsi təşkilatlara yeni qanunları həyata keçirməkdə dəstək göstərəcəkdir.

APEC üzvləri, həmçinin, kiberhücumlara qarşı erkən xəbərdarlıq müdafiə sistemi kimi CERT-lərin tətbiqi üçün birgə iş aparırlar. Koreya Respublikası inkişaf etməkdə olan ölkələrə təlimlər keçirir və CERT-ləri təsis etmək və işlətmək üçün rəhbər prinsiplər işlənib hazırlanmışdır.

Kiçik və orta müəssisələri və özəl istifadəçiləri kiberhücumlardan və viruslardan qorumaq bir prioritet məsələ hesab edilir və bu məqsədlə bir sıra vasitələr işlənib hazırlanmışdır. İnternetdən necə təhlükəsiz istifadə olunmasına və simsiz texnologiyalarla bağlı təhlükəsizlik məsələlərinə və təhlükəsiz e-məktub mübadiləsinə dair informasiya təmin edilir.

İnformasiya mübadiləsi, prosedurlar və qarşılıqlı yardıma dair qanunların işlənib hazırlanması və biznes müəssisələrini və vətəndaşları qorumaq üçün digər tədbirlər vasitəsilə informasiyadan cinayətkar məqsədlərlə sui-istifadəni azaltmaq APECTEL üçün prioritet məsələ olaraq qalacaqdır. Təhlükəsizlik məsələlərinə dair öz proqramının bir hissəsi kimi, APECTEL 2007-ci ildə “Botnetlərə qarşı Siyasət və Texniki Yanaşma üzrə Rəhbrə Qaydaları” qəbul etmişdir və Kiber Təhlükəsizlik və Mühüm İnformasiya İnfrastrukturu üzrə Seminar təşkil etmişdir.

2009-cu ildə APEC-in Terrorçuluq Əleyhinə İşçi Qrupu (CTTF) və APECTEL tərəfindən təsdiq edildiyi kimi, 7 – 8 sentyabr 2011-ci il tarixdə, 16 ölkədən 86 nümayəndənin, moderatorun və natiqlərin iştirakı ilə, Koreya Respublikasının Seul şəhərində “İT təhlükəsizliyi vasitəsilə öz iqtisadiyyatlarımızı daha yaxşı müdafiə etmək üçün kiberməkanın qorunması üzrə APEC-in üçüncü seminarı” keçirilmişdir. Seminara Xarici İşlər və Ticarət Nazirliyi,

---

30 Bu bölüm APEC-dən götürülmüşdür, "Telekommunikasiya və informasiya üzrə işçi qrup", http://www.apec.org/Home/Groups/ SOM-Steering-Committee-on-Economic-and-Technical-Cooperation/Working-Groups/Telecommunications-and-Information.

31 Texniki tərəqqinin fəsadlarından biri kimi virtual dünyada cinayətkar fəaliyyətin artıdığını etiraf edən “İnformasiyadan cinayətkar məqsədlərlə sui-istifadə halları ilə mübarizə” .

32 Kompüter sistemlərinin bütövlüyünü pozan hər hansı bir hərəkəti cinayət əməli hesab etməklə bu bütövlüyü saxlamaq məqsədini daşıyan, Budapeştdə qəbul edilmiş Saziş. Bax, http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.

Dövlət İdarəetməsi və Təhlükəsizlik Nazirliyi və KKK ev sahibliyi etmişdir və o, Koreya İnternet və Təhlükəsizlik Agentliyi (KİSA) tərəfindən maliyyələşdirilmişdir.

Seminar iki əvvəlki CTTF-TEL birgə layihələrinin, dəqiq desək 15 – 30 noyabr 2007-ci il tarixlərdə Seulda keçirilmiş "Asiya və Sakit Okean hövzəsi regionunda kibertəhlükəsizliyin möhkəmləndirilməsi üzrə APEC-in təlim proqramı"nın və 26 – 27 iyun 2008-ci il tarixlərdə Seulda keçirilmiş "Kiberməkanın terrorçuların istifadəsindən və hücumlarından qorunması üzrə APEC Seminarı"nın davamıdır. Təlim proqramının və birinci seminarın nəticələri üzərində qurulmaqla, üçüncü seminar, mühüm infrastrukturun terror hücumlarından qorunması da daxil olmaqla, kibertəhlükəsizliklə bağlı müxtəlif məsələləri həll etmək üçün hökumət rəsmilərini və APEC-ə üzv ölkələrin ekspertlərini bir araya gətirmişdir.

BTİ-nin informasiya təhlükəsizliyi tədbirləri[33]

BTİ İKT-lər üzrə BMT-nin aparıcı agentliyidir. İsveçrənin Cenevrə şəhərində yerləşən BTİ 191 üzv-ölkəyə və 700-dən çox sektor üzvünə və tərəfdaşa malikdir.

Dünya kommunikasiyasına köməyin göstərilməsində BTİ-nin rolu üç əsas sektoru əhatə edir. Radiokommunikasiya sektoru (BTİ-R) beynəlxalq radio tezlik spektrinin və peyk orbit resurslarının idarə olunmasını diqqətdə saxlayır. Telekommunikasiya Standartlaşdırma Sektoru (BTİ-T) diqqəti informasiya-kommunikasiya şəbəkələrinin və xidmətlərinin standartlaşdırılmasına yönəltmişdir. İnkişaf Sektoru (BTİ-D) daha geniş sosial və iqtisadi inkişafı stimullaşdırma vasitəsi kimi İKT-yə bərabər, davamlı və uyğun çıxış imkanının genişləndirilməsinə kömək etmək üçün təsis edilmişdir. BTİ də telekommunikasiya ilə bağlı tədbirlər təşkil edir və o, İCÜS-nin aparıcı təşkilati qurumu olmuşdur.

İCÜS-dən sonra BTİ-nin əsas rolu İKT-lərdən istifadə sahəsində inam və təhlükəsizlik yaratmaqdır. İCÜS-də dövlət başçıları və dünya liderləri, BTİ-yə, C.5 Fəaliyyət bəndinin ("İKT-lərdən istifadə sahəsində inam və təhlükəsizlik yaratma") yerinə yetirilməsində yeganə vasitəçi qismində, kibertəhlükəsizlik sahəsində beynəlxalq səylərin əlaqələndirilməsində aparıcılığı həvalə etmişlər. Kibertəhlükəsizlik BTİ-D-nin nəzarətində olan əsa sahələrdən biridir.
İCÜS-nin C.5-ci Fəaliyyət bəndindəki əsas sahələr aşağıdakılardır:

- CIIP
- Qlobal kibertəhlükəsizlik mədəniyyətinin təşviq olunması
- Milli hüquqi yanaşmaları uyğunlaşdırmaq, beynəlxalq hüquqi əlaqələndirmə və tətbiqetmə
- Reklam xarakterli sui-istifadə halları ilə mübarizə
- Müşahidə, xəbərdarıq və hadisələr zamanı cavab tədbirləri görmə imkanlarının inkişaf etdirilməsi
- Milli yanaşmalara, qabaqcıl təcrübələrə və rəhbər prinsiplərə dair informasiya mübadiləsi
- Şəxsi həyatın toxunulmazlığı, məlumat və istehlakçının qorunması

BTİ-nin Qlobal Kibertəhlükəsizlik Proqramı (GCA), informasiya cəmiyyətində inamı və təhlükəsiliyi artırmaq üçün həll yollarının təklif edilməsi məqsədini güdən beynəlxalq əməkdaşlıq üçün BTİ çərçivəsidir. GCA-nın beş strateji

33 Bu bölüm BTİ-nin vebsaytından götürülmüşdür, http://www.itu.int

istiqaməti vardır: hüquqi çərçivə, texniki tədbirlər, təşkilati strukturlar, potensialın inkişaf etdirilməsi və beynəlxalq əməkdaşlıq. Strategiyalar aşağıdakı məqsədlərlə işlənib hazırlanır:

- Hüquqi tədbirlər
- Texniki və prosessual tədbirlər
- Təşkilati strukturlar
- Potensialın gücləndirilməsi
- Beynəlxalq əməkdaşlıq

Strategiyalar aşağıdakı məqsədlərə uyğun hazırlanır:

- Kibercinayətkarlığa dair qlobal səviyyədə tətbiq edilə bilən və mövcud milli / regional qanunvericilik tədbirləri ilə qarşılıqlı uyğun olan model qanunvericiliyin işlənib hazırlanması

- Kibercinayətkarlığa dair milli və regional təşkilati strukturlar və siyasətlər yaratmaq
- Qlobal səviyyədə qəbul edilən minimum təhlükəsizlik meyarlarını və proqram təminatları və sistemləri üçün akkreditasiya planlarını təsis etmək
- Layihələrin trans-sərhəd əlaqələndirilməsini təmin etmək məqsədilə müşahidə, xəbərdarlıq və hadisələrin nəticələrinin aradan qaldırılması üçün çərçivə yaratmaq
- Coğrafi sərhədlər boyu fərdlər üçün rəqəmsal mandatın tanınmasını təmin etmək məqsədilə ümumi və universal rəqəmsal şəxsiyyət sistemini və zəruri təşkilati strukturları yaratmaq və qəbul etmək
- Sektorlar-arası və yuxarıda göstərilən sahələrin hamısında bilik və vərdişləri gücləndirmək məqsədilə insan və təşkilati potensialın inkişaf etdirilməsinə şərait yaratmaq üçün qlobal strategiyanın işlənib hazırlanması
- Yuxarıda göstərilən sahələrin hamısında beynəlxalq əməkdaşlıq, dialoq və əlaqələndirmə üçün qlobal çoxtərəfli strategiya üçün mümkün çərçivəyə dair məsləhətlərin verilməsi

GCA özünün İMPACT ilə tərəfdaşlığı və aparıcı qlobal iştirakçıların dəstəyi ilə Uşaqların Onlayn Müdafiəsi Təşəbbüsü kimi layihələrə şərait yaratmışdır.

Digər bir təşəbbüs, milli və beynəlxalq kibercinayətkarlıqla bağlı olan təşəbbüslər üzrə asanlıqla istifadə oluna bilən və interaktiv informasiya resursunu təmin etmək məqsədini güdən BTİ-nin Kibertəhlükəsizliyə Girişdir. O, vətəndaşlar, hökumətlər, biznes müəssisələri və beynəlxalq təşkilatlar üçün əlçatandır. Onun göstərdiyi xidmətlərə informasiya mübadiləsi, müşahidə və xəbərdarlıq, qanunlar və qanunvericilik, Şəxsi həyatın toxunulmazlığı və qoruma, sənaye standartları və həll yolları aiddir.

BTİ-İ, həmçinin, kiberməkanın yüksək səviyyədə təhlükəsizliyi üçün ölkələrdə texnologiyaların inkişaf etdirilməsinə kömət etmək məqsədilə təsis edilmiş BTİ-nin Kibertəhlükəsizlik üzrə Fəaliyyət Proqramına nəzarət edir. O, aşağıdakılarla bağlı yardım göstərir:

- Kibertəhlükəsizlik və CİİP üçün milli strategiyaları və imkanları yaratma
- Kibercinayətkarlıqla bağlı müvafiq qanunvericiliyi və tətbiqetmə mexanizmlərini müəyyənləşdirmə
- Müşahidə, xəbərdarlıq və hadisələrin nəticələrinin aradan qaldırılması imkanlarını yaratma
- Reklam xarakterli sui-istifadə halları və bununla bağlı təhlükələrlə mübarizə aparma
- İnkişaf etməkdə olan və inkişaf etmiş ölkələr arasında təhlükəsizliklə bağlı standartlaşdırmadakı fərqi aradan qaldırma
- BTİ-nin Kibertəhlükəsizlik / CİİP məlumat kitabını, əlaqələrə dair məlumat bazasını və kimin kim olması barədə nəşri təsis etmə

- Kibertəhlükəsizliklə bağlı standartları müəyyənləşdirmə
- Regional əməkdaşlıq tədbirlərinə kömək etmə
- BTİ-nin Kibercinayətkarlığa Girişə dair informasiya mübadiləsi və dəstək göstərmə
- Müvafiq tədbirlərin genişləndirilməsi və təşviq olunması

BTİ-İ-nin kibertəhlükəsizliklə bağlı digər tədbirlərinə StopSpamAlliance.org ilə birgə tədbirlər; kibercinayətkarlıq haqqında qanunvericilik və tətbiqetmə üzrə regional səviyyədə potensialın inkişaf etdirilməsi tədbirləri; və resursların və vasitələrin işlənib hazırlanması və yayılması, o cümlədən botnetlərin azaldılması üzrə vasitələr[34], inkişaf etməkdə olan ölkələr üçün kibercinayətkarlıq haqqında qanunvericilik modeli üzrə vasitələr, kibertəhlükəsizliklə bağlı milli özünü-qiymətləndirmə üzrə vasitələr[35] və kibertəhlükəsizlik / kibercinayətkarlıq üzrə nəşrlər və sənədlər aiddir.[36]

BTİ-T sektoru, həmçinin, təhlükəsizliklə bağlı 70-dən çox standartı işləyib hazırlamaqla (BTİ-T), kibertəhlükəsizlik sahəsinə kömək edir. Son vaxtlarda kibertəhlükəsizliyə dair simpoziumda iştirakçılar BTİ-T-dən bu sahədə öz fəaliyyətini sürətləndirməyi xahiş etmişlər və buna cavab olaraq BTİ-T indi təhlükəsizlik standartlarının işlənib hazırlanmasına əlavə önəm verir. Bu prosesə yardım etmək üçün BTİ-T "İKT Təhlükəsizlik Standartlarının Yol Xəritəsini işləyib hazırlamışdır və həmin sənəd mövcud standartlar, hazırlanmaqda olan standartlar və təhlükəsizliklə bağlı gələcək standartarlaşdırma sahələri barədə informasiyanı bir araya gətirir.[37]

Standartlaşdırma işi texniki sorğu qrupları (SG-lər) tərəfindən aparılır, bu qruplarda BTİ-T üzvlərinin nümayəndələri beynəlxalq telekommunikasiyanın müxtəlif sahələri üçün tövsiyələr (standartlar) işləyib hazırlayırlar. SG-lər öz işlərini ilk növbədə sorğu sualları formasında aparırlar. Hər bir sual telekommunikasiyanın ayrıca bir sahəsində standartlaşdırma üçün texniki araşdırmaya yönəlmişdir.

BTİ-T çərçivəsində 17 nörməli Sorğu Qrupu (SG17)[38] bütün sorğu qrupları boyu təhlükəsizliklə bağlı işi əlaqələndirir.

SG17 təhlükəsizliklə, o cümlədən kibertəhlükəsizlik, reklam xarakterli sui-istifadə hallarına qarşı mübarizə və istifadəçilərin eyniləşdirmə materiallarının idarə olunması ilə bağlı sorğulara görə cavabdehdir. O, həmçinin, açıq sistem kommunikasiyası, o cümlədən məlumat kitabları və obyekt müəyyənləşdiricilərin tətbiqinə və texniki dillərə, onların istifadəsi metoduna və telekommunikasiya sistemlərinin proqram təminatı aspektləri ilə bağlı digər məsələlərə görə cavabdehdir.

2017 – 2020-ci illəri əhatə edən sorğu müddəti üçün SG17-nin strukturu aşağıdakı kimidir:

- 1-ci İşçi Qrup. Telekommunikasiya / İKT təhlükəsizliyi
  - Sual 1 – Telekommunikasiya / İKT təhlükəsizliyinin əlaqələndirilməsi
  - Sual 2 – Təhlükəsizlik quruluşu və çərçivəsi
  - Sual 3 – Telekommunikasiya sahəsində informasiya təhlükəsizliyinə nəzarət
  - Sual 4 – Kibertəhlükəsizlik

---

34 Sureş Ramasubramanian və Robert Şo, "BTİ Botnetlərin azaldılması layihəsi: ilkin şərait və yanaşma" BTİ təqdimatı, sentyabr 2007-ci il, http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-botnet-mitigation-toolkit.pdf.

35 BTİ-nin Tətbiqi Proqramlar və Kibertəhlükəsizlik Bölməsi, "BTİ-nin Milli Kibertəhlükəsizlik / CİİP Özünü-Dəyərləndirmə vasitəsi", BTİ, http://www.itu.int/ ITU-D/cyb/cybersecurity/projects/readiness.html.

36 BTİ-nin Tətbiqi Proqramlar və Kibertəhlükəsizlik Bölməsi, "Vasitələr, sənədalər və nəşrlər", BTİ, http://www.itu.int/ITU-D/cyb/ cybersecurity/.

37 BTİ,"BTİ Təhlükəsizlik Standartları üzrə Yol Xəritəsi", http://www.itu.int/ITU-T/studygroups/com17/ict/index.html.

38 BTİ-T, 17 nömrəli Sorğu Qrupu (2009 – 2012-ci illər Sorğu müddəti), http://www.itu.int/ITU-T/studygroups/com17/index.asp.

- Sual 5 – Texniki vasitələrlə spamla mübarizə

- 2-ci İşçi Qrup. Kiberməkanın təhlükəsizliyi
  - Sual 6 – Ümumi telekommunikasiya xidmətlərinin təhlükəsizlik aspektləri
  - Sual 7 – Təhlükəsizlik üzrə tətbiq xidmətləri
  - Sual 8 – Xidmət yönümlü quruluşun təhlükəsizliyi
  - Sual 9 – Telebiometriya

- 3-cü İşçi Qrup. Tətbiqetmə təhlükəsizliyi
  - Sual 10 – Eyniləşdirmə məlumatlarını idarəetmənin quruluşu və mexanizmləri
  - Sual 11 – Yönləndirmə xidmətləri, yönləndirmə sistemləri və ümumi açar / atribut şəhadətnamələri
  - Sual 12 – Abstract Syntax Notation One (Abstrakt Sintaktik Hesablama Sistemi) (ANS.1), obyekt müəyyənedicilər və bununla bağlı qeydiyyat
  - Sual 13 – Formal dillər və telekkomunikasiya proqram təminatı
  - Sual 14 – Yoxlama dilləri, metodologiyalar və çərçivə
  - Sual 15 – Açıq sistemlərin qarşılıqlı əlaqəsi

İnformasiya və kommunikasiya texnologiyalarının (İKT) istifadəsində inam və təhlükəsizliyin yaradılması üzrə işlər daha təhlükəsiz şəbəkə infrastrukturunun, xidmətlərin və tətbiqlərin asanlaşdırılması məqsədilə intensivləşməyə davam edir. Təhlükəsizliyə yönəlmiş 170-dən çox standart (ITU-T Recommendations and Supplements-- ITU-T Tövsiyələri və Əlavələri) nəşr edilmişdir.

ITU-T Tədqiqat Qrupu 17 (SG17) bütün ITU-T Tədris Qruplarında təhlükəsizliklə bağlı işi əlaqələndirir. Tez-tez digər standartların işlənib hazırlanması təşkilatları (SDO-lar) və müxtəlif İKT sənayesi konsorsiumları ilə əməkdaşlıqda işləyən SG17 geniş intervallı standartlaşdırma məsələləri ilə məşğul olur.

Bir neçə nümunə vermək üçün SG17 hazırda kibertəhlükəsizlik üzərində işləyir; təhlükəsizlik idarəetməsi; təhlükəsizlik arxitekturaları və çərçivələri; spamla mübarizə; şəxsiyyətin idarə edilməsi; şəxsiyyəti müəyyən edən məlumatların qorunması; və Əşyaların İnterneti (IoT), ağıllı şəbəkə, smartfonlar, proqram təminatı ilə müəyyən edilmiş şəbəkə (SDN), veb xidmətləri, böyük məlumat analitikası, sosial şəbəkələr, bulud hesablamaları, mobil maliyyə sistemləri, IPTV üçün tətbiqlərin və xidmətlərin təhlükəsizliyi və telebiometriya.

Bu gün istifadədə olan təhlükəsizlə bağlı standartlar üçün bir əsas məqam ictimai şəbəkər üzərində elektron autentikləşdirmə üçün BTİ-T-nin X.509 nömrəli Tövsiyəsidir. X.509 əsas ictimai infrastrukturla bağlı tətbiqi proqramların hazırlanması üçün istifadə edilir və ondan Veb şəbəkədə brauzer və server arasında təhlükəsizliyin təmin olunmasından tutmuş e-kommersiya əqdlərinə imkan verən rəqəmsal imzaların təmin olunmasına qədər geniş istifadə olunur. SG17-nin digər bir nailiyyəti, telekommunikasiya şəbəkə operatorlarına və müəssisələrə, təhlükəsizlik baxımından birbaşa (iki tərəfə çıxan) quruluşu təsvir etmək imkanını verəcək X.805 nömrəli Tövsiyədir.[39]

SG 17, həmçinin, texniki dilləri və təsviretmə üsullarını öyrənmək üçün bir yerdir. Buna misal kimi, protokolu detallaşdırma və ya sistemlərin quruluşu üçün mühüm component olan formal ASN.1 dilini göstərmək olar. ASN.1 bu günkü şəbəkələrin hədsiz mühüm bir hissəsidir. ASN.1-dən, məsələn, əksər telefon zənglərinin

[39] BTİ "17 nömrəli Sorğu Qrupu ilk baxışdan", http://www.itu.int/net/ITU-T/info/sg17.aspx.

siqnallaşdırma sistemində, paket izləmə, kredit kart yoxlaması və rəqəmsal şəhadətnamələr və əksər istifadədə olan proqram təminatlarında istifadə olunur. Bu günkü iş BTİ-T-nin dilləri üçün vahid modelləşdirmə dil profillərinin işlənib hazırlanmasına yönəlmişdir.[40]

İSO/İEC-nin informasiya təhlükəsizliyi tədbirləri

İnformasiya Təhlükəsizliyinə Nəzarət Sistemi (İSMS), adından da göründüyü kimi, informasiya təhlükəsizliyinə nəzarət eləmək üçün sistemdir. O, informasiya aktivlərinin məxfiliyini, bütövlüyünü və mövcudluğunu təmin etmək, eyni zamanda təhlükəsizliklə bağlı riskləri minimum endirmək üçün proseslərdən və sistemlərdən ibarətdir. İSMS şəhadətnaməsi, iki sənədin buraxılması səbəbindən, beynəlxalq standartlaşdırılmış İSMS tarixində dönüş nöqtəsi kimi 2005-ci ildən sonra dünyada getdikcə daha çox tanınır: İS 27001 İSMS-in müəyyən olunması üçün tələbləri bəyan edir və İS 17799: 2005 kimi buraxılan İS 17799: 2000 İSMS-in tətbiqi üçün əsas yoxlamaları nəzərdə tutur.

Faktiki olaraq İSMS standartı, ilk dəfə Britaniya Standartlar İnstitutu (BSİ) tərəfindən, 1995-ci ildə, informasiya təhlükəsizliyinə nəzarət üçün prosessual məcəllə (norma və qaydalar) kimi işlənib hazırlanmış BS 7799 olmuşdur. 1998-ci ildə bu standart əsasında texniki tapşırıq (tələblərin müəyyənləşdirilməsi) işlənib hazırlandığından "informasiya təhlükəsizliyinə nəzarət üçün prosessual məcəllə (norma və qaydalar) 1-ci Hissə və texniki tapşırıq isə 2-ci Hissə olmuşdur. 1-ci Hissədə informasiya təhlükəsizliyinin idarə olunması üçün nəzarətlər müəyyən edildiyi halda, 2-ci Hissədə İSMS-in müəyyən edilməsi üçün tələblər qeyd olunur və risk idarəetmə bazasının davamlı şəkildə təkmilləşdirilməsi üçün informasiya təhlükəsizlik prosesi (Planlaşdır-Et-Yoxla-Hərəkət Elə dövrü) təsvir olunur.

1-ci Hissə ISO/IEC JTC 1/SC27 WG1 tərəfindən İS 17799 kimi 2000-ci ildə müəyyən edilmişdir. Həmin vaxtdan bəri İS17799 dəfərlərlə nəzərdən keçirilmiş (2,000-dən çox qeydlə) və ona düzəlişlər edilmişdir və yekun variant 2005-ci ilin noyabr ayında beynəlxalq standart kimi qeydə alınmışdır. İS 17799: 2000 10 domendə 126 yoxlamanı nəzərdə tutur. 2005-ci ildə düzəlişlər edilmiş İS 17799 11 inzibati nəzarət domenini və 133 yoxlamanı nəzərdə tutur.

1999-cu ildə müəyyən edilən BS 7799-un 2-ci Hissəsi İSMS şəhadətnaməsi üçün standart qismində istifadə edilmişdir. Digər məsələlərlə yanaşı, İSO 9001 və İSO 14001-i uyğunlaşdırmaq üçün 2002-ci ilin sentyabrında ona düzəlişlər edilmişdir. İSO beynəlxalq standartlaşdırılmış İSMS üçün sorğularla bağlı sürətli izləmə metodu vasitəsilə BS7799 Hissə 2:2000-i qəbul etmişdir və qısa müddət ərzində kiçik düzəlişlər etməklə onu İSO27001 beynəlxalq standartı kimi qeydə almışdır. Əsas dəyişikliklər effektivliklə bağlı məzmunun əlavə edilməsini və qoşmadakı dəyişikliyi əhatə edir.

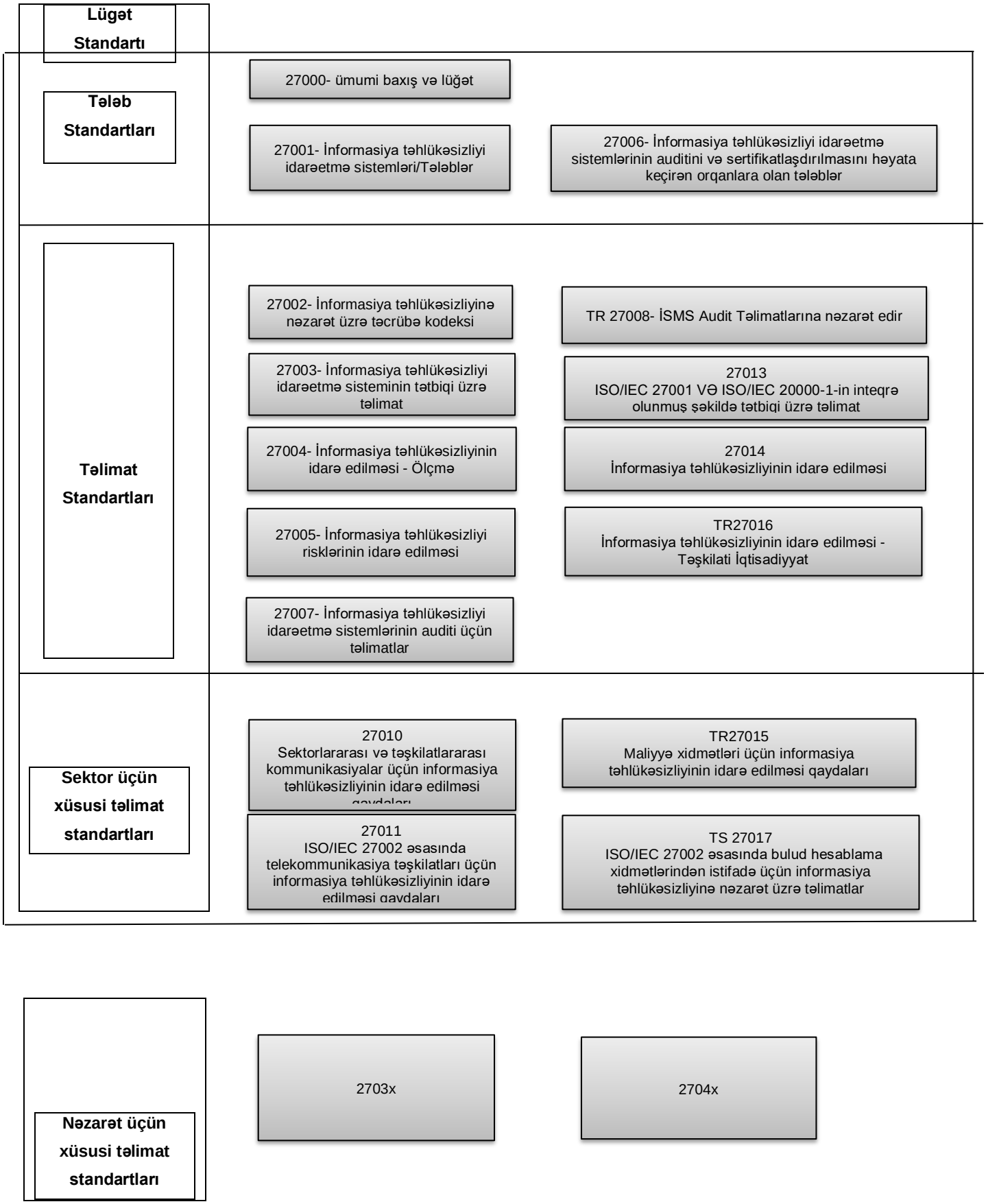
İSMS-lə bağlı iki mühüm sənəd beynəlxalq səviyyədə standartlaşdırıldığına görə, digər nəzarət sistemləri (keyfiyyət biznes: 9000 seriya, ekoloji nəzarət: 14000 seriya) ilə eyni olan 27000 seriya nömrəli sxem altında beynəlxalq təhlükəsizlik standartları meydana gəlmişdir. İS 17799:2005-in düzəlişlər edilmiş variantı olan İS 27001 İSMS-in müəyyən edilməsi üçün tələbləri nəzərdə tutur və İSMS-in tətbiqi üçün əsas yoxlamaları əhatə edən İS177099:2005 2007-ci ildə dəyişdirilərək İS27002 olmuşdur. İSMS-in tətbiqi üçün rəhbər qaydalar, informasiya təhlükəsizliyi üzrə risk idarəetmə standartı və informasiya təhlükəsizliyinə nəzarət ölçüsü JTC1 SC27 tərəfindən işlənib hazırlanmışdır və 27000 seriyasındadır.

---

40 Eyni mənbə

Şəkil 9-da İSMS-lə bağlı standartlar göstərilir. İSMS təsdiqetmə tədbirləri tədricən əhəmiyyət kəsb edir və ümumi sistemlər üçün ümumi İSMS əsasında xüsusi sənayelər üçün uyğun olan İSMS standartlarının və ya tövsiyələrinin işlənib hazırlanacağı gözlənilir. Buna misal olaraq, kommunikasiya sənayesi üçün səciyyəvi xüsusiyyətləri əks etdirən İSMS tövsiyələrinin işlənib hazırlanmasına cəhdi göstərmək olar.

