Azərbaycan Milli Elmlər Akademiyasi
İNFORMASİYA TEXNOLOGİYALARI
İNSTİTUTU

Rasim Əliquliyev

Yadigar İmamverdiyev

İNFORMASİYA TƏHLÜKƏSİZLİYİ İNSİDENTLƏRİ

Bakı - 2012

Əliquliyev R.M., İmamverdiyev Y.N. **İnformasiya təhlükəsizliyi insidentləri** Bakı: "İnformasiya Texnologiyaları" nəşriyyatı, 2012, 219 səh.

Kitabda informasiya təhlükəsizliyi insidentlərini cavablandırma komandalarının (Computer Emergency Responce Team, CERT) təşkilinə və fəaliyyətinə müasir yanaşmalar öz əksini tapmışdır. İnformasiya təhlükəsizliyi insidentlərinin növləri, insidentləri cavablandırma servisləri və insidentləri cavablandırma prosedurları analiz edilmişdir. CERT komandalarının növləri, onların təşkilati modelləri və strukturları, komanda üzvlərinə yönəldilən peşə və şəxsi keyfiyyət tələbləri, komanda heyətinin təlimi məsələləri ətraflı nəzərdən keçirilir. CERT komandalarının tarixi, bu sahədə fəaliyyət göstərən beynəlxalq qurumların məqsədləri, funksiyaları və onlara üzvlük prosedurları haqqında ətraflı məlumat verilir.

İnformasiya təhlükəsizliyi üzrə mütəxəssislər və bu sahədə ixtisaslaşan tələbələr, aspirantlar, elmi tədqiqat aparan şəxslər üçün nəzərdə tutulmuşdur.

Kitab AMEA İnformasiya Texnologiyaları İnstitutu Elmi şurasının qərarı ilə çapa tövsiyə olunmuşdur.

Elmi redaktor: tex.f.d. Rəşid Ələkbərov

ISBN: 978- 9952-434-36-1

MÜNDƏRİCAT

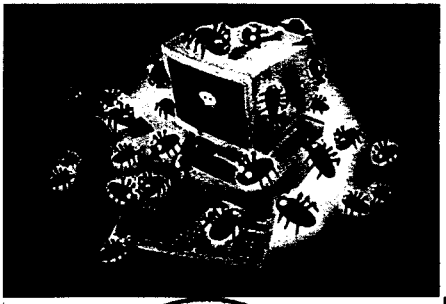
Giriş

Qlobal informasiya cəmiyyətində informasiya iqtisadiyyatın, elmin, təhsilin, siyasi və ictimai fəaliyyətin digər sahələrinin aparıcı amilinə çevrilir. Müxtəlif informasiya və telekommunikasiya sistemləri cəmiyyətin və dövlətin mühüm amili kimi çıxış edir. Lakin informasiya cəmiyyəti informasiyanın cinayətkar qruplar tərəfindən antisosial məqsədlərlə tətbiqi imkanlarını da genişləndirir.

Onların qarşısının alınması həm Azərbaycan, həm də dünyanın bir çox digər ölkəsi üçün aktualdır. Onlara qarşı mübarizə vasitələrindən biri də Kompyuter Qəzalarını Cavablandırma Qrupu (Computer Emergency Response Team, CERT) kimi komandaların təşkilidir. Hazırda müxtəlif ölkələrdə çox sayda CERT komandaları fəaliyyət göstərir.

Azərbaycan Respublikası ərazisində də transmilli informasiya təhlükəsizliyi insidentlərinə qısa müddətdə cavab verilməsi və kompyuter cinayətlərinin müxtəlif növlərinə kollektiv əks-təsir üçün CERT komandalarının yaradılması üzrə işlər gedir. Xeyli müddətdir ki, AMEA İnformasiya Texnologiyaları İnstitutunun nəzdində CERT komandası (AZ-CERT) fəaliyyət göstərir. AZ-CERT-in əsas məqsədi AzScinceNet elm kompyuter şəbəkəsində informasiya təhlükəsizliyinin təmin olunması, müxtəlif təhlükəsizlik insidentlərinin qarşısının alınmasıdır.

AZ-CERT-in təşkili və fəaliyyəti prosesində bir sıra ölkələrdə bu sahədə toplanmış təcrübə öyrənilmiş, elmi-metodiki ədəbiyyat analiz edilmiş, bir sıra beynəlxalq təşkilatlarla birgə işlər aparılmışdır. Təqdim edilən bu vəsait AZ-CERT-in təcrübəsinin ölkəmizdə yaradılacaq digər CERT-lərə ötürülməsi məqsədilə tərtib edilmişdir.



FƏSİL 1

CERT KOMANDALARININ TƏŞƏKKÜLÜ

CERT KOMANDALARININ TƏŞƏKKÜLÜ

- **Morris soxulcanı**
- **CERT/CC-nin yaradılması**
- **FIRST forumu**
- **CERT yoxsa CSIRT?**
- **Avropada CSIRT təşəbbüsləri**
- **Asiya-Sakit Okean regionunda CERT-lər**
- **İnsidentləri cavablandırma standartları**

FƏSİL 1 CERT KOMANDALARININ TƏŞƏKKÜLÜ

1.1. Morris soxulcanı

Qlobal informasiya infrastrukturunda kompyuter viruslarının ilk böyük epidemiyası 1988-ci ilin 2 noyabrında baş vermişdi. Sonralar KİV-də müəllifinin şərəfinə «Morris soxulcanı», hakerlər tərəfindən isə «Böyük Soxulcan» adlandırılan bu kompyuter soxulcanı ildırım sürəti ilə yayılaraq o zamankı İnternetdə olan qovşaqların 10%-ni sıradan çıxarmış, İnterneti əlaqəsiz ayrı-ayrı hissələrə parçalamışdı. Yoluxmuş kompyuterlərin siyahısına MIT (Massaçusets Texnologiya İnstitutu), Berkli, Stenford, Karnegi-Mellon, Minnesota, Şimali Karolina, Pittsburq, Merilend, Pensilvaniya, Kolorado, Perdyu universitetlərinin, RAND korporasiyasının, Ballistik Tədqiqatlar Laboratoriyasının və bir çox başqa təşkilatların kompyuterləri daxil idi.

Robert Morris (Kiçik) Kornel Universiteti informatika kafedrasının aspirantı idi. "Morris soxulcanı" bu tələbənin tədqiqat layihəsinin bir hissəsi idi. Tədqiqatın məqsədi şəbəkədə müstəqil yayılmaq qabiliyyəti olan proqramın yaradılması idi. Şəbəkədə öz-özünə yayılan proqramların ilk təsviri hələ 6 il əvvələ təsadüf edirdi. 1982-ci ildə Palo-Altodakı məşhur Xerox laboratoriyasının əməkdaşları Con Şok və Con Happ özü yayıla bilən proqramın elmi təsvirini vermişdilər, bu proqram eksperimentlər zamanı laboratoriyanın lokal şəbəkəsində 100 kompyuteri "yıxmışdı". Lakin bu heç bir ziyan vurmayan bir elmi tədqiqat işi idi.

Morris güman etmirdi ki, soxulcan hər hansı ziyan vura bilər – o, ziyankar əməllər üçün proqramlaşdırılmamışdı. Ola bilsin ki, Morris öz universitetinə diqqəti çəkməmək üçün əjdahasını MIT

kompyuterindən (prep.ai.mit.edu – açıq girişli kompyuterdən) işə salmışdı. Təəssüf ki, soxulcanın işində səhv buraxılmışdı. Kompyuteri yoluxdurduqda o, burada öz kopyasının olmasını yoxlamırdı və eyni bir kompyuter dəfələrlə yoluxurdu. Bunun nəticəsində minlərlə server "yıxıldı" və Morris soxulcanı İnternetdə yayılan ilk soxulcan oldu.

Morris soxulcanı ilə SUN və BSD Unix əməliyyat sistemləri işləyən təxminən 6000 VAX kompyuterə yoluxmuşdu. Administratorların çoxu öz istifadəçilərini şəbəkədən ayırmağa məcbur oldular ki, yoluxmanın qarşısını bir qədər alsınlar.

Morris soxulcanı BSD 4-cü versiya UNIX əməliyyat sistemi ilə işləyən yalnız Sun3 və VAX kompyuterlərini yoluxdurdu. İş prosesində soxulcan /usr/tmp kataloqunda qeyri-adi fayllar və bir sıra utilitlərin, məsələn, Sendmail utilitinin loq-fayllarında qəribə məlumatlar yerləşdirirdi.

Soxulcan iki hissədən: yükləyici (C dilində 99 sətir) və nüvədən ibarət idi. Nüvə iki binar moduldan – BSD üçün kompilyasiya edilmiş və Sun arxitekturası üçün kompilyasiya edilmiş koddan ibarət idi. Bütün daxili prosedurların müəyyən məna daşıyan adları var idi (məsələn, "doit" və ya "cracksome"), bu binar modulların dizassemblerlənməsi işini xeyli asanlaşdırmışdı.

Yoluxmuş hər bir kompyuter onunla əlaqəsi olan bütün kompyuterləri də yoluxdurmağa çalışırdı. Soxulcan yoluxmuş kompyuterə BSD Unix və Sun-3 olan kompyuterlərin qoşulduğunu aşkarladıqda öz surətini ora köçürürdü və işə salırdı. Soxulcan mühafizəsiz şəbəkədə öz surətlərini yayaraq, əsası hələ Con Fon Neyman tərəfindən qoyulmuş özüçoxalan mexanizmlər nəzəriyyəsinə tam uyğun olaraq çığ kimi çoxalırdı.

İlk əvvəl heç kim heç nə anlamırdı, lakin bir neçə saatdan sonra ən qoçaq administratorlar kim necə gəldi hərəkət etməyə başladılar, kimisi öz istifadəçilərini şəbəkədən ayıraraq kompyuterləri söndürüb-yükləyirdilər ki, əlavə yük götürülsün (bu tamamilə mənasız idi, çünki kompyuter yenidən yüklədikdə soxulcan özünün daha bir neçə surətini yaradırdı ki, bu da sistemin yükünü yalnız artırırdı), kimisi çaxnaşmaya düşüb "Bizə

hücum edirlər" məlumatını göndəriş siyahısı ilə göndərməyə çalışırdı (bu da mənasız idi, çünki soxulcanın hərəkətləri nəticəsində siyahılar artıq bir neçə saat idi ki, işləmirdilər), kimisi isə soxulcanın ani yayılmasının səbəblərini axtarmağa girişirdi.

Unix-də həmin vaxtlar proqramların məsafədən yerinə yetirilməsi üçün r-proqramlar istifadə edilirdi. Onların ən zəif yerləri "inam" ideyası idi – "etibarlı qovşaqlar" siyahısında olan kompyuterlərin istifadəçiləri hər hansı əlavə yoxlama olmadan öz proqramlarını "etibar edən" kompyuterdə işə sala bilərlər. Bundan başqa, etibar münasibəti çox vaxt qarşılıqlı olurdu. Soxulcan digər kompyuterlərə hücum etmək üçün rsh proqramından – cari istifadəçinin adı və parolu ilə və ya "etibar edildikdə" autentifikasiya olmadan istifadə etməyə çalışırdı.