Şəkil 9: ISO/IEC 27000 qrupu



Düşündürücü suallar

Beynəlxalq təşkilatların nəzarət etdiyi informasiya təhlükəsizliyi ilə bağlı hansı tədbirlər sizin ölkədə qəbul edilmişdir və ya edilməkdədir? Onlar necə tətbiq edilir?

Özünü sına

1. Bu bölümdə qeyd olunan ölkələr tərəfindən informasiya təhlükəsizliyi ilə bağlı həyata keçirilən tədbirlərdə oxşarlıqlar hansılardır? Onlar arasında fərqlər nədən ibarətdir?

2. Bu bölümə daxil edilən beynəlxalq təşkilatların informasiya təhlükəsizliyi ilə bağlı prioritetləri nədir?

4. İNFORMASİYA TƏHLÜKƏSİZLİYİ METODOLOGİYASI

Bu bölümdə məqsəd beynəlxalq səviyyədə istifadə edilən inzibati, fiziki və texniki informasiya təhlükəsizliyi metodologiyası barədə məlumat verməkdir.

4.1İnformasiya təhlükəsizliyinin müxtəlif aspektləri

İnformasiya təhlükəsizliyi metodologiyasının məqsədi, informasiya aktivləri ilə bağlı bütün mümkün zəif məqamları və təhlükələri nəzərə alaraq zərəri minimum endirmək və işin davamlılığını qoruyub saxlamaqdır. İşin davamlılığına zəmanət vermək üçün, informasiya təhlükəsizliyi metodologiyası daxili informasiya aktivlərinin məxfiliyini, bütövlüyünü və mövcudluğunu təmin etməyə çalışır. Burada risk dəyərləndirmə metodlarından və nəzarət tədbirlərindən istifadə olunur. Ən əsası isə, informasiya təhlükəsizliyinin inzibati, fiziki və texniki aspektlərini əhatə edən yaxşı plan tələb olunur.

İnzibati aspekt

İnzibati aspektə diqqət yetirilən bir çox İSMS-lər vardır. İSO/İEC27001 ən geniş istifadə edilənlərdən biridir.

Beynəlxalq İSMS standartı olan ISO/IEC27001 BSİ tərəfindən müəyyən edilmiş BS7799-a əsaslanır. BS7799 İSMS-i tətbiq etmək və ona nəzarət etmək üçün tələbləri və müxtəlif təşkilatların təhlükəsizlik standartları və təhlükəsizliyə effektiv şəkildə nəzarət üçün tətbiq edilən ümumi standartları müəyyən edir. BS7799-un 1-ci Hissəsi təşkilatlarda təhlükəsizlik tədbirlərinə dair qabaqcıl təcrübələr əsasında tələb olunan təhlükəsizlik tədbirlərini təsvir edir. Hazırki İSO/İEC27001 olan 2-ci Hissədə İSMS üçün tələb olunan minimum şərtlər və təhlükəsizlik tədbirlərinin dəyərləndirilməsi təklif olunur.

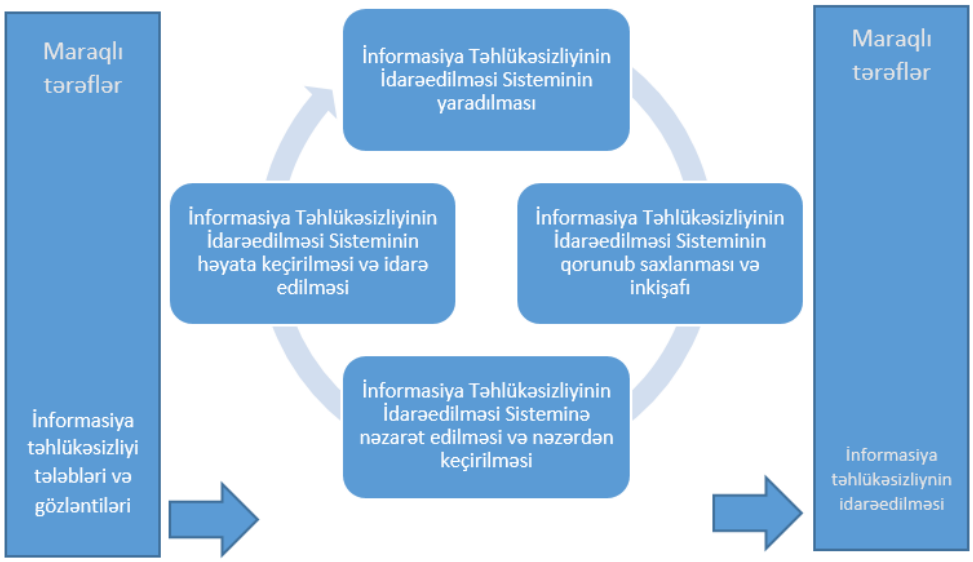
Cədvəl 5. ISO/IEC27001-də nəzarətlər

Domenlər	**Bəndlər**
A5.	Təhlükəsizlik siyasətləri
A6.	İnformasiya təhlükəsizliyi təşkili
A7.	İnsan resurslarının təhlükəsizliyi
A8.	Aktivlərin idarə olunması
A9.	Giriş nəzarəti
A10.	Kriptoqrafiya
A11.	Fiziki və ekoloji təhlükəsizlik
A12.	Əməliyyat təhlükəsizliyi
A13.	Kommunikasiya təhlükəsizliyi
A14.	Sistemlərin əldə olunması, inkişaf etdirilməsi və onlara xidmət
A15.	Təchizatçı ilə əlaqələr
A16.	İnformasiya təhlükəsizliyi insidentlərinin idarə edilməsi
A17.	Biznesin davamlılığının idarə edilməsinin informasiya təhlükəsizliyi aspektləri
A18.	Uyğunluq

İSO/İEC27001-də təhlükəsizlik tədbirləri 140 nəzarət tədbirindən və 14 domendən ibarətdir (bax, 5-ci Cədvəl).

ISO/IEC27001 bütün İSMS proseslərinə tətbiq edilən Planlaşdır-Et-Yoxla-Hərəkət Elə modelini qəbul edir. İSO/İEC27001-də İSMS dəyərləndirməsi ilə bağlı bütün dəlillər sənədləşdirilməlidir; təsdiqetmə (şəhadətnamələrin verilməsi) hər altı aydan bir audit yoxlamasından keçməlidir; və İSMS-I davamlı şəkildə idarə etmək məqsədilə, bütöv proses üç ildən sonra təkrarlanmalıdır.

Şəkil 10. İSMS proseslərinə tətbiq edilən Planlaşdır-Et-Yoxla-Hərəkət Elə modeli



Mənbə: ISO/IEC JTC 1/SC 27.

Təhlükəsizlik bağlı nəzarət tədbirləri təhlükəsizlik tələblərini nəzərə almaqla planlaşdırmalıdır. Bütün insan resursları, o cümlədən təchizatçılar, podratçılar, istehlakçılar və kənar mütəxəssislər bu tədbirlərdə iştirak etməlidirlər. Təhlükəsizliklə bağlı tələblərin müəyyənləşdirilməsi növbəti üç faktora əsaslanır:

- Risk dəyərləndirmə
- Hüquqi tələblər və müqavilə bəndləri
- Təşkilatın fəaliyyəti üçün informasiya prosesləri

Boşluqların təhlili dedikdə hazırki informasiya təhlükəsizliyi səviyyəsinin dəyərləndirilməsi və informasiya təhlükəsizliyi ilə bağlı gələcək istiqamətin müəyyənləşdirilməsi prosesi nəzərdə tutulur. Boşluqların təhlilinin nəticəsi aktiv sahiblərinin 13 nəzarət tədbiri və 11 domenə cavablarından alınır. Boşluqların təhlil edilməsi sayəsində çatışmazlıqların olduğu sahələr müəyyən edildikdən sonra hər bir sahə üçün müvafiq nəzarət tədbirləri müəyyənləşdirilməlidir.

Risk dəyərləndirmə aktivlərin dəyərinin müəyyənləşdirilməsinə və təhlükələrin və zəif tərəflərin müəyyənləşdirilməsinə bölünür. Aktivlərin dəyərinin müəyyənləşdirilməsi informasiya aktivlərinin miqdarının dəyərləndirilməsidir. Təhlükələrin dəyərləndirilməsi isə informasiyanın məxfiliyinə, bütövlüyünə və mövcudluğuna qarşı təhlükələrin qiymətləndirilməsidir. Aşağıdakı misalda risk dəyərləndirməsində hesablamalar göstərilir.

Aktivin adı	Aktivin dəyəri	Təhlükə			Zəif tərəf			Risk		
		C	I	A	C	I	A	C	I	A
Aktivin adı #1	2	3	3	1	3	1	1	8	6	5

- Aktivin dəyəri + Təhlükə + Zəif tərəf = Risk
- Məxfilik: Aktivin dəyəri (2) + Təhlükə(3) + Zəif tərəf(3) = Risk(8)
- Bütövlük: Aktivin dəyəri (2) + Təhlükə (3) + Zəif tərəf(1) = Risk(6)
- Mövcudluq: Aktivin dəyəri(2) + Təhlükə (1) + Zəif tərəf (1) = Risk(5)

Nəzarət tədbirlərinin tətbiqi: Risk dəyərləndirməsinin nəticəsinə uyğun olaraq hər bir riskin dəyəri fərqli olacaqdır. Fərqli dəyərə malik aktivlərə müvafiq nəzarət tədbirlərinin tətbiq olunması üçün qərarların verilməsi tələb olunur. Təhlükəsizlik Dərəcəsi meyarına uyğun olaraq, risklər, qəbul edilə bilən və qəbul edilə bilməyən risklərə bölünür. Nəzarət tədbirləri qəbul edilə bilməyən riskin olduğu informasiya aktivlərinə tətbiq edilməli olacaqdır. Nəzarət tədbirləri İSO/İEC nəzarətləri əsasında tətbiq edilir, lakin nəzarət tədbirlərini təşkilatın real vəziyyətindən asılı olaraq tətbiq etmək daha effektivdir.

Texniki aspekt

Texniki aspektlər üçün İSMS yoxdur. Bunun əvəzinə Ümumi Meyarlar (CC) şəhadətnaməsi kimi beynəlxalq ümumi qiymətləndirmə standartlarından istifadə edilə bilər.

CC şəhadətnaməsinin kommersiya kökləri vardır. O, müxtəlif ölkələrdən İT məhsullarının təhlükəsizlik səviyyələrindəki fərqlərə dair problemləri həll etmək üçün müəyyən olunmuşdur. Kanada, Fransa, Almaniya, BK və ABŞ tərəfindən İT məhsullarının qiymətləndirilməsi üçün müəyyən olunmuşdur.

Xüsusilə də, CC, funksional tələblərin və zəmanətlə bağlı tələblərin müxtəlif kateqoriyaları əsasında məhsulun və ya sistemin İT təhlükəsizliyi üçün tələblərdir. CC funksional tələbləri təhlükəsizliklə bağlı arzu olunan rejimi müəyyən edir. Zəmanətlə bağlı tələblər tələb olunan təhlükəsizlik tədbirlərinin effektiv və düzgün yerinə yetirilməsinə əminlik üçün əsasdır. CC təhlükəsizlik funksiyaları 65 qrup təşkil edən 11 kateqoriyadan olan 134 komponentdən ibarətdir. Zəmanətlə bağlı tələblər isə 38 qrup təşkil edən səkkiz kateqoriyadan olan 81 komponentdən ibarətdir.

Təhlükəsizliklə bağlı funksional tələb (SFR): SFR-lər Qiymətləndirmə Cədvəli üçün təhlükəsizliklə bağlı bütün funksiyaları müəyyən edir. 6-cı Cədvəldə SFR-lərə daxil edilən təhlükəsizlik funksiyalarının növləri sadalanır.

Cədvəl 6. SFR-lərdə kateqoriyalar

Kateqoriyalar		**Detallar**
FAU	Təhlükəsizlik auditi	Burada audit məlumat mühafizəsi, qeydə alma formatı və tədbir seçimi, habelə təhlil vasitələri, pozulma hallarında həyəcan və real vaxtda aparılan təhlil nəzərdə tutulur.
FCO	Kommunikasiya	İnformasiyanın ötürülməsində istifadə edilən TOE-lər üçün xüsusi maraq kəsb edən tələblər təsvir olunur.

Classes		**Detallar**
FCS	Kriptoqrafik dəstək	Kriptoqrafik açar nəzarət və kriptoqrafik əməliyyatlardan istifadəni müəyyən edir
FDP	İstifadəçi ilə bağlı məlumatların mühafizəsi	İstifadəçi ilə bağlı məlumatların qorunmasına dair tələbləri müəyyən edir.
FIA	Eyniləşdirmə və autentikləşdirmə	Müraciət edən istifadəçinin şəxsiyyətini müəyyən etmək və yoxlamaq funksiyaları ilə bağlı tələbləri müəyyən edir.
FMT	Təhlükəsizliyə nəzarət	TOE Təhlükəsizlik Funksiyalarının (TSF) bəzi aspektlərini müəyyən edir: təhlükəsizlik əlamətləri, TSF məlumatları və funksiyaları.
FPR	Şəxsi həyatın toxunulmazlığı	İstifadəçilərin şəxsi həyatının toxunulmazlığı ilə bağlı tələbləri təmin edə biləcək, eyni zamanda sistemin çevikliyinə imkan verən, habelə sistemin fəaliyyəti üzərində lazımi nəzarəti mümkün edən tələbləri təsvir edir.
FPT	TSF-in mühafizəsi	TSF-i və TSF məlumatlarının bütövlüyünü təşkil edən mexanizmlərin bütövlüyü və idarə olunması ilə bağlı funksional tələblərin qruplarını özündə birləşdirir.
FRU	Resurslardan istifadə	İşləmə potensialı və / və ya saxlama imkanları kimi tələb olunan resursların mövcudluğunu təmin edir.
FTA	TOE-yə çıxış imkanı	İstifadəçi seansının müəyyən edilməsinə nəzarətlə bağlı müəyyən edir.
FTP	Etibar olunan keçid /kanallar	İstifadəçilər və TSF arasında etibarlı əlaqə üçün tələbləri təmin edir

Mənbə: Common Criteria, Common Criteria for Information Technology Security Evaluation, July 2009, CCMB-2009-07-001.

Təhlükəsizliyə zəmanət komponentləri (SAC-lar): CC fəlsəfəsi təhlükəsizliyə hədələrin və müvafiq və uyğun təhlükəsizlik tədbirləri vasitəsilə təşkilatın təhlükəsizlik siyasətinin vəzifələrinin aydınlaşdırılmasını tələb edir. Qəbul edilməli olan tədbirlər zəif tərəfləri müəyyənləşdirməyə, onlardan istifadə ehtimallarını azaltmağa və bu zəif tərəflərdən istifadə olunduğu təqdirdə zərərin həcmini azaltmağa kömək eləməlidir.[41] Cədvəl 7-də SAC-a daxil olan kateqoriyalar sadalanır.

Cədvəl 7. SAC-larda kateqoriyalar

Kateqoriyalar		**Detallar**
APE	Mühafizə Profilinin (PP) qiymətləndirilməsi	PP-nin möhkəm və daxili baxımdan uyğun olduğunu və PP-nin bir və ya daha çox başqa PP-lərə və ya onların qruplarına əsaslanıb-əsaslanmadığını və bu ST-nin həmin PP-lərin və onların qruplarının düzgün realizəsi olduğunu nümayiş etdirmək üçün tələb olunur.
ASE	Təhlükəsizlik hədəfinin (ST) qiymətləndirilməsi	ST-nin möhkəm və daxili baxımdan uyğun olduğunu və PP-nin bir və ya daha çox başqa PP-lərə və ya onların qruplarına əsaslanıb-əsaslanmadığını və bu PP-nin həmin PP-lərin və onların qruplarının düzgün realizəsi olduğunu nümayiş etdirmək üçün tələb olunur.
ADV	İnkişaf	Bu, TOE barəsində informasiyanı təmin edir. Əldə olunan biliklər, ATE və AVA kateqoriyalarında təsvir olunduğu kimi, zəif tərəflərlə bağlı təhlillərin və TOE əsasında sınaqların aparılması üçün əsas qismində istifadə olunur.

41 Ümumi Meyarlar, İnformasiya Texnologiyasının Təhlükəsizliyinin Qiymətləndirilməsi üçün Ümumi Meyarlar, iyul 2009-cu il, CCMB-2009-07-001

Siniflər		Detallar
AGD	İstiqamətverici sənədlər	TOE-nin təhlükəsiz şəkildə hazırlanması və fəaliyyət göstərməsi üçün TOE-nin təhlükəsiz şəkildə idarə olunmasının bütün müvafiq aspektlərini aydınlaşdırmaq zəruridir. Bu kateqoriyada, həmçinin, məqsədli şəkildə olmadan TOE-nin qeyri-düzgün konfiqurasiyasının və ya idarə olunmasının mümkünlüyünə də diqqət yetirilir.
ALC	İstismar dövrü ilə bağlı dəstək	Konfiqurasiyaya nəzarət (CM) imkanları, CM-nin əhatə dairəsi, çatdırılma, inkişaf təhlükəsizliyi, çatışmazlıqların aradan qaldırılması, istismar dövrü anlayışı, vasitələri və üsulları əhatə edən istismar dövründə TOE-nin onu hazırlayanın yoxsa istifadəçinin məsuliyyəti altında olması fərqləndirilir.
ATE	Sınaqlar	Bu kateqoriyada diqqət, TSF-nin, öz layihəsində təsvir olunanlara uyğun fəaliyyət göstərməsinin təsdiqinə yönəldilir. Bu kateqoriya nüfuzetmə ilə bağlı sınaqdan keçirməni əhatə etmir.
AVA	Zəif məqamların dəyərləndirilməsi	Zəif məqamların dəyərləndirilməsi TOE-nin işlənib hazırlanması və fəaliyyəti zamanı müxtəlif zəif məqamları əhatə edir.
ACO	Tərkib	Təşkil edilmiş TOE-nin, əvvəldən qiymətləndirilən proqram təminatı, proqram-aparat vasitələri və avadanlıq komponentləri ilə təmin olunmuş təhlükəsizliyə güvənərək fəaliyyət göstərəcəyinə inam yaratmaq üçün nəzərdə tutulan zəmanətlə bağlı xüsusi tələblər

Source: Common Criteria, Common Criteria for Information Technology Security Evaluation, July 2009, CCMB-2009-07-001

CC qiymətləndirmə metodu

1. **PP qiymətləndirməsi (APE):** TOE kateqoriyaları üçün, yerinə yetirilmədən asılı olmayan təhlükəsizlik tələblərini müəyyən edir və uyğun məhsulun onu həll etməli olduğu təhlükəsizliklə bağlı problem bildirir. O, CC funksional və zəmanətlə bağlı tələblərini müəyyən edir və seçilmiş funksional və zəmanətlə bağlı tələblər üçün səbəbi izah edir. O, səciyyəvi olaraq İT təhlükəsizlik tələbləri üçün istehlakçı və ya istehlakçı birliyi tərəfindən yaradılır.

2. **ST qiymətləndirməsi (ASE):** ST TOE-nin hansı təhlükəsizliyi təklif etməsinə dair TOE-ni işləyib hazırlayanlar, istehlakçılar, qiymətləndirən tərəflər və qiymətləndirmə orqanları arasında saziş və qiymətləndirmənin əhatə dairəsi üçün əsasdır. ST üçün heyətə, həmçinin, TOE-ni idarə edənlər, reklam edənlər, alanlar, quraşdıranlar, konfiqurasiya verənlər və istifadə edənlər də daxil edilə bilərlər. O, bir və ya daha çox PP-yə istinad edə bilər. Bu halda, ST, bu PP-lərin hər birində verilən ümumi təhlükəsizliklə bağlı tələbləri yerinə yetirməlidir, yaxud da əlavə tələblər müəyyən edilə bilər.

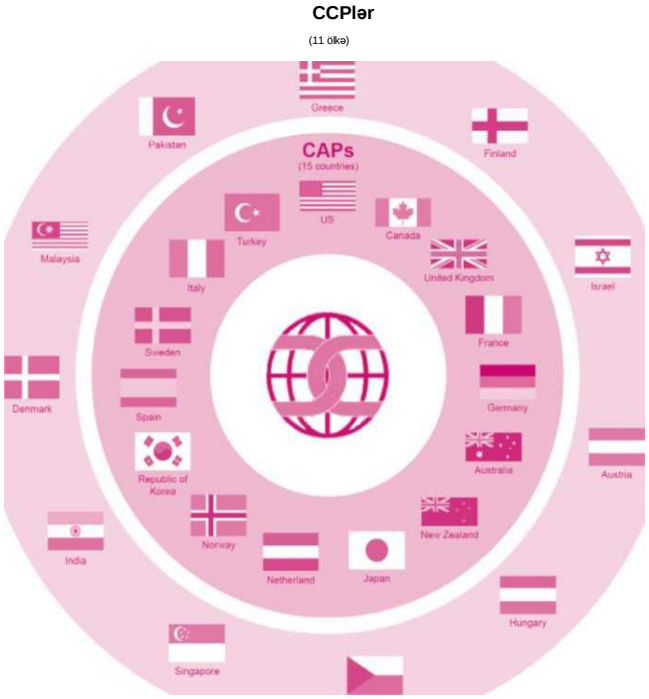
3. **Digərləri:** ADV, AGD, ALC, ATE, AVA və ACO qiymətləndirməsi.

Ümumi Meyarları Tanıma Sazişi

Ümumi Meyarları Tanıma Sazişi (CCRA) ölkələr arasında CC şəhadətnamələrinin təsdiq olunması üçün təşkil edilmişdir. Onun məqsədi CC qiymətləndirmələrinin uyğun standartlarla aparılmasını təmin etmək, İT məhsullarının və ya mühafizə profillərinin təkrar qiymətləndirilməsini aradan qaldırmaq və ya azaltmaq və ölkələr arasında şəhadətnamənin təsdiq olunması ilə İT sənayesi üçün qlobal bazar imkanlarını yaxşılaşdırmaqdır.

CCRA 26 üzv ölkədən ibarətdir, onlardan 15-I Şəhadətnamələrə İcazə Verən İştirakçılar (CAP-lar) və 11 Şəhadətnamələrdən İstifadə Edən İştirakçılardır (CCP-lər) CAP-lar qiymətləndirmə şəhadətnamələrini hazırlayanlardır. Onlar öz ölkələrində faəliyyət göstərən müvafiq şəhadətnamə verən qurumu maliyyələşdirən tərəfdirlər və onlar şəhadətnamələrə icazə verirlər. Ölkə, CAP olmaq üçün müraciət etməzdən əvvəl, minimum iki il müddətinə CCP qismində CCRA-nın üzvü olmalıdır. CCP-lər qiymətləndirmə şəhadətnamələrinin istehlakçılarıdır. Onlar İT təhlükəsizlik qiymətləndirmə potensialına malik olmasalar da, təsdiq olunmuş / etibarlı sayılmış məhsullardan və mühafizə profillərindən istifadəyə maraq göstərirlər. CCRA-ya üzv olmaq üçün ölkə Nəzarət Komitəsinə yazılı müraciət etməlidir.

Şəkil 11. CAP-lar və CCP-lər



4.2 İnformasiya Təhlükəsizliyi Metodologiyasının Nümunələri

Amerika Birləşmiş Ştatlarının Milli Standartlar və Texnologiya İnstitutu

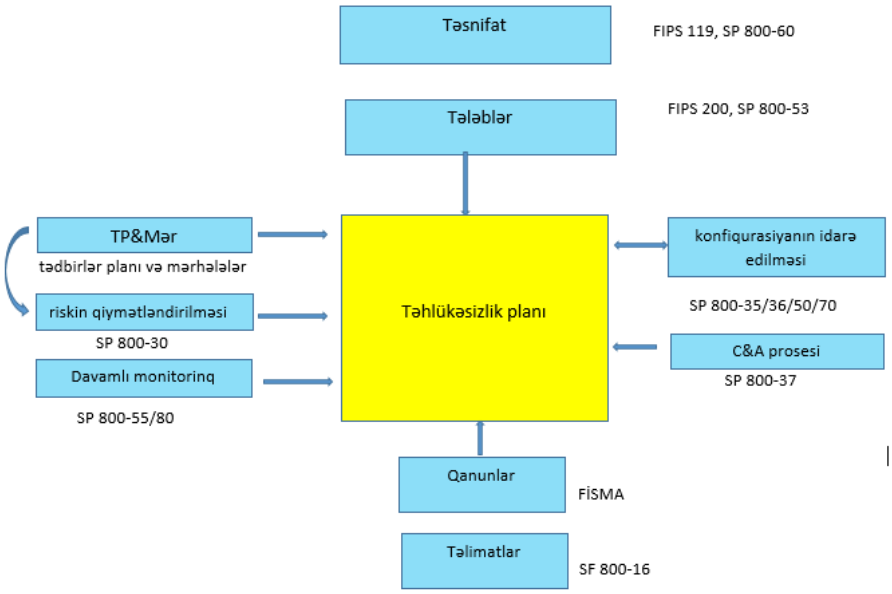
FİSMA əsasında, ABŞ Milli Standartlar və Texnologiya İnstitutu federal təşkilatların istifadə edə biləcəyi informasiya və informasiya sistemlərinin təhlükəsizliyinin gücləndirilməsi üçün tövsiyələr və standartlar işləyib hazırlamışdır. Bu tövsiyələrin və standartların məqsədləri aşağıdakılardan ibarətdir:

- Federal informasiya və informasiya sistemlərinin kateqoriyalaşdırılması üçün istifadə edilə bilən standartları işləyib hazırlamaqla minimum təhlükəsizlik tələblərini müəyyənləşdirmək;
- İnformasiya və informasiya sistemlərinin təhlükəsizliyə görə kateqoriyalaşdırılmasına imkan yaratmaq;

- Federal hökumətin icra orqanlarına dəstək göstərən informasiya sistemləri üçün təhlükəsizliklə bağlı nəzarət tədbirlərini seçmək və müəyyən etmək; və
- Zəif tərəflər üzərində təhlükəsizliklə bağlı nəzarətlərin səmərəliliyini və effektivliyini yoxlamaq.

FİSMA ilə bağlı Tövsiyələr xüsusi nərşlər və Federal İnformasiya İşlətmə Standartlarına dair Nəşrlər kimi nəşr edilir. İki xüsusi nəşr seriyası vardır: 500 seriya informasiya texnologiyaları üçün və 800 seriya kompüter təhlükəsizliyi üçün. 13-cü Cədvəldə bu standart əsasında ABŞ hökumətinin öz təhlükəsizlik planlarını müəyyənləşdirməsi prosesi göstərilir.

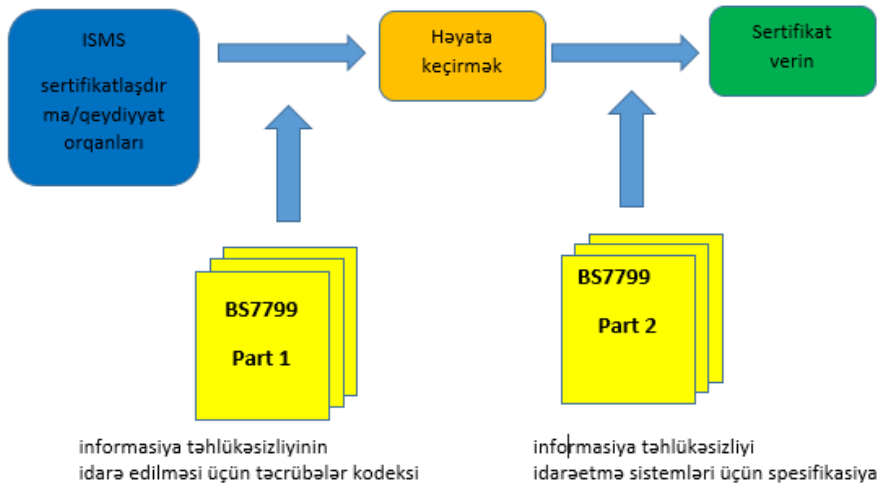
Şəkil 13. Təhlükəsizliyin planlaşdırılması prosesinin giriş/çıxışı



Birləşmiş Krallıq (BS7799)

Əvvəldə qeyd olunduğu kimi, BK-də BSİ təşkilatların təhlükəsizliklə bağlı tədbirlərini təhlil edir və BS7799 şəhadətnaməsini verir, hansı ki indi, bu, ISO27001 (BS7799 2-ci hissə) və ISO27002 (BS7799 1-ci hissə) şəhadətnamələridir. 14-cü Təsvirdə həyata keçirilən prosedur göstərilir.

Şəkil 13. BS7799 sertifikatlaşdırma prosesi

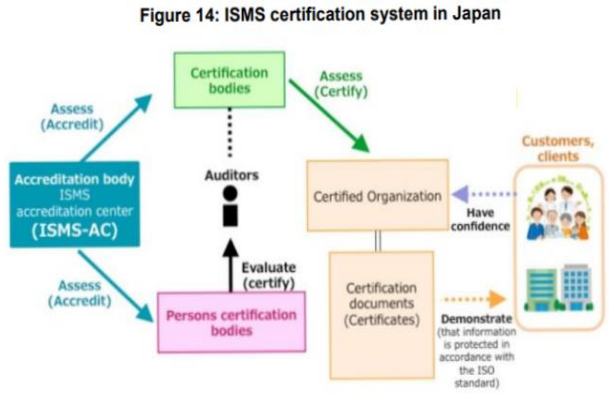


Yaponiya (ISMS Ver2.0-dən JIS Q 27001:2014-ə doğru)

Yaponiya İnformasiya Emal İnkişaf Korporasiyasının ISMS Ver2.0 variantı 2002-ci ilin aprel ayından Yaponiyada tətbiq edilir. Həmin vaxtdan bəri, o, BS7799 Hissə 2 ilə əvəzlənmişdir: 2002, JIS Q 27001: 2006, ISO/IEC 27001: 2005-in nəşrinə uyğun olaraq 2006-cı ilin martında və sonra yenidən işlənmiş və ISO/IEC 27001-in yenidən nəzərdən keçirilmiş, 2014-cü ilin martında buraxılmışdır JIS Q 27001.
Yaponiyada İSMS uyğunluq qiymətləndirməsi sxemi, ISO/IEC 27001 əsasında təşkilatın İSMS-ni dəyərləndirən və təsdiqləyən "sertifikatlaşdırma orqanları", İSMS auditorları təsdiqləyən və qeydiyyata alan "heyəti sertifikatlaşdırma orqanları" və bu vəzifələri yerinə yetirərkən həmin orqanların sərištəsini dəyərləndirən "akkreditasiya orqanından" ibarət olan geniş struktura malikdir. "Auditorların təlim orqanları"na gəldikdə, heyətin sertifikatlaşdırılması orqanları həmin orqanların qiymətləndirilməsini aparır və qiymətləndirmənin nəticəsinə əsasən onları təsdiqləyir.

Şəkil 14-də Yaponiyada İSMS şəhadətnamələrinin verilmə sistemi təsvir olunur.

Şəkil 14. Yaponiyada ISMS şəhadətnamələrinin verilməsi



Source : ISMS Accreditation Centre. Overview of the ISMS conformity assessment scheme. ISMS-AC. https://isms.jp/english/isms/about.html.

Koreya Respublikası (KISA ISMS)

2002-ci ildən bəri KKK və KİSA İSMS şəhadətnamələrinin verilməsi proqramını tətbiq etməyə və həyata keçirməyə başlamışdır. KKK və KİSA İSMS şəhadətnamələrinin verilməsi proqramını təşviq etmək üçün böyük səylər göstərmişdir və bu gün, o, çox uğurlu proqram hesab edilir. İSMS şəhadətnamələrinin verilmə sxemi və prosedurları müvafiq olaraq 16 və 17-ci təsvirlərdə göstərilir. 2011-ci ildə İSMS şəhadətnamələrinin sayı 114-ə çatmışdır. Say artdığından, hər bir şəhadətnamə alan təşkilatda informasiya təhlükəsizliyinin xeyli artacağı gözlənilir. Şəhadətnamə alan təşkilatlar arasında müxtəlif biznes sahələrində KT, Korean Air, NHN, Daum və sairə kimi aparıcı şirkətlər də vardır.

Şəkil 15. Koreya Respublikasında ISMS şəhadətnamələrinin verilmə sxemi

- Müvafiq qanunlar, qaydalar və siyasət
- İSMS büdcəsinə dəstək

Şəhadətnamə verən qurum (KISA)

Şəhadətnamələr Komitəsi

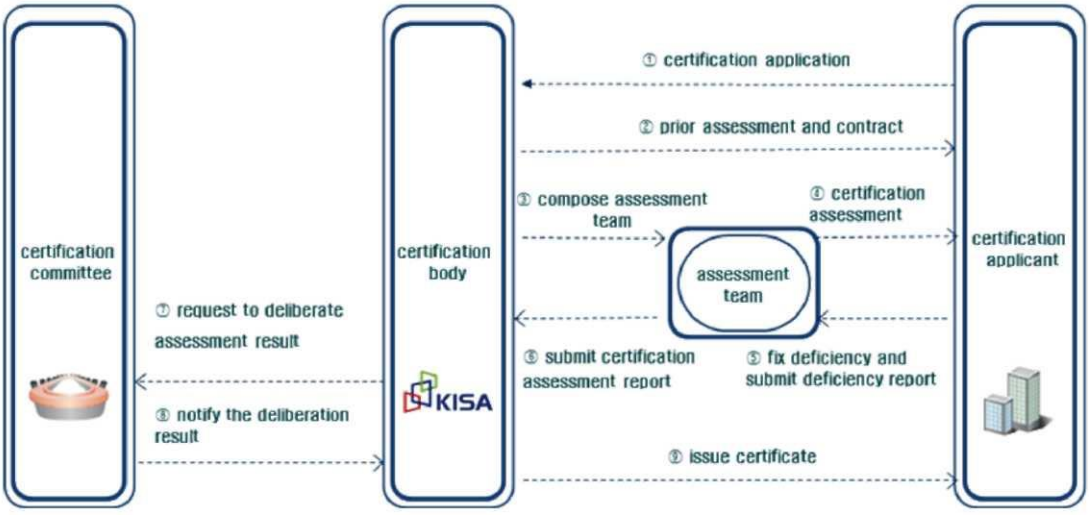
- Dəyərləndirmənin nəticələrini nəzərdən keçirmək və təsdiq etmək
- İnformasiya | Təhlükəsizlik ekspertlərindən ibarətdir

- Şəhadətnamə verilmə üçün meyarları və tövsiyələri işləyib hazırlamaq
-İSMS şəhadətnamələr proqramını işlətmək və təkmilləşdirmək
- Şəhadətnamələri vermək / nəzarət etmək
- Texniki məsləhətlər vermək
- Davamlı dəyərləndirmə aparmaq

Daxil olma vasitəsi

- Şəhadətnamə üçün dəyərləndirmə
- Dəyərləndirmə hesabatını hazırlama
- KİSA heyət üzvlərindən və kənar ekspertlərdən ibarətdir

Şəkil 16. Koreya Respublikasında sertifikatlaşdırma prosedurları



Almaniya (IT üzrə İlkin Mühafizə Şərti)

Almaniyada BSI (Bundesamt fur Sicherheit in der Informationstechnik) informasiya təhlükəsizliyi üzrə milli orqandır. O, Almaniyada hökumətə, şəhərlərə, təşkilatlara və fərdlərə İT təhlükəsizlik xidmətləri göstərir.

BSİ, İT üzrə İlkin Mühafizə Şərtini, İSO Guide 25 (GUİ25) beynəlxalq standartı və İT Yoxlama və Şəhadətnamələrin Verilməsi üzrə Avropa Komitəsi tərəfindən qəbul edilmiş EN45001 Avropa standartı əsasında təsis etmişdir. Şəhadətnamə növlərinə İT İlkin Mühafizə Şəhadətnaməsi, Özü-bəyan edilmə (İT İlkin Mühafizə üzrə daha yüksək səviyyə) və Özü-bəyan edilmə (İT İlkin Mühafizə giriş səviyyəsi) aiddir. 1999-cu ildə EN45001 ISO / IEC / EN 17025 ilə əvəzlənmişdir.

Əlavə olaraq, İlkin mühafizə üzrə əyani vəsaiti (BPM) və BSİ Standart Seriyası:100-X yardımçı əyani vəsaiti işlənib hazırlanmışdır. Bura aiddir: BSİ Standart 100-1 İSMS, BSİ Standart 100-2 BPM Metodologiyası və BSİ Standart 100-3 Risklə bağlı təhlillər.[42]

2011-ci ildə Almaniya rəsmi olaraq Bonn-da yerləşən yeni Alman Milli Kiber Müdafiə Mərkəzini (NCAZ-National Center for Cyber Defense, Nationales Cyber-Abwehrzentrum) açdı. NCAZ milli təhlükəsizlik aspektlərinə diqqət yetirən Almaniyanın BSI, BKA (Federal Polis Təşkilatı), BND (Federal Kəşfiyyat Xidməti), MAD (Hərbi Kəşfiyyat Xidməti) və digər milli təşkilatlar ilə sıx əməkdaşlıq edir. NCAZ-ın əsas vəzifəsi milli infrastruktura qarşı hücumları aşkar etmək və qarşısını almaqdır. Almaniya, Darmstadtda Avropanın İT təhlükəsizliyi üzrə ən böyük tədqiqat institutunu yaradıb, Təhlükəsizlik və Şəxsi Həyatın Toxunulmazlığı üzrə Araşdırma Mərkəzi (the Center for Research in Security and Privacy- CRISP).

Digər

Cədvəl 8-də digər mövcud olan İSMS şəhadətnamələri sadalanır.

[42] Antonius Sommer, "Almaniyada, habelə Avropada təhlükəsizlik strategiyası meylləri" , 10 aprel 2006-cı tarixdə Koreya Respublikasının Seul şəhərində Kiber Təhlükəsizlik Sammitində təqdim olunmuşdur, http://www.unapcict.org/ecohub/resources/trends-of-security-strategy-2.

Cədvəl 8. Digər ölkələrin ISMS şəhadətnaməsi

	Şəhadətnamə verən təşkilatlar	Standartlar
Kanada	Kommunikasiya Təhlükəsizlik Müəssisəsi	MG-4 Məlumat üçün Şəhadətləndirmə və Akkreditasiya Bələdçisi Texnologiya Sistemləri
Almaniya	DAkkS	
Hindistan	Sınaq üzrə Milli Akkreditasiya Şurası və Kalibrləmə Laboratoriyaları (NBAL)	
İndoneziya	Milli Akkreditasiya Komitəsi (KAN)	
İrlandiya	İrlandiya Milli Akkreditasiya Şurası (INAB)	
Yeni Zelandiya	Beynəlxalq Akkreditasiya Yeni Zelandiya (IANZ)	
Çinin Tayvan əyaləti	Standartlar, Meteorologiya və Təftiş Bürosu	CNS 17799 & CNS 17800
Hollandiya	Hollandiya Akkreditasiya Şurası (DAC)	
Sinqapur	İnformasiya Texnologiyaları Standartları Komitəsi	SS493: Hissə 1 (İT Təhlükəsizlik Standart Çərçivəsi) və SS493: Hissə 2 (Təhlükəsizlik Xidmətləri) inkişaf mərhələsindədir
Koreya Respublikası	Koreya Laboratoriya Akkreditasiya Sxemi (KOLAS)	
Vyetnam	Akkreditasiya Bürosu	

5. ŞƏXSİ HƏYATIN TOXUNULMAZLIĞININ QORUNMASI

Bu bölümün məqsədləri aşağıdakılardan ibarətdir:

- Şəxsi həyatın toxunulmazlığı **konsepsiyasında dəyişiklikləri izləmək;**
- Şəxsi həyatın toxunulmazlığı nın **qorunmasında beynəlxalq meyllərə dair məlumat vermək; və**
- Şəxsi həyatın toxunulmazlığına **Təsirin Dəyərləndirilməsinə nəzər salmaq və nümunələr gətirmək.**

5.1 Şəxsi həyatın toxunulmazlığı konsepsiyası

Fərdi informasiya şəxsiyyəti müəyyən edilə bilən fərdə[43] və ya şəxsiyyəti müəyyən edilmiş və ya edilə bilən şəxsə aid informasiyadır.[44] Bura şəxsin adı, telefon nömrəsi, ünvanı, e-poçt ünvanı, avtomobilinin dövlət nömrə nişanı, fiziki xüsusiyyətləri (sifət quruluşu, əl barmaq izləri, yazı xətti və s.), kredit kart nömrəsi və ailə münasibətləri kimi informasiya aiddir.

Fərdin şəxsi informasiyasına qanunsuz çıxış və bu informasiyanı toplama, təhlil etmə və istifadə həmin fərdə qarşı digərlərinin davranışına təsir göstərir və yekunda onun sosial vəziyyətinə, əmlakına və təhlükəsizliyinə neqativ təsir göstərir. Buna görə də, şəxsi informasiya icazəsiz daxil olma, toplama, saxlama, təhlil etmə və istifadə hallarından qorunmalıdır. Bu mənada, şəxsi informasiya qorunmalıdır.

Əgər qorunan şəxsi informasiyaya malik olma hüququdursa, şəxsi informasiyanın özü deyilsə, bu, şəxsi həyatın toxunulmazlığı konsepsiyasıdır. Şəxsi həyatın toxunulmazlığı hüququ beş üsulla izah edilir:

- Arzu olunmaz müdaxilələrə məruz qalmama hüququ (məsələn, fiziki müdaxilə, qısa məktub xidməti vasitəsilə müdaxilə)
- Şəxsi informasiyanın arzu olunmaz yolla istifadəsinə icazə verməmək hüququ (məsələn, informasiyanın satışı, informasiyanın açıqlanması, üzləşdirmə)
- Məlumat və razılıq olmadan digərləri tərəfindən şəxsi informasiyanın toplanmasına icazə verməmək hüququ (CCTV-dən və məxfi sözləri öyrənməklə)
- Şəxsi informasiyanın dəqiq və düzgün ifadə olunması hüququ (tamlıq)
- Öz şəxsi informasiyasının dəyərinə görə qarşılıq alma hüququ

Passiv Şəxsi həyatın toxunulmazlığı konsepsiyası isə sərbəst buraxılmaq hüququnu və insanların ləyaqəti ilə bağlı təbii hüququ əhatə edir. Bu, sui-istifadəni qadağan edən qanunla bağlıdır.

---

43 Kabinet , Şəxsi həyatın toxunulmazlığı *və məlumatları bölüşmə: ictimai xidmətlərə doğru yol (aprel 2002-ci il),* http://ctpr.org/wp-content/ uploads/2011/03/Privacy-and-data-sharing-the-way-forward-for-public-services-2002.pdf.

44 EurLex, "Şəxsi məlumatların işlənməsi ilə bağlı fərdlərin qorunmasına və belə məlumatların azad hərəkətinə dair Avropa Parlamentinin və Şurasının 95/46/EC nömrəli Direktivi", http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=en&type_doc=Directive&an_doc=1995&nu_doc=46.

Aktiv Şəxsi həyatın toxunulmazlığı hüququ isə şəxsi informasiyaya özü tərəfindən nəzarət və ya şəxsi informasiyanı pozitiv idarə etmək / ona nəzarət etmək hüququ, o cümlədən qeyri-dəqiq şəxsi informasiyanın nəticələrinə düzəlişlər etmək hüququnu əhatə edir.

5.2 Şəxsi həyatın toxunulmazlığı siyasətində meyllər

Şəxsi həyatın toxunulmazlığının qorunmasına dair OECD-nin tövsiyələri

1980-ci ildə OECD, "OECD-nin Ədalətli İnformasiya Təcrübələri" kimi də məlum olan, "Şəxsi həyatın toxunulmazlığının Qorunması və Şəxsi Məlumatların Transsərhəd Axınları üzrə Tövsiyələri" qəbul etmişdir. 2002-ci ildə "Onlayn məkan Şəxsi həyatın toxunulmazlığı: siyasət və təcrübə üzrə istiqamətlər" elan edilmişdir.[45] Tövsiyələr, şəxsi məlumatların işlənmə tərzinə və ya bu məlumatların mahiyyətinə və ya istifadə olunma kontekstinə görə Şəxsi həyatın toxunulmazlığı və fərdi azadlıqlar üçün təhlükə doğuran, ictimai və ya özəl sektorda olmasına baxmayaraq bu cür məlumatlara aiddir. Tövsiyələrdə müəyyən olunmuş OECD prinsipləri şəxsi məlumatların avtomatlaşdırılmış şəkildə işlənməsi kontekstində fərdlərin hüquq və vəzifələrini və bu prosesdə iştirak edənlərin hüquq və vəzifələrini bəyan edir. Bundan əlavə, Tövsiyələrdə təsbit olunmuş əsas prinsiplər həm milli, həm də beynəlxalq səviyyələrdə tətbiq oluna bilər.

OECD tövsiyələrini təşkil edəb səkkiz prinsip aşağıdakılardır:

1.Məlumatların toplanmasına məhdudiyyət prinsipi

Şəxsi məlumatların toplanmasında məhdudiyyətlər olmalıdır və belə məlumatlar qanuni və ədalətli vasitələrlə və zəruri olduqda, məlumatın aid olduğu şəxsə bildirməklə və onun razılığı ilə əldə edilməlidir.

2.Məlumatların keyfiyyətliliyi prinsipi

Şəxsi məlumatlar onlardan istifadə olunma məqsədlərinə uyğun və məqsədlər üçün zəruri olan həcmdə olmalıdır, habelə dəqiq, tam və yenilənmiş olmalıdır.

3.Məqsədin göstərilmə prinsipi

Şəxsi məlumatların toplanma məqsədləri həmin məlumatlar toplanılarkən və sonrakı istifadə zamanı isə bu məqsədlər və ya onlarla uyğunsuzluq təşkil etməyən digər məqsədlər yerinə yetirilənədək və məqsədin dəyişdiyi hər bir hal üçün göstərilməlidir.

4.İstifadəyə məhdudiyyət prinsipi

45 OECD, "Onlayn məkan toxunulmazlıq: siyasət və təcrübə üzrə istiqamətlər", http://www.oecd.org/document/49/0,3343, en_2649_34255_19216241_1_1_1_1,00.html.

Şəxsi məlumatlar, məlumatın aid olduğu şəxsin özünün razılığı ilə və ya qanunla nəzərdə tutulmuş hallar istisna olmaqla, məqsədlərin göstərilmə prinsipinə uyğun olaraq göstərilmiş məqsədlərdən başqa məqsədlər üçün açıqlanmamalı, mövcud olmamalı və ya digər bir şəkildə istifadə edilməməlidir.

5. Təhlükəsizliyin qorunması prinsipi

Şəxsi məlumatlar, itmə və ya icazəsiz müdaxilə, məhv edilmə, istifadə, dəyişdirilmə və açıqlanma kimi risklərə qarşı uyğun təhlükəsizlik tədbirləri ilə qorunmalıdır.

6. Aşkarlıq prinsipi

Şəxsi məlumatlarla bağlı inkişafa, təcrübələrə və siyasətlərə dair ümumi aşkarlıq siyasəti olmalıdır. Şəxsi məlumatların mövcudluğunun və mahiyyətinin və onlardan istifadənin əsas məqsədlərin, habelə məlumata nəzarət edənin şəxsiyyətinin və adi yaşayış ünvanının müəyyənləşdirilməsi üçün vasitələr hazır şəkildə olmalıdır.

7. Fərdin iştirakı prinsipi

Fərd aşağıdakı hüquqlara malik olmalıdır:

Məlumatlara nəzarət edəndən onda müvafiq şəxslə bağlı məlumatın olub-olmamasını öyrənmək;
Məntiqli vaxt çərçivəsində, tətbiq edildiyi halda həddən yuxarı olmayan ödənişlə, məntiqli şəkildə və şəxsin özünə bəlli olan formada özü ilə bağlı məlumatı öyrənmək;
Əgər (a) və (b) bəndlərində nəzərdə tutulmuş sorğuya imtina edildiyi təqdirdə səbəbləri öyrənmək və belə imtinalara bağlı iddia qaldırmaq imkanına malik olmaq;
Özü ilə bağlı məlumatlara dair iddia qaldırmaq və iddia uğurlu olduqda silinmiş, dəyişdirilmiş, tam və ya düzəliş edilmiş məlumatı almaq.

8.Cavabdehlik prinsipi

Məlumatlara nəzarət edən şəxs yuxarıda qeyd olunan prinsiplərdən irəli gələn ölçülərə uyğun davranmaqla bağlı cavabdehlikd daşıyır.[46]

Şəxsi həyatın toxunulmazlığının qorunması ilə bağlı BMT-nin tövsiyələri

1960-cı illərdən bəri, dünya, informasiyanın avtomatlaşdırılmış şəkildə işlənməsinin toxunulmazlığa təsirinə diqqət yetirmişdir. Birləşmiş Millətlər Təşkilatının Elm, Təhsil və Mədəniyyət Təşkilatı (YUNESKO) xüsusilə, 1990-cı ildə Baş Assambleya tərəfindən "Kompüterləşdirilmiş Şəxsi Məlumat Fayllarının Tənzimlənməsi üzrə BMT Tövsiyələri" qəbul edildiyi vaxtdan bəri toxunulmazlığa və toxunulmazlığın qorunmasına maraq göstərmişdir.

[46] Bu prinsiplərin sadalandığı bütöv sənədi oxumaq, bax, Toxunulmazlığın Qorunması və Şəxsi Məlumatların Transsərhəd Axınları üzrə OECD Tövsiyələri , http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html.

BMT Tövsiyələri, ictimai və özəl sektorlarda sənədlərə, habelə kompüterləşdirilmiş məlumat fayllarına tətbiq edilir. Tövsiyələr milli qanunvericilikdə və ya beynəlxalq təşkilatların daxili qanunlarında təmin edilməli olan minimum zəmanətlərlə bağlı aşağıdakı prinsipləri müəyyən edir:

1.Qanunilik və ədalətlilik prinsipi

Şəxslər barəsində informasiya nə ədalətsiz və ya qanunsuz yollarla toplanmamalı, nə də Birləşmiş Millətlər Təşkilatının Nizamnaməsindəki məqsədlərə və prinsiplərə zidd olan məqsədlər üçün istifadə edilməməlidir.

2.Dəqiqlik prinsipi

Faylların toplanmasına görə cavabdeh olan şəxslər və ya onların saxlanmasına görə cavabdeh olan şəxslər, qeydə alınmış məlumatların dəqiqliyi və uyğunluğuna dair mütəmadi yoxlamalar aparmaq və səhvlərə yol verməmək üçün onların mümkün qədər tam saxlanmasını və mütəmadi olaraq və ya faylda saxlanılan informasiyadan istifadə edilərkən işlənənə qədər yenilənməsini təmin etmək vəzifəsini daşıyırlar.

3.Məqsədin dəqiq göstərilməsi prinsipi

Faylın xidmət etdiyi məqsəd və bu məqsəd baxımından ondan istifadə dəqiq göstərilməli, qanuni olmalı və müəyyən edildiyi təqdirdə, onu, aşağıdakıların təmin edilməsi məqsədilə, mümkün etmək üçün müəyyən qədər açıqlanmalı və ya aidiyyəti şəxsin diqqətinə çatdırılmalıdır:

a) Bütün toplanan və saxlanılan şəxsi məlumatlar dəqiq göstərilmiş məqsədlərə uyğun və lazımi şəkildə qalır;
b) Müvafiq şəxsin özünün razılığı ilə olan hallar istisna edilməklə, qeyd olunan şəxsi məlumatlardan heç biri göstərilənlərlə bir araya sığmayan məqsədlər üçün istifadə olunmur və ya açıqlanmır; və
c) Şəxsi məlumatın saxlandığı müddət göstərilən məqsədlərə nail olmağa imkan verən müddətdən artıq saxlanmır.

4.Maraqlanan şəxsin daxil olma imkanı prinsipi

Öz şəxsiyyətini təsdiq edən hər kəs onun barəsində informasiyanın işlənib-işlənməməsini bilmək və bunu hədsiz ləngimə və ya məsrəf olmadan, aydın formada əldə etmək və qanunsuz, zərurət olmadan və ya qeyri-düzgün daxil olma hallarında müvafiq düzılişlərin və ya təmizləmələrin aparılmasına nail olmaq və bu, bildirildiyi halda, ünvan sahibiləri barədə məlumat almaq hüququ vardır.

5.Ayrı-seçkiliyin yolverilməzliyi prinsipi

6-cı prinsipdə məhdudlaşdırıcı şəkildə nəzərdə tutulan hallar istisna olmaqla, qanunsuz və ya despotik ayrı-seçkiliyə yola açan məlumatlar, o cümlədən irqi və ya etnik mənşə, rəng, cinsi həyat, siyasi baxışlar, dini, fəlsəfi və ya digər inamlar, habelə hər hansı bir assosiasiyaya və həmkarlar ittifaqına üzvlük barədə informasiya toplanmamalıdır.

6.İstisnalar etmək səlahiyyəti

1 – 4-cü prinsiplərdən istisnalara yalnız milli təhlükəsizliyi, ictimai qaydanı, əhalinin sağlamlığını və ya əxlaqı, habelə, eyni zamanda digərlərinin, xüsusən də təqib olunan (humanitar səbəbdən) şəxslərin hüquq və azadlıqlarını qorumaq üçün zəruri olan hallarda icazə verilir. Lakin, bu istisnalar, hüdudların aydın şəkildə qeyd olunduğu və müvafiq ehtiyat tədbirlərinin təyin olunduğu daxili hüquqi sistemə uyğun olaraq bəyan edilən qanunda və ya digər eyni qüvvəli qaydada aydın şəkildə göstərilməlidir.

1 - 4-cü prinsiplərə istisnalar üçün nəzərdə tutulan eyni ehtiyat tədbirlərinə riayət eləməkdən əlavə olaraq, ayrı-seçkiliyin qadağan olunması ilə bağlı 5-ci prinsipə istisnalara, yalnız insan hüquqlarının qorunması və ayrı-seçkiliyin qadağan olunması sahəsində İnsan Hüquqları haqqında Beynəlxalq Bill və digər müvafiq sənədlərdə nəzərdə tutulan hüquqlarda icazə verilə bilər.

7.Təhlükəsizlik prinsipi

Müvafiq tədbirlər, faylları, həm qəza nəticəsində itmə və ya məhv olma kimi təbii təhlükələrə, həm də icazəsiz daxil olma, məlumatdan dələduzluq məqsədilə sui-istifadə və kompüter viruslarına yoluxdurma kimi insanın törətdiyi təhlükələrə qarşı qorumaq üçün görülməlidir.

8.Nəzarət və sanksiyalar

Hər bir ölkənin qanunu, daxili hüquq sisteminə uyğun olaraq, yuxarıda qeyd olunan prinsiplərə riayət olunmasına nəzarətə görə cavabdeh olan orqanı təyin etməlidir. Hər bir orqan qərəzsizliyə, məlumatların işlənməsinə və müəyyənləşdirilməsinə görə cavabdeh şəxslər və orqanların bilavasitə müstəqilliyinə və texniki səriştəyə görə zəmanətlər təklif etməlidir. Yuxarıda göstərilən prinsipləri tətbiq edən milli qanunun müddəaları pozulduğu halda müvafiq şəxsin hüquqlarının bərpası ilə yanaşı cinayət və ya digər cəzalar nəzərdə tutulmalıdır.

9.Transsərhəd məlumat axınları

Transsərhəd məlumat axınları ilə bağlı iki və ya daha çox ölkənin qanunvericiliyində toxunulmazlığın qorunması üçün müqayisə edilə bilən ehtiyat tədbirləri təklif olunduğu təqdirdə, informasiya, aidiyyəti ərazinin hər birinin daxilində olduğu sərbəst şəkildə yayımlana bilər. Qarşılıqlı ehtiyat tədbirləri olmadığı təqdirdə, belə yayıma məhdudiyyətlər hədsiz şəkildə yox və yalnız toxunulmazlığın qorunması üçün tələb olunan qədər qoyulmalıdır.

10. Tətbiq olunma sahəsi

Bu prinsiplər, ilk növbədə, bütün əhali və özəl kompüterləşdirilmiş fayllara və könüllü genişləndirmə vasitəsilə və müvafiq düzəlişlər edilməklə, əl ilə yığılmış qeydiyyatlara tətbiq edilməlidir. Xüsusi müddəalar, həmçinin, könüllü şəkildə bu prinsiplərin hamısının və ya bir hissəsinin, xüsusilə də fərdlərlə bağlı informasiyaya malik olduqları halda hüquqi şəxslərə də şamil edilməsini nəzərdə tuta bilər.[47]

[47] Bu prinsiplər İnsan Hüquqları üzrə Ali Komissarlıqdan sitat gətirilmişdir, "Kompüterləşdirilmiş Şəxsi Məlumat Faylarının Tənzimlənməsi üzrə Tövsiyələr", http://www.unhcr.org/refworld/publisher,UNGA,THEMGUIDE,,3ddcafaac,0.html.

Məlumatın məxfiliyi, etika və mühafizəsi Birləşmiş Millətlər Təşkilatının İnkişaf Qrupu (United Nations Development Group - UNDG) tərəfindən dərc edilib və BMTİG qurumlarına şamil edilir.

Bu sənəd böyük məlumatların istifadəsi ilə bağlı məlumatların məxfiliyi, məlumatların qorunması və məlumat etikasına dair ümumi təlimatları müəyyən edir. Özəl sektor qurumları tərəfindən biznes təkliflərinin bir hissəsi kimi real vaxt rejimində toplanmış və 2030-cu il Gündəliyinə nail olunmasını dəstəkləmək üçün proqramlarının operativ icrasını gücləndirmək məqsədilə BMT-nin İnkişaf Proqramının üzvləri ilə paylaşılmışdır.

Təlimatda aşağıdakı kimi göstərilir:

1. Hüquqi, qanuni və ədalətli istifadə

Məlumata daxil olmaq, onu təhlil etmək və ya digər istifadə Birləşmiş Millətlər Təşkilatının Nizamnaməsinə uyğun olmalıdır və Dayanıqlı İnkişaf Məqsədlərinə uyğun olmalıdır.

2. Məqsədin göstərilməsi, istifadə məhdudiyyəti və məqsəd uyğunluğu

Məlumatların istifadəsi uyğun və ya başqa yolla əlaqəli olmalıdır və əldə edilmə məqsədindən kənara çıxmamalıdır

3. Riskin azaldılması və risk, zərər və faydanın qiymətləndirilməsi

Məlumatların yeni və ya əhəmiyyətli dərəcədə dəyişdirilmiş istifadəsi həyata keçirilməzdən əvvəl məlumatların qorunmasının və məlumatların məxfiliyinin, eləcə də məlumatdan istifadə etikasını nəzərə alan risk, zərər və faydaların qiymətləndirilməsi aparılmalıdır.

4. Həssas məlumatlar və kontekstlər

Həssas əhali və risk altında olan şəxslər, uşaqlar və gənclər və ya hər hansı digər həssas məlumatların əldə edilməsi, toplanması, təhlili və ya başqa şəkildə istifadəsi zamanı daha ciddi məlumatların qorunması standartlarından istifadə edilməlidir.

5. Məlumat təhlükəsizliyi

Məlumat təhlükəsizliyi məlumatın məxfiliyinin və məlumatların qorunmasının təmin edilməsində çox vacibdir. Mövcud texnologiya və həyata keçirmə xərclərini nəzərə alaraq, məlumatların həyat dövrü ərzində düzgün idarə olunmasını təmin etmək və hər hansı icazəsiz istifadənin, açıqlamanın və ya icazəsiz girişin qarşısını almaq üçün möhkəm texniki və təşkilati təminatlar və prosedurlar (məlumatlara girişin səmərəli monitorinqi və məlumatların pozulması barədə bildiriş prosedurları daxil olmaqla) həyata keçirilməlidir.