Soxulcan yoluxmuş kompyuterin qonşularına sendmail və fingerd utilitlərində olan boşluqdan və rsh-da olan "inamdan" istifadə edərək keçirdi. Bu zaman hücum edilən kompyuterə yükləyicilər yerləşdirilirdi, yükləyicinin kompilyasiyası, yerinə yetirilməsi və bütün müvəqqəti faylların silinməsi komandası verilirdi. Sonra yükləyici hər üç faylı cəlb edirdi və əvvəlcə bir, sonra digər hissəni işə salmağa çalışırdı. Əgər iki hissədən heç biri işə düşmürdüsə, yükləyici həm onları, həm də özünü silərək işini dayandırırdı.

Soxulcan işə düşdükdə hər vəhclə maskalanmağa çalışırdı, özünün yerinə yetirilən faylını pozurdu, onları yaddaşa oxuyurdu, diskdən də silirdi; mümkün olduqca özü haqqındakı informasiyanı dəyişdirirdi.

Daha sonra yoluxmuş kompyuterin şəbəkə interfeysləri və qonşu kompyuterlər haqqında informasiya toplanırdı və qonşuların bir hissəsinə hücum edilirdi. Yoluxdurmaq mümkün olanları "yoluxmuş" kimi, yoluxdurula bilməyənləri "immunitent" kimi nişanlayırdı. Kodun bu hissəsində – kompyuterlərin təkrar yoluxmasının qarşısını alan kod hissəsində mütəxəssislərə görə səhvlər buraxılıb.

Soxulcanın yaşama qabiliyyəti üçün bu səhvlər əsas rol oynayırdı: kompyuterlərin bir çoxu təkrar yoluxurdu, sistemin və

şəbəkənin yükü artırdı və olduqca hissedilən olurdu, çox zaman xidmətdən imtinaya səbəb olurdu, bunun nəticəsində soxulcan daha tez aşkarlandı və zərərsizləşdirildi, təkrar yoluxmalar olmasaydı, soxulcanın həyatı daha uzun olardı. Bir neçə dəfə yoluxmuş kompyuterlər soxulcanı daha tez yayırdılar, bu, yəqin ki, soxulcanın kompyuterlərdəki surətlərinin sayı ilə mütənasib idi, xidmətdən imtina isə çaxnaşmaya və bəzi əsas qovşaqların sıradan çıxmasına, nəticədə şəbəkənin altşəbəkələrə parçalanmasına səbəb olurdu.

Soxulcanda parolların tapılması çox sadə və eyni zamanda səmərəli üsulla aparılmışdı: Login mövzusunda 4 variasiya və təxminən 200-400 sözdən ibarət siyahı istifadə edilirdi. Bəzi məlumatlara görə, ayrı-ayrı kompyuterlərdə parolların yarıdan çoxu bu üsulla tapılmışdı.

Morris proqramın kodunu yaxşı gizlətmişdi, çətin ki, kimsə onun bu işlə əlaqəsi olmasını sübut edə bilərdi. Lakin onun atası oğluna hər şeyi etiraf etməyi məsləhət gördü. Böyük Morris bu zaman Kompyuter Təhlükəsizliyi Mərkəzində (National Computer Security Center) baş elmi işçi işləyirdi, uzun müddət Bell Labaratories-də çalışmışdı, Darvin oyununun – özüçoxalan proqramlar sahəsində ilk eksperimentlərdən birinin müəlliflərindən idi. Sonralar UNIX-in yaradılmasında, xüsusən də parol sisteminin işlənməsində iştirak etmişdi.

Məhkəmədə Robert Morrisi 5 ilədək azadlıqdan məhrumetmə və 250 min dollar cərimə gözləyirdi, lakin məhkəmə yüngülləşdirici şərtləri nəzərə alaraq onu 3 il azadlıqdan şərti məhrumetmə, 10 min dollar cərimə və 400 saat ictimai işə məhkum etdi.

Morris soxulcanının vurduğu ziyan təxminən 100 milyon dollar qiymətləndirilmişdi. Kompyuter cəmiyyəti üçün bu böyük şok idi. Kompyuter təhlükəsizliyinin fundamental əsaslarına yenidən baxıldı.

Bəzi məlumatlara görə, Morris soxulcanı ABŞ-da prezident seçkiləri haqqında materialları qəzetlərin birinci səhifələrindən sıxışdırmış tarixdə yeganə kompyuter proqramıdır, təşkilatlar bir neçə həftəyə və hətta aya İnternet bağlantılarını kəsmişdilər.

Təhlükənin real miqyaslarını təsəvvür etməyən administratorlar özlərini sığortalayırdılar.

Morris soxulcanı ilə mübarizənin xronologiyası belədir. 2 noyabr axşama yaxın Berklidə başa düşdülər ki, hücum rsh və sendmail-dən edilir. Ehtiyat tədbirləri kimi şəbəkə servislərini bağlamağa başladılar.

Bir neçə saatdan sonra məlum oldu ki, sendmail üçün yamaqlar kömək etmir, kompyuterlər hansısa digər yolla yoluxurlar. Soxulcanın hərəkətləri sayəsində MILNET və ARPANET bir-birindən ayrıldı.

Daha bir neçə saat keçdikdən sonra müxtəlif laboratoriyalarda bir-birindən asılı olmadan fingerd demonunun boşluqları aşkarlandı və yamaq hazırlandı.

3 noyabr səhəri Berkli Kaliforniya Universitetinin və Massaçusets Texnologiya İnstitutunun əməkdaşları virusun kopyasını əldə etdilər və onun analizinə başladılar. 3 noyabr axşam saat 5-də Berkli Universitetinin əməkdaşları yayılmanın qarşısını almaq üçün bir sıra tədbirlər işlədilər. Müvafiq məlumat şəbəkəyə ötürülsə də, onun yayılması soxulcanın şəbəkədə yaratdığı yüklə və şəbəkənin bəzi hissələrinin "karantin" üçün açılması səbəbindən gecikdi. Axşam saat 9-a yaxın Pedyu Universitetində daha sadə və effektiv mübarizə metodu tapıldı və tez, bütün maraqlı istifadəçilərə yayımlandı. Günün sonunda Morris soxulcanının işi bitmişdi.

4 noyabr cümə günü səhər MIT-də mətbuat konfransı keçirildi, burada "virus ovu"nun aparıcı iştirakçıları çıxış etdilər. 8 noyabr çərşənbə axşamı Baltimorda Morris virusu üzrə konfrans keçirildi, burada hadisələrin xronologiyası, baş vurulmuş tədbirlər və virusun fəaliyyəti ətraflı müzakirə edildi. Bundan başqa, insidentin dərsləri və yeni hücumlara hazırlıq məsələləri də müzakirə edildi.

Artıq 5 noyabr axşama yaxın yoluxmuş qovşaqların əsas hissəsi müalicə edilmiş, yamaqlar qoyulmuşdu.

Epidemiya şəbəkələrə qeyd-şərtsiz etibar etməyin necə təhlükəli olmasını göstərdi. Nəticədə proqram kodlarının təhlükəsizliyi, şəbəkə qovşaqlarına nəzarət edilməsi, parolların

seçilməsi üzrə ciddi kompyuter təhlükəsizliyi normaları qəbul edildi.

"Böyük Soxulcan"ın törətdiyi fövqəladə vəziyyətə qarşı ən ağıllı tədbir isə CERT-in yaradılması oldu.

1.2. CERT/CC-nin yaradılması

«Morris soxulcanı insidenti»nin cavablandırılması zamanı ən problemli hissə kommunikasiya mexanizminin olmaması idi. Qovşaqların çoxunu şəbəkədən ayırmışdılar ki, sistemləri soxulcandan müalicə etsinlər, İnternet poçt xidmətlərinin çoxu serverlərin yoluxması səbəbindən fəaliyyət göstərmirdi, buna görə də İnternet cəmiyyətinə öz sistemlərini necə qorumaq və yoluxmuş sistemləri necə müalicə etmək barəsində tez xəbər verməyin yaşama qabiliyyəti olan bir yolu yox idi. Bununla yanaşı, əsas problem onda idi ki, belə kompyuter insidentlərini cavablandırma zamanı koordinasiyanın formal metodu da yox idi.

Morris soxulcanı cəmiyyətə həyəcan siqnalı kimi təsir etdi, insidentdən sonra insanlar başa düşdülər ki, oxşar insidentlərlə gələcəkdə uğurla mübarizə aparmaq üçün sistem administratorları və IT-menecerlər arasında birgə fəaliyyətin kooperasiyasına və koordinasiyasına böyük ehtiyac var. Baxılan situasiyada boş dayanma müddətinin əsas kritik faktor olduğunu nəzərə alaraq, kompyuter təhlükəsizliyi insidentlərinin emalı prosesinə daha mütəşəkkil və strukturlaşdırılmış yanaşmanın olması zəruri idi.

Bu problemi həll etmək üçün 17 noyabr 1988-ci ildə Perspektiv Müdafiə Tədqiqat Layihələri Agentliyi (ing. Defense Advanced Research Projects Agency, DARPA) İnternet təhlükəsizliyi insidentləri üçün koordinasiya mərkəzi yaratmaq niyyətini elan etdi. DARPA Karneqi-Mellon Universitetinin (Pittsburq şəhəri, Pensilvaniya ştatı) Proqram təminatı Mühəndisliyi İnstitutunu (ing. Software Engineering Institute, SEI) bu mərkəzin ev sahibi kimi seçdi. DARPA SEI-nin öhdəsinə gələcək insidentlərin qarşısını almaq üçün təhlükəsizlik

insidentləri zamanı ekspertlər arasında kommunikasiyanı effektiv koordinasiya etmək üçün lazımi imkanların yaradılmasını qoydu. Yeni mərkəzə İnternet istifadəçilərinin təhlükəsizlik məsələləri barədə biliklərinin artırılması da tapşırıldı. İlkin olaraq pilot tədqiqat layihəsi maliyyələşdirildi. Mərkəzə Computer Emergency Response Team (CERT) adı verildi. Sonralar CERT Karnegi Mellon Universiteti üçün xidmət nişanına çevrildi və adı CERT/CC-yə (CERT/Coordinating Center, Kompyuter təhlükəsizliyi insidentlərini operativ cavablandırma qrupu/Əlaqələndirmə mərkəzi) dəyişdirildi. CERT/CC öz qapılarını 1988-ci ilin dekabrında açdı və ilk gündən telefon zənglərini qəbul etməyə başladı. İlkin heyət SEI daxilində başqa proqramların ştatından təşkil edilmişdi, onlar CERT/CC qaynar xəttinə cavab verirdilər və zəngləri insident bildirişlərinin emalı üçün təyin edilmiş şəxslərə ötürürdü. İlkin ştatda dörd texniki işçi və bir menecer var idi.