6. Məlumatların saxlanması və məlumatların minimuma endirilməsi

Məlumata çıxış, təhlil və ya digər istifadə onun məqsədini yerinə yetirmək üçün lazım olan minimum məbləğdə saxlanılmalıdır. Məlumatların miqdarı, o cümlədən onun təfərrüatları minimum lazımi qədər məhdudlaşdırılmalıdır. Məlumatdan istifadə zamanı onun istifadəsinin qanuni ehtiyaclarını aşmamasını təmin etmək üçün monitorinq edilməlidir.

7. Məlumatın keyfiyyəti

Məlumatla bağlı bütün fəaliyyətlər adekvat keyfiyyət və şəffaflıq səviyyəsində tərtib edilməli, həyata keçirilməli, hesabat verilməli və sənədləşdirilməlidir. Daha konkret desək, ağlabatan mümkün ölçüdə olmalıdır və məlumatlar dəqiqlik, uyğunluq, kafilik, bütövlük, tamlıq, istifadəyə yararlılıq, etibarlılıq və uyğunluq baxımından təsdiq edilməli və yenilənməlidir.

8. Açıq məlumat, şəffaflıq və hesabatlılıq

Müvafiq qanunlara, o cümlədən məxfilik qanunlarına və məlumatların istifadəsi ilə bağlı ən yüksək məxfilik standartlarına, əxlaqi və etik davranışa riayət olunmasına nəzarət etmək üçün müvafiq idarəetmə və hesabatlılıq mexanizmləri yaradılmalıdır.

9. Üçüncü tərəf əməkdaşları üçün lazımi araşdırma

Məlumatdan istifadə ilə məşğul olan üçüncü tərəf əməkdaşları müvafiq qanunlara, o cümlədən məxfilik qanunlarına, eləcə də ən yüksək məxfilik standartlarına və əxlaqi və etik davranış qaydalarına uyğun hərəkət etməlidirlər.

Avropa İttifaqında Məlumatların Mühafizəsi

Avropa İttifaqının Nazirlər Şurası ilkin olaraq tənzimləyici normaları təmin etmək üçün və həmçinin, şəxsi məlumatların saxlandığı, ötürüldüyü və ya işləndiyi hər yerdə şəxsi məlumatlar ətrafında təhlükəsizlik təməlinin qurulmasına əlavə olaraq, Avropa İttifaqına üzv ölkələrin milli sərhədləri boyunca şəxsi məlumatların sərbəst hərəkətini təmin etmək üçün 24 oktyabr 1995-ci ildə Fərdi məlumatların emalı və bu cür məlumatların sərbəst hərəkəti ilə əlaqədar şəxslərin qorunmasına dair Avropa Direktivini (Aİ Direktivi 95/46/EC) qəbul etdi.

Bu direktiv 2016-cı ilin aprel ayında rəqəmsal dövrdə fərdlərin əsas hüquqlarını gücləndirən və rəqəmsal vahid bazarda şirkətlər və dövlət qurumları üçün qaydaları aydınlaşdırmaqla biznesi asanlaşdıran 2016/679 saylı Qayda (Aİ) ilə ləğv edilib. Vahid qanun həm də müxtəlif milli sistemlərdə mövcud parçalanmanı və lazımsız inzibati yükləri aradan qaldıracaq. Qayda (Aİ) 2016/679 24 may 2016-cı ildə qüvvəyə minib və 25 may 2018-ci ildən tətbiq edilir.

Amerika Birləşmiş Ştatlarında şəxsi həyatın toxunulmazlığının qorunması

Hökumət tərəfindən qoyulan həddən çox məhdudiyyətlər e-kommersiya fəaliyyətinə mane olduğundan, ABŞ, toxunulmazlığın qorunması tədbirlərini bazara həvalə etmişdir. Nəticədə, e-İnan və ya Daha Yaxşı Biznes Bürosu Onlayn kimi toxunulmazlığa zəmanətlər meydana çıxmışdır və Şəxsi həyatın toxunulmazlığı qorunması haqqında qanunlar birləşdirilməmişdir. 1974-cü il Şəxsi həyatın toxunulmazlığı haqqında Akt ictimai sektorda toxunulmazlığın qorunmasını nəzərdə tutduğu halda, özəl sektorda bu məsələlər fərqli qanunlarla tənzimlənir. Özəl sektorda toxunulmazlığın qorunması ilə bağlı bütün məsələlərlə məşğul olan heç bir təşkilat yoxdur. İctimai sektorda, Toxunulmazlıq haqqında Akta uyğun olaraq, OBM, federal hökumətin toxunulmazlıq siyasətinin müəyyənləşdirilməsində rol oynayır. Özəl sektorda Federal Ticarət Komissiyası uşaqların onlayn şəbəkədə toxunulmazlığını, müştəri kredit məlumatlarını və ədalətli ticarət təcrübələrini qoruyan qanunları icra etmək səlahiyyətinə malikdir.

ABŞ-da şəxsi həyatın toxunulmazlığının qorunması ilə bağlı qanunlara aşağıdakılar aiddir:

- Şəxsi həyatın toxunulmazlığı haqqında Qanun, 1974
- İstehlakçı kreditin mühafizəsi haqqında Qanun, 1984
- Elektrik kommunikasiyasnın toxunulmazlığı haqqında Qanun, 1986
- İdarə edənin şəxsi həyatının toxunulmazlığı haqqında Qanun, 1986
- Sağlamlıq sığortasının daşınması və cavadehlik haqqında Qanun, 1996
- Uşaqların onlayn məkanda şəxsi həyatın toxunulmazlığının qorunması haqqında Qanun, 1998
- Qramma-Liça-Blileya haqqında Qanun, 1999
- Sarbeyns-Oksli Aktı haqqında Qanun, 2002
- Federal səviyyədə informasiya təhlükəsizliyinin idarə olunması haqqında Qanun, 2002

Bundan əlavə, Amerika Birləşmiş Ştatlarında hər bir ştat üçün şəxsi həyatın toxunulmazlığı qaydaları qəbul edilmişdir.

Düşündürücü suallar

1. Sizin ölkədə informasiyanın toxunulmazlığını qorumaq üçün hansı siyasətlər və qanunlar vardır?

2. Belə siyasətlərin və qanunların qəbul edilməsinə və / və ya icrasına hansı məsələlər və fikirlər təsir göstərir?

3. Sizin ölkədə Şəxsi həyatın toxunulmazlığının qorunması ilə bağlı hansı siyasətlərin və qanunların əsasını hansı prinsiplər (bax, OECD Prinsipləri və BMT Prinsipləri) təşkil edir?

5.3 Şəxsi həyatın toxunulmazlığına təsirin dəyərləndirilməsi (PİA)

PIA nədir?

Şəxsi həyatın toxunulmazlığına Təsirin Dəyərləndirilməsi (PİA) yeni informasiya sistemlərinin tətbiqinin və ua mövcud informasiya sistemlərində modifikasiyasının istehlakçıların və ya ölkənin toxunulmazlığına təsirinin araşdırılmasından, təhlil edilməsindən və qiymətləndirilməsindən ibarət olan sistematik bir prosesdir. PİA ilk olaraq qarşısını alma prinsipinə əsaslanır – yəni qarşısını alma aradan qaldırmadan daha yaxşıdır. Bu, sadəcə sistemin qiymətləndirilməsi deyil, eyni zamanda yeni sistemələrin tətbiqinin və ya dəyişdirilməsinin toxunulmazlığa ciddi təsirlərinin nəzərdən keçirilməsidir. Beləliklə də, bu, Şəxsi həyatın toxunulmazlığı ilə bağlı daxili siyasətə və xarici tələblərə riayət olunmasını təmin edən toxunulmazlığın qorunması auditindən fərqlənir.

PİA, yeni sistem qurularkən Şəxsi həyatın toxunulmazlığı müdaxilə faktorunun təhlil edilməsi üçün aparıldığından, o, inkişaf xüsusiyyətlərində nizamlamanın aparılmasının hələ mümkün olduğu erkən işlənib hazırlanma mərhələsində edilməlidir. Lakin, mövcud xidmət fəaliyyət göstərərkən şəxsi informasiyanın toplanmasında, istifadəsində və idarə olunmasında ciddi müdaxilə riski baş
verdiyi halda, PİA-nın aparılması və bundan sonra sistemdə müvafiq dəyişikliklərin edilməsi məqsədəuyğundur.

PIA prosesi[48]

[48] Bu bölüm İnformasiya və Şəxsi həyatın toxunulmazlığı idarəsindən götürülmüşdür, *Toxunulmazlığa Təsirin Dəyərləndirilməsi: İstifadəçi üçün məlumat*

PİA, ümumiyyətlə, üç mərhələdən ibarətdir (bax, 10-cu Cədvəl).

Cədvəl 9. PIA prosesi

Konseptual təhlil	**Məlumat axınının təhlili**	**Növbəti təhlil**
Təklif olunan layihənin həcmini və iş baxımından məntiqli izahını təsvir etmək üçün aydın dil seçin. İlk olaraq Şəxsi həyatın toxunulmazlığı ilə bağlı mümkün məsələləri və riskləri və əsas maraqlı tərəfləri müəyyən edin. Təklifin əsas aspektlərini təfsilatlı şəkildə təsvir edin, o cümlədən əsas məsələlərin siyasi təhlilini aparın Fərdi informasiyanın əsas axınlarını sənədlərlə təsdiqləyin. Digər yurisdiksiyalar altında oxşar layihənin necə idarə olunduğunu icmallaşdırmaq üçün ətraf-mühitlə bağlı məsələləri diqqətlə nəzərdən keçirin. Maraqlı tərəflərlə bağlı məsələləri və onların maraqlarını müəyyənləşdirin. Əhalinin reaksiyasını öyrənin	İş prosesi diaqramları vasitəsilə məlumat axınlarını təhlil edin və xüsusi məlumat ünsürlərini və ya məlumat qruplarını müəyyən edin. Təklifin informasiya azadlığına və toxunulmazlıqla bağlı qanunvericiliyə və proqramla bağlı qanunlara uyğunluğunu dəyərləndirin. Təklifin geniş baxımdan toxunulmazlıqla bağlı ümumi prinsiplərə uyğunluğunu dəyərləndirin. Təklifin toxunulmazlıqla bağlı təhlil əsasında risk məsələsini təhlil edin və mümkün həll yollarını müəyyənləşdirin. Quruluşlar bağlı seçimləri nəzərdən keçirin və toxunulmazlıqla bağlı diqqət yetirilməyən məsələləri / problemləri müəyyən edin. Toxunulmazlıqla bağlı həll edilməyən məsələlərə cavab hazırlayın.	Toxunulmazlıqla bağlı layihə tələblərinə uyğunluğu təmin etmək üçün avadanlığı və təklif olunan layihənin sistem quruluşunu nəzərdən keçirin və təhlil edin. Təklif olunan layihəyə dair yekun icmal aparın. FOİ və toxunulmazlıqla bağlı qanunvericiliyə, proqramla bağlı müvafiq qanunlara və toxunulmazlıqla bağlı ümumi prinsiplərə uyğunluğu təmin etmək üçün avadanlığa və proqram təminatına dair təklif olunan layihədəki hər hansı dəyişikliklərin toxunulmazlıq və risk baxımından təhlilini aparın. Kommunikasiya planını hazırlayın.

Mənbə: İnformasiya və Toxunulmazlıq İdarəsi, Toxunulmazlığa Təsirin Dəyərləndirilməsi: İstifadəçi üçün məlumat kitabı (Ontario, İdarəetmə Şurasının Katibliyi, 2001-ci il), səh.5

.

PİA-nın əhatə dairəsinin dəyərləndirilməsi

PİA aşağıdakı hallarda aparılır:

1. Böyük həcmdə şəxsi informasiyanı saxlayacaq və idarə edəcək yeni informasiya sistemi yaradılarkən;

kitabı (Ontario, İdarəetmə Şurasının Katibliyi, 2001-ci il).

2. Şəxsi həyatın toxunulmazlığının pozula biləcəyi yeni texnologiyadan istifadə edərkən;
3. Fərdi informasiyanın saxlandığı və idarə olunduğu mövcud informasiya sistemində dəyişikliklər edilərkən;və
4. Şəxsi həyatın toxunulmazlığına müdaxilənin baş verə biləcəyi şəxsi informasiya toplanarkən, istifadə edilərkən, saxlanılarkən və / və ya məhv edilərkən.

Lakin bütün informasiya sistemlərində PİA-nın aparılması zəruri deyildir. Mövcud proqram və sistemdə yalnız cüzi dəyişiklik edildiyi halda PİA aparılmamalıdır.

PİA-nın nümunələri

Amerika Birləşmiş Ştatlarında PİA tələbləri

2002-ci il E-Hökumət Aktı, Bölmə 208, agentliklərin elektron informasiya sistemləri və kolleksiyaları üçün şəxsi həyatın toxunulmazlığına təsirin dəyərləndirilməsini (PIA) icra etməsi tələbini müəyyən edir. Qiymətləndirmə informasiya sistemlərində və kolleksiyalarda məxfiliyin qiymətləndirilməsinin praktiki üsuludur və məxfilik məsələlərinin müəyyən edildiyi və adekvat şəkildə həll edildiyinə dair sənədləşdirilmiş əminlikdir.

Avropa İttifaqında PİA tələbləri

Qayda (Aİ) 2016/679 digər adı ilə Ümumi Məlumatların Qorunması Qaydası (General Data Protection Regulation- GDPR) bəzi hallarda məlumatların qorunması təsirinin qiymətləndirilməsini (Data Protection Impact Assessment- DPIA) tələb edir. Yeni İT sistemləri və layihələri ilə yanaşı, PIA yanaşması təşkilatın məxfilik tənzimləmələrinin strukturlaşdırılmış, dövri nəzərdən keçirilməsi və ya auditi üçün dəyərlidir.

Özünü sınama

1. Fərdi informasiya digər növ informasiyadan nə ilə fərqlənir?
2. Fərdi informasiya necə qorunmalıdır?
3. Şəxsi həyatın toxunulmazlığı ilə bağlı OECD və BMT prinsiplərinin əhəmiyyəti nədən ibarətdir?

4. Şəxsi həyatın toxunulmazlığına təsirin dəyərləndirilməsi nə üçün aparılır?

6. CSIRT-in TƏSİS OLUNMASI VƏ FƏALİYYƏTİ

Bu bölümün məqsədi aşağıdakılardan ibarətdir:

- **Kompüter təhlükəsizliyi ilə bağlı hadisələrin nəticələrinin aradan qaldırılması üzrə qrupun (CSİRT) necə təsis ediliyini və fəaliyyət göstərdiyini izah etmək; və**
- **Müxtəlif ölkələrdə CSİRT modellərini göstərmək.**

İqtisadiyyata böyük təsir göstərmə səbəbindən kibercinayətkarlıq və müxtəlif təhlükələr ciddi şəkildə nəzərə alınmalıdır. Rusiyanın təhlükəsizlik şirkəti İB-Qrupu kibercinayətkarlıq bazarının 2.5 milyard ABŞ dolları olacağını və 7 milyard ABŞ dollarına qədər yüksələcəyini proqnozlaşdırmışdır. İDC-nin apardığı sorğuya görə, müxtəlif ölçülü şirkətlərin təxminən yarısı, hər bir hadisədən maliyyə itkisinin "ümumi" məbləğinin 100,000 ABŞ dollarından yuxarı olduğunu, eyni zamanda şirkətlərin 8.5 faizi isə hər bir hadisə nəticəsində maliyyə itkisinin 1 milyon ABŞ dollarından yüksək olduğunu bildirmişdir.

CSİRT-nin təsis olunması, informasiya sistemlərinə hücumlardan və informasiya təhlükəsizliyinin pozulması hallarından dəyən ziyanı yüngülləşdirməyin və minimum endirməyin ən effektiv yoludur.

6.1 CSİRT-in inkişaf etdirilməsi və fəaliyyəti

Bu cür və ya müvəqqəti (ad hoc) əsaslarla yaradılan CSİRT, kompüter təhlükəsizliyi ilə bağlı hadisələrə və tədbirlərə dair məlumatların alınmasına, nəzərdən keçirilməsinə və nəticələrin aradan qaldırılmasına görə cavabdehlik daşıyan təşkilatdır. CSİRT-in əsas məqsədi, kompüter təhlükəsizliyi ilə bağlı hadisələr nəticəsində dəyən ziyanı minimum endirmək və effektiv şəkildə bərpaya imkan yaratmaq üçün bu hadisələr zamanı idarəetmə xidmətlərini təmin etməkdir.[49]

1988-ci ildə ilk dəfə Morris adlı zərərverici virus (soxulcan) yayılmağa başladı və sürətlə dünyanın hər yerinə yayıldı. Bundan sonra, Müdafiə üzrə Qabaqcıl Tədqiqat Layihələr Agentliyi Proqram Təminatı üzrə Mühəndislik İnstitutunun əsasını qoydu və ABŞ hökuməti ilə müqavilə əsasında Karnegi Melon Universitetində CERT/CC-ni təsis etdi. Bundan sonra, Avropa hər bir ölkə oxşar təşkilat yaratdı. Tək bir CSİRT-in zəif məqamlarla bağlı bu hadisələrin öhdəsindən gələ bilməyəcəyinə görə, 1990-cı ildə Hadisələrin Nəticələrinin Aradan Qaldırılması və Təhlükəsizlik Qruplarının Forumu (FİRST) təsis olundu. FİRST vasitəsilə, bir çox informasiya təhlükəsizliyi agentlikləri və CSİRT-lər fikir mübadiəsi apara bilir və məlumatları bölüşürlər.

Düzgün CSİRT modelinin seçilməsi [50]

CSİRT-lər üçün beş ümumi təşkilati model vardır. Təşkilata ən uyğun model – yəni, ətra-mühit, maliyyə vəziyyəti və insan resursları kimi müxtəlif şərtləri nəzərə almaqla – qəbul edilməlidir.

1. Təhlükəsizlik qrupu modeli (mövcud İT heyətindən istifadə etməklə)

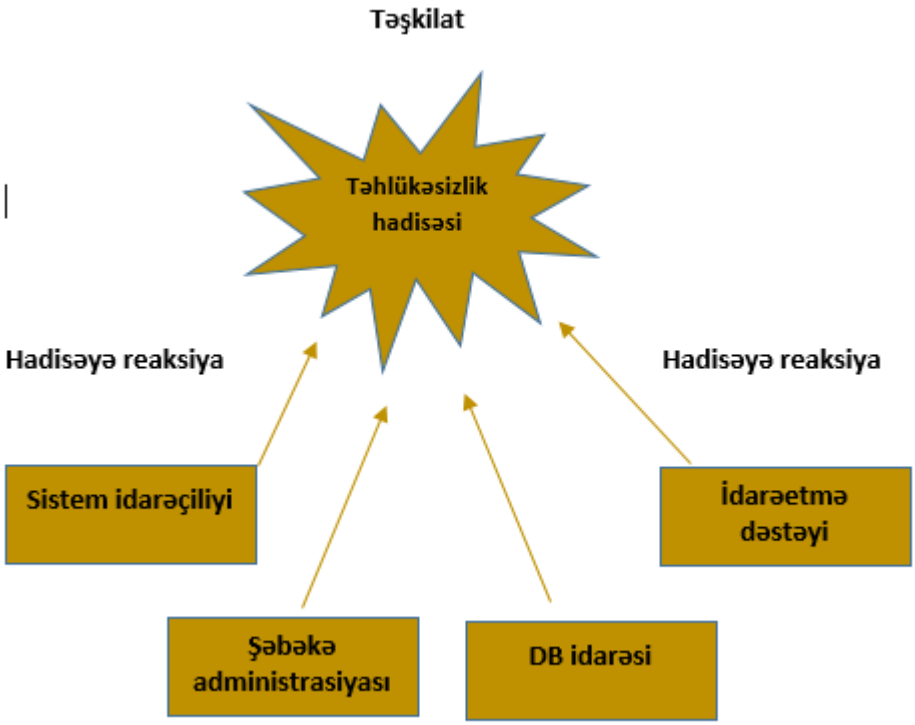
---

49 CERT,"CSIRT FAQ", Karnegi Mellon Universiteti, http://www.cert.org/csirts/csirt_faq.html.

50 Bu bölüm Georgi Killkres, Klaus-Piter Kossakovski, Robin Ruefle və Mark Zajiçekin *Təşkilati modellər: Kompüter Təhlükəsizliyi ilə bağlı Hadisələrin Nəticələrinin Aradan Qaldırılması üzrə Qruplar (CSİRT)* adlı yazılarından götürülmüşdür (Pitsburq, Karnegi Melon Universiteti, 2003-cü il), http://www.cert.org/archive/pdf/03hb001.pdf.

Təhlükəsizlik qrupu modeli CSİRT modeli üçün səciyyəvi deyildir. Faktiki olaraq, o, səciyyəvi CSİRT modelinə əksdir. Bu modeldə, kompüter təhlükəsizliyi ilə bağlı hadisələr baş verdiyi təqdirdə idarəetmə məsələlərinə görə cavabdehlik daşıyan mərkəzləşdirilmiş təşkilat yoxdur. Bunun əvəzinə, hadisələr zamanı idarəetmə üzrə bu vəzifələr sistem və şəbəkə administratorları və ya digər sistem təhlükəsizliyi üzrə mütəxəssislər tərəfindən yerinə yetirilir.

10-cu Cədvəl. Təhlükəsizlik qrupu modeli



2. Daxildə paylanmış CSİRT modeli

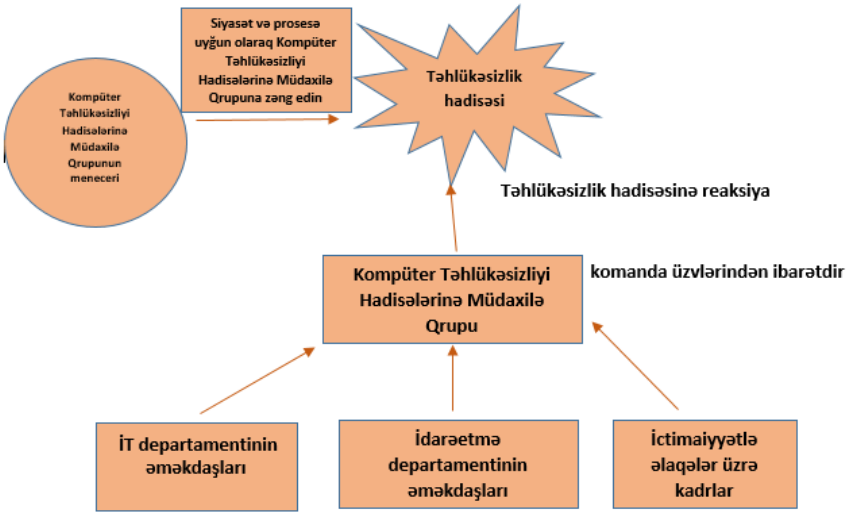
Bu model eyni zamanda “paylanmış CSİRT” də adlanır. Bu modeldə qrup hesabatların verilməsinə və ümumi idarəetməyə görə cavabdeh olan CSİRT administratorundan və müvafiq qurumun / agentliyin digər bölmələrinin heyətindən ibarətdir. Bu modeldə CSİRT, hadisələr zamanı nəticələrin aradan qaldırılması üzrə bütün tədbirlərin idarə olunmasına görə cavabdehlik daşıyan rəsmi qəbul olunmuş təşkilatdır. Şirkət və ya agentlik daxilində yaradıldığından, bu qrup, “daxili” qrup hesab edilir.

Daxildə paylanmış CSİRT modeli aşağıdakılara görə təhlükəsizlik qrupu modelindən fərqlənir:

1. Hadisələr zamanı idarəetmə üzrə daha formal siyasətlərin, prosedurların və proseslərin mövcudluğu;
2. Təhlükəsiliyə hədələr və nəticələrin aradan qaldırılması üzrə strategiyalarla bağlı bütün müəssisə üçün müəyyən edilmiş kommunikasiya metodu; və
   - Hadisələr zamanı idarəetmə vəzifələrinin həvalə olunduğu təyin edilmiş CSİRT rəhbəri və qrup üzvləri

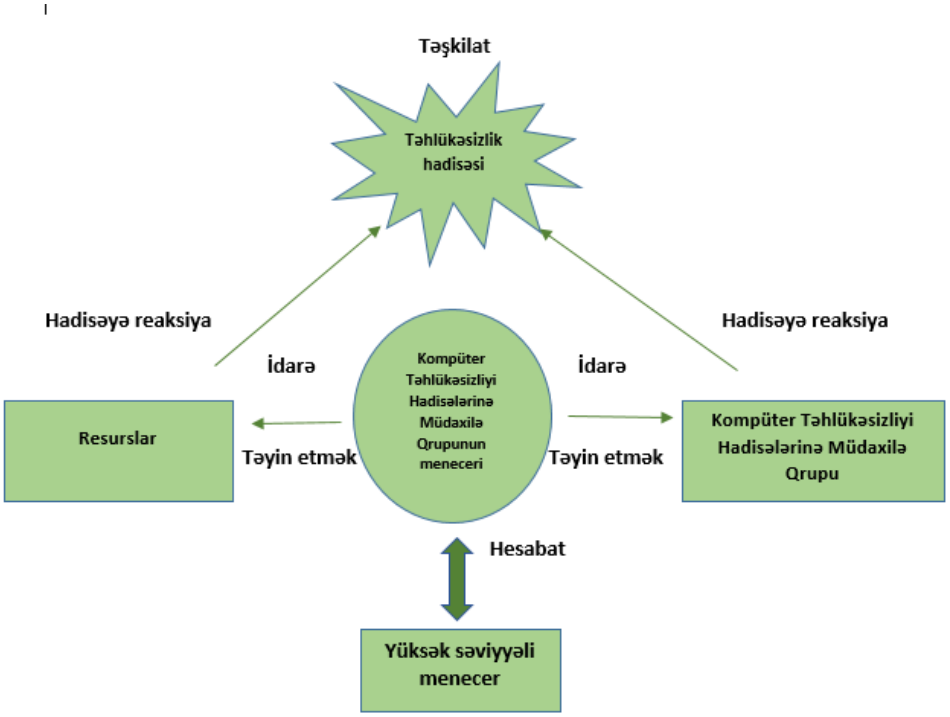
3. Daxili mərkəzləşdirilmiş CSİRT modeli

Şəkil 17. Daxildə paylanmış CSİRT modeli



Daxili mərkəzləşdirilmiş CSİRT modelində mərkəzdə yerləşən qrup təşkilatın fəaliyyətinə nəzarət edir və ona dəstək göstərir. CSİRT bu növ bütün hadisələr zamanı məlumat vermə, təhlil aparma və nəticələrin aradan qaldırılması işinə görə ümumi cavabdehlik daşıyır. Beləliklə, qrup üzvləri digər işləri idarə edə və bütün vaxtlarını qrup üçün işləməyə və bütün hadisələr zamanı idarəetməyə sərf edə bilməzlər. Həmçinin, CSİRT rəhbəri Baş İnformasiya Əməkdaşı, Baş Təhlükəsizlik Əməkdaşı və ya Baş Risk Əməkdaşı kimi yuxarı səviyyədə rəhbərliyə hesabat verir.

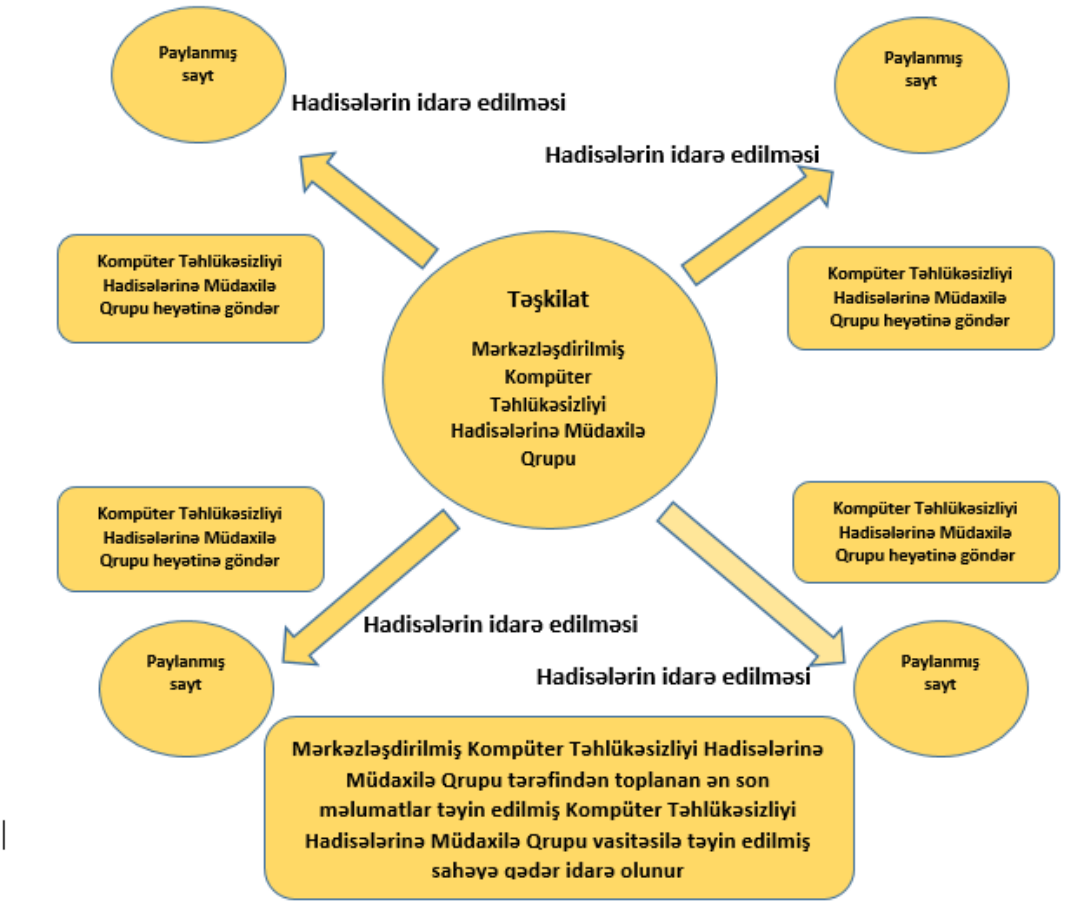
Şəkil 18. Daxili mərkəzləşdirilmiş CSİRT modeli



4. Vahid paylanmış və mərkəzləşdirilmiş CSİRT modeli

Buna, həmçinin, “vahid CSİRT” deyilir. Mərkəzləşdirilmiş CSİRT bütün təşkilata nəzarət edə və dəstək göstərə bilmədikdə, cavabdehlik daşıdıqları ərazilərdə mərkəzləşdirilmiş CSİRT tərəfindən göstərilənlərlə eyni səviyyədə xidmətlər göstərmək üçün qrup üzvləri təşkilatın yerləri / hissələri / bölmələri arasında bölüşdürülə bilər.