CERT/CC əlaqələndirmə mərkəzinin vəzifələri aşağıdakı məsələlərin həll edilməsi idi:

- hücumlar haqqında məlumatlara cavab vermək üçün daimi və etibarlı rabitəni təmin etmək;
- informasiya təhlükəsizliyi sahəsində işləyən ekspertlər arasında qarşılıqlı əlaqəni təmin etmək;
- kompyuter sistemlərində olan boşluqların identifikasiyası və korreksiyası üçün mərkəz rolu oynamaq;
- müvafiq sistemlərin təhlükəsizliyi səviyyəsinin yüksəldilməsi üçün elmi tədqiqatlar aparmaq.

CERT/CC laboratoriyalarında (tədqiqat) proqram və aparat təminatının aşkarlanmış boşluqları haqqında istifadəçiləri məlumatlandırmaq üçün veb-serverdə (http://www.cert.org), ftp-serverdə (ftp://ftp.cert.org/pub/cert_advisories), Usenet telekonfransında (comp.security.announce) və göndəriş siyahılarında boşluqların təsviri və onların aradan qaldırılması üsulları – **Advisories** nəşr olunur. Təhlükəsizlik problemləri və onların həlli haqqında istehsalçı firmalardan alınmış məlumatlar

xüsusi informasiya bülletenlərində (Vendor-Initiated Bulletins) nəşr olunur, onlar da Advisories kimi həmin kanallarla yayılır.

CERT/CC aşağıdakı sahələrdə iş və ya tədqiqatlar aparır:

Proqram təminatının qiymətləndirilməsi – mərkəzin əsas məqsədi İnternet təhlükəsizliyinin vəziyyətini analiz etməkdir, açıq mənbələri izləyir və boşluqlar haqqında məlumatlar alır, informasiyanı texnologiya istehsalçıları ilə bölüşdürür və problemin həllini tapmaq üçün onlarla əməkdaşlıq edir.

Təhlükəsiz sistemlər – CERT "yaşaya bilən" sistemlər sahəsində tədqiqatlar aparır və sistemlərin layihələrini yaxşılaşdırmaq yolları tapır; İnternetə yönəlmiş cari, potensial və mürəkkəb təhdidləri qiymətləndirməyə və proqnozlaşdırmağa imkan verən strategiyalar hazırlayır.

Təşkilati təhlükəsizlik – mərkəzin yaratdığı OCTAVE risk qiymətləndirmə metodu təşkilatlara kritik informasiya aktivlərini identifikasiya etməyə, bu aktivlərə olan riskləri qiymətləndirməyə kömək edir. Təşkilatlar bu nəticələrdən öz strategiyalarını təkmilləşdirmək, öz informasiya sistemlərinin informasiya təhlükəsizliyinin səviyyəsini təmin etmək və yüksəltmək üçün istifadə edə bilərlər.

Əlaqələndirilmiş cavab – veb-saytlar vasitəsilə bütün dünyada informasiya təhlükəsizliyi problemlərinin həllində dəstək almağı müntəzəm əlaqələndirir və yeni CSIRT komandalarının yaradılmasına kömək edir. Mərkəz şəbəkə məhkəmə ekspertizası sahəsində də alətlər və təlimlər təklif edir ki, sistem administratorları zəruri bacarıq və resurslarla təmin olunsunlar və informasiya təhlükəsizliyi insidentlərini effektiv cavablandıra bilsinlər. CERT/CC ABŞ üçün milli CSIRT olan US-CERT-in və Qatar üçün milli CSIRT olan Q-CERT-in yaradılması və davamlı inkişafında fəallıq göstərir.

Təhsil və təlim – CERT/CC CSIRT-lərin texniki heyəti və menecerləri, sistem administratorları və şəbəkə təhlükəsizliyi ilə maraqlanan digər texniki heyət üçün təlim kursları təqdim edir. Kursların bəziləri insidentlərin emalı üzrə sertifikatlaşdırma proqramının tərkibinə daxildir. CERT/CC mərkəzi Karnegi Mellon Universitetində informasiya sistemlərinin menecmenti

magistr proqramının informasiya təhlükəsizliyi menecmenti ixtisasını və yaşama qabiliyyəti və informasiya təhlükəsizliyini tədris edir.

1.3. CIAC komandası

Bir CERT-in müxtəlif istifadəçilərin ehtiyaclarının və iş yükünün öhdəsindən gələ bilməyəcəyi aydın idi. Digər agentliklərə də öz istifadəçiləri üçün CERT komandaları yaratmaları tövsiyə olundu. Sonrakı il digər təşkilatlar – ABŞ Energetika Nazirliyi, Milli Aeronavtika və Kosmik Agentliyi (ing. National Aeronautics and Space Administration NASA), NIST (National Institute of Standards and Technology) və ABŞ Müdafiə Nazirliyi də öz komandalarını yaratdılar.

Computer Incident Advicory Capability (CIAC) mərkəzi 1989-cu ildə ABŞ Energetika Nazirliyi yanında yaradılmışdı. CIAC mərkəzinin əsas məqsədi Energetika Nazirliyi qulluqçularının və podratçılarının kompyuter təhlükəsizliyinin təmin edilməsi idi. CIAC aşağıdakılar da daxil olmaqla bir çox funksiya yerinə yetirirdi:

- insidentlər haqqında məlumatların emalı;
- Energetika Nazirliyi və onun podratçılarının kompyuter təhlükəsizliyinin təmin edilməsi;
- informasiya təhlükəsizliyi məsələləri üzrə simpoziumların keçirilməsi;
- informasiya təhlükəsizliyi məsələləri üzrə məsləhətlər.

CIAC qrupu təhlükəsiz kompyuter texnologiyaları mərkəzinin tərkibinə daxil idi (Computer Security Technology Center, CSTC) və Lawrence Livermore milli laboratoriyasında yerləşirdi.

Boşluqlar haqqında İnternet istifadəçilərinə periodik məlumat verilməsi üçün CIAC mərkəzi də CERT/CC-yə analoji olaraq öz veb serverində (http://llnl.ciac.gov) və göndəriş siyahılarında informasiya bülletenləri (ing. Advisories) nəşr edirdi.

1.4. FIRST forumu

1989-cu ilin avqustunda CERT/CC seminar təşkil etdi, fəaliyyətinin birinci ilində öyrənilənlərlə yanaşı, komandalar arasındakı münasibətləri koordinasiya etmək üçün növbəti addımlar müzakirə edildi. 1989-cu ilin oktyabrında artıq təxminən 170 000 hostdan ibarət olan İnternetə yeni soxulcan hücum etdi. WANK adlandırılan bu soxulcan Digital Equipment Corporation şirkətinin DECNET şəbəkəsinə qoşulan sistemlərdəki boşluqları istismar edirdi. Bu soxulcana cavab vermək üçün üç komanda öz fəaliyyətlərini əlaqələndirdi: CIAC, CERT/CC və NASA Space Physics Analysis Network. CIAC və CERT/CC tərəfindən müxtəlif xəbərdarlıq bülletenləri buraxıldı, lakin buna baxmayaraq administratorların çoxu xəbərdarlıqlara diqqətlə yanaşmadılar və iki həftə sonra WANK soxulcanın OILZ adlı variantına ilə yoluxdular.

Hər birinin öz məqsədləri, maliyyə mənbələri və tələbləri olan cavablandırma qrupları yarandıqdan sonra məlum oldu ki, vahid əlaqələndirici mərkəz olmadan keçinmək olmayacaq. Müxtəlif saat qurşaqlarında yerləşən qrupların qarşılıqlı əlaqəsi zamanı dil və digər problemlər meydana çıxırdı. Cavablandırma komandaları şəbəkəsinin yaradılması üçün müzakirələr başlandı. Belə bir şəbəkənin ideyaları NIST və CERT/CC-nin birgə 1990-cı il seminarının bir sessiyasında təqdim və müzakirə edildi. Bu müzakirələrdən sonra gələcək əməkdaşlıq üçün məqsədlər müəyyən edildi. Bu məqsədlər CSIRT-lər arasında informasiya paylaşımı və ehtiyac olduqda insidentlər və şəbəkə hücumları zamanı bir-birinə kömək etmək idi. CSIRT cəmiyyəti bu gün də həmin məqsədləri güdür.

Seminardan sonrakı müzakirələr nəticəsində 1990-cı ilin noyabrında 11 təsisçi üzv (biri Fransadan olmaqla) insidentləri cavablandırma və təhlükəsizlik qruplarını birləşdirən FIRST **(Forum of Incident Response and Security Teams)** forumunu yaratdılar (http://www.first.org).

Cədvəl 1.1. FIRST-in təsisçi üzvləri

Air Force Computer Emergency Response Team (AFCERT)
CERT Coordination Center
Defense Communication Agency/Defense Data Network
Department of the Army Response Team
Department of Energy's Computer Incident Advisory Capability (CIAC), Lawrence Livermore National Laboratory
Goddard Space Flight Center
NASA Ames Research Center Computer Network Security Response Team (NASA ARC CNSRT)
NASA Space Physics Analysis Network (SPAN CERT)
Naval Computer Incident Response Team (NAVCIRT)
National Institute of Standards and Technology Computer Security Resource and Response Center (CSRC)
SPAN-France

2010-cu il oktyabrına olan məlumata görə FIRST-in tərkibinə dünyanın 48 ölkəsindən 226 insident cavablandırma komandası daxildir.

FIRST-in məqsədləri aşağıdakılardır:

- kompyuter insidentlərinin qarşısının effektiv alınması, aşkarlanması və informasiya sistemlərinin insidentdən sonra bərpası üçün forum iştirakçıları arasında əməkdaşlığın təmin edilməsi;
- potensial təhdidlər və boşluqlar haqqında qəza və konsultativ informasiya üçün forum iştirakçıları arasında əlaqənin təmin edilməsi;
- informasiya təhlükəsizliyi sahəsində tədqiqat aparan forum iştirakçıları arasında qarşılıqlı əlaqənin təmin edilməsi;
- informasiya təhlükəsizliyini təmin edən alətlərin, mexanizmlərin və informasiyanın yayılmasını asanlaşdırmaq.

FIRST illik Computer Security Incident Handling Workshop simpoziumunun təşkilatçısıdır. Bu simpoziumda təkcə FIRST iştirakçıları deyil, bütün arzu edənlər iştirak edə bilər. İldə 2-3

dəfə FIRST yalnız öz iştirakçıları üçün qapalı kollokviumlar da təşkil edir.

İnsidentlərə cavabvermə qruplarının əlaqələndiricisi olan FIRST forumu kompyuter sistemlərinin boşluqlar və onlara hücumlar haqqında informasiya nəşr etmir.

1.5. CERT yoxsa CSIRT?

CERT modeli tezliklə Avropada da qəbul edildi və 1992-ci ildə Danimarkanın SURFnet akademiya provayderi SURFnet-CSIRT adlı Avropada ilk CSIRT (Computer Security and Incident Response Team, Kompyuter təhlükəsizliyi insidentlərini cavablandırma qrupu) yaratdı. Bir çox qrup da bu nümunənin iziylə getdilər, hazırda Avropada 100-dən artıq CSIRT mövcuddur.

İllər keçdikcə CERT qrupları öz potensiallarını insidentlərə sadə cavabdan xəbərdarlıq xidmətləri, təhlükəsizlik üzrə tövsiyələr, treninqlər və təhlükəziklik sistemlərinin idarə edilməsi daxil olmaqla təhlükəsizlik xidmətlərinin geniş siyahısını göstərməyə başladılar. Tezliklə «CERT» terminini yetərli hesab etməməyə başladılar. Nəticədə 1990-cı illərdə yeni «CSIRT» termini qəbul edildi. Hazırda hər iki termin (CERT və CSIRT) sinonim kimi istifadə edilir, lakin CSIRT daha dəqiq termin hesab edilir. CSIRT termini CERT/CC-yə məxsus müəlliflik hüququ ABŞ-da rəsmi qeydiyyatdan keçirilmiş CERT terminini işarə etmək üçün daha çox Avropada istifadə edilir.

İnsidentləri cavablandırma qruplarını bildirən digər qısaltmalar da var:

Cədvəl 1.2. İnsidentləri cavablandırma qrupları

CERT	Computer Emergency Readiness Team, Kompyuter Qəzalarına Hazırlıq Komandası
CSIRT	Computer Security Incident Response Team, Kompyuter təhlükəsizliyi insidentlərini cavablandırma qrupu
CSIRC	Computer Security Incident Response Capability, Kompyuter təhlükəsizliyi insidentlərini cavablandırma mərkəzi
CIRC	Computer Incident Response Capability, Kompyuter insidentlərini cavablandırma mərkəzi
CIRT	Computer Incident Response Team, Kompyuter insidentlərini cavablandırma qrupu
IHT	Incident Handling Team, İnsident Emalı Komandası
IRC	Incident Response Center və ya Incident Response Capability, İnsidentləri cavablandırma mərkəzi
IRT	Incident Responce Team, İnsidentləri cavablandırma qrupu
SERT	Security Emergency Response Team, Təhlükəsizlik insidentlərini operativ cavablandırma qrupu
SIRT	Security Incident Response Team, Təhlükəsizlik insidentlərini cavablandırma qrupu

1.6. Avropada ilk cavablandırma komandaları

1991 və 1992-ci illərdə CSIRT ideyasının tərəfdarları ABŞ-da artırdı, lakin digər ölkələr hələlik CSIRT komandaları olmadan keçinirdilər. Avropada ilk CSIRT Fransada Space Physics Analysis Network (SPAN) şəbəkəsində qurulmuşdu. Bu şəbəkə ənənəvi olaraq NASA şəbəkələrinin hissəsi idi və komandaya ehtiyac daha əvvəl, xüsusilə də WANK və OILZ soxulcan hücumlarından sonra hiss edilmişdi.

Həmin vaxtlar CERT/CC-nin təşkil etdiyi illik CERT konfranslarında bir və ya iki avropalı ekspert iştirak edirdi. Vəziyyət 1992-ci ildə, xüsusilə də Avropa tədqiqat şəbəkəsində dəyişməyə başladı. Müxtəlif Avropa şəbəkələrində hostların sayı 10 000-ni keçmişdi və şəbəkə təhlükəsizliyinə ehtiyac artmışdı. Baş verən insidentlər artdıqca CSIRT konsepsiyasını başa düşənlər birgə işləməyin yollarını axtarmağa başladılar. 1992-ci ildə Avropa Tədqiqat Şəbəkələri Assosiasiyasının yaratdığı işçi

qrup vəziyyəti analiz etdi. Hər bir milli tədqiqat şəbəkəsində CSIRT üzrə səylərin real fayda verməsində anlaşma var idi. Hər bir komandanın öz kliyent icmasında diqqəti cəmləyərək və bütün komandalara toxunan yeni boşluqlar və təhlükəsizlik əməliyyatları üzrə kommunikasiya üçün məsuliyyəti paylaşmaqla Avropa komandalarının əməkdaşlıq edəcəyi gözlənilirdi. Bu konsepsiya bu gün də CSIRT ictimaiyyətinin dəyişməz prinsipidir.

İşçi qrupunun işinin nəticəsi olaraq müxtəlif milli tədqiqat şəbəkələri öz təşkilatları üçün CSIRT yaratmaq layihələrinə başladılar. İcmanın ehtiyaclarına əsaslanaraq müxtəlif xidmətlər təqdim edən komandalar yaradıldı. Avropa tədqiqat icması çərçivəsində qurulmuş iki müxtəlif komandaya nümunə CERT-NL və DFN-CERT-dir.

SURnet Computer Security İnsident Response Team (CERT-NL) Niderland tədqiqat şəbəkəsi olan SURFnet tərəfindən mərkəzləşdirilmiş komanda kimi yaradılmışdı. Komanda SURFnet-in iki üzvündən ibarət idi, onlar tədqiqat şəbəkəsində digər universitetlərin təcrübəli mütəxəssisləri ilə əməkdaşlıq edirdilər, bu daha geniş ekspertiza və normal iş saatlarından sonra da yardım təmin edirdi. SURFnet-in çərçivəsində daxili layihə kimi yaradıldığı üçün komandanın işə başlamasında gecikmə olmadı və CERT-NL 1992-ci ildə fəaliyyətə keçdi.

DFN (Deutsches Forschungsnetz) – Almaniya Tədqiqat Şəbəkəsi üçün DFN-CERT komandası mərkəzləşdirilmiş komanda kimi yaradıldı. Komanda şəbəkənin üzvü olan universitetdə yerləşirdi. Deməli, digər universitetlər baxımından insidentlər "kənar" heyət tərəfindən (onların təşkilatına nəzərən), lakin "daxili" təşkilat (bütün şəbəkəyə nəzərən) cavablandırılırdı. Bu, kənar layihə olduğundan tender prosesi zəruri idi və komandanın yaradılmasında gecikməyə səbəb oldu. DFN-CERT 1993-cü ilin birinci iş günü fəaliyyətə başladı.

Erkən Avropa komandaları struktur və xidmətlər baxımından CERT/CC modelinə əməl edirdilər. Onlar insidentləri cavablandırmanı əsasən tövsiyələr verməklə, xəbərdarlıqlar, həyəcan siqnalları və bülletenlər yaymaqla və təhlükəsizlik

sahəsində məlumatlandırma yolu ilə yerinə yetirirdilər. Onlar yerində dəstək göstərmirdilər.

Avropa işçi qrupunun işindən nəticələnən digər ideya komandaların səylərini koordinasiya etmək üçün mərkəzləşdirilmiş Avropa komandasının yaradılması idi. Bunun işləyib-işləməyəcəyini müəyyən etmək üçün RARE (Réseaux Associéspour la Recherche Européene) CERT Task Force tərəfindən 1993-cü ilin ortalarında birillik tədqiqat layihəsi başladıldı. 1994-cü ilin sonunda yekun hesabat Avropada insident cavablandırmasının həqiqətən də yuxarıdan aşağı yanaşma ilə daha yaxşı əldə ediləcəyini bəyan etdi. Bütün Avropa tədqiqat şəbəkələrinin öz komandalarını maliyyələşdirmək imkanlarını nəzərə alaraq tövsiyə edirdi ki, CERT/CC modelinə uyğun güclü Avropa komandası yaradılmalıdır.

Belə mərkəzləşdirilmiş komandanın maliyyə tələb etməsi və mövcud Avropa komandalarına rəqib olacağı faktı bu tövsiyənin əleyhinə işlədi və onun birbaşa nəticəsi olmadı.

1990-cı illərin ortalarına kimi mövcud Avropa komandaları arasında qarşılıqlı əlaqələri, eləcə də bu əlaqə və kommunikasiyaları digər regionlardakı CSIRT-lərlə (ABŞ, Kanada, Avstraliya) necə strukturlaşdırmaq məsələləri var idi.

1993-cü ilin sonlarında Avropa CSIRT-lərin ilk görüşü CERT-NL və DFN-CERT üzvləri tərəfindən təşkil edildi. Ümid edilirdi ki, ünsiyyət dərhal əməkdaşlığa gətirəcək. Bu görüş ABŞ xaricində ilk CSIRT görüşü olması baxımından qiymətlidir. 1994 və 1995-ci illərdə daha çox komandanı bir yerə yığan daha iki görüş də keçirildi.

CSIRT-lər barəsində informasiya toplamaq üçün şablon yaradıldı ki, digər komandalarla paylaşıla bilsin. Yenidən Avropa tədqiqat şəbəkələri icması mərkəzləşdirilmiş Avropa CSIRT-i ideyasını dəstəklədi və məqsədi Avropa CSIRT-lərin gələcəyi üçün yol xəritəsi işləmək olan işçi qrupu üçün fond təsis edildi.

1.7. EuroCERT layihəsi

TERENA-nın "Avropada CERT-lər" işçi qrupunun yekun hesabatı hücum və insidentlərə məruz qalan kliyentlərə daha yaxın yerləşən lokal komandaların yaradılması ilə yanaşı, komandalar arasında əlaqəni yaxşılaşdırmaq üçün müəyyən növ koordinasiyaya ehtiyac olduğunu da etiraf edirdi. Bu fərdi fəaliyyət göstərən bir komandanın təmin etdiyindən daha yüksək səviyyədə insident cavablandırma fəaliyyəti təmin etməyin yolu kimi nəzərdən keçirilirdi. Bu yanaşma üçillik müddətdə müxtəlif layihələrin təklif edilməsinə, hazırlanmasına gətirib çıxarırdı və nəhayət, Avropa koordinasiya mərkəzi üçün təkliflə kulminasiya nöqtəsinə çatdı. Bu layihə 1997-ci ilin sonlarında başladı və 1999-cu il boyunca EuroCERT kimi davam etdi.

Bu layihə ilə bağlı bir sıra problemlər var idi, bəzi CSIRT-lər EuroCERT-i özlərinə rəqib kimi görürdülər, komandalar arasında olan razılaşmalar kifayət qədər səmərəli hesab edilirdi və digər təşkilat və ya iyerarxik səviyyə tərəfindən kömək və dəstəyə ehtiyac hiss edilmirdi. EuroCERT-in iflası isbat etmirdi ki, CSIRT-lərin fəaliyyəti koordinasiyası edilməməlidir, o göstərirdi ki, mövcud olandan fərqli olan hər hansı koordinasiya tələb edilir. Bu artıq qüvvədə olan proseslərə yeni dəyər əlavə etmək və mövcud fərdi CSIRT razılaşmaları çərçivəsində mümkün olmayan funksiyalar təmin etmək üçün tələb edilirdi. Bu təkcə Avropa CSIRT-lərinə və təşkilatlarına xas olan problem deyil, oxşar problemlər müxtəlif təşkilatlarda, dövlət, kommersiya və təhsil təşkilatlarında CSIRT-lərin koordinasiyası zamanı müşahidə edilmişdir.