Mərkəzləşdirilmiş qrup yüksək səviyyədə məlumat təhlilini, bərpa metodlarını və yüngülləşdirmə strategiyalarını təmin edir. O, həmçinin, hadisələr, zəiflik və artefaktlarla bağlı cavab tədbirlərinin görülməsində qrup üzvlərinə dəstək göstərir. Paylanmış qrup üzvləri öz ərazilərində hər bir sahədə strategiyaları həyata keçirir və ekspert dəstəyini təmin edirlər.



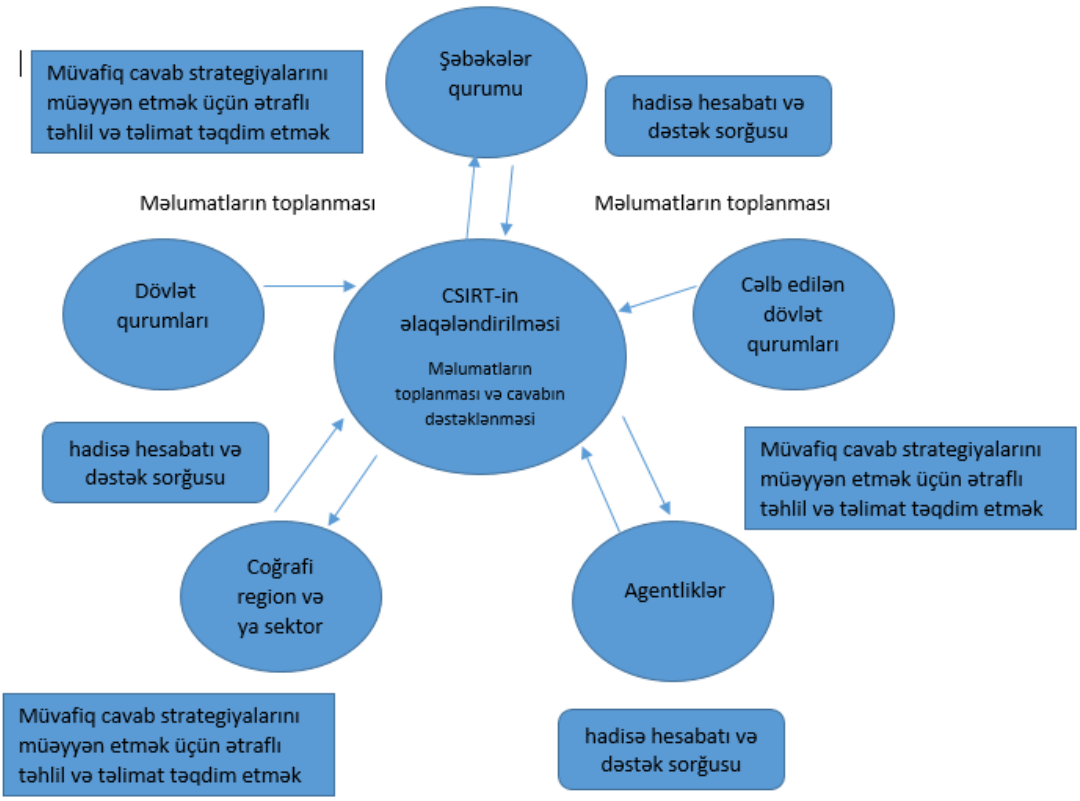
5. Əlaqələndirici CSİRT modeli

Əlaqələndirici CSİRT vahid CSİRT-də paylanmış qrupların funksiyasını gücləndirir. Əlaqələndirici CSİRT modelində, vahid CSİRT-dəki qrup üzvləri, şəbəkənin qoşulma imkanı, coğrafi sərhədlər və bu kimi xüsusiyyətlər əsasında müstəqil CSİRT-də qruplaşdırılırlar. Onlara mərkəzləşdirilmiş CSİRT tərəfindən nəzarət olunur.

Əlaqələndirici CSİRT modeli milli CSİRT sistemi üçün uyğundur. Bu model təşkilatda daxili tədbirlərə və xarici agentliklərə dəstək və sıx əlaqələndirmə üçün tətbiq edilə bilər.

Əlaqələndirmə və yardım tədbirləri informasiyanı bölüşmə, yüngülləşdirmə strategiyalarını təmin etmə, hadisələrin nəticələrinin aradan qaldırılması, bərpa metodu, meyllərin araşdırılması / təhlil edilməsi və hadisələrin modelləşdiriməsi, zəif tərəflərlə bağlı məlumat bazaları, təhlükəsizlik vasitələri üçün təmizləmə, məsləhət və xəbərdarlıq xidmətlərini əhatə edir.

Şəkil 20: Əlaqələndirici CSIRT



CSİRT-nin təsis olunması: milli CSİRT-nin yaradılması üçün addımlar[51]

[51] Bu bölüm Georgi Killresin *Milli CSİRT-nin yaradılması üçün addımlar* yazısından götürülmüşdür (Pitsburq, Karnegi Melon University, 2004-cü il), http://www.cert.org/archive/pdf/NationalCSIRTs.pdf.

CSİRT-nin yaradılması üçün beş mərhələ vardır. Bu mərhələlərlə irəliləmə üçün məqsəd, CSİRT-nin rolunun nədən ibarət olmasına diar baxışlar istiqamət verməyə xidmət edir.

1-ci Mərhələ - Maraqlı tərəfləri milli qrupun yaradılması barədə məlumatlandırmaq

1-ci Mərhələ, maraqlı tərəflərin CSİRT-nin yaradılması üçün nə lazım olduğunu başa düşməyə çalışdıqları maarifləndirmə mərhələsidir. Müxtəlif tədris metodları vasitəsilə, onlar, aşağıdakılar barədə öyrənirlər:

a) İş baxımından hansı amillər və məqsədlər milli CSİRT-nin yaradılması tələbini qoyur.
b) Milli CSİRT-nin hadisələr zamanı nəticələri aradan qaldırma imkanlarının inkişaf etdirilməsi üçün tələblər
c) Milli qrupun yaradılması üçün müzakirələrdə iştirak etməli şəxsləri müəyyənləşdirmək
d) Ölkədə mövcud olan əsas resurslar və mühüm infrastruktur
e) CSİRT dairəsi ilə əlaqə üçün təyin edilməli olan kommunikasiya kanallarının növləri
f) Milli CSRİT-in yaradılmasına təsir göstərəcək xüsusi qanunlar, qaydalar və digər siyasətlər
g) Nəticələrin aradan qaldırılması potensialını inkişaf etdirmək, planlaşdırmaq, həyata keçirmək və tətbiq etmək üçün istifadə oluna bilən maliyyələşdirmə strategiyaları
h) Milli qrupun fəaliyyətinə dəstək göstərmək üçün ehtiyac duyulacaq texnologiya və şəbəkə informasiya infrastrukturu
i) Müxtəlif sektorlar boyu tətbiq edildiyindən əsas tədbirlər planları və qarşılıqlı asılılıqlar
Milli CSRİT-nin öz əhatə dairəsinə göstərə biləcəyi əsas xidmətlər
Qabaqcıl təcrübələr və istiqamətlər

2-ci Mərhələ - CSİRT-nin planlaşdırılması: 1-ci Mərhələdə əldə olunmuş bilik və informasiya üzərində qurulma

2-ci Mərhələ, 1-ci Mərhələdə əldə olunmuş bilik və informasiya üzərində qurulmaqla CSRİT-nin planlaşdırılma mərhələsidir. 1-ci Mərhələdə müzakirə olunmuş məsələlər nəzərdən keçirilir və bir qədər də müzakirə edilir və daha sonra detallar müəyyənləşdirilir və icra planına tətbiq edilir. Plan, aşağıdakı tədbirlər nəzərdən keçirilməklə hazırlanır:

a. Milli CSİRT üçün tələbləri və ehtiyacı müəyyənləşdirmə ---
   - Milli qrupun fəaliyyətinə təsir göstərəcək qanunlar və qaydalar
   - Müəyyən edilməli və qorunmalı mühüm resurslar
   - Hazırda bildirilən və bildirilməli olan hadisələr və meyllər
   - Hadisələrin nəticələrini aradan qaldırma potensialının və kompüter təhlükəsizliyi üzrə ekspert rəyinin mövcudluğu
b. CSİRT-yə dair baxışların müəyyən olunması
c. Milli qrupun missiyasının müəyyən olunması
d. Onun xidmət edəcəyi dairənin (və ya dairələrin) müəyyənləşdirilməsi
e. Dairə və milli qrup arasında əlaqə interfeysinin müəyyənləşdirilməsi
f. Milli səviyyədə (hökumət tərəfindən) təsdiq edilmə, rəhbərlik və maliyyələşdirmə növünün müəyyənləşdirilməsi
g. Qrupun fəaliyyəti üçün heyətin malik olmalı olduğu vərdişləri və bilikləri müəyyənləşdirmə
h. Milli CSİRT üçün rolların və məsuliyyətin növlərinin müəyyən edilməsi

i. CSİRT-nin hadisələr zamanı idarəetmə proseslərinin dəqiq şəkildə göstərilməsi, habelə kənar struktur təşkilatlarında oxşar proseslərlə əlaqələrin müəyyənləşdirilməsi

j. Hadisələr zamanı fəaliyyətin və tədnbirlərin kateqoriyalaşdırılması və müəyyənləşdirilməsi üçün standartlaşdırılmış meyarların və uyğun terminologiyanın işlənib hazırlanması

k. Milli CSİRT-nin dairə və digər qlobal CSİRT-lər və kənar tərəfdaşlarla necə qarşılıqlı əlaqədə olacağını müəyyənləşdirmə

l. Mövcud fəlakət bərpa, hadisələr zamanı nəticələrin aradan qaldırılması üzrə planlar, işin davamlılığına dair planlar, böhran vəziyyətlərində və digər fövqəladə hallarda idarəetmə planları ilə inteqrasiya üçün tələb olunan proseslərin müəyyənləşdirilməsi.

m. Layihə üçün müddətlərin müəyyənləşdirilməsi

n. Planlaşdırma fəaliyyətinin nəticələri, baxışlar və uyğun çərçivə əsasında milli CSİRT planının yaradılması

3-cü Mərhələsi – CSİRT-nin həyata keçirilməsi

3-cü Mərhələdə, layihə qrupu, CSİRT-I həyata keçirmək üçün 1 və 2-ci Mərhələlərdə toplanmış informasiyadan istifadə edir. Həyata keçirmə prosesi aşağıdakı kimidir:

a. Planlaşdırma mərhələsi ərzində müəyyən olunmuş mənbələrdən vəsaitlərin əldə olunması
b. Milli CSİRT-nin yaradıldığını və bu barədə ətraflı məlumatın haradan alına biləcəyi barədə geniş bəyanat vermə (inkişaf prosesi, hesabatvermə tələbləri və s.)
c. Maraqlı tərəflər və digər müvafiq əlaqə mərkəzləri ilə əlaqələndirmə və kommunikasiya mexanizmlərinin formallaşdırılması.
d. Milli CSİRT-nin fəaliyyəti üçün təhlükəsiz informasiya sistemlərinin və şəbəkə infrastrukturunun yaradılması (yəni, təhlükəsizlik serverləri, tətbiqi proqramlar, telekommunikasiya avadanlığı və digər infrastruktura yardımçı resurslar)
e. CSİRT-nin heyəti üçün fəaliyyət və prosesin, o cümlədən planlaşdırma mərhələsində razılaşdırılmış standartın və hesabatvermə qaydalarının işlənib hazırlanması
f. CSİRT avadanlığına və şəxsi avadanlığa çıxış imkanı və onların işlədilməsi üçün daxili siyasətlərin və prosedurların, habelə məqbul istifadə siyasətlərinin işlənib hazırlanması
g. Milli CSİRT-nin öz əhatə dairəsi ilə qarşılıqlı əlaqələri üçün proseslərin həyata keçirilməsi
h. Heyətin müəyyənləşdirilməsi və cəlb edilməsi (və ya yenidən təyin olunması), CSİRT heyəti üçün müvafiq təlimin və təhsilin təmin edilməsi, habelə dairədə təlim və təhsil üçün digər mümkün yardım səylərinin müəyyənləşdirilməsi

4-cü Mərhələ - CSİRT-nin fəaliyyət göstərməsi

Fəaliyyət mərhələsində, milli CSİRT-nin təmin etməli olduğu əsas xidmətlər müəyyənləşdirilir və hadisələr zamanı idarəetmə potensialından istifadə etmək üçün fəaliyyətin səmərəliliyi qiymətləndirilir. Nəticələrə əsaslanmaqla, fəaliyyətin detalları müəyyənləşdirilməli və təkmilləşdirilməlidir. Bu mərhələdə tədbirlər aşağıdakılardır:

a. Milli CSİRT tərəfindən təmin olunan müxtəlif xidmətlərin aktiv şəkildə icrası
b. Milli CSİRT-in fəaliyyətinin effektivliyini qiymətləndirmə mexanizminin işlənib hazırlanması və tətbiq edilməsi
c. Qiymətləndirmənin nəticələrinə görə milli CSİRT-nin təkmilləşdirilməsi

d. Missiyanın, xidmətlərin və heyətin müvafiq şəkildə və dairəyə xidməti gücləndirmək üçün davamlı ola bilən şəkildə genişləndirilməsi
e. CSİRT siyasətlərinin və prosedurlarının inkişaf etdirilməsini və gücləndirilməsini davam etdirmək

5-ci Mərhələ - Əməkdaşlıq

Milli CSİRT səmərəli fəaliyyət vasitəsilə əsas maraqlı tərəflərlə etibarlı münasibətləri inkişaf etdirə bilər (4-cü Mərhələ). Lakin milli CSİRT, həmçinin, əməkdaşlıq etdiyi təşkilatlarla, daxili CSİRT-lərlə və beynəlxalq CSİRT-lərlə əməkdaşlıq etməklə, uzun-müddətli mübadilələr vasitəsilə, hadisələr zamanı idarəetməyə dair mühüm informasiyanın və təcrübələrin mübadiləsini də aparmalıdır. Bu mərhələdə tədbirlərə aşağıdakılar aiddir:

a. Məlumat və informasiya mübadiləsi ilə bağlı tədbirlərdə iştirak etmə və tərəfdaşlar, digər CSİRT-lər, tərkibdəki qurumlar və kompüter təhlükəsizliyi üzrə digər ekspertlər arasında məlumat və informasiya mübadiləsi üçün standartların işlənib hazırlanmasına dəstək göstərmə
b. CSİRT cəmiyyətinə dəstək göstərmək üçün qlobal "müşahidə və xəbərdarlıq" funksiyalarında iştirak etmə
c. Hücum meyllərinin və nəticələrin aradan qaldırılması strategiyalarının müzakirə olunduğu təlim, seminarlar və konfransların keçirilməsini təmin etməklə CSİRT tədbirlərinin keyfiyyətinin artırılması
d. Qabaqcıl təcrübə sənədlərinin və tövsiyələrin işlənib hazırlanması üçün cəmiyyətdə digərləri ilə əməkdaşlıq etmə
e. Cari təkmilləşdirmə prosesinin bir hissəsi kimi hadizələr zamanı idarəetmə üçün prosesləri nəzərdən keçirmə və düzəlişlər etmə

CSIRT xidmətləri[52]

CSİRT-lərin göstərdiyi xidmətləri reaktiv, proaktiv xidmətlərə və xidmətin keyfiyyətinə nəzarətlə bağlı xidmətlərə bölmək olar.

Reaktiv xidmətlər CSİRT tərəfindən göstərilən əsas xidmətlərdir. Onlara aiddir:

1. **Həyəcan və xəbərdarlıqlar** – Bu xidmətə, təhlükəsizliklə bağlı zəif tərəf, müdaxilə həyəcanı, kompüter virusu və dələduzluq kimi problemlərlə məşğul olmaq üçün informasiya və nəticələri aradan qaldırma metodlarının təmin edilməsi.

2. **Hadisələr zamanı idarəetmə** - Bura sorğuların və hesabatların qəbul edilməsi, çeşidlənməsi və cavablandırılması və hadisələrin və tədbirlərin təhlili və prioritetləşdirilməsi aiddir**.** Nəticələrin aradan qaldırılması üzrə xüsusi tədbirlərə aşağıdakılar aiddir:

    - **Hadisələrin təhlil olunması** – Hadisə və ya tədbirlərlə bağlı bütün mövcud məlumatların və dəlillərin və ya araşdırma zamanı aşkarlanan məqamların yoxlanması**.** Təhlilin aparılmasında məqsəd

52 Bu bölüm Karnegi Melon Universitetindən götürülmüşdür, CSİRT Xidmətləri (2002-ci il), http://www.cert.org/archive/pdf/CSIRT-services-list.pdf.

hadisənin miqyasını, hadisə nəticəsində dəyən ziyanın həcmini, hadisənin mahiyyətini və nəticələrin aradan qaldırılması üçün mövcud strategiyaları və ya metodları müəyyən etməkdir.

- **Məhkəmə dəlillərinin toplanması** - Sistemdə dəyişiklikləri müəyyən etmək və riskli hala gətirib çıxaran hadisələrin üzə çıxarılmasına kömək etmək üçün dəlillərin toplanması, saxlanması, sənədləşdirilməsi və təhlil edilməsi.

- **İzləmə** - Müdaxilə edən şəxsin təsirə məruz qalmış sistemlərə və müvafiq şəbəkələrə necə daxil olmasını izləmə nəzərdə tutulur. Müdaxilə edən şəxsin mənbələrinin izlənməsi və ya onun çıxış imkanı olduğu sistemlərin müəyyənləşdirilməsi də bu tədbirə aiddir.

3. **Hadisələrin nəticələrinin yerində aradan qaldırılması –** CSİRT, müvafiq şəxslərə, hadisədən sonra nəticələrin aradan qaldırılmasında birbaşa, yerində kömək göstərir.

4. **Hadisələr zamanı nəticələrin aradan qaldırılmasına dəstək** – CSİRT, hücuma məruz qalmış şəxslərə, hadisənin nəticələrinin aradan qaldırılmasında telefon, e-poçt, faks və ya sənədlər vasitəsilə kömək edir və istiqamət verir.

5. **Hadisələrin nəticələrinin aradan qaldırılmasında əlaqələndirmə** - Hadisələrdə iştirakçı olan tərəflər arasında nəticələrin aradan qadırılması səyləri əlaqələndirilir. Bura adətən hücuma məruz qalmış şəxs, hücumda iştirakçı olan digər saytlar və hücumla bağlı təhlilin aparılmasında yardıma ehtiyacı olan istənilən saytlar aid edilir. Bura, zərərçəkmişə İT dəstəyi göstərən, İSP-lər və digər CSİRT-lər kimi tərəflər də aid edilə bilər.

6. **Zəif tərəfin idarə olunması** – Bura avadanlıqdakı və proqram təminatındakı zəif tərəflərə dair informasiyanın və hesabatların alınması, zəif tərəflərin təsirlərinin təhlil edilməsi və zəif tərəflərin aşkar olunması və aradan qaldırılması üçün strategiyaların işlənib hazırlanması aiddir.

- **Zəif tərəflə bağlı təhlilin aparılması** – Avadanlıqdakı və proqram təminatındakı zəif tərəflərin texniki analizi və yoxlanması nəzərdə tutulur. Təhlillərə, zəifliyin harada baş verdiyini müəyyən etmək üçün bərpa proqramından istifadə etməklə, mənbə kodun (proqramın) nəzərdən keçirilməsi və ya test sistemdə problemin üzə çıxarılmasına səy göstərmə aiddir**.**

- **Zəif tərəfin aradan qaldırılması** – Zəif tərəfləri yüngülləşdirmək və ya aradan qaldırmaq üçün müvafiq cavab tədbirlərinin müəyyənləşdirilməsini əhatə edir. Bu xidmətə əvəzedici, möhkəmləndirici vasitələr quraşdırmaqla və ya digər metodlarla nəticələrin aradan qaldırılması da aid edilə bilər. Bura, həmçinin, digərlərini yüngülləşdirmə strategiyaları barədə məlumatlandırmaq, bildirişlərin və xəbərdarlıqların göndərilməsi də aiddir.

- **Zəif tərəflərin aradan qaldırılmasında əlaqələndirmə** - CSİRT müəssisənin müxtəlif hissəslərini və ya onun tərkibində olan qurumları zəif tərəf barədə məlumatlandırır və onları müəyyən etmə və ya yüngülləşdirmə barədə informasiyanı bu qurumlarla bölüşür. CSİRT, həmçinin, zəif tərəflərin aradan qaldırılması üçün uğurlu strategiyaların təsnifatını aparır. Bu tədbirlərə, zəif tərəfin və ya zəif tərəflər bağlı hesabatların təhlil olunması və müxtəlif tərəflərin apardığı texniki təhlillərin ümumiləşdirilməsi də aiddir. Bu xidmət, həmçinin, zəif tərəflərə dair informasiya və onların aradan qaldırılması üzrə strategiyaların dövlət və ya özəl arxivinin və ya bilik bazasının saxlanması da əhatə edə bilər**.**

7. **Aşkar edilmiş məqamların idarə edilməsi** – Buraya kompüter virusları, Troyan atları proqramları, zərərverici ünsürlər (soxulcanlar), istismar modelləri və proqram vasitələrinin cəlb olunduğu aşkar edilmiş məqamlara dair təhlil, nəticələrin aradan qaldırılması, əlaqələndirmə və idarəetmə aiddir.

    - **Aşkar edilmiş məqamlara dair təhlil** – CSİRT sistemdə aşkar olunmuş neqativ halların texniki yoxlamasını və təhlilini aparır.

    - **Aşkar edilmiş məqamların aradan qaldırılması** – Sistemdə neqativ halları aşkar etmək və kənarlaşdırmaq üçün müvafiq tədbirlərin müəyyənləşdirilməsi aiddir.

    - **Aşkar edilmiş məqamların aradan qaldırılmasında əlaqələndirmə -** Aşkar edilmiş neqativ hallarla bağlı təhlillərin nəticələrini və onların aradan qaldırılması üzrə strategiyaları digər tədqiqatçılar, CSİRT-lər, satış müəssisələri və digər təhlükəsizlik ekspertləri ilə bölüşməni və ümumiləşdirməni əhatə edir.

Proaktiv xidmətlər hadisə baş verməmişdən və ya aşkar edilməmişdən qabaq infrastrukturun və təhlükəsizlik proseslərinin dayanıqlığının təkmilləşdirilməsi üçün nəzərdə tutulur. Bu xidmətlərə aşağıdakılar aiddir:

1. **Elanlar** – Bura müdaxilələrlə bağlı həyəcan siqnalları, zəif tərəflərlə bağlı xəbərdarlıqlar, təhlükəsizliklə bağlı məsləhətlərin verilməsi və bu kimi xidmətlər aiddir. Belə elanlar tərkib hissələri orta – uzun-müddətli təsirlərlə, yenicə aşkar edilmiş zəif tərəflər və ya müdaxilə vasitələri kimi yeniliklər barədə məlumatlandırır. Elanlar tərkib hissələrə, öz sistemlərini və şəbəkələrini yenicə aşkar edilmiş problemlərə qarşı, hələ onlar istismar edilməmişdən qabaq, qorumaq imkanını verir.

2. **Texnoloji müşahidə** - Bura, yeni texniki inkişafın, müdaxilələrin və gələcək təhlükələri müəyyən etmək üçün əlaqədar meyllərin monitorinqi və müşahidə olunması aiddir. Bu xidmətin nəticəsi daha çox orta - uzun müddətli təhlükəsizlik məsələlərinə diqqət yetirilən bəzi növ rəhbər qaydalar və tövsiyələr ola bilər.

3. **Təhlükəsizlik auditləri və ya dəyərləndirmələri** – Bu xidmət, təşkilat tərəfindən müəyyən olunmuş tələblər və ya tətbiq edilən digər sənaye standartları əsasında, təşkilatın təhlükəsizlik infrastrukturunun təfsilatlı şəkildə nəzərdən keçirilməsini və təhlil olunmasını təmin edir**.**

4. **Təhlükəsizlik vasitələri, tətbiqi proqramlar, infrastrukturlar və xidmətlərin konfiqurasiyası və qorunması –** Bu xidmət, vasitələrin, tətbiqi proqramların və ümumi hesablama infrastrukturunun necə təhlükəsiz şəkildə qurulmasına və saxlanmasına dair istiqamətverici rol oynayır.
5. **Təhlükəsizlik vasitələrinin inkişaf etdirilməsi** – Bu xidmət, təhlükəsizlik üçün inkişaf etdirilən və paylanan yeni, tərkib hissələrə uyğun vasitələrin, proqram təminatlarının, əlavə proqram modullarının və əvəzedici vasitələrin işlənib hazırlanmasını əhatə edir**.**

6. **Müdaxilələri aşkarlama xidmətləri** – Bu xidməti göstərən CSİRT-lər mövcud İDS loqları (qeydiyyatları) nəzərdən keçirir, onları təhlil edir və müəyyən olunmuş hüdudlarda hadisələr üçün nəticələrin aradan qaldırılması tədbirləri ilə bağlı təşəbbüslər irəli sürürlər.

7. **Təhlükəsizliklə bağlı informasiyanın yayımlanması** – Bu xidmət, tərkib hissələri, təhlükəsizliyi yaxşılaşdırmağa kömək edən hərtərəfli və ümumi faydalı informasiya toplusu ilə təmin edir.

Təhlükəsizliklə bağlı keyfiyyəti idarəetmə xidmətləri hadisələrin, zəif tərəflərin və hücumların nəticələrinin aradan qaldırılmasından əldə olunmuş biliklərlə təminetmə üçün nəzərdə tutulur. Bu xidmətlərə aiddir:

1. **Risklə bağlı təhlillər** – Bu, CSİRT-in, real təhlükələri dəyərləndirmək, informasiya aktivlərinə qarşı risklərin keyfiyyət və kəmiyyətlə bağlı real dəyərləndirmələrini aparmaq və müdafiə və nəticələri aradan qaldırma strategiyalarını qiymətləndirilmək imkanlarının təkmilləşdirilməsini nəzərdə tutur.

2. **İşin davamlılığı və fəlakətlərdən sonra bərpanın planlaşdırılması** – İşin davamlılığı və kömpüter təhlükəsizliyinə qarşı hücumların səbəb olduğu fəlakətlərdən sonra bərpa müvafiq planlaşdırma vasitəsilə təmin edilir.

3. **Təhlükəsizliklə bağlı məsləhətlərin verilməsi** – CSIRT-lər iş (biznes) fəaliyyəti üçün praktiki məsləhət və istiqamətlər verə bilər**.**

4. **Maarifləndirmə** - CSIRT-lər, təkrib hissələrin tələb etdiyi təhlükəsizliklə bağlı təcrübələrə və siyasətlərə dair informasiya və istiqamətləri müəyyən və təmin etməklə təhlükəsizliklə bağlı məlumatlılığı artıra bilərlər**.**

5. **Təhsil/Təlim** – Bu xidmət, kompüter təhlükəsizliyi ilə bağlı hadisələrindən qorumaq, onları aşkar etmək, onlara dair məlumat vermək və nəticələri aradan qaldırmaq üçün hadisələrə dair məlumat vermə üzrə rəhbər qaydalar, nəticələrin aradan qaldırılması üzrə müvafiq metodlar, hadisələrin nəticələrinin aradan qaldırılması vasitələri, hadisələrin qarşısının alınması metodları və digər zəruri informasiyalar kimi mövzulara dair tədris və təlimin təmin olunmasını əhatə edir. Təlim modellərinə seminarlar, işçi görüşlər, kurslar və əyani vəsaitlər aiddir.

6. **Məhsulun qiymətləndirilməsi və ya onlara şəhadətnamələrin verilməsi** - CSIRT məhsulların təhlükəsizliyini və qəbul edilmiş CSİRT və ya təşkilati təhlükəsizlik təcrübələrinə uyğunluğunu təmin etmək üçün vasitələr, tətbiqi proqramlar və ya digər xidmətlərin məhsul qiymətləndirməsini apara bilər.

Cədvəl 11 hər bir CSİRT modelində CSİRT xidmətinin səviyyəsi – yəni, onun əsas, əlavə və ya qeyri-adi xidmət olduğu göstərilir.