Avropa CSIRT-ləri arasında koordinasiya problemlərinə aşağıdakılar daxil idi:

- Olduqca çox sayda komandanın mövcud olması bütün digər komandalarla eyni keyfiyyətdə münasibətlərin təmin edilməsini getdikcə daha qeyri-praktiki edirdi.
- Bir ölkə CSIRT-lərinin digər ölkədəki CSIRT-lər arasındakı fərqləri başa düşəcəyi çox da inandırıcı deyil. Digər ölkədə hansı CSIRT-ə müraciət etməyi və ya

koordinasiya etməyi qərarlaşdırmaq üçün bir ümumi təmas nöqtəsinin təmin edilməsi daha əlverişlidir.

1.8. TF-CSIRT qrupu

EuroCERT layihəsi 1999-cu ilin sonlarında başa çatırdı, TERENA Avropada CSIRT-in uzunmüddətli dəstəkçisi kimi bunun Avropada CSIRT fəaliyyətinə təsirini müzakirə etmək üçün iclas çağırdı. EuroCERT-in fəaliyyəti ilə əldə edilən bütün hədəflər bir daha yoxlandı, bütün iştirakçılar həmin hədəflərə aşağıdakı yanaşma ilə razılaşdılar.

- Tam təminatlı xidmət əvəzinə üzvlərin dəstəklədiyi faydalı fəaliyyətlər könüllü işçi qrupları tərəfindən icra edilməlidir.
- Müxtəlif komandaların mərkəzi koordinasiya orqanı əvəzinə komandaların imkanları aşağıdakı mexanizmlər təmin edilməklə gücləndirilməlidir:
    - əməkdaşlıq;
    - yeni komandaların inteqrasiyası;
    - digər komandaların yerinə yetirdiyi xidmətləri başa düşməklə və bilməklə inam şəbəkəsinin qurulması;
- Avropa komandaları arasında görüşləri təşkil edən mərkəzi orqan əvəzinə bu görüşləri vasitəçi təşkil etməlidir.

TERENA (Trans-European Research and Education Networking Association) vasitəçi kimi xidmət etməyə və iştirakçı Avropa CSIRT-lərinin ildə üç dəfə iclaslarını təşkil etməyə könüllü razı oldu. Belə könüllü yanaşmanın nəticəsində 2000-ci ildə TF-CSIRT işçi qrupu – ümumi fəaliyyətin/layihələrin koordinasiyası və təcrübə mübadiləsi üçün forum yaradıldı. (Bu qrupun iclaslarının protokollarını TF-CSIRT saytından əldə etmək olar.)

TF-CSIRT Avropada CSIRT qrupları arasında əməkdaşlığı inkişaf etdirir. TF-CSIRT qrupunun əsas məqsədləri aşağıdakılardır:

- təcrübə və bilik mübadiləsi, razılaşdırılmış siyasətin formalaşdırılması üçün forumun təşkili;
- yeni layihələrə təşəbbüs və Avropa CSIRT-ləri üçün pilot servislərin işə salınması;
- informasiya təhlükəsizliyi insidentlərinə cavab üçün ümumi standartların və prosedurların inkişaf etdirilməsi;
- yeni CSIRT-lərin yaradılmasında kömək və CSIRT heyətinin hazırlanmasında kömək;
- CSIRT təşəbbüslərinin koordinasiyası və Avropa Komissiyası ilə koordinasiya orqanı funksiyasının yerinə yetirilməsi.

TF-CSIRT qrupunun fəaliyyəti TERENA Texniki Komissiyasının 15 sentyabr 2004-cü ildə təsdiqlədiyi Vəzifələr Siyahısına uyğun olaraq Avropa və qonşu ölkələrdə cəmlənib.

TF-CSIRT işçi qrupunun uğurlu nəticələrinə daxildir.

- Insident Object Description and Exchange Format (IODEF) layihəsi. Bu layihəyə XML istifadə edilməklə CSIRT-lər arasında insident məlumatlarının mübadiləsi üçün verilənlər modelinin və spesifikasiyalarının yaradılması daxil idi. Bu layihə başa çatmış və IETF-in Incident Handling (INCH) işçi qrupuna təqdim edilmişdir.
- Training of Network Security Incident Teams Staff (TRANSITS) layihəsi. Müxtəlif Avropa komandalarının üzvləri treninq materialları çoxluğunun yekun versiyasını yeni insident cavablandırma heyəti üçün kurs yaratdılar. Layihədə CSIRT təlimi üçün təqdimatlar və materiallar toplanmışdır. Bu treninqlər Avropa İttifaqı tərəfindən dəstəklənir və yeni CSIRT üzvləri treninqdə nominal ödənişlə iştirak edə bilərlər.

Bu qrupun digər faydası müxtəlif komandaların üzvlərinə il ərzində iclaslarda üzbəüz görüşmələr üçün fürsətdir. İnsanlar bir-birini tanıdıqda telefon zəngləri və məlumat mübadiləsi daha asan olar. TF-CSIRT bu növ forumların keçirilməsində Avropa CSIRT-lərinin çoxu üçün uğurlu olmuşdur, koordinasiya və əməkdaşlıq üçün real fürsətlər təqdim etmişdir, bunu yuxarıda

adı çəkilmiş layihələrdən görmək olar. Qrupun əhəmiyyətli nailiyyətlərindən biri onun fəaliyyətinin ilkin tədqiqat qrupları çərçivəsindən uğurla genişlənməsi və kommersiya və dövlət təşkilatlarını da cəlb etməsidir.

1.9. Asiya-Sakit Okean regionunda CERT-lər

Qeyri-formal əsasda Asiya-Sakit Okean regionunda 1990-cı illərin əvvəlində yaradılmış təhlükəsizlik komandaları olsa da, ilk tanınmış CSIRT AusCERT oldu. AusCERT 1993-cü ildə Security Emergency Response Team (SERT) adı altında yaradılmışdı. Maliyyələşdirmə və dəstək əməkdaşlıq yolu ilə üç universitet (Kuinsland Texnologiya Universiteti, Qriffit Universiteti və Kunisland Universiteti) tərəfindən təmin edilirdi. Zaman keçdikcə SERT AusCERT-ə çevrildi. Hazırda onun maliyyəsi üzvlük abunə haqlarından və dövlət fondlarındandır. AusCERT 1999-cu ildə Asiya Sakit Okean regionunda komandaların artmasına diqqəti çəkmək üçün FIRST konfransına ev sahibliyi etmişdi.

1996 və 1997-ci illərdə Asiya-Sakit Okean regionunda bir çox CSIRT yaradılmışdır. Bəzi komandalar könüllü təşkilatlar kimi işə başlamış və sonradan onlara milli komanda olmaları üçün dövlət maliyyəsi verilmişdir. KrCERT/CC (Korea CERT Coordination Center, 1996-cı il), JPCERT/CC (Japan CERT/CC, 1996-cı il) və SingCERT (Singapore CERT) belə nümunələrdəndir. Onların hamısı FIRST üzvləri oldular. 2000-ci ildə Çində CNCERT/CC yaradıldı.

Bu ilk komandalar həmin regionda lider oldular, öz icmaları və ölkə arasında komandalara fəaliyyətə başlamağa və insident cavablandırmasına dəstək verməyə kömək etdilər.

1.10. Latın Amerikasında CERT təşəbbüsləri

1990-cı illərin sonu – 2000-ci illərin əvvəlində Latın Amerikasında bir çox CSIRT-lər yaradılmışdı. Bu komandalardan yalnız bir neçəsi FIRST üzvləridir. Latın

Amerikasnda TF-CSIRT, APCERT kimi regional təşəbbüslər yoxdur.

Meksikada yaradılmış ilk komanda Mx-CERT olmuşdur. Bu komanda FIRST-in üzvü idi və Latın Amerikasında FIRST-in keçirdiyi ilk konfransa ev sahibliyi etmişdi (1998-ci il). Lakin Mx-CERT hazırda fəaliyyət göstərmir.

2000-ci ildə UNAM-CERT komandası Meksika National Autonomous University-də yaradılmışdı, 2001-ci ildən FIRST-in üzvüdür. Həmin vaxtdan UNAM-CERT insidenti cavablandırma təşəbbüsləri üzrə akademik, dövlət və kommersiya təşkilatları ilə təmas nöqtəsidir.

Braziliyada CSIRT təşəbbüsləri 1995-ci ilin mayında Internet İdarəetmə Komitəsinin (Internet Steering Committe – CGI.br) yaradılması ilə başlanmışdır. CGI.br dövlət, akademik, biznes və qeyri-hökümət sektorlarını təmsil edən maraqlı tərəflərin iştirakı ilə yaradılmışdı. CGI-nin missiyası şəbəkələrin və İnternet servislərinin təhlükəsizliyi sahəsində strateji istiqamətləri müəyyən etməkdir.

CGI.br 1997-ci ilin iyununda CERT.br-i milli CSIRT kimi yaratdı. 1997-ci ilin avqustunda Braziliya elm şəbəkəsi (Brazilian Research Network) və Rio Grande do Sul Academic Network özlərinin CSIRT-komandalarını təsis etdilər.

1999-cu ildə digər təşkilatlar – universitetlər və telekommunikasiya şirkətləri də CSIRT-komandalarını yaratmağa başladılar. 2004-cü ildə Braziliya federal hökuməti tərəfindən dövlət təşkilatları üçün CSIRT – CTIR GOV yaradıldı.

Argentinada 1998-ci ildə yaradılmış informasiya təhlükəsizliyi komandasının bazasında ArCERT 1999-cu ilin mayından federal dövlət təşkilatları üçün CSIRT xidmətləri göstərir və 2004-cü ildən FIRST-in üzvüdür.

1.11. US-CERT

US-CERT (United States Computer Emergency Readiness Team) 2003-cü ilin sentyabrında yaradılıb. US-CERT DHS ilə dövlət və özəl sektorlar arasında tərəfdaşdır və İnternetdən təhlükəsizlik təhdidlərinə cavab və əlaqələndirmə üçün nəzərdə tutulmuşdur.

US-CERT federal hökumətin İnsidentlərin Federal İdarə edilməsi Mərkəzidir və ABŞ-ın kompyuter təhlükəsizliyi məsələləri üzrə koordinator kimi çıxış edir. National Cyber Alert System-i vasitəsilə təhlükəsizliyin cari məsələləri, boşluqlar və eksploytlar haqqında informasiya yayır və proqram təminatı istehsalçıları ilə təhlükəsizlik sistemlərində boşluqların aradan qaldırılması üçün patçların (yamaqların) yaradılması üçün işləyir.