Cədvəl 12. CSIRT xidmətləri

Xidmət kateqoriyası	Xidmətlər		Təhlükəsizlik qrupu	Paylanmış	Mərkəzləşdirilmiş	Vahid	Əlaqələndirici
Reaktiv	Həyəcanlar və xəbərdarlıqlar		Əlavə	Əsas	Əsas	Əsas	Əsas
	Hadisələr zamanı idarəetmə	Hadisələrin təhlili.	Əsas	Əsas	Əsas	Əsas	Əsas
		Hadisələrlə bağlı nəticələrin yerində (saytda) aradan qaldırılması.	Əsas	Əlavə	Əlavə	Əlavə	Qeyri-adi
		Hadisələrin nəticələrinin aradan qaldırılmasına dəstək.	Qeyri-adi	Əsas	Əsas	Əsas	Əsas
		Hadisələrin nəticələrinin aradan qaldırılmasında əlaqələndirmə.	Əsas	Əsas	Əsas	Əsas	Əsas
		Zəif tərəfin təhlili.	Əlavə	Əlavə	Əlavə	Əlavə	Əlavə
		Zəif tərəfin aradan qaldırılması.	Əsas	Əlavə	Qeyri-adi	Əlavə	Əlavə
	Araşdırma zamanı aşkarlanan məqamlar üzrə idarəetmə	Zəif tərəfindən aradan qaldırılmasında əlaqələndirmə.	Əlavə	Əsas	Əsas	Əsas	Əsas
		Aşkarlanan məqamın təhlili.	Əlavə	Əlavə	Əlavə	Əlavə	Əlavə
		Aşkarlanan neqativ halın aradan qaldırılması.	Əsas	Əlavə	Əlavə	Əlavə	Əlavə
		Aşkarlanan neqativ halın aradan qaldırılmasında əlaqələndirmə.	Əlavə	Əlavə	Əsas	Əsas	Əsas
Proaktiv	Elanlar.		Qeyri-adi	Əsas	Əsas	Əsas	Əsas
	Texniki müşahidə.		Qeyri-adi	Əlavə	Əsas	Əsas	Əsas
	Təhlükəsizlik auditləri və dəyərləndirmələr.		Qeyri-adi	Əlavə	Əlavə	Əlavə	Əlavə
	Təhülkəsizlik vasitələrinin, tətbiqi proqramların, infrastrukturların və xidmətlərin konfiqurasiyası və qorunması.		Əsas	Əlavə	Əlavə	Əlavə	Qeyri-adi
	Təhlükəsizlik vasitələrinin inkişaf etdirilməsi.		Əlavə	Əlavə	Əlavə	Əlavə	Əlavə
	Müdaxilələri aşkarlama xidmətləri.		Əsas	Əlavə	Əlavə	Əlavə	Qeyri-adi
	Təhlükəsizliklə bağlı informasiyanın yayınlanması.		Qeyri-adi	Əlavə	Əsas	Əsas	Əsas
Təhlükəsizliklə bağlı keyfiyyət İdarəetmə	Risklə bağlı təhlillər		Qeyri-adi	Əlavə	Əlavə	Əlavə	Əlavə
	İşin davamlılığı və Fəlakətlərdən sonra bərpanın planlaşdırılması		Qeyri-adi	Əlavə	Əlavə	Əlavə	Əlavə
	Təhlükəsizliklə bağlı məsləhətlərin verilməsi		Qeyri-adi	Əlavə	Əlavə	Əlavə	Əlavə
	Maarifləndirmə - Təlim/təhsil i		Qeyri-adi Qeyri-adi	Əlavə Əlavə	Əlavə Əlavə	Əlavə Əlavə	Əsas Əsas
	Məhsulun qiymətləndirilməsi və ya onlara şəhadətnamələrin verilməsi		Qeyri-adi	Əlavə	Əlavə	Əlavə	Əlavə

Source: Georgia Killcrece, et. al., *Organizational Models for Computer Security Incident Response Teams (CSIRTs)* (Pittsburgh, Carnegie Mellon University, 2003), http://www.cert.org/archive/pdf/03hb001.pdf.

6.2 Beynəlxalq CSİRT Assosiasiyaları

Hazırda, dünyada kompüter təhlükəsizliyi ilə bağlı hadisələrin nəticələrini aradan qaldırmaq üçün təsis edilmiş bir sıra ixtisaslaşmış beynəlxalq CSİRT assosiasiyaları vardır. CSİRT-lər hücumların nəticələrini aradan qaldırmağa və digər funksiyaları yerinə yetirməyə qadir olduğu halda, ikidən artıq ölkənin təsirə məruz qaldığı trans-sərhəd hücum hallarında beynəlxalq CSİRT assosiasiyasının buna diqqəti tələb olunur.

Hadisələrin Nəticələrinin Aradan Qaldırılması üzrə Təhlükəsizlik Qruplarının Forumu[53]

Hadisələrin Nəticələrinin Aradan Qaldırılması üzrə Təhlükəsizlik Qruplarının Forumu (FIRST) 98 ölkədən olan CERT-lərdən, hökumət orqanlarından və təhlükəsizlik şirkətlərindən ibarətdir. 585 təşkilat, o cümlədən CERT/CC və US-CERT bu forumun üzvüdür (2021-ci ilin iyul ayına olan məlumat). FİRST, hadisələrin nəticələrinin aradan qaldırılması üzrə qruplar arasında informasiya mübadiləsi və əməkdaşlıq üçün bir birlikdir. Onun məqsədi, hadisələrin nəticələrinin aradan qaldırılması və müdafiə tədbirlərini aktivləşdirmək və üzvləri, hadisələrin nəticələrinin aradan qaldırılması üçün texnologiya, bilik və vasitələrlə təmin etməklə onlar arasında əməkdaşlığı motivləşdirməkdir. FİRST-ün həyata keçirdiyi tədbirlər aşağıdakılardır:

- Hadisələrin nəticələrinin aradan qaldırılması və müdafiə üçün ən qabaqcıl təcrübələri, prosedurları, vasitələri, texniki informasiyanı və metodologiyaları inkişaf etdirmək və bölüşmək;
- Siyasətlərin, xidmətlərin və yaxşı keyfiyyətli təhlükəsizlik məhsullarının inkişafını motivləşdirmək;
- Kompüter təhlükəsizliyi üzrə müvafiq rəhbər qaydalara dəstək və onların inkişaf etdirilməsi;
- Hökumətlərə, müəssisələrə və təhsil müəssisələrinə hadisələrin nəticələrinin aradan qaldırılması üzrə qrup yaratmaqda kömək etmə; və
- Daha təhlükəsiz elektron mühit üçün üzvlər arasında texnologiya, təcrübə və biliklərin bölüşdürülməsinə şərait yaratma.

6.3 Regional CSIRT Assosiasiyaları

Asiya-Sakit okean hövzəsi üzrə CERT[54]

Asiya-Sakit okean hövzəsi üzrə Kompüterlə bağlı Fövqəladə Hallar Qrupu (APCERT), 2003-cü ilin fevral ayında, təhlükəsizlik ekspertlərinin şəbəkəsi qismində çıxış etmək, hadisələrin nəticələrin aradan qaldırılması işini gücləndirmək və Asiya – Sakit okean hövzəsi regionunda təhlükəsizliklə bağlı maariflənməni artırmaq üçün yaradılmışdır. Asiya – Sakit okean hövzəsi CSİRT-lərin birinci konfransı 2002-ci ildə Yaponiyada keçirilmişdir. APCERT, bundan bir il sonra, Asiya – Sakit okean hövzəsindən 14 CSİRT-in iştirakı ilə Taipeidə keçirilən konfransda təsis olunmuşdur. 2021-ci ilin sentyabrına olan məlumata görə, APCERT-in 23 ölkədən 33 tamhüquqlu üzvü və 12 ümumi üzvü vardır.

APCERT üzvləri təsdiq edirlər ki, bu gün kompüter təhlükəsizliyi ilə bağlı hadisələr kifayət qədər çoxdur, mürəkkəbdir və buna hər hansı bir təşkilat və ya ölkənin nəzarət etməsi çətindir və APCERT-in digər üzvləri ilə əməkdaşlıq etməklə daha effektiv cavab tədbirləri tətbiq edilə bilər. FİRST-də olduğu kimi, APCERT-də

53 FİRST "FİRST haqqında", FIRST.org, Inc., http://www.first.org/about/.

54 APCERT, "Background", http://www.apcert.org/about/background/index.html.

ən mühüm konsepsiya üzvlər arasında informasiya mübadiləsi və bir-birilə əməkdaşlıq üçün inama əsaslanan etibarlı münasibətlərin olmasıdır. Beləliklə, APCERT tədbirləri aşağıdakılar üçün nəzərdə tutulmuşdur:

- Asiya – Sakit okean hövzəsi üzrə regional və beynəlxalq əməkdaşlığı gücləndirmək;
- Iri-miqyaslı və ya regional şəbəkə təhlükəsizliyi ilə bağlı hadisələrin öhdəsindən gəlmək üçün tədbirləri birgə inkişaf etdirmək;
- Təhlükəsizliklə bağlı informasiyanı bölüşməni və texnologiya mübadiləsini, o cümlədən kompüter virusları, istismar modelləri və sairə ilə bağlı informasiya mübadiləsini təkmilləşdirmək;
- Ümumi problemlərə dair birgə tədqiqatları artırmaq;
- Kompüter təhlükəsizliyi ilə bağlı hadisələrin nəticələrinin effektiv şəkildə aradan qaldırılmasında regionda digər CERT-lərə yardım etmək; və
- Regional informasiya təhlükəsizliyi və hadisələrin nəticələrinin aradan qaldırılması ilə bağlı hüquqi məsələlərə dair məsləhətlər vermək və həll yollarını təklif etmək.

Avropa Hökuməti CERT-i[55]

Avropa Hökuməti CERT-i (EGC), Avropa ölkələrində hökumət CSİRT-ləri ilə əlaqəli olan qeyri-rəsmi komitədir. Finlandiya, Fransa, Almaniya, Macarıstan, Niderland, Norveç, İsveç, isveçrə və BK bu komitənin üzvüdürlər. Onun rolları və vəzifələri aşağıdakılardan ibarətdir:

- Iri-miqyaslı və ya regional şəbəkə təhlükəsizliyi ilə bağlı hadisələrin öhdəsindən gəlmək üçün tədbirləri birgə inkişaf etdirmək;
- Təhlükəsizliklə bağlı hadisələrə və zərərli proqramların yaratdığı təhlükələrə və zəif məqamlara dair informasiya və texnologiya mübadiləsini təşviq etmə;
- Qrup daxilində mübadilə edilə bilən bilik və ekspert təcrübəsi sahələrini müəyyən etmək;
- Üzvlər üçün maraq kəsb edən mövzular izrə birgə tədqiqat və inkişaf sahələrini müəyyən etmək; və
- Avropa ölkələrində hökumət CSİRT-lərin yaradılmasını təşviq etmək.

Avropa Şəbəkəsi və İnformasiya Təhlükəsizliyi Agentliyi[56]

Avropa Şəbəkəsi və İnformasiya Təhlükəsizliyi Agentliyinin (ENİSA) məqsədi, NİS mədəniyyətini yaratmaqla, Aİ-də şəbəkə təhlükəsizliyini və informasiya təhlükəsizliyini gücləndirməkdir. O, "yüksək texnologiya" sahəsində cinayətkarlığa qarşı 2004-cü ilin yanvarında Nazirlər Şurası və Avropa Parlamenti tərəfindən təsis olunmuşdur. Onun rolu aşağıdakılardan ibarətdir:

- ENİSA və ya Aİ üzvləri arasında NİS-i təmin etməyə dəstək göstərmə;
- Maraqlı tərəflər arasında stabil informasiya mübadiləsini təşviq etmə; və
- NİS-lə bağlı əlaqələndirmə funksiyalarını təkmilləşdirmə.

ENISA-nın viruslar və hakerlik hallarını azatmağa yönələn beynəlxalq səylərə kömək edəcəyi və təhlükələrin onlayn monitorinqini təsis edəcəyi gözlənilir.

55 EGC, http://www.egc-group.org.

56 ENISA, "ENISA haqqında", http://www.enisa.europa.eu/about-enisa.

AfricaCERT

Kompyuter insidentlərinə cavab verən qrupların Afrika forumunun məqsədi Afrika İnternet Ekosistemində internet sağlamlığı üçün problemlərin həllini təklif etməkdir. AfricaCERT-in məqsədlərinə aşağ daxildir.

• CSIRTS arasında əməkdaşlığın əlaqələndirilməsi;
• Ekspertiza və məsləhət verməklə Afrika ölkələrinə CSIRT-lərin yaradılmasında köməklik göstərmək; və
• Afrika ölkələrində və onlar arasında İKT Təhlükəsizliyi sahəsində təhsil və təbliğat proqramlarının təşviqi və dəstəklənməsi.

6.4 Milli CSİRT-lər

Bir sıra ölkələr milli CSİRT təşkil etmişlər. Cədvəl 12-də ölkələr və onların müvafiq CSİRT-ləri, habelə onların hər birinin vebsaytı sadalanır:

Cədvəl 12. Milli CSİRT-lərin siyahısı

Ölkə	Rəsmi adı	Vebsaytlar
Əbu Dabi	Abu Dabi Polisinin Kompüterlə bağlı Fövqəladə Hallar Qrupu	https://adsic.abudhabi.ae
Argentina	ICIC-CERT	http://www.icic.gob.ar
Avstraliya	Avstraliyanın Kompüterlə bağlı Fövqəladə Hallar Qrupu	http://www.auscert.org.au
Avstraliya	Avstraliya Kiber Təhlükəsizlik Mərkəzi	http://www.cyber.gov.au
Avstriya	**C**ERT.at	https://www.cert.at
Azərbaycan	CERT.az	http://www.cert.az
Banqladeş	Banqladeş Hökumətinin Kompyuter İnsidentlərinə Müdaxilə Qrupu	https://www.cirt.gov.bd
Braziliya	Kompyuterlə bağlı Fövqəladə Hallar Qrupu Braziliya	http://www.cert.br
Bruney Dərüssalam	Bruneyin Kompyuterlə bağlı Fövqəladə Hallar Qrupu	http://www.brucert.org.bn
Belarus	CERT.BY	http://cert.by
Belçika	Belçika Federal Kiber Fövqəladə Hallar Komandası	http://www.cert.be
Butan	Butan Kompyuter İnsidentlərinə Müdaxilə Qrupu	http://www.btcirt.bt
Boliviya	Boliviya Kompyuter İnsidentləri İdarəetmə Mərkəzi	https://cgii.gob.bo/
Bruney	Bruneyin Kompyuterlə bağlı Fövqəladə Hallar Qrupu	http://www.brucert.org.bn
Kanada	Kanada Kiber Təhlükəsizlik Mərkəzi	http://www.cyber.gc.ca
Çili	Çilinin Kompyuterlə bağlı Fövqəladə Hallar Qrupu	http://www.clcert.cl
Çin	Çinin Milli Kompyuter Şəbəkəsi üzrə Fövqəladə Hallar Texniki Qrupu – Əlaqələndirmə Mərkəzi	http://www.cert.org.cn
Xorvatiya	CarNet CERT	http://www.carnet.hr
Çex Respublikası	CSIRT.CZ	http://www.clcert.cl
Danimarka	Danimarkanın Kompyuterlə bağlı Fövqəladə Hallar Qrupu	http://www.cert.dk

Misir	Misirin Kompyuterlə bağlı Fövqəladə Hallar Qrupu	http://www.egcert.eg
Estoniya	CERT-EE	https://ria.ee
Finlandiya	Milli Kiber Təhlükəsizlik Mərkəzi Finlandiya	http://www.ncsc.fi
Fransa	CERT-FR	http://www.cert.ssi.gouv.fr
Almaniya	CERT-Bund	http://www.bsi.bund.de/certbund
Qana	CERT-GH Qana Milli Kiber Təhlükəsizlik Mərkəzi	https://cybersecurity.gov.gh
Honq Konq, Çin	Honq Konq Kompüter Cavab Koordinasiya Mərkəzi	http://www.hkcert.org
Macarıstan	Macarıstanın Kompyuterlə bağlı Fövqəladə Hallar Qrupu	https://nki.gov.hu
İslandiya	CERT-IS Kompyuter İnsidentlərinə Müdaxilə Qrupu İslandiya	https://www.cert.is
Hindistan	CERT- Hindistan Kompyuterlə bağlı Fövqəladə Hallar Qrupu	http://www.cert-in.org.in
Indoneziya	İndonesiyanın İnternet İnfrastrukturu üzrə Təhlükəsizliklə bağlı Hadisələrin Nəticələrinin Aradan Qaldırılması Qrupu	http://www.idsirtii.or.id
İran	CERT CC Maher	https://www.ircert.com
İtaliya	CSIRT İtaliya	https://www.csirt-ita.it/
Yaponiya	JP CERT Koordinasiya Mərkəzi	http://www.jpcert.or.jp
Qazaxıstan	Qazaxıstanın Kompyuterlə bağlı Fövqəladə Hallar Qrupu	http://www.cert.kz
Makao	MOCERT	http://www.mocert.org
Litva	LITNET CERT	http://cert.litnet.lt
Malayziya	Malayziyanın Kompyuterlə bağlı Fövqəladə Hallar Qrupu	http://www.mycert.org.my
Meksika	Universidad Nacional Autonoma de Mexico	http://www.cert.org.mx
Monqolustan	Monqolustan Kiber Fövqəladə Hallara Cavab/Koordinasiya Mərkəzi	http://www.mncert.org
Mərakeş	maCERT	
Hollandiya	Hollandiya Milli Kibertəhlükəsizlik Mərkəzi	http://www.ncsc.nl
Yeni Zelandiya	CERT NZ	http://www.cert.govt.nz
Nigeriya	ngCERT Nigeriyanın Kompyuterlə bağlı Fövqəladə Hallar Qrupu	http://www.cert.gov.ng
Norveç	Norveçin Kompyuterlə bağlı Fövqəladə Hallar Qrupu	https://nsm.stat.no/norcert
Pakistan	PakCERT	http://www.pakcert.org
Papua Yeni Qvineya	PNGCERT	https://www.pngcert.org.p
Filippin	Filippinin Kompyuterlə bağlı Fövqəladə Hallar Qrupu	http://www.phcert.org
Polşa	Polşanın Kompyuterlə bağlı Fövqəladə Hallar Qrupu	http://www.cert.pl
Portuqaliya	CERT.PT	https://www.cncs.gov.pt
Qətər	Qətər İnformasiya Təhlükəsizliyi Milli Mərkəzi	http://www.qcert.org
İrlandiya Respublikası	CSIRT-IE	https://ncsc.gov.ie/csirt
Rumıniya	Rumıniya Milli Kompyuter Təhlükəsizliyi Hadisələrinə Müdaxilə Qrupu	http://cert.ro
Rusiya	RU-CERT Kompüter Təhlükəsizliyi Hadisələrinə Müdaxilə Qrupu	http://www.cert.ru

Səudiyyə Ərəbistanı	Kompyuterlə bağlı Fövqəladə Hallar Qrupu - Səudiyyə Ərəbistanı	http://www.cert.gov.sa
Sinqapur	Sinqapurun Kompyuterlə bağlı Fövqəladə Hallar Qrupu	https://www.csa.gov.sg/singcert
Slovakiya	SK-CERT	https://www.sk-cert.sk
Sloveniya	Sloveniyanın Kompyuterlə bağlı Fövqəladə Hallar Qrupu	http://www.cert.si
Koreya Respublikası	CERT Koordinasiya Mərkəzi Koreya	http://www.krcert.or.kr
İspaniya	INCIBE-CERT İspaniya Milli Kibertəhlükəsizlik İnstitutu - Milli CSIRT	https://www.incibe-cert.es
Şri Lanka	SL CERT | CC	http://www.cert.gov.lk
İsveç	İsveç Hökümətinin Kompyuterlə bağlı Fövqəladə Hallar Qrupu	http://www.melani.admin.
Çinin Tayvan əyaləti	Tayvanın Kompyuterlə bağlı Fövqəladə Hallar Qrupu /Koordinasiya Mərkəzi	http://www.twcert.org.tw
Tonqa	CERT Tonqa	http://www.cert.gov.to
Tunis	TunCERT – Tunisin Kompyuterlə bağlı Fövqəladə Hallar Qrupu	https://www.ansi.tn
Türkiyə	TP-CERT Milli Kibertəhlükəsizlik Hadisələrinə Müdaxilə Qrupu	http://www.uekae.tubitak.gov.tr
Ukrayna	Ukraynanın Kompyuterlə bağlı Fövqəladə Hallar Qrupu	https://cert.gov.ua
Birləşmiş Ərəb Əmirlikləri	Birləşmiş Ərəb Əmirliklərinin Kompyuterlə bağlı Fövqəladə Hallar Qrupu	http://www.aecert.ae
Uqanda	CERT.UG Uqandanın Kompyuterlə bağlı Fövqəladə Hallar Qrupu	http://www.ug-cert.ug
Birləşmiş Krallıq	Milli Kibertəhlükəsizlik Mərkəzi	http://www.ncsc.gov.uk
Amerika Birləşmiş Ştatları	Amerika Birləşmiş Ştatları Kompyuter Təcili Hazırlıq Mərkəzi	https://www.us-cert.gov
Özbəkistan	Özbəkistanın Kompyuterlə bağlı Fövqəladə Hallar Qrupu	http://uzcert.uz
Vyetnam	Vyetnamın Kompyuterlə bağlı Fövqəladə Hallar Qrupu	http://www.vncert.gov.vn

Çalışma

Sizin ölkədə milli CSİRT vardırmı?

1. Əgər vardırsa, onun hansı modeldə olduğunu və necə işlədiyini təsvir edin. Onun öz funksiyalarının icrasında nə qədər effektiv olduğunu dəyərləndirin.

2. Əgər yoxdursa, hansı CSİRT modeli sizin ölkə üçün uyğun olardı və sizin ölkədə milli CSİRT-in yaradılması üçün nə tələb olunur?

Özünü sına

1. CSİRT-lərin əsas funksiyaları hansılardır?

2. Beynəlxalq CSİRT-lər milli CSİRT-lərdən nə ilə fərqlənir?

3. CSİRT-nin yaradılması üçün hansı tələblər vardır?

7. İNFORMASİYA TƏHLÜKƏSİZLİYİ SİYASƏTİNİN MƏRHƏLƏLƏRİ

Bu bölümün məqsədi aşağıdakılardan ibarətdir:

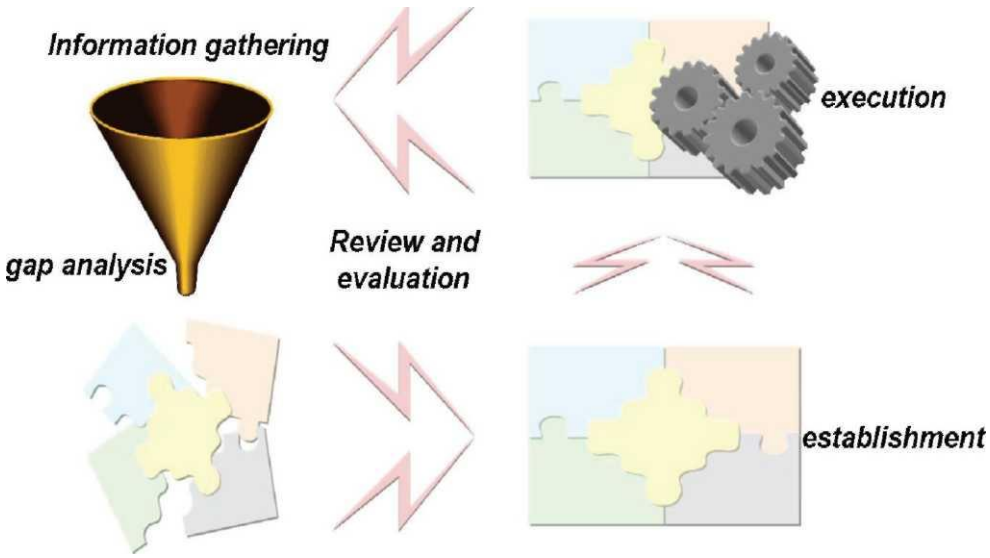
- **İnformasiya təhlükəsizliyi siyasətinin formalaşdırılması prosesini nəzərdən keçirmək; və**
- **İnformasiya təhlükəsizliyi siyasəti formalaşdırılarkən siyasəti müəyyən edən şəxslər tərəfindən nəzərdən keçirilməli məsələləri müzakirə etmək.**

Siyasəti müəyyən edən tərəflər bir sıra fikirləri nəzərə almalıdırlar, onlar arasında bu siyasət üçün əsas səbəb, mövcud resurslar, siyasətin istiqaməti, büdcə və hüquqi tələblər və siyasətdən gözlənilən nəticələr də vardır. Bu bölümdə, bu mülahizələr informasiya təhlükəsizliyi üzrə siyasətin formalaşdırılmasının müxtəlif mərhələri kontekstində müzakirə olunur.

Qeyd olunmalıdır ki, müxtəlif ölkələr bir qədər fərqli siyasi mülahizələrə və kontekstlərə malik olacaqlar. Bu bölümdə təsvir olunan siyasətin formalaşdırılması prosesi ümumidir və milli informasiya təhlükəsizliyi siyasətinin mövcud olmaması fərziyyəsinə əsaslanır.

Digər siyasətlərdə olduğu kimi, informasiya təhlükəsizliyi siyasətinin formalaşdırılma prosesini dörd mərhələyə bölmək olar: (1) informasiya toplama və boşluqların təhlil edilməsi; (2) siyasətin müəyyənləşdirilməsi; (2) siyasətin həyata keçirilməsi; və (4) nəzarət və əks təsir (23-cü Təsvirə bax). Bundan əlavə, milli informasiya təhlükəsizliyi siyasətinə, informasiya təhlükəsizliyi strategiyası, hüquqi münasibətlər, informasiya təhlükəsizliyi təşkilatı, informasiya təhlükəsizliyi texnologiyası və onlar

Şəkil 21. İnformasiya təhlükəsizliyi siyasətinin mərhələləri



arasında qarşılıqlı əladə də daxil edilməlidir.

7.1 İnformasiyanın toplanması və boşuqların təhlili

İnformasiya təhlükəsizliyi siyasətinin formalaşdırılmasında birinci mərhələ informasiyanın toplanması və boşluqların təhlil edilməsidir.

İnformasiya toplanarkən, digər ölkələrin informasiya təhlükəsizliyi və digər əlaqədar siyasət nümunələrini, habelə ölkənin özündə əlaqədar siyasətləri nəzərdən keçirmək faydalıdır.

Boşluqlar təhlil olunarkən, mövcud qanunlar və sistemlər kimi, informasiya təhlükəsizliyi ilə bağlı mövcud infrastrukturu, habelə doldurulmalı olan sahələri və ya boşluqları başa düşmək vacibdir. Bu, vacib addımdır, belə ki, o, müəyyən edilməli olan informasiya təhlükəsizliyi siyasətinin istiqamətini və ya prioritetini təyin edir.

İnformasiyanın toplanması

Xarici ölkələrdən nümunələrin toplanması: Digər ölkələrdə müvafiq nümunələri müəyyənləşdirərkən, siyasətçilər aşağıdakılarla bağlı oxşarlıqları nəzərə almalıdırlar —

- Milli informasiya təhlükəsizliyi səviyyəsi
- Siyasətin müəyyənləşdirilməsində istiqamət
- Şəbəkə və sistem infrastrukturu

Bu oxşarlıqları nəzərdən keçirərkən, aşağıdakı materiallar toplanmalıdır -

- İnformasiya təhlükəsizliyində iştirak edən təşkilatların təsis edilməsinə və fəaliyyətinə dair informasiya (bax, bu modulun 3 və 6-cı bölümləri)
- İnformasiya təhlükəsizliyinə dair siyasətlər, qanunlar və qaydalar (bax, 3-cü bölüm)
- Müxtəlif ölkələrdən beynəlxalq səviyyədə istifadə edilən informasiya təhlükəsizliyi metodologiyası və nümunələri (bax, 4-cü bölüm)
- Təhlükə meylləri və hücumun növlərinə görə əks tədbirlər və ya nəzarətlər (bax, 2 və 6-cı bölümlər)
- Şəxsi həyatın toxunulmazlığının qorunması üçün əks tədbirlər (bax, 5-ci bölüm)

Daxili materialların toplanması: Əksər siyasətçilər informasiya təhlükəsizliyi üzrə ekspert olmasalar da, onlar informasiya təhlükəsizliyi ilə bağlı və ya ona uyğun tədbirlər görürlər. Xüsusən də, onlar, informasiya təhlükəsizliyi ilə bağlı qanunlar, qaydalar və siyasətlər hazırlayırlar. Lakin, qanunlarda, qaydalarda və siyasətlərdə diqqət spesifik məsələlərə yönəldiyinə görə, onlar arasında əlaqə ilk olaraq siyasətçilərin nəzərindən qaça bilər. Beləliklə, informasiya təhlükəsizliyi ilə bağlı və ya ona uyğun bütün qanunlar, qaydalar və siyasətlər toplanmalı, təhlil edilməli və qiymətləndirilməlidir.

Boşlquların təhlil olunması

Sun Tzunun *Müharinə aparmaq bacarığı* əsərində deyilir: “Düşmənini tanı” Bu, o deməkdir ki, sən hüdudlarını, habelə düşmənin hüdudlarını bilməlisən. İnformasiya təhlükəsizliyi siyasətinin formalaşdırılmasında, bu, informasiya təhlükəsizliyi siyasəti vasitəsilə nəyin qorunmalı olduğunu, habelə informasiya təhlükəsizliyində zəif tərəfləri və hədələri bilmək deməkdir.

Boşluqların təhlil edilməsi iki mərhələyə bölünə bilər:

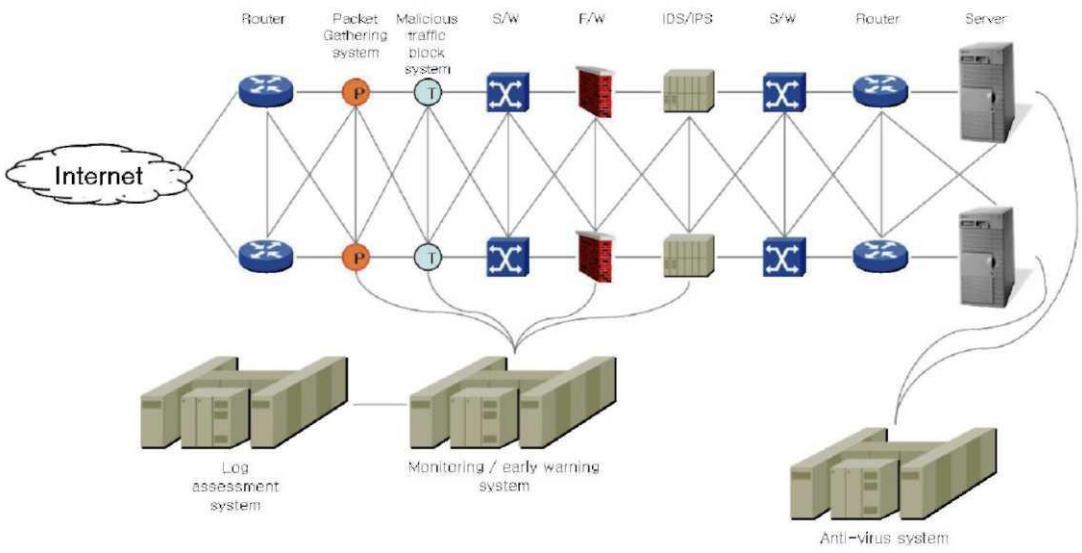
1. Ümumi informasiya təhlükəsizliyi sahəsində ölkənin imkanlarını və potensialını - yəni təşkilat və insan resurslarını, habelə informasiya və kommunikasiya infrastrukturunu başa düşmək; və
2. İnformasiya təhlükəsizliyinə kənar təhdidləri müəyyənləşdirmək.