US-CERT-in tərkibinə beş bölmə daxildir:

1. **Cari əməliyyatlar bölməsi** (Operations branch). İnsidentlər haqqında alınmış informasiyanın emalına cavabdehdir, insidentləri cavablandırmanı təmin edir, zəruri informasiyanı yayır, milli infrastrukturun kritik vacib elementləri üçün məlum və yeni təhdidlərin qiymətləndirilməsi keyfiyyətini yüksəltmək məqsədi ilə müxtəlif verilənlərin analizini təmin edir (şəbəkə infrastrukturu, ziyankar proqram təminatı və s. daxil olmaqla).
2. **Situativ məlumatlandırma bölməsi** (Situational Awareness branch). Şəbəkə aktivliyinin kompleks analizinə (tendensiyaların və magistral şəbəkələrin yüklənməsinin dəyişmə xarakterinin) və təhlükəsizliyi yüksəltmək məqsədi ilə federal strukturların məlumatlandırılmasına cavabdehdir. İnsidentlərin həllində dəstəyi də təmin edir.
3. **İstintaq bölməsi** (Law Enforcement and Intelligence branch). Qanuna zidd hərəkətlərin aşkarlanması və istintaq zamanı hüquq-mühafizə orqanları ilə qarşılıqlı əlaqəni təmin edir.
4. **Perspektiv inkişaf bölməsi** (Future Operation branch). US-CERT-in insidenti cavablandırma üzrə işini təmin edən perspektiv planların, prosedurların, reqlamentlərin işlənib hazırlanmasına məsuldur.

5. **Dəstək bölməsi** (Mission Support branch). US-CERT-in işi üçün veb-sayt dəstəyi də daxil olmaqla, zəruri kommunikasiya vasitələri təmin edir, eləcə də inzibati dəstək, heyətin təhlükəsizliyi, təchizat və digər köməkçi funksiyalara görə cavabdehdir.

US-CERT-in işini təmin etməklə yanaşı, DHS aşağıdakı istiqamətlər üzrə də işləri yerinə yetirir:

- informasiya təhlükəsizliyi sahəsində fövqəladə hallara hazırlığı yoxlamaq məqsədilə mütəmadi olaraq (iki ildə bir dəfə) Cyber Storm təlimlərini keçirir;
- kibertəhlükəsizlik üzrə ildə bir dəfə informasiya-təhsil aylığı keçirir;
- ümummilli miqyasda insidentin baş verməsi halında 13 federal idarədən (kəşfiyyat, hüquq-mühafizə strukturları və US-CERT daxil olmaqla) ibarət qrupun işini koordinasiya edir;
- kibercinayət törətmiş cinayətkarların aşkarlanması və axtarışı məqsədilə hüquq-mühafizə orqanları əməkdaşları arasında informasiya mübadiləsi sisteminin (Cyber Cop Portal) işini dəstəkləyir.

US-CERT öz fəaliyyəti zamanı oxşar təşkilatlarla qarşılıqlı əlaqədə olur. Lakin yalnız CERT/CC onun rəsmi tərəfdaşıdır. Bu qarşılıqlı əlaqədə US-CERT ABŞ-a kiberhücumların qarşısının alınması, onlardan müdafiə və cavab tədbirləri üçün koordinasiya mərkəzidir.

Milli Kiberhəyəcan sistemi boşluqların və təhdidlərin identifikasiyasını, analizini və ranqlaşdırılmasını həyata keçirir. Bu sistem daxil olan informasiyanı süzgəcdən keçirir və zəruri olduqda avtomatik rejimdə bütün istifadəçilərə həyəcan siqnalı göndərir.

- kiberhəyəcan siqnalı – iki formada mümkündür: qeyri-texniki istifadəçilər və texniki istifadəçilər üçün;
- bülletenlər – texniki mütəxəssislər üçün nəzərdə tutulur, boşluqlara, təhdidlərə, eləcə də təhdidləri azaltmaq üçün yerinə yetirilməsi zəruri olan tədbirlərə həsr olunan həftəlik icmaldır.

1.12. İnsidentləri cavablandırma üzrə standartlar

Hazırda informasiya təhlükəsizliyi insidentlərinin idarə edilməsi məsələlərini tənzimləyən çox sayda beynəlxalq və milli normativ sənədlər mövcuddur. İnsidentlərin idarə edilməsi mövzusu üzrə ISO/IEC standartları, elektrorabitə təşkilatları üçün ITU-T E 409:2004 standartı, CERT/CC-nin sənədlər toplusu, NIST SP 800-61, ISO/PAS 22399, NFPA 1600 və bir sıra digər sənədlər. Qeyd etmək lazımdır ki, insidentlərin idarə edilməsi yalnız informasiya təhlükəsizliyinin təmin edilməsi çərçivəsində deyil, bütövlükdə İT-sevislərin idarə edilməsində meydana çıxır. ISO/IEC 20000:2005 standartında "servisin göstərilməsi və dəstək" bölməsində İT-infrastrukturda insidentlərin idarə edilməsi prosesinin təşkilinə bir sıra tələblər təsvir edilir.

ISO/IEC 27001:2005 Information security management system. Requirements. Bu standart çərçivəsində informasiya təhlükəsizliyini idarəetmə sisteminin qurulmasına, o cümlədən insidentlərin idarə edilməsi proseslərinə də aid olan ümumi tələblər irəli sürülür.

ISO/IEC TR 18044 Information Security Incident Management yüksək səviyyə standartıdır. Bu sənəd tsiklik PDCA modeli çərçivəsində insidentləri idarəetmə infrastrukturunu təsvir edir: ilkin informasiya, planlaşdırma və hazırlıq, insidentlərin idarə edilməsinin istismarı, analiz, tənəkmilləşdirmə. Planlaşdırma, istismar, analiz və proseslərin təkmilləşdirilməsi mərhələləri üçün ətraflı spesifikasiyalar verilir. Normativ-sərəncamverici sənədlərlə, resurslarla təminat məsələlərinə baxılır, zəruri prosedurlar barəsində müfəssəl tövsiyələr verilir.

CERT/CC Koordinasiya Mərkəzinin İnT insidentlərinin idarə edilməsi məsələlərinə aid aşağıdakı sənədlərini göstərmək olar:

- Defining Incident Management Processes for CSIRTs: A Work in Progress;
- Handbook for Computer Security Inscident Response Teams (CSIRTs);

- State of the Practice of Computer Security Insident Response Teams;
- Incident Management Capability Metrics;
- Incident Management Mission Diagnostic Method;
- Staffing Your Computer Security Incident Response Team-Whot Basic Skills are Needed?
- Action List for Developing a Computer Security Incident Response Team (CSIRT).

CMU/SEI-2004-TR-015 Defining Incident Management Processes for CSIRTs: A Work in Progress. Bu sənəd insidentləri idarəetmə proseslərini planlaşdırma, tətbiq, qiymətləndirmə və təkmilləşdirmə metodologiyasını təsvir edir. Əsas fikir informasiya təhlükəsizliyi insidentlərini cavablandırma xidmətinin işinin təşkilinə verilir. Bir sıra meyarlar daxil edilir ki, onların əsasında baxılan xidmətlərin səmərəliliyini qiymətləndirmək olar, müfəssəl proses kartları da təklif edilir.

NIST İnstitutu informasiya təhlükəsizliyi insidentlərinin idarə edilməsinin müxtəlif məsələlərinə aid bir sıra sənədlər işləyib hazırlamışdır:

- NIST SP 800-3 Establishing a Computer Incident Response Capability (CSIRT) (1991-ci il, noyabr);
- NIST SP 800-61 Computer Security Incident Handling Guide (2004-cü il, yanvar);
- NIST SP 800-83 Guide to Malware Incident Prevention and Handling (2005-ci il, noyabr)
- NIST SP 800-86 Guide to Integrating Forensic Techniques into Incident Response (2006-cı il, avqust).

NIST SP 800-61 Computer Security Incident Handling Guide xüsusi nəşrində informasiya təhlükəsizliyi hadisələrinin idarə edilməsi və onlara cavab verilməsi prosedurlarının qurulması üzrə "ən yaxşı təcrübələr" toplusu təqdim olunur. Təhdidlərin ziyankar proqram təminatının yayılması, icazəsiz giriş və başqa müxtəlif növlərinə cavabvermə məsələləri ətraflı təhlil edilir.

NIST SP 800-86 Guide to Integrating Forensic Techniques into Incident Response xüsusi nəşrində informasiya

təhlükəsizliyi insidentlərinin təhqiqatında təşkilatlara kömək məqsədi ilə kompyuter və şəbəkə ekspertizasının keçirilməsində praktiki rəhbərlik tövsiyələri verilir. Tövsiyələr hüquq-mühafizə baxımından deyil, informasiya texnologiyaları baxımından təqdim olunur. NIST SP 800-86 fayllar, əməliyyat sistemləri, şəbəkə trafiki və tətbiqi proqramlar daxil olmaqla müxtəlif məlumat mənbələri üzrə effektiv ekspertizanın keçirilməsi proseslərini təsvir edir və məsləhətlər verir.

Standartlarla yanaşı, informasiya təhlükəsizliyi insidentlərinin cavablandırılması sahəsində bir sıra digər sənədlər də mövcuddur.

GRIP (Guidelines and Recommendations for Security Incident Processing) – təhlükəsizlik insidentlərinin email üçün tövsiyələr. 1998-2001-ci illərdə IETF tərəfindən işlənmiş bir sıra RFC sənədlər (RFC 2196, RFC 2505, RFC 3013, RFC 322, RFC 2828) daxildir. "RFC 2350 – Təhlükəsizlik insidentlərini cavablandırma komandalarından gözləntilər" sənədi fəsil 7-də ətraflı araşdırılır.

IDMEF (Intrusion Description and Exchange Format) – müdaxilələrin təsviri və mübadiləsi formatı. IDS sistemləri arasında şübhəli hadisələr haqqında xəbərdarlıq məlumatlarının ötürülməsi üçün istifadə edilir. Bu format kommersiya və pulsuz IDS sistemləri arasında uyarlığı və onların birgə istifadəsi imkanını təmin etməlidir.

IODEF (Incident Object Description and Exchange Format) – insidentlər haqqında informasiyanın təsviri və mübadiləsi formatı şəbəkədə bütün insidentlərin XML-formatda təqdim olunmasını tələb edir. Standartın yenilənmiş versiyasında birqiymətli vaxt nişanlarının isifadəsi, dilin seçilməsi və nümunələrin qoşma-faylda göndərilməsi kimi əlavə imkanlar da var. Kiberinsidentlər (fişinq və İnternet-dələduzluq daxil olmaqla) üzrə məlumatların formatının unifikasiyası onların analizini və ümumi bazada axtarışı avtomatlaşdırmağa, ümumi meyilləri daha tez aşkarlamağa və şəbəkə hücumlarını cavablandırmağa imkan verir.