Siyasətçilər, informasiya təhlükəsiziyi ilə bağlı sahələrdə ictimai və özəl təşkilatlar olan informasiya təhlükəsizliyi təşkilatı və insan resursları ilə tanış olmalıdırlar. Onlar informasiya təhlükəsizliyi ilə bağlı işdə iştirak edən təşkilatları bilməli və onların iş həcmini, rolunu və vəzifələrini başa düşməlidirlər. Bu informasiya təhlükəsizliyi üzrə mövcud strukturların işinin təkrarlanmaması üçün vacibdir.

Bu mərhələdə, həmçinin, informasiya təhlükəsizliyi sahəsində ekspertlər müəyyən edilməli və cəlb olunmalıdır. Belə ekspertlər, səciyyəvi olaraq hüquq, siyasət, texnologiya, təhsil və əlaqədar sahələrdə müəyyən təcrübəyə malikdirlər.

İnformasiya-kommunikasiya infrastrukturu dedikdə elektron nəzarət idarəetmə sistemlərini və informasiyanı toplayan, işləyən, saxlayan, axtaran, ötürən və alan İT strukturu anlaşılır. Qısaca olaraq, bu, informasiya sistemi və şəbəkədir. İnformasiya-kommunikasiya infrastrukturunun hazırki vəziyyətini başa düşmək iqtisadi baxımdan xüsusilə vacibdir. Ona görə ki, bütün dünyanı birləşdirmək üçün böyük investisiyalar tələb olunur, mövcud informasiya-kommunikasiya xidmətlərinin əksəriyyətinin olması əlverişlidir. 24-cü Təsvirdə informasiya təhlükəsizliyi üçün informasiya-kommunikasiya infrastrukturunun nümunəsi göstərilir. Bura tələb oluna bilən bütün bəndlər daxil deyildir və o, yalnız nümayiş etdirmə məqsədləri üçün verilir. Şəbəkənin müxtəlif komponentləri arasında əlaqələri qeyd edin.

Şəkil 22. Şəbəkə və sistem strukturunun nümunəsi



Siyasətçilər, informasiya təhlükəsizliyi üçün ümumi şəbəkə və sistemlərin necə qurulduğunu başa düşməlidirlər.

Boşluqların təhlil edilməsində ikinci addım informasiya təhlükəsizliyinə kənar təhdidləri müəyyənləşdirməkdir. 2-ci bölümdə göstərildiyi kimi, mühüm informasiyaya təhdidlər tək artmır, eyni zamanda daha da mürəkkəb xarakter alır. Hansı əks tədbirlərin zəruri olduğunu qərarlaşdıra bilmək məqsədilə, siyasətçilər, bu hədələri başa düşməlidirlər. Xüsusilə də, siyasətçilər aşağıdakıları başa düşməlidirlər:

- İnformasiya təhlükəsizliyinə hədələrin nüfuzetmə səviyyəsi
- Ən çox yayılan və hazırki hücum növləri
- Hədələrin növləri və gələcəkdə onların gözlənilən güclənmə dərəcəsi

Milli təşkilatları, insan resurslarını və informasiya-kommunikasiya infrastrukturunu təhlil etdikdən, habelə informasiya təhlükəsizliyi sahəsində təhlükə komponentlərini başa düşdükdən sonra, zəif tərəf komponentlərini əldə etmək lazımdır. Bu, ölkənin nə qədər kənar təhlükə komponentlərinə müqavimət göstərə biləcəyini müəyyənləşdirməkdir. Bu, aşağıdakıları yoxlamaqla müəyyən edilə bilər:

- CERT-in hazırki vəziyyəti və onun cavab vermə imkanları
- Informasiya təhlükəsizliyi üzrə ekspertlərin hazırki vəziyyəti
- İnformasiya təhlükəsizliyi sisteminin qurulma səviyyəsi və intensivliyi
- İnformasiya aktirlərinə müdaxilələrə qarşı hüquqi müdafiə
- Informasiya aktivlərinin qorunması üçün fiziki mühit

Boşluqların təhlilinin aparılmasında məqsəd həyata keçirilməli olan praktiki əks tədbirləri müəyyənləşdirmək imkanına malik olmaqdır. Vurğulamaq lazımdır ki, bu, informasiya təhlükəsizliyi siyasətinin formalaşdırılmasında ən əsas addımdır.

7.2 İnformasiya təhlükəsizliyi siyasətinin formalaşdırılması

Milli informasiya təhlükəsizliyi siyasətinin formalaşdırılmasına aşağıdakılar aiddir (1) siyasətin istiqamətini müəyyən etmək; (2) informasiya təhlükəsizliyi təşkilatını yaratmaq və onun rol və vəzifələrini müəyyənləşdirmək; (3) informasiya təhlükəsizliyinin siyasət çərçivəsini dəqiqləşdirmək; və (5) informasiya siyasətinin həyata keçirilməsi üçün büdcəni ayırmaq.

1.Siyasətin istiqamətinin müəyyən edilməsi və irəliyə doğru hərəkət etmə

Əksər hallarda, informasiya təhlükəsizliyi siyasəti üçün səylər, özəl sektorun ixtiyarına buraxılmaq əvəzinə, hökumət tərəfindən yönləndirilməlidir. Xüsusilə də, hökumət, siyasəti müəyyən etməli, lazımi infrastrukturun yaradılmasında aparıcı rol oynamalı və uzun-müddətli dəstək göstərməlidir. Özəl sektor, müəyyən vaxtdan sonra, əsasən tədqiqat və inkişaf etdirilmə işində və sistemin qurulmasında iştirak etmək üçün layihəyə qoşulur.

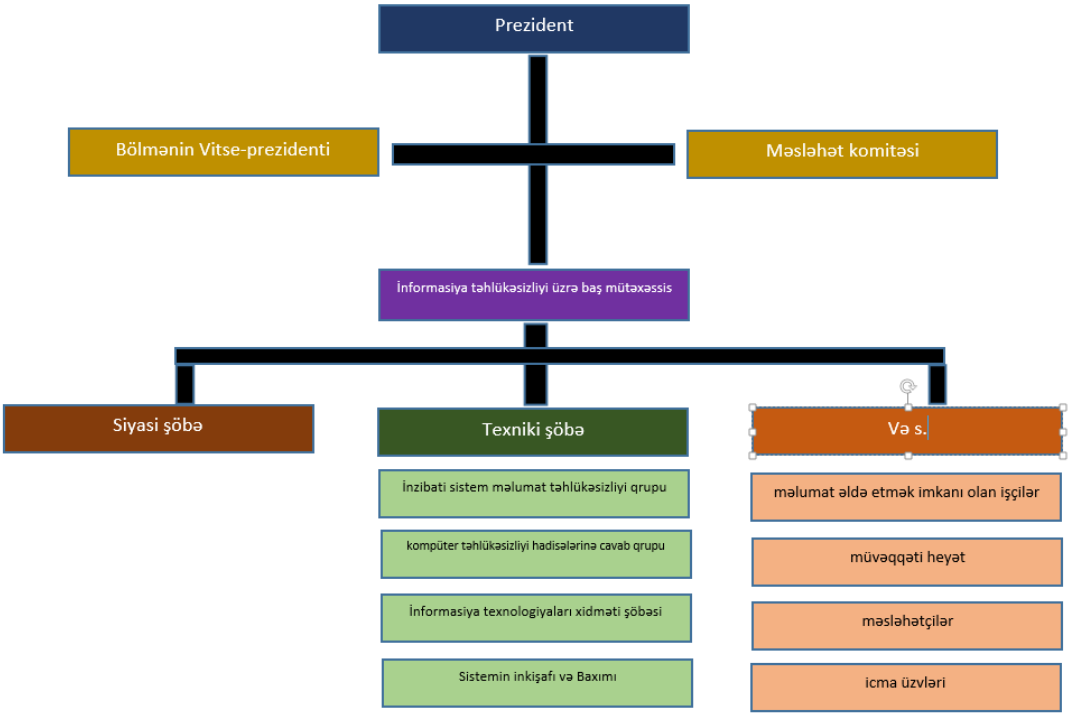
Özəl sektorun iştirakı üçün planlaşdırma işinə bina boyu maarifləndirmə və informasiya-kommunikasiya infrastrukturunun gücləndirilməsi aiddir. Əgər hökumət, özəl sektoru, informasiya təhlükəsizliyi ilə bağlı

strategiyanı qəbul etməyə həvəsləndirmək məqsədini daşıyırsa, hökumət nəzarətedici roldan daha çox dəstəkverici rol oynamalıdır. Bu, informasiya təhlükəsizliyi ilə bağlı tövsiyələrin yayımlanması da aiddir.

2. İnformasiya təhlükəsizliyi təşkilatının yaradılması və rolların və vəzifələrin təyin edilməsi[57]

İnformasiya siyasətinin istiqaməti müəyyən edildikdən sonra, icraedici orqan yaradılmalıdır. 25-ci Cədvəldə ümumi olaraq informasiya təhlükəsizliyi təşkilatının strukturu göstərilir.

Şəkil 23. Ümumi milli informasiya təhlükəsizliyi təşkilatı



57 Bu bölüm Sinkler Cəmiyyəti Kollecindən götürülmüşdür, "İnformasiya təhlükəsizliyi təşkilatı – roller və vəzifələr", http://www.sinclair.edu/about/information/usepolicy/pub/infscply/Information_Security_Organization_-_Roles_and_Responsibilities.htm.

Milli informasiya təhlükəsizlik təşkilatları hər bir ölkənin xüsusiyyətlərinə və mədəniyyətinə görə bir-birlərindən cüzi fərqlənir. Lakin, əsas prinsip, rol və vəzifələrin aydın şəkildə göstərilməsidir.

İnzibati quruluş

Bölmənin vitse-prezidentləri, onların öz müvafiq bölmələri tərəfindən istifadə oldunduğu və "sahib çıxıldığı" kimi, ilk növbədə toplanan, saxlanan və / və ya müəyyən olunan informasiyaya görə cavabdehlik daşıyırlar. Onlar Informasiya Təhlükəsizliyi üzrə Əməkdaş və informasiya təhlükəsizliyi siyasətinin həyata keçirilməsində İnformasiya Təhlükəsizliyi üzrə Əməkdaşa kömək etmək üçün digər fərdləri təyin edə bilərlər. Bu təyin olunmuş heyət, onların nəzarətində olan informasiya aktivlərinin təyin olunmuş sahiblərinin olmasını, risklə bağlı dəyərləndirmələrin aparılmasını və həmin risklər əsasında yünüglləşdirmə proseslərinin həyata keçirilməsini təmin etməlidir.

Supervayzerlər (Direktorlar, Sədrlər, Rəhbərlər və s.) informasiyaya və informasiya sistemlərinə çıxış imkanı olan əməkdaşları idarə edirlər və onların müvafiq sahələrinə tətbiq edilə bilən informasiya təhlükəsizliyinə nəzarət tədbirlərini müəyyən edir, həyata keçirir və onların icrasını təmin edir. Onlar bütün əməkdaşların informasiya təhlükəsizliyi ilə bağlı öz vəzifələrini başa düşmələrini və öz işlərini yerinə yetirmək üçün tələb olunan çıxış imkanına malik olmalarını təmin etməlidirlər. Nəzarətçilər mütəmadi olaraq uyğunluğu təmin etmək üçün bütün istifadəçilərin çıxış imkanına malik olma səviyyələrini nəzərdən keçirir və ziddiyyətləri və çatışmazlıqları düzəltmək üçün müvafiq tədbirlər görürlər.

Baş İnformasiya Təhlükəsizliyi Əməkdaşı (CİSO) informasiya təhlükəsizliyi siyasətinin əlaqələndirilməsinə və ona nəzarət olunmasına görə cavabdehlik daşıyır. Müxtəlif bölmələrlə sıx faəliyyət göstərərək, CİSO, xüsusi bölmələrin nəzarətçilərinə, siyasətin ayrı-ayrı ünsürlərinə nəzarət etmək və əlaqələndirmək üçün digər nümayəndələri təyin etməyi tövsiyə edə bilər. CİSO, həmçinin, aşağıdakılarla bağlı informasiya təhlükəsizliyinə dair qabaqcıl təcrübələrin tətbiq olunmasında informasiya sahiblərinə yardım edirlər:

- İnformasiya resurslarına çıxış imkanı və onlardan məqbul şəkildə istifadə ilə bağlı tətbiq edilə bilən qaydaların müəyyən edilməsi və yayımlanması;
- İnformasiya təhlükəsizliyi riskinin dəyərləndirilməsi və bununla bağlı təhlillərin aparılması / əlaqələndirilməsi;
- Məlumat və sistemləri qorumaq üçün təhlükəsizliklə bağlı uyğun qaydaların və tədbirlərin müəyyənləşdirilməsi;
- Sistemlərin təhlükəsizlik baxımından zəif tərəflərinin monitorinqini aparmağa və idarəetməyə yardım göstərmə;
- İnformasiya təhlükəsizliyi ilə bağlı auditlərin aparılması / əlaqələndirilməsi; və
- Problemlərin və / və ya milli informasiya təhlükəsizlik siyasətlərinin pozulması halları ilə bağlı araşdırmaların aparılmasına / həll yolunun tapılmasına yardım etmə.

Texniki quruluş

İnzibati Sistem üzrə İnformasiya Təhlükəsizliyi Qrupu, özəl, həssas və mühüm informasiyanı qorumaq kimi milli hüquqi və etik vəzifələri yerinə yetirməklə yanaşı, inzibati qaydada tətbiq edilən təhlükəsizliyə nəzarət tədbirlərinin, maraqlı tərəflərə, informasiyaya müvafiq çıxış imkanı verməsini təmin etmək üçün tədbirləri inkişaf etdirir və həyata keçirir. Qrup, inzibati sistemdəki informasiyanın optimal mövcudluğunu, bütövlüyünü və məxfiliyini təmin etmək üçün prosesləri və standartları, o cümlədən istifadəçilər üçün ilkin çıxış imkanın verilməsini və bu imkanda dəyişikliklərin edilməsini; istifadəçiyə icazə verilmiş çıxış imkanının, habelə istifadəçinin / nəzarətçinin hüquq və vəzifələrinin sənədləşdirilməsini; və təhlükəsizliklə bağlı ziddiyyətlərin və problemlərin həll edilməsini sorğu etmək proseslərini müəyyənləşdirir.

Qrupa Bölmənin İnformasiya Təhlükəsizlik Əməkdaşları və CİSO daxildir. Qrupa Departamentin İnformasiya Təhlükəsizliyi Əməkdaşları və İnzibati Sistemin İnzibatçıları tərəfindən məsləhətlər verilir.

CSİRT, kompüter təhlükəsizliyi ilə bağlı hadisə risklərini azaltmaq üçün proaktiv tədbirlərin həyata keçirirlməsində və belə hadisələr baş verdiyi təqdirdə onlardan dəyən ziyanın araşdırılmasında, nəticələrin aradan qaldırılmasında və minimuma endirilməsində maraqlı tərəflər üçün informasiyanı təmin edir və onlara yardım göstərir. CSİRT, həmçinin, davamlı tədbirləri müəyyənləşdirir və tövsiyə edir. İki-səviyyəli CSİRT, ilkin müəyyənləşdirmə, nəticələrin aradan qaldırılması, çeşidləmə və genişləmə tələblərinin təyin edilməsi kimi vəzifələrin həvalə olunduğu əməliyyat qrupundan və iri və əhəmiyyətli hadisələrin nəticələrinin milli səviyyədə aradan qaldırılması işinə rəhbərliyi həyata keçirən idarəetmə qrupundan ibarətdir. CİSO və İT Xidmətləri və Sistemlərin İnkişafı və Onlara Xidmət Bölməsindən olan səlahiyyətləndirilmiş İT heyəti CSİRT-nin əməliyyat qrupuna daxildirlər. CSİRT-nin idarəetmə qrupu, Baş İnformasiya Əməkdaşından, Polisin Rəhbərindən, İctimai İnformasiya Rəhbərindən, İT Xidmətlərinin Rəhbərindən, Sistemlərin İnkişafı və Xidmət Bölməsinin Rəhbərindən, CİSO, sistem və şəbəkə nəzarətçisindən, hüquqi məsləhətçidən, insan resursları üzrə məsləhətçidən və xüsusilə də Vitse Prezidentlər tərəfindən təyin olunmuş texniki təcrübəyə malik nümayəndələrdən ibarətdir.

İT Xidmətləri Departamentinin heyəti sistem və şəbəkə administratorlarından və mühəndislərdən və İT Köməkçi Xidməti, istifadəçiyə dəstək göstərən texniki işçilər və səs əlaqə inzibatçıları kimi texniki xidmət təminatçılarından ibarətdir. Onlar, şəbəkə mühitində informasiya təhlükəsizliyi ilə bağıə texniki vasitələrin, nəzarətlərin və təcrübələrin birləşdirilməsinə görə cavabdehlik daşıyırlar. Onlar, son istifadəçilər tərəfindən informasiya təhlükəsizliyinə riayət olunmamasına dair şübhəli hallar və ya hadisələr barədə hesabatlar alırlar.

Sistemlərin İnkişafı və Xidmət Bölməsinin heyətinə layihəni işləyib hazırlayanlar və məlumat bazalarının inzibatçıları aid edilir. Onlar, milli tətbiqi proqramlar üçün təhlükəsizliklə bağlı qabaqcıl təcrübələri inkişaf etdirir, tətbiq edir, birləşdirir və həyata keçirirlər və tətbiqetmə təhlükəsizliyi ilə bağlı prinsiplərdən istifadə üzrə Veb tətbiqi proqramını hazırlayanlara təlim keçirlər.

Digərləri

İnformasiyaya çıxış imkanı olan əməkdaşlar və informasiya sistemləri tətbiq edilən milli siyasətlərə və prosedurlara, habelə onların bölmələrinin rəisləri və ya rəhbərləri tərəfindən müəyyən edilən hər hansı əlavə təcrübələrə və ya prosedurlara riayət etməlidirlər. Bura, onların öz hesablarına daxil olmaları üçün məxfi sözlərin qorunması və informasiyadan sui-istifadə ilə bağlı şübhəli hallar və informasiya təhlükəsizliyi ilə bağlı hadisələr barədə müvafiq tərəfə (adətən öz nəzarətçilərinə) məlumat vermələri aiddir.

Müvəqqəti heyət üzvləri əməkdaş hesab edilirlər və informasiya və informasiya sistemlərinə çıxış imkanına malik olmaqlq tam və ya yarımştat əməkdaşlarla eyni vəzifələri daşıyırlar.

Məsləhəçilər, xidmət təminatçıları və müqavilə əsasında cəlb edilən üçüncü tərəflərə informasiyaya çıxış imkanı "bilməlidir" əsası ilə verilir. Üçüncü tərəf üçün tələb olunan şəbəkə hesabı, təşkilat çərçivəsində üçüncü tərəf istifadəçisinin şəbəkədə hesabla bağlı fərdi öhdəliklərini başa düşməsini təmin edən "maliyyələşdirən" tərəfindən sorğu edilməli və vitse-prezident və ya director tərəfindən təsdiq olunmalıdır. İstifadəçi öz məxfi sözlərini təhlükəsiz şəraitdə saxlamalı və öz nəzarəti çərçivəsində onun istifadəçi adından istifadə nəticəsində hər bir hərəkətə görə cavabdeh olmalıdır.

3. İnformasiya təhlükəsizliyi siyasətinin çərçivəsini müəyyənləşdirmə

İnformasiya təhlükəsizliyi çərçivəsi

İnformasiya təhlükəsizliyi çərçivəsi informasiya təhlükəsizliyi siyasəti üçün parametrləri müəyyən edir. O, siyasətdə İT resurslarının (insanlar, informasiya sənədləri, avadanlıq, proqram təminatı, xidmətlər) nəzərə alınmasını; beynəlxalq qanunları və qaydaları əks etdirməsini; informasiyanın mövcudluğu, məxfiliyi, tamlığı, cavabdehlik və zəmanətlə bağlı prinsiplərə cavab verməsini təmin edir.

İnformasiya təhlükəsizliyi siyasəti informasiya təhlükəsizliyi çərçivəsinin ən mühüm hissəsidir. Siyasətə aşağıda müzakirə olunan beş sahə aiddir:

a. **Plan və təşkilat:** Bu sahəyə təşkilat və fəaliyyətin təhlükəsizliyi və aktivlərin təsnifatı və onlara nəzarət aiddir.

Təhlükəsizlik təşkilatı və fəaliyyət aşağıdakıları əhatə edir —

- Milli informasiya təhlükəsiliyi təşkilatının təşkil edilməsi və sistemi
- Hər bir informasiya təhlükəsizliyi təşkilatının proseduru
- Milli informasiya təhlükəsizliyinin yaradılması və idarə olunması
- Müvafiq beynəlxalq agentliklə əməkdaşlıq
- Ekspert qrupu ilə əməkdaşlıq

Aktivlərin təsnifatı və nəzarət tədbirlərinə aşağıdakılar aiddir —

- Mühüm informasiya aktivləri üçün sahibliyin verilməsi və təsnifat standartı
- Mühüm informasiya aktivləri üçün qeydiyyata dair təlimat və risk dəyərləndirməsi
- Mühüm informasiya aktivlərinə cıxış imkanında üstünlüklərə nəzarət
- Mühüm informasiya aktivlərinin nəşri və ixracı
- Mühüm informasiya aktivlərinin yenidən qiymətləndirilməsi və tükənməsi
- Sənədlərə təhlükəsizliklə bağlı nəzarət

b. Əldə etmə və həyata keçirmə: Bu sahəyə insan resurslarının təhlükəsizliyi və informasiya sistemlərinin əldə edilməsi və inkişaf təhlükəsizliyi aiddir.

İnsan resurslarının təhlükəsizliyi, aşağıdakıları əhatə edən, yeni əməkdaşları cəlb etmək üçün idarəetmə metodunun təyin edilməsini əhatə edir —

- İnsan resurslarının təhlükəsizliyi ilə bağlı əks tədbir və təhlükəsizlik üzrə təlim
- Təhlükəsizliklə bağlı qaydanın və qanunun pozulması halları üzrə araşdırma prosesi
- Üçüncü tərəfin çıxış imkanı ilə bağlı təhlükəsizliyə nəzarət
- Autsorsinq (kənar resursları cəlb etmə) heyətinin çıxış imkanı ilə bağlı təhlükəsizliyə nəzarət
- Üçüncü tərəflərin və autsorsinq heyətinin işi və nəzarət
- Kompüter otağı və avadanlıqla bağlı təhlükəsizliyə nəzarət
- Əsas qurğulara və binalara daxil olma imkanı
- Təhlükəsizliklə bağlı hadisələr üzrə araşdırma prosesi

İnformasiya sistemlərinin əldə olunması və inkişaf təhlükəsizliyi aşağıdakıları tələb edir —

- İnformasiya sistemi əldə olunarkən təhlükəsizliklə bağlı yoxlamalar
- Tətbiqi proqramların daxili istifadə və autsorsinqi üçün təhlükəsizliyə nəzarət
- Milli şifrələmə sistemi (şifrələmə proqramı və açar və sairə)
- Proqramın inkişaf etdiriməsindən sonra sınaqlar
- Autsorsinq inkişaf zamanı təhlükəsizliklə bağlı təklif olunan tələblər
- İnkişaf və əldə etmə ilə bağlı təhlükəsizlik yoxlaması

c. Şəxsi həyatın toxunulmazlığının qorunması: Şəxsi həyatın toxunulmazlığının qorunmasının informasiya təhlükəsizliyi siyasətinə daxil edilməsi məcburi deyildir. Lakin, bunun daxil edilməsi üstünlükdür, belə ki, bu, beynəlxalq məsələdir. Şəxsi həyatın toxunulmazlığının qorunması aşağıdakıları əhatə etməlidir -

- Fərdi informasiyanı toplama və ondan istifadə
- İnsanların şəxsi həyatının toxunulmazlığından sui-istifadə edildikdə əvvəlcədən verilən razılıq.
- PIA

d. Fəaliyyət və dəstək: Bu sahədə fiziki və texniki təhlükəsizliyə diqqət yetirilir. Şəbəkədən və sistemdən istifadə təfsilatlı şəkildə tənzimlənir və informasiya və kommunikasiya infrastrukturunun fiziki təhlükəsiliyi müəyyən edilir.

İnformasiya sisteminin fəaliyyəti və təhlükəsizliyə nəzarət aşağıdakıları əhatə edir -

- Serverin, şəbəkənin, tətbiqetmənin və məlumat bazasının fəaliyyəti və təhlükəsizliyə nəzarət.
- İnformasiya təhlükəsizlik sisteminin inkişaf etdirilməsi.
- Hüquqi tədbirə qarşı loq və ehtiyat.
- İnformasiyanın saxlanılmasına nəzarət
- Mobil hesablama
- Saxlama standartı və kompüter məlumatlarının təhlükəsizliyi
- Elektron kommersiya xidmətləri

Hesab üstünlüyü ilə bağlı təhlükəsizliyin idarəedilməsi – Milli informasiya saxlancından istifadədə məxfiliyə zəmanət vermək üçün daxil olmaya nəzarət və hesab idarəetməsi. Bura daxildir -

- milli informasiya sistemi istifadəçilərin qeydiyyatı, ləğvi və imtiyazlarının idarəedilməsi
- şifrələnmiş şəbəkədə Hesab və imtiyazların idarəedilməsi

Fiziki təhlükəsizlik – Fiziki təhlükəsizlik dedikdə mühüm informasiyanın saxlandığı informasiya və kommunikasiya xidmətlərinin qorunması nəzərdə tutulur. Bura daxildir -

- Təhlükəsizlik sahələrinin konfiqurasiyası və nəzarətetmə metodları
- Kompüter mərkəzi üçün daxil olma və nəqletməyə nəzarət
- Təbii və digər fəlakətlərdən dəyən ziyanın qarşısının alınması

e. Monitorinq və Dəyərləndirmə: İnformasiya təhlükəsizliyi siyasətinin bu sahəsində təhlükəsizliklə bağlı hadisələrin qarşısının alınması və təhlükəsizliklə bağlı hadisələr üzrə idarəetmə və nəticələrin aradan qaldırılması üçün standartların və proseslərin formalaşdırılması tələb olunur.

Təhlükəsizlik təftişinə aiddir —

- Təhlükəsizliklə bağlı təftiş planının müəyyənləşdirilməsi
- Mütəmadi təhlükəsizlik təftişinin aparılması
- Hesabat formalarının hazırlanması / təşkil edilməsi
- Təhlükəsizlik təftişlərinin obyektinin və hesabat hədəflərinin müəyyən olunması

Təhlükəsizliklə bağlı hadisələr üzrə idarəetmə və nəticələrin aradan qaldırılması
aşağıdakıların müəyyənləşdirilməsini tələb edir —

- Təhlükəsizliklə bağlı hadisələr araşdırılarkən hər bir təşkilatın işi və rolu
- Təhlükəsizliklə bağlı hadisələrin əlamətlərinin müşahidə olunması və tanınması üzrə prosedurlar
- Təhlükəsizliklə bağlı hadisələrin araşdırılma proseduru və nəticələrin aradan qaldırılması metodu
- Təhlükəsizliklə bağlı hadisələr araşdırıldıqdan sonra görülməli olan tədbirlər

4. İnformasiya təhlükəsizliyi siyasətinə uyğun olmaq üçün qanunların qəbul edilməsi və / və ya onlara düzəlişlərin edilməsi

Qanunlar informasiya təhlükəsizliyi siyasətinə uyğun olmalıdırlar. Dövlət təşkilatları və özəl müəssisələri tənzimləyən qanunlar olmalıdır. 14 - 16-cı Cədvəllərdə Yaponiyada, Aİ-də və ABŞ müvafiq olaraq informasiya təhlükəsizliyi ilə bağlı qanunar sadalanır. Yaponiyada İT ilə bağlı qanunlardan biri Qabaqcıl informasiya və telekommunikasiya şəbəkə cəmiyyətinin formalaşdırılması üzrə əsas qanundur. Bu qanun ölkədə informasiya təhlükəsizliyi üzrə əsas standartdır və digər müvafiq qanunlar ona uyğun olmalıdır.

Cədvəl 13.Yaponiyada informasiya təhlükəsizliyi ilə bağlı qanunlar

Qanunlar	Hədəf seçilən sənaye	Tənzimləmə hədəfi	Cəza
Kompyuterə icazəsiz daxil olmalar haqqında Qanun	Bütün sənaye	Xəbərdarlıq etmədən digər şəxsin şəxsi informasiyasına icazəsiz daxil olma və ya təmin etməni təşviq edən hərəkət	
Fərdi informasiyanın qorunması haqqında qanun	Biznes məqsədləri üçün özəl informasiyadan istifadə edən özəl müəssisələr	Şəxsi həyatın toxunulmazlığı ilə bağlı informasiyanın (ünvan, telefon nömrəsi, e-poçt, və sairə) idarə olunması	Cinayət məsuliyyəti, cərimə
Elektron imzalar və təsdiqetmə haqqında qanun		Şəbəkələr vasitəsilə İnternet və iqtisadi fəaliyyətdən yararlanan elektron kommersiyaya şərait yaratma	

5. İnformasiya siyasətinin həyata keçirilməsi üçün büdcənin ayrılması

Siyasətin həyata keçirilməsi üçün büdcə tələb olunur. 17-ci Cədvəldə son illərdə Yaponiyada və ABŞ-da informasiya təhlükəsizliyi üçün büdcə göstərilir.