VEDEF (Vulnerability and Exploit Description and Exchange Format) – başlıqlar və eksploytlar haqqında informasiyanın təsviri və mübadiləsi formatı. TF-CSIRT, JPCERT/CC və başqa qurumlar tərəfindən birlikdə işlənməsi nəzərdə tutulurdu.

FƏSİL 2

İNFORMASİYA TƏHLÜKƏSİZLİYİ İNSİDENTLƏRİ

İNFORMASİYA TƏHLÜKƏSİZLİYİ İNSİDENTLƏRİ

- **İnsident anlayışı**
- **İnsidentlərin növləri**
- **Ziyankar proqramlar**
- **DoS-hücumları**
- **Kibercasusluq insidentləri**
- **İcazəsiz giriş insidentləri**
- **İntellektual mülkiyyət insidentləri**

FƏSİL 2 İNFORMASİYA TƏHLÜKƏSİZLİYİ İNSİDENTLƏRİ

2.1. İnsident anlayışı

"İnformasiya təhlükəsizliyi insidenti" anlayışının müxtəlif tərifləri ilə rast gəlmək mümkündür. Geniş mənada informasiya təhlükəsizliyi insidenti informasiya sistemində baş verən istənilən qanunsuz, icazə verilməyən (o cümlədən, informasiya təhlükəsizliyi siyasəti ilə) və ya qəbul edilməz hərəkətlərə deyilir.

İnformasiya təhlükəsizliyi insidentlərinin idarə edilməsi üzrə ISO/IEC TR 18044 standartında insident anlayışı bir qədər dar mənada işlədilir. Bu standarta informasiya təhlükəsizliyi hadisəsi anlayışı daxil edilir və onun vasitəsi ilə informasiya təhlükəsizliyi insidenti anlayışına tərif verilir:

İnformasiya təhlükəsizliyi hadisəsi – sistem, xidmət və ya şəbəkənin informasiya təhlükəsizliyi siyasətinin mümkün pozuntularını və ya mühafizə tədbirlərinin sıradan çıxmasını göstərən müəyyən vəziyyətinin məlum təzahürü, yaxud da təhlükəsizliklə bağlı ola biləcək, əvvəllər məlum olmayan vəziyyətinin meydana çıxmasıdır.

İnformasiya təhlükəsizliyi insidenti – bir və ya bir neçə arzuolunmaz və ya gözlənilməz informasiya təhlükəsizliyi hadisəsinin nəticəsi olan və biznes-əməliyyatları nüfuzdan salma və informasiya təhlükəsizliyinə təhlükə yaratma ehtimalı böyük olan hadisədir.

İnformasiya təhlükəsizliyi insidentlərinin aşağıdakı kateqoriyalarını və misal olaraq aşağıdakı hadisələri göstərmək olar.

Qəsdən törədilmiş insidentlər	Təsadüfi insidentlər	Səhvlər
xidmətdən imtina; oğurluq, xakerlik; dələduzluq; resurslardan sui-istifadə; sabotaj/fiziki ziyan vurma; ziyankar kod və s.	avadanlıqda nasazlıq; proqram təminatında nasazlıq; kommunikasiyada nasazlıq; yanğın; daşqın və s.	əməliyyatlarda səhvlər; aparat təminatında səhvlər; proqram təminatında səhvlər; istifadəçilərin səhvləri və s.

Qeyd edildiyi kimi, ISO/IEC 18044 standartında "informasiya təhlükəsizliyi hadisəsi" – "informasiya təhlükəsizliyi insidenti" xəttinə baxılır. ITU-T E.409 standartında isə "yalançı siqnal" – "hadisə" – "insident" – "informasiya təhlükəsizliyi insidenti" – "fəlakət, böhran" məntiqi ardıcıllığına baxılır.

ITU-T E.409 standartına görə:

İnsident – ciddi olmayan hadisə və epizoda gətirib çıxara bilən hadisədir.

Təhlükəsizlik insidenti – nəticəsində təhlükəsizliyin hər hansı aspektinin təhdidə məruz qala bildiyi istənilən arzu edilməyən hadisədir.

İnformasiya-kommunikasiya şəbəkələrinin (İKŞ) təhlükəsizlik insidenti – İKŞ-nin təhlükəsizliyinə qarşı istənilən faktiki və ya güman edilən arzuolunmaz hadisədir.

Daha bir neçə vacib terminə də baxaq. İnsidentlərin emalı (ing. incident handling), insidentlərin cavablandırılması (ing. incident response), insidentlərin idarə edilməsi (ing. incident management) kimi terminlər tez-tez işlədilir.

İnsidentlərin emalına insidentlərin aşkarlanması (hadisələr, insidentlər, həyəcan siqnalları haqqında məlumatların alınması və analizi), sistemləşdirmə (insidentlərə prioritetlərin verilməsi), analiz (nə baş verib, ziyan nə qədərdir, hansı təhdidə səbəb ola

bilər, dəf etmək və bərpa üçün hansı addımlar lazımdır) və insidentlərin cavablandırılması (planlaşdırma, koordinasiya və həyata keçirilmə, koordinasiya və informasiyanın yayılmasının, əks əlaqənin və dərs çıxarmanın) daxildir.

İnsidentlərin idarə edilməsi təkcə insidentlərin emalı və insidentlərin cavablandırılmasını deyil, onların qarşısının alınmasına yönəlik fəaliyyəti də bildirir. Bu fəaliyyətə boşluqların idarə edilməsi, artefaktların idarə edilməsi, istifadəçilərin təlimi və məlumat səviyyəsinin artırılması daxildir.

2.2. İnsidentlərin növləri

İnsidentlərin effektiv idarə edilməsi üçün təşkilatlar insidentlərin müəyyən edilməsi metodikasına malik olmalı, onların əməkdaşları isə hansı hadisələrin insident hesab edildiyini bilməlidirlər. Bu informasiya təhlükəsizliyi insidentləri üçün xüsusilə vacibdir – onlar heç də həmişə normal işə problem yaratmırlar. Məsələn, konfidensial sənədin stolun üstündə nəzarətsiz qalması informasiya təhlükəsizliyi insidentidir, ona kimsə fikir verməyə bilər, lakin bədniyyətli (təşkilatın əməkdaşı da ola bilər) belə sənədləri mütləq görəcək.

İnformasiya texnologiyaları inkişaf etdikcə və onların tətbiq sahələri genişləndikcə informasiya sisteminə nəzərən daxili və xarici mənbələrdən qaynaqlanan süni və ya təsadüfi xarakterli texniki və qeyri-texniki informasiya təhlükəsizliyi insidentlərinin sayı da artır və insidentlərin yeni növləri meydana çıxır. CSIRT qarşısına qoyulan məqsəd və vəzifələrdən, malik olduğu texniki və insan resurslarından çıxış edərək cavablandıracağı insidentlərin növlərini müəyyən edir. Müxtəlif CSIRT komandalarının cavablandırdığı insidentlərin növləri fərqli ola bilər, burada vahid yanaşma yoxdur. Əksər CSIRT komandaları ziyankar proqram təminatı, xidmətdən imtina hücumları (Denial of Service, DoS), informasiya sistemlərinə icazəsiz giriş, şəbəkənin daranması (ing. scanning) kimi insidentləri cavablandırırlar.

NIST SP 800-61 Computer Security Incident Handling Guide xüsusi nəşrində insidentlərin 5 növünün emalı üçün detallı tövsiyələr verilir: DoS-hücumlar, ziyankar kodlar, icazəsiz giriş, uyğunsuz istifadə və çoxkomponentli insidentlər (iki və daha artıq insidentin kombinasiyası). SANS İnstitutunun "Kompyuter təhlükəsizliyi insidentlərinin addımbaaddım emalı" adlı sənədində isə insidentlərin 8 növü sadalanır: ziyankar proqram təminatı, şəbəkənin daranması, DoS-hücumlar, uyğunsuz istifadə, kibercasusluq, hoax-proqramlar, icazəsiz giriş və intellektual mülkiyyət.

Aşağıda informasiya təhlükəsizliyi insidentlərinin bu növləri haqqında məlumat verilir.

2.2.1. Ziyankar proqram təminatı

Kompyuter sistemlərində informasiya təhlükəsizliyinə təhdidlərin əsas mənbələrindən biri "ziyankar proqramlar" kimi ümumi ad verilmiş xüsusi proqramlardır. "Ziyankar proqramlar" (ing. malware **mal**icious – ziyankar və so**ftware** – proqram təminatı) anlayışı icazəsiz və çox zaman ziyankar əməllərin həyata keçirilməsi üçün yaradılan və istifadə edilən bütün proqramları əhatə edir.

Təsir mexanizmindən asılı olaraq, ziyankar proqramlar məntiqi bombalara; kompyuter viruslarına; soxulcanlara; troya atlarına və s. bölünür.

Məntiqi bombalar – kompyuterdə daimi yerləşən və yalnız müəyyən şərtlər ödəndikdə yerinə yetirilən proqramlardır. Belə şərtlərə misal: verilmiş tarixin başlaması, kompyuter sisteminin müəyyən iş rejiminə keçməsi, bəzi hadisələrin müəyyən dəfə baş verməsi və s. ola bilər.

Kompyuter virusları – digər proqramlara yeridilmə yolu ilə müstəqil yayılan, müəyyən şərtlər yerinə yetirildikdə kompyuter sisteminə mənfi təsir göstərən kiçik proqramlardır.

Soxulcanlar – müstəqil, yəni başqa proqramlara yeridilmədən öz surətlərini kompyuter sistemlərində yaymağa və onları işə

salmağa qabil olan proqramlardır (virusun aktivləşməsi üçün yoluxmuş proqramın işə salınması tələb olunur). Soxulcanların axın kimi yayılması rabitə kanallarının, yaddaşın həddən artıq yüklənməsinə və son nəticədə sistemin bloka alınmasına gətirib çıxarır.

Troyanlar – funksional cəhətdən faydalı proqram kimi görünən ziyankar proqramlardır. İşə düşdükdə troyanlar elan edilmiş faydalı funksiyalarla yanaşı, elan olunmamış funksiyaları da yerinə yetirirlər.

Son vaxtlar ziyankar proqram təminatının yeni növləri meydana çıxmışdır:

Adware – istifadəçinin kompyuterində reklam göstərilməsi proqramlarıdır. Çox vaxt belə proqramlar rəsmi satılan məhsulların tərkibinə daxil olurlar, onların istehsalçıları öz proqram təminatlarının şərti pulsuz versiyalarını təklif edirlər.

Spyware – casus-proqramlar, kompyuter və istifadəçi haqqında fərdi məlumatların toplanması ilə məşğul olurlar: kompyuterin İP-ünvanı, əməliyyat sisteminin və İnternet-brauzerin versiyası, ən çox başvurulan İnternet-resursların siyahısı, axtarış sorğuları və sonrakı reklam kampaniyalarında istifadə edilə bilən digər verilənlər (çox vaxt Spyware ilə Adware bir məhsulda olur).

Keyloqqer (ing. key – klaviş və logger – loq yazan) – klaviaturada düymələrin basılmasını fayla (loqa) yazan proqramdır, onun köməyi ilə bədniyyətli konfidensial məlumatları (login, parol, kredit kartlarının nömrəsi, PIN-kodlar və s.) toplayır və istifadəçinin razılığı olmadan bədniyyətliyə göndərir, yəni keyloqqerlər Spyware proqram təminatına aiddir.

Snoopware (ing. **snoop** – özgəsinin işlərinə qarışan adam və soft**ware** – proqram təminatı) – iş prinsipi və məqsədləri Spyware ilə oxşardır. Adətən, snoopware korporativ və fərdi casusluq üçün istifadə edilir. Belə proqramların ən tipik nümayəndələri Catch Cheat Spy, SpectorSoft Eblaster, Spector və WinWhatWhere Investigator-dur. Snoopware mobil

telefonları da yoluxdurur və telefonun kamerasını işə salaraq çəkilmiş şəkilləri bədniyyətliyə göndərə bilir.

Proksi-proqramlar – faylların və ya poçt məlumatlarının (spamın) qəbulu və/və ya ötürülməsi üçün hədəf kompyuterin 'zombi' kimi istifadəsi üçün proqramlar.

Porno-dialerlər – Dial-Up birləşmədən istifadə etməklə pullu pornoqrafik resurslara giriş verən proqramlar, bu zaman birləşmənin qiyməti çox yüksəkdir;

Riskware – bəzi şərtlərdə istifadəçi üçün riskli ola bilən proqram təminatı (FTP, IRC, proxy, məsafədən administrator utilitləri).

Rutkit (rootkit) – ziyankar proqramların sistemdə fəaliyyətini maskalamaq üçün istifadə edilən proqram və ya proqramlar toplusudur. Bu topluya, adətən, sistemə müdaxilənin «izlərinin silinməsi» üçün müxtəlif utilitlər, snifferlər, skanerlər, keyloqqerlər, əməliyyat sisteminin əsas utilitlərini əvəz edən troya proqramları daxildir. Rootkit xakerə sındırılmış sistemdə möhkəmlənməyə və faylları, prosesləri, rutkitlərin sistemdə olmasını gizlətmək yolu ilə fəaliyyətinin izlərini ört-basdır etməyə imkan verir.

Rootkit termini tarixən Unix-sistemlərdən gəlmişdir və bu termin altında xakerin sındırılmış sistemin kompyuterində superistifadəçi hüququnu ələ keçirən kimi sistemdə işə saldığı utilitlər toplusu və ya nüvənin xüsusi modulu başa düşülür.

Sistemdə quraşdırılan rutkitləri nəinki istifadəçilər görmürlər, onları çox vaxt heç antivirus proqram təminatı da aşkarlaya bilmir. İstifadəçilərin çoxu sistemdə gündəlik iş üçün məhdud hüquqlu ayrıca uçot yazısı yaratmırlar və sistemə administrator kimi daxil olurlar, bunun hesabına bədniyyətlinin rutkitləri sistemdə quraşdırması məsələsi olduqca asanlaşır.

Butkit (ing. boot – yükləmə və kit – alətlər dəsti) – öz kodunu tərpənməz diskdə əsas yükləmə yazısına (ing. Master Boot Record) yazan ziyankar proqramdır. Bunun nəticəsində, diskə ilk müraciət zamanı idarəetmə butkitə verilir, butkit yaddaşa

yüklənir və o, tərpənməz diskə müraciətləri ələ keçirərək və onları dəyişərək öz iştirakını maskalayır.

Butkit əməliyyat sisteminin yüklənməsinə qədər yüklənərək, administrator (superistifadəçi) hüququ əldə edə və istənilən ziyankar əməlləri yerinə yetirə bilər. Məsələn, diskdə ümumiyyətlə mövcud olmayan müəyyən DLL faylı yaddaşa yükləyə bilər. Belə faylı antivirusların istifadə etdikləri üsullarla aşkarlamaq çox çətindir.

Droneware (ing. **drone** – idarə edilən mərmi və soft**ware** – proqram təminatı) kompyuterə məsafədən nəzarəti ələ keçirməyə imkan verən istənilən ziyankar proqramlar nəzərdə tutulur. Adətən, droneware spamın göndərilməsi, DDoS-hücumlar və digər qanunsuz əməllər üçün istifadə edilir.

Backdoor (ing. back door, arxa qapı) – sistemə sonradan təkrar giriş əldə etmək üçün sındırılmış kompyuterlərdə bədniyyətli tərəfindən ilk giriş zamanı quraşdırılan proqram və ya proqramlar toplusu. Qoşulma zamanı sistemə müəyyən giriş verir (bir qayda olaraq, bunlar komanda interpretatorudur: GNU/Linux-də – Bash, Microsoft Windows NT-də – cmd). Backdoor – rutkitin xüsusilə vacib komponentdir.

Məşhur BackDoor-lar antivirus sistemlərin bazasına daxil edilir. Yüksək peşəkar xakerlər özlərinin yazdıqları və ya dəyişiklik edilmiş BackDoor və rutkitlərdən istifadə edirlər, bu onların aşkarlanmasını və təmizlənməsini çətinləşdirir.

BackDoor-un əsas təyinatı – kompyuterin gizlincə idarə edilməsidir. Adətən, BackDoor yoluxmuş kompyuterdən faylları köçürməyə və əksinə, fayl və proqramları yoluxmuş kompyuterə göndərməyə imkan verir. BackDoor reyestrə məsafədən girməyə, sistem əməliyyatlarını (kompyuterin yenidən işə salınması, yeni şəbəkə resurslarının yaradılması, parolların modifikasiyası və s.) yerinə yetirməyə imkan verir. Mahiyyətcə, BackDoor istifadəçinin kompyuterində xaker üçün "arxa qapı" açır. Son vaxtlar BackDoor-un təhlükəsi artır – müasir şəbəkə soxulcanlarının çoxunda ya BackDoor olur, ya da onlar kompyuteri yoluxdurduqdan sonra orada BackDoor quraşdırırlar.

BackDoor-ların bir çoxu istifadəçinin kompyuterindən şəbəkəni daramaq, şəbəkə hücumları etmək üçün istifadə etməyə imkan verir.

Şell-kod (ing. shell – örtük və code – kod) – yerinə yetirilərək idarəetməni komanda örtüyünə (shell) verən proqram kodudur. Komanda örtüyü – Windows ƏS-də cmd.exe, Unix-sistemlərdə '/bin/sh'-dir. Şell-kod eksploytun «faydalı» hissəsi ola bilər.

Şell-kod komanda örtüyündən istifadə edərək xakerin əvvəlcədən müəyyən etdiyi şəbəkə portunu açа və bağlantını gözləyə bilər. Əksinə – xakerin kompyuteri ilə özü bağlantı qura bilər.

Örtüyün adı daxil olan sətirlər olduqda şəbəkə paketləri, demək olar ki, həmişə antiviruslarda şübhə yaradırlar. Şell-kodu aşkarlanmaqdan qorumaq üçün onu şifrləyir və özüdəyişən edirlər.

Eksployt (ing. exploit – istismar etmək) – xakerə müəyyən ziyankar hərəkətləri yerinə yetirməyə imkan verən proqram və ya komandalar çoxluğudur. Eksploytların əsas xüsusiyyəti – əməliyyat sistemlərinin modullarında və proqramlarda olan boşluqlardan istifadə etməsidir.

Eksploytlar uzaq və lokal olurlar. Uzaq eksploytlar sistemdə və ya proqramda əvvəlcədən xakerə məlum boşluqdan istifadə edərək sistemə və ya proqrama giriş əldə edirlər. Lokal eksploytlar əvvəlcə sistemə nüfuz edirlər, sonra orada işə düşərək xakerə giriş üçün lağım verirlər.

Eksploytu istənilən proqramlaşdırma dilində yazmaq olar (boşluqdan asılı olaraq). C/C++, Perl, PHP HTML ilə birlikdə JavaScript (brauzerlərdə işə salmaq üçün) dilləri daha tez-tez istifadə edilir.

Xakerlər, adətən, az məlum olan boşluqlardan istifadə edirlər. Bu boşluqlar məlum olduqdan və istehsalçılar onları bağladıqdan sonra bədniyyətlilər başqa boşluqlar axtarırlar. Xaker yeni boşluğu nə qədər tez aşkarlasa, eksploytu uğurla yerinə yetirməkdə onun şansı bir o qədər çox olur.

2.2.2. Şəbəkənin daranması

Şəbəkəyə hücum etməmişdən əvvəl bir sıra hazırlıq tədbirlərini yerinə yetirmək lazımdır. Dəqiq və sarsıdıcı zərbə endirmək və bu zaman ələ keçməmək üçün mümkün qədər çox informasiya toplamaq lazımdır. Buna görə də xakerlər təşkilatın informasiya təhlükəsizliyi sisteminə hər hansı aidiyyəti olan hər şeyi öyrənməyə cəhd edirlər. Bu prosesin sonunda xakerin əlində bütöv bir dosye (profil) olacaq, orada təşkilatın İnternetə qoşulma üsulları, şəbəkəyə məsafədən giriş imkanları, daxili şəbəkənin konfiqurasiyası təsvir olunur. Aşağıdakı kimi strukturlaşdırılmış metodologiyaya əməl edərək xaker ən müxtəlif mənbələrdən zərrə-zərrə istənilən təşkilat üçün dosye toplaya bilər.

Mərhələ 1. Fəaliyyət növünün müəyyən edilməsi. Hər şeydən əvvəl informasiyanın toplanması zamanı həyata keçirilən fəaliyyətin hüdudlarını müəyyən etmək zəruridir. Məsələn, təşkilatın bütün kompyuter şəbəkəsi, yoxsa onun yalnız müəyyən seqmenti (məsələn, əsas ofisin şəbəkəsi) haqqında məlumat toplanacağı dəqiq qərarlaşdırılır.

Mərhələ 2. Şəbəkənin inventarlaşdırılması. Şəbəkənin inventarlaşdırılmasında (ing. network enumeration) ilk addım konkret təşkilatla əlaqəli domen və şəbəkə adlarının müəyyən edilməsidir.

Mərhələ 3. DNS-serverləri dinləmə. Bütün domenləri tapdıqdan sonra DNS-serverlərlə işə keçmək olar. Əgər DNS-serveri maksimal təhlükəsizlik səviyyəsini təmin etməyə sazlanmayıbsa, onda onun köməyi ilə təşkilatın daxili şəbəkəsi haqqında informasiya əldə etmək olar.

Mərhələ 4. Şəbəkənin