Cədvəl 16: Böyük Britaniya və Amerika Birləşmiş Ştatlarının informasiya təhlükəsizliyi büdcəsi

Birləşmiş Krallıq	2016	2017	2018	2019	2020
İnformasiya təhlükəsizliyi büdcəsi	1092	1137	-	-	-
Amerika Birləşmiş Ştatları	2016	2017	2018	2019	2020
Ümumi illik İT büdcəsi	-	81, 495	137, 489	-	-

Sources: OMB for US figu

İnformasiya təhlükəsizliyi büdcəsi	-	13, 150	14, 980	16, 650	17, 430
Ümumi İT büdcəsinin faizi	-	16.13	10.89	9.10	-

Çalışma

Əgər sizin ölkədə informasiya təhlükəsizliyi siyasəti vardırsa, yuxarıda göstərilən informasiya təhlükəsizliyi siyasətinin formalaşdırılmasının beş mərhələsi baxımından onun inkişaf etdirilməsini izləyin. Burada aşağıdakılar nəzərdə tutulur:

1. Siyasətin istiqaməti
2. İnformasiya təhlükəsizliyinə cavabdeh təşkilat
3. Siyasət çərçivəsi
4. İnformasiya təhlükəsizliyi siyasətinə dəstək göstərən qanunlar
5. İnformasiya təhlükəsizliyi üçün büdcə ayırması

Əgər sizin ölkədə hələ informasiya təhlükəsizliyi siyasəti yoxdursa, siyasətin formalaşdırılmasına doğru yuxarıda göstərilən beş aspektdən hər biri üçün mümkün məqamları açıqlayın. İstiqamət üçün aşağıdakı suallardan istifadə edin:

1. Sizin ölkədə informasiya siyasəti təhlükəsizliyinin istiqaməti nədən ibarət olmalıdır?

2. Hansı təşkilati quruluş olmalıdır? Sizin ölkədə informasiya təhlükəsizliyi siyasətinin işlənib hazırlanmasına və yerinə yetirilməsinə hansı təşkilatlar cəlb olunmalıdır?

3. Siyasi çərçivədə hansı səciyyəvi məsələlərə diqqət yetirilməlidir ?

4. İnformasiya siyasətinə dəstək olaraq hansı qanunlar qəbul edilməlidir / ləğv edilməlidir?

5. Hansı büdcə məsələləri nəzərə alınmalıdır? Büdcə haradan maliyyələşməlidir?

Eyni ölkədən olan təlim iştirakçıları bu çalışmanı bir yerdə edə bilərlər?

7.3 Siyasətin icrası / yerinə yetirilməsi

İnformasiya təhlükəsizliyi siyasətinin maneəsiz şəkildə həyata keçirilməsi üçün hökumət orqanları, özəl və beynəlxalq agentliklər arasında əməkdaşlıq tələb olunur. 27-ci Təsvirdə informasiya siyasətinin həyata keçirilməsində əməkdaşlığın vacib olduğu spesifik sahələr göstərilmişdir.

27-ci fiqur. İnformasiya təhlükəsizliyi siyasətinin həyata keçirilməsində əməkdaşlıq

İnformasiya və kommunikasiya infrastrukturuna nəzarət və onun mühafizəsi

İnformasiyadan effektiv istifadə (toplama, nəzarət və s.) üçün İT infrastrukturunun lazımi şəkildə idarə və mühafizə edilməsi tələb olunur. Güclü İT infrastrukturu olmadan yaxşı informasiya təhlükəsizliyi siyasəti faydasızdır.

İnformasiya və kommunikasiya infrastrukturunun effektiv idarə və mühafizə edilməsi şəbəkə, sistem və İT sahə menecerləri arasında əməkdaşlığın olmasını tələb edir. O, həmçinin dövlət və özəl təşkilatlar arasında əməkdaşlıqdan faydalanır. (bax, 19-ci Cədvəl).

Cədvəl 18. İnformasiyanın idarə və mühafizə edilməsində əməkdaşlıq (nümunə)

Sektor	. İnformasiya və kommunikasiya infrastrukturunun idarə və mühafizə edilməsinə dəstək
Hökumət sektoru	• İnformasiya və kommunikasiya şəbəkəsi ilə bağlı təşkilat: milli informasiya və kommunikasiya şəbəkəsinin quruluşu və təhlükəsizlik səviyyəsini müəyyənləşdirmə. • İKT laboratoriyası: dövlət standartlarını yayımlama və istifadə edilə bilən texnologiyanı qəbul etmə.
Özəl sektor	• İSP: milli informasiya və kommunikasiya şəbəkəsinin quruluşuna dair əməkdaşlıq etmə. • İKT laboratoriyası: texniki inkişaf xidmətlərini təmin etmə və stabil informasiya və kommunikasiya infrastrukturunun fəaliyyətində əməkdaşlıq etmə.
Beynəlxalq təşkilatlar	• Beynəlxalq informasiya və kommunikasiya və etibarlı yeni İT üçün beynəlxalq texnologiya standartarı təşkilatı ilə əməkdaşlıq etmə.

Təhlükələrin və hadisələrin qarşısının alınması və onların nəticələrinin aradan qaldırılması

Təhlükələrə və informasiya təhlükəsizliyinin pozulması hallarına qarşı effektiv mübarizə üçün milli informasiya təşkilatları, araşdırma orqanları və hüquqi təşkilatlar, habelə təhlükəsizliklə bağlı hadisələrin təftişini aparan və dəyən ziyanı hesablayan təşkilatlar arasında əməkdaşlıq tələb olunur. Texniki zəif məqamları təhlil edə və texniki baxımdan əks tədbirləri müəyyən edə bilən təşkilatla əməkdalıq da vacibdir.

Cədvəl 19. İnformasiya təhlükəsizliyi ilə bağlı hadisələrin nəticələrinin aradan qaldırılmasında əməkdaşlıq (nümunə)

Sektor	Dəstək
Hökumət təşkilatları	• Təhlükəsizliklə bağlı hadisələrin nəticələrinin aradan qaldırılması üzrə təşkilat: vəziyyətin təhlilini təmin etmək, hakerliklə bağlı hadisələrin nəticələrinin aradan qaldırılması və pozuntulara və hadisələri qarşı mübarizə üçün texnologiya. • Milli informasiya təşkilatı: informasiya təhlükəsizliyi ilə bağlı pozuntuları və hadisələri təhlil etmək. • Araşdırma orqanları: cinayətkarların həbs olunması və təqib edilməsində iştirak edən təşkilatla əməkdaşlıq • Təhlükəsizliklə bağlı qiymətləndirmə aparan təşkilat: istehsal əsasında informasiya şəbəkəsi və informasiya təhlükəsizliyinin etibarlılığını yoxlama. • İnformasiya təhlükəsizliyi üzrə maarifləndirmə təşkilatı: təhlükəsizliklə

	bağlı hadisələrin səbəblərini təhlil etmək və onların yenidən baş verməsinin qarşısını almaq üçün insanları maarifləndirmək.
Özəl qruplar	• Hadisələrin nəticələrinin aradan qaldırılması üzrə özəl təşkilat: nəticələrin aradan qaldırılmasını və texniki dəstəyi təmin etmə. • Özəl araşdırma orqanları: milli araşdırma orqanları ilə əməkdaşlıq
Beynəlxalq təşkilatlar	• Beynəlxalq hədələr və hadisələr olduqda, İnterpol CERT/CC-yə məlumat vermə və onlarla əməkdaşlıq etmə.

İnformasiya təhlükəsizliyi ilə bağlı hadisələrin qarşısının alınması

Maarifləndirmə və dəyişiklərə nəzarəti əhatə edir. Milli CSİRT əsas monitorinq təşkilatıdır. Mühüm məsələ informasiya siyasəti və real monitorinq məlumatlarını uyğunlaşdırmaqdır. Beləliklə də, informasiya siyasəti monitorinqinin əhatə dairəsini müzakirə etmək zəruridir. Bundab əlavə, hökumət və özəl sektor işçilərini, habelə ümumi əhalini informasiya təhlükəsizliyi siyasəti haqqında maarifləndirmək vacibdir. İnformasiyaya qarşı bəzi münasibətləri və təhlükəsizliklə bağlı informasiyaya təsir edə bilən davranışları dəyişmək zəruridir. İnformasiya təhlükəsizliyinə dair maarifləndirmə və dəyişiklərə nəzarət US SP 800-16-də (İnformasiya Texnologiyalarının Təhlükəsizliyi üzrə Təlimə dair Tələblər)

Sektor	Əlaqələndirmə
Özəl təşkilatlar	• Fərdi informasiya təhlükəsizliyi üzrə təşkilat: tələbləri qeydə almaq və şəxsi informasiya təhlükəsizliyi üzrə əməkdaşlıq assosiasiyalarını təşkil etmək. • Fərdi informasiya təhlükəsizliyi üzrə məsləhətlərin verilməsi.
Beynəlxalq təşkilatlar	• Fərdi informasiya təhlükəsizliyi ilə bağlı standartları tətbiq etmək üçün əməkdaşlıq etmək.

Beynəlxalq əməkdaşlıq

İnformasiya təhlükəsizliyinə bir ölkənin səyləri ilə nail olmaq olmaz, belə ki, informasiya təhlükəsizliyinin pozulması halları miqyas baxımından beynəlxalq xarakter almağa yönümlüdür. Beləliklə də, həm hökumət, həm də özəl sektorda informasiya təhlükəsizliyinin qorunmasında beynəlxalq əməkdaşlıq müəyyən təşkilatı forma almalıdır.

Özəl sektorda, informasiya təhlükəsizliyinin təşviqi və qorunması üçün müvafiq beynəlxalq təşkilat CERT/CC-dir. Hökumətlər arasında ENİSA (Aİ üçün) və BTİ ölkələr arasında informasiya təhlükəsizliyi üzrə əməkdaşlığı sürətləndirmək məqsədini daşıyır.

Hər bir ölkədə, beynəlxalq agentliklər və institutlarla həm hökumət, həm də özəl təşkilatlar vasitəsilə əməkdaşlığa kömək etmək rolunu daşıyan hökumət qurumu olmalıdır.

7.4 İnformasiya təhlükəsizlik siyasətinin icmalı və qiymətləndirilməsi

Informasiya təhlükəsizliyi siyasətinin formalaşdırılmasında yekun mərhələ siyasətin qiymətləndirilməsi və inkişaf etməyən sahələri tamamlamaqdır. İnformasiya təhlükəsizliyi siyasətinin səmərəli olduğu müəyyən edildikdən sonra siyasətin nəzərdən keçirilməsi vacibdir.

Milli informasiya təhlükəsizliyi siyasətinin səmərililiyini müəyyənləşdirmək üçün daxili siyasət qiymətləndirmə metodu tətbiq edilə bilər. Bu metodun aspektləri aşağıda müzakirə olunur.

Audit təşkilatlarından istifadə

Siyasətin qiymətləndirilməsini və dəyərləndirilməsini aparan təşkilatlar vardır. Belə təşkilat mütəmadi olaraq milli informasiya təhlükəsizliyinin auditini aparmalıdır. Bundan əlavə, bu təşkilat informasiya təhlükəsizliyi siyasətini formalaşdıran və onu həyata keçirən təşkilatdan ayrı olmalıdır.

İnformasiya təhlükəsizliyi siyasətinin nəzərdən keçirilməsi

Siyasət auditi zamanı adətən problemli sahələr müəyyən edilir. Bu problemli sahələri həll etmək üçün siyasətin nəzərdən keçirilməsi prosesi olmalıdır.

Mühitdə dəyişikliklər

Siyasəsi mühitdə dəyişikliklərə çevik reaksiya vermək vacibdir. Beynəlxalq təhlükələrdən (hücumlardan) və zəif məqamlardan irəli gələn dəyişikliklər, İT infrastukturunda dəyişikliklər, mühüm informasiyada meyllərin dəyişməsi və digər bu kimi vacib dəyişiklilər milli informasiya təhlükəsizliyi siyasətində dərhal öz əksini tapmalıdır.

Çalışma

Ölkənizdə milli informasiya təhlükəsizliyi siyasətinin həyata keçirilməsində əməkdaşlıq etməli olan dövlət qurumlarını və özəl təşkilatları müəyyən edin. Habelə onların öz fəaliyyətlərini əlaqələndirməli olduqları beynəlxalq təşkilatları da müəyyənləşdirin. Eyni ölkədən olan təlim iştirakçıları bu fəaliyyəti birlikdə edə bilərlər.

İstinadlar

(ISC)². (2020). Kibertəhlükəsizliyin sertifikatlaşdırılması: CISSP – Sertifikatlaşdırılmış İnformasiya Sistemlərinin Təhlükəsizliyi üzrə Mütəxəssis: (ISC)². Kibetəhlükəsizliyin sertifikatlaşdırılması | CISSP - Sertifikatlaşdırılmış İnformasiya Sistemlərinin Təhlükəsizliyi üzrə Mütəxəssis:| (ISC)². http://www.isc2.org/cissp.

Asiya və Sakit Okean Hövzəsi üzrə Kompyuterlə bağlı fövqəladə halların nəticələrinin qaradan qaldırılması qrupu. İlkin məlumat:
APCERT haqqında . http://www.apcert.org/about/background/index.html.

Karnegi Melon Universiteti. (18 yanvar 2017-ci il). CSIRT Tez-tez soruşulan suallar (FAQ). https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=485652.

Karnegi Melon Universiteti. Proqram Təminatı Mühəndislik İnstitutu. CERT Bölməsi. https://www.sei.cmu.edu/about/divisions/cert/index.cfm.

CERT. (2002). CSIRT Xidmətləri. Proqram Təminatı Mühəndislik İnstitutu. Götürüldüyü mənbə:https://resources.sei.cmu.edu/asset_files/WhitePaper/2002_019_001_53048.pdf

Avropa İcmaları Komissiyası, Mühüm İnfrastrukturun Mühafizəsi üzrə Avropa Proqramı (2006). Brüssel, Belçika.
https://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:EN:PDF.

Avropa İcmaları Komissiyası, Təhlükəsiz İnformasiya Cəmiyyəti – "Dialoq, tərəfdaşlıq və səlahiyyətləndirmə" (2006). Brüssel, Belçika.
https://eurlex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:52006DC0251&qid=1612332935197&from=EN.

Avropa İcmaları Komissiyası, Mühüm İnformasiya İnfrastrukturunun Mühafizəsi: "Avropanı iri-miqyaslı kiberhücumlardan və parçalanmalardan qoruma: hazırlığı, təhlükəsizliyi və davamlılığı artırma" (2009). Brüssel, Belçika.
https://eurlex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:52009DC0149&qid=1612333230526&from=EN.

Azad, ədalətli və təhlükəsiz kiberməkan öhdəliyi. NISC. (2018).
https://www.nisc.go.jp/eng/.

Ümumi meyarlar. (2009). (publication). İnformasiya Texnologiyalarının Təhlükəsizliyinin Qiymətləndirilməsi üçün Ümumi Meyarlar. Götürüldüyü mənbə
https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R3.pdf

Ümumi meyarlar.: Yeni CC Portalı. http://www.commoncriteriaportal.org/.

Avropa Şurasının Kibercinayətkarlığa qarşı tədbiri. Avropa Şurası. https://www.coe.int/en/web/portal/coe-action-against-cybercrime.
117

Avropa İttifaqı Şurası, Avropa üçün Rəqəmsal Gündəliyə dair Şuranın Nəticələri (2010). Brüssel, Belçika. https://data.consilium.europa.eu/doc/document/ST-10130-2010-INIT/en/pdf.

Avropa İttifaqı Şurası, Şuranın Şəbəkə və İnformasiya Təhlükəsizliyinə birgə Avropa yanaşması haqqında 18 dekabr 2009-cu il tarixli Qətnaməsi (2009). Belçika, Brüssel. https://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2009:321:0001:0004:EN:PDF.

Kross, D. (10 yanvar 2017-ci il). Dünyanın Ən Son və Ən Böyük Hakerlik Hadisələri. Veb Hostinq Media. https://webhostingmedia.net/recent-biggest-hacking-incidents.

Denning, D. E., Arquilla, J., & Ronfeldt, D. (2001). Fəallıq, Haktivizm və Kiberterrorizm: İnternet Xarici Siyasətə Təsir Etmək Üçün Vasitə Kimi. Şəbəkələrdə və Şəbəkə Mhüaribələrində. Terrorun, Cinayətin və Hərbçiliyin Gələcəyi (səh. 239–288). essay, RAND Corporation.

Avropa Parlamentinin və Şuranın 24 oktyabr 1995-ci il tarixli 95/46/EC saylı Direktivi fərdi məlumatların emalı ilə bağlı fərdlərin müdafiəsi və bu cür məlumatların sərbəst hərəkəti haqqında. (1995). Avropa Birliyinin rəsmi jurnalı, 38(281), 31–50. https://doi.org/https://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN

EGC Group. EGC group. Avropa Hökumət CERT-lərinin (EGC) qrupu. http://www.egcgroup.org/.

Egede, I. (31 iyul 2018-ci il). IOC olaraq Fayl Haşları üçün Təhdid Ovçuluğu. Infosec Resursları. https://resources.infosecinstitute.com/topic/threat-hunting-for-file-hashes-as-an-ioc.

ENISA. (2021, 15 yanvar). ENISA haqqında - Avropa İttifaqının Kibertəhlükəsizlik Agentliyi. ENISA. http://www.enisa.europa.eu/about-enisa.

EUR-Lex, Avropa Parlamentinin və Şuranın 27 aprel 2016-cı il tarixli 2016/679 saylı Qaydası (Aİ) fərdi məlumatların emalı və bu cür məlumatların sərbəst hərəkəti ilə bağlı fiziki şəxslərin müdafiəsi və 95/46/EC Direktivini ləğv edən (Ümumi Məlumatları Qorunma Qaydası) (2016). https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=CELEX%3A02016R0679-20160504.

Avropa Komissiyası, Avropa üçün Rəqəmsal Gündəm (2010). Brüssel, Belçika.https://eurlex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:52010DC0245&qid=1612333676302&from=EN.

Avropa Komissiyası, Avropa Parlamentinin və Şuranın İnformasiya sistemlərinə qarşı hücumlara dair və Şuranın Çərçivə Qərarını ləğv edən Direktivinə dair Təklif (2010). Brüssel, Belçika. https://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:52010PC0517&qid=1612334410667&from=EN.

Avropa Komissiyası, Avropa Şəbəkəsini və 118 İnformasiya Təhlükəsizliyi Agentliyini təsis edən 460/2004 saylı Qaydaya (AK) dəyişiklik edən Avropa Parlamenti və Şuranın Reqlamentinə dair Təklif (2010). Brüssel, Belçika.https://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:52010PC0520&qid=1612335155929&from=EN.

Avropa Komissiyası, Avropa Parlamenti və Avropa Şəbəkə və İnformasiya Təhlükəsizliyi Agentliyi (ENISA) ilə bağlı Şuranın Nizamnaməsi üçün Təklif (2010). Brüssel, Belçika.https://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:52010PC0521&qid=1612334562226&from=EN.

Avropa Şurası, Avropa Şurasının Nəticələri (25/26 Mart 2010) (2010). Brüssel, Belçika.https://www.consilium.europa.eu/uedocs/cms_Data/docs/pressdata/en/ec/113591.pdf.

İnsidentlərə Müdaxilə və Təhlükəsizlik Komandalarının Forumu, Inc. (2020). FIRST haqqında. FIRST.http://www.first.org/about.

Gillis, A. S. (2020, February 12). Müdaxilələrin qarşısının alınması sistemi (IPS) nədir? Axtarış Təhlükəsizliyi. https://searchsecurity.techtarget.com/definition/intrusion-prevention.

HM Hökuməti. (2016). (rep.). Milli Kibertəhlükəsizlik Strategiyası 2016-2021. Götürüldüyü mənbə:https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

Ontarionun Məlumat və Məxfilik Komissarı, Uğur üçün Planlaşdırma: Məxfiliyə Təsir Qiymətləndirmə Bələdçisi (2015). https://www.ipc.on.ca/wp-content/uploads/2015/05/planningfor-success-pia-guide.pdf.

Beynəlxalq Telekommunikasiya İttifaqı. İKT Təhlükəsizlik Standartları Yol Xəritəsi.http://www.itu.int/ITU-T/studygroups/com17/ict/index.html.

Beynəlxalq Telekommunikasiya İttifaqı. (2006). İnformasiya Cəmiyyəti üzrə Ümumdünya Sammiti: WSIS haqqında.http://www.itu.int/wsis/basic/about.html.

Beynəlxalq Telekommunikasiya İttifaqı. (2021). BTİ-nin Kibertəhlükəsizlik Fəaliyyətləri.http://www.itu.int/en/action/cybersecurity/Pages/default.aspx.

Beynəlxalq Telekommunikasiya İttifaqı. (2021). ITU-D Kibertəhlükəsizlik. BTİ-D.https://www.itu.int/en/ITU-D/Cybersecurity/Pages/default.aspx.

Beynəlxalq Telekommunikasiya İttifaqı. SG17 - Tədris Qrupu Strukturu (Təhsil Müddəti 2017-2020). BTİ. http://www.itu.int/net4/ITU-T/lists/sgstructure.aspx?Group=17&Period=16.

Beynəlxalq Telekommunikasiya İttifaqı. Tədris Qrupu 17 bir baxışda.http://www.itu.int/net/ITU-T/info/sg17.aspx.

İnternet İdarəçilik Forumu. (2021). http://www.intgovforum.org/.

ISMS Akkreditasiya Mərkəzi. İBS uyğunluğunun qiymətləndirilməsi sxeminin icmalı. ISMS-AC.https://isms.jp/english/isms/about.html.

ITU-D İKT Tətbiqləri və Kibertəhlükəsizlik Bölməsi. (2009). BTİ Milli Kibertəhlükəsizlik/CIIP Özünü Qiymətləndirmə Aləti.http://www.itu.int/ITUD/cyb/cybersecurity/projects/readiness.html.

Killcrece, G. (2004). Milli CSIRT-lərin yaradılması üçün addımlar. Proqram Mühəndisliyi İnstitutu. Götürüldüyü mənbə: https://resources.sei.cmu.edu/asset_files/WhitePaper/2004_019_001_53064.pdf

Killcrece, G., Kossakowski, K.-P., Ruefle, R., və Zajicek, M. (2003). Kompyuter Təhlükəsizliyi Hadisələrinə Müdaxilə Qrupları (CSIRTs) üçün təşkilati modellər. Proqram Mühəndisliyi İnstitutu. Götürüldüyü mənbə 10.1184/R1/6575921.v1

Korolov, M. (2019, June 27). Botnet nədir? Yoluxmuş IoT cihazlarının orduları hücum etdikdə. CSO Online.https://www.csoonline.com/article/3240364/what-is-a-botnet.html.

Kotadia, M. (2005, April 5). E-poçt qurdlarını IM-ə göndərir. ZDNet.https://www.zdnet.com/article/e-mail-worm-graduates-to-im/.

OECD, Şəxsi Məlumatların Məxfiliyin Mühafizəsi və Transsərhəd Axınlarına dair Təlimatlar 9–17 (2013). Paris, Fransa. https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

OECD, İnformasiya Sistemlərinin və Şəbəkələrinin Təhlükəsizliyi üzrə OECD Təlimatları: Təhlükəsizlik Mədəniyyətinə Doğru (2002). Paris, Fransa. https://www.oecd.org/digital/ieconomy/15582260.pdf.

OECD. (2006, May). İƏİT İnformasiya Təhlükəsizliyi və Məxfilik üzrə İşçi Qrupu WPISP.Paris. https://www.gpdp.it/documents/10160/10704/Working+Party+on+Information+Security+and+Privacy.pdf/586b9ff2-0ae8-4cb1-873a-2025fb6f5a15?version=1.1

İqtisadi Əməkdaşlıq və İnkişaf Təşkilatı. Məxfilik Onlayn: Siyasət və Təcrübə üzrə OECD Rəhbərliyi. OECD.https://www.oecd.org/digital/ieconomy/privacyonlineoecdguidanceonpolicyandpractice.htm.

Daimi Maraqlı Tərəflər Qrupu. (P. Dorey & S. Perry, Red.), ENİSA üçün PSG baxışı (2006). https://www.enisa.europa. eu/about-enisa/structure-organization/psg/files/psgvision.

Ramasubramanian, S., & Shaw, R. (2007, sentyabr). ITU Botnet Təsirinin Azaldılması Layihəsi: Fon və yanaşma. Beynəlxalq Telekommunikasiya İttifaqı. http://www.itu.int/ITUD/cyb/cybersecurity/docs/itu-botnet-mitigation-toolkit.pdf

Ramasubramanian, S., Ansari, S., & Purcell, F. (2005). İdarəetmə İnternet İstifadəsi: Spam, Kibercinayətkarlıq və e-ticarət. D. Butt (Red.), İnternet idarəçiliyi: Asiya-Sakit Okean
120
Perspektivlər (səh. 89–104). essay, APDIP. https://www.unapcict.org/sites/default/files/2019-01/Internet%20Governance%20-%20Asia-Pacific%20perspectives.pdf.

Rosencrance, L. (2020, 27 avqust). Qabaqcıl davamlı təhlükə nədir? Axtarış Təhlükəsizliyi.https://searchsecurity.techtarget.com/definition/advanced-persistent-threat-APT.

SecureAuth. (2017, July 14). secureauth_ciam_infographic_170714.pdf. Irvine.

Shimeall, T. J. və Williams, P. (2002). İnformasiya təhlükəsizliyi trendinin təhlili modelləri. Vətən Müdafiəsi və Hüquq Mühafizəsi üçün Sensorlar və Komanda, Nəzarət, Rabitə və Kəşfiyyat (C3I) Texnologiyaları. https://doi.org/10.1117/12.479291

Sinclair İcma Kolleci. İnformasiya Təhlükəsizliyi Təşkilatı – Rol və Məsuliyyətlər. İnformasiya Təhlükəsizliyi Siyasəti.https://it.sinclair.edu/index.cfm/services/student-and-guestsservices/policies-and-security-information/information-security-policy/.

Stack, B. (2017, 6 dekabr). Qaranlıq İnternetdə Şəxsi Məlumatlarınızın Nə qədər Satıldığı Budur. Experian. https://www.experian.com/blogs/ask-experian/heres-howmuch-your-personal-information-is-selling-for-on-the-dark-web/.

Tan, D. R. (1999). İnformasiya əsrində şəxsi məxfilik: İnternet məlumatlarının müqayisəsi

Birləşmiş Ştatlarda və Avropa İttifaqında Mühafizə Qaydaları. Los-Ancelesdən Loyola Beynəlxalq və Müqayisəli Hüquq İcmalı, 21(4). https://digitalcommons.lmu.edu/ilr/vol21/iss4/5.

Telekommunikasiya və İnformasiya. Asiya-Sakit Okean İqtisadi Əməkdaşlıq Təşkilatı. (2020, aprel).https://www.apec.org/Groups/SOM-Steering-Committee-on-Economic-and-TechnicalCooperation/Working-Groups/Telecommunications-and-Information.

ABŞ Hökumətinin Çap Ofisi. (2014). Kibertəhlükəsizliyi Təkmilləşdirmək üçün Davamlı, Könüllü Dövlət Özəl Tərəfdaşlığını Təmin etmək və Kibertəhlükəsizliyi Gücləndirmək üçün Tədqiqat və İnkişaf, İşçi Qüvvənin İnkişafı və Təhsili və Əhalini
Maarifləndirmə və Hazırlıq və Digər Məqsədlər üçün Akt

BMT Baş Assambleyası, Kompyuterləşdirilmiş Şəxsi Məlumatların Tənzimlənməsi üzrə Təlimat (1990). https://www.refworld.org/docid/3ddcafaac.html.
Baş Assambleyanın 14 dekabr 1990-cı il tarixli 45/95 saylı qərarı ilə qəbul edilmişdir. Kompüterləşdirilmiş şəxsi məlumat faylları ilə bağlı qaydaların həyata keçirilməsi üçün prosedurları ehtiva edir.

Ağ Ev. (2003). (rep.). Kiberməkanın Təhlükəsizliyi üzrə Milli Strategiya. Götürüldüyü mənbə https://www.hsdl.org/?view&did=1040

Ağ Ev. (2018). (rep.). Amerika Birləşmiş Ştatlarının Milli Kiber Strategiyası. Götürüldüyü mənbə https://www.defense.gov/Explore/News/Article/Article/1641969/whitehouse-releases-first-national-cyber-strategy-in-15-years/
121

Wikimedia Fondu. (2020, 31 dekabr). Sıfır gün (hesablama). Vikipediya.https://en.wikipedia.org/wiki/Zero-day_(computing).

Wikimedia Fondu. (2021, 1 fevral). Antivirus proqramı. Vikipediya.http://en.wikipedia.org/wiki/Antivirus_software.

WSIS, WSIS: Fəaliyyət Planı (2003). Beynəlxalq Telekommunikasiya İttifaqı.https://www.itu.int/net/wsis/docs/geneva/official/poa.html.

APCICT/ESCAP

Asiya və Sakit Okean Hövzəsi ölkələri üçün İnkişaf naminə İnformasiya və Kommunikasiya Texnologiyaları üzrə Təlim Mərkəzi (APCİCT) Asiya və Sakit Okean Hövzəsi üzrə İqtisadi və Sosial Komissiyasının (ESCAP) regional institutudur.
APCICT-in məqsədi ESCAP-a üzv ölkələrdə insan və institusional potensialı inkişaf etdirməklə onların sosial-iqtisadi inkişaflarında İKT-dən istifadə səylərini gücləndirməkdir. səylərini gücləndirməkdir. APCICT-in işi üç sütun üzərində cəmlənib: təlim, bilik mübadiləsi və çoxtərəfli dialoq və tərəfdaşlıq. Onlar birlikdə İKT insan potensialının yaradılmasına inteqrə olunmuş yanaşmanı formalaşdırırlar.

APCICT Koreya Respublikasının İnçxon şəhərində yerləşir.

http://www.unapcict.org

ESCAP

Asiya və Sakit Okean Hövzəsi üzrə İqtisadi və Sosial Komissiya (ESCAP) Asiya-Sakit okean regionunda ən əhatəli hökumətlərarası platformadır. Komissiya dayanıqlı inkişafla bağlı problemlərin həll yollarının axtarılmasında 53 üzv dövlət və 9 assosiativ üzv arasında əməkdaşlığı təşviq edir.ESCAP Birləşmiş Millətlər Təşkilatının beş regional komissiyasından biridir.
ESCAP katibliyi, milli inkişaf məqsədlərinə, regional sazişlərə və 2030-cu il Dayanıqlı İnkişaf Gündəliyinə dəstək olaraq, fəaliyyət yönümlü biliklər yaratmaqla və texniki yardım və potensialın inkişaf etdirilməsi üzrə xidmətlər göstərməklə regionda inklüziv, davamlı və davamlı inkişafı dəstəkləyir.

http://www.unescap.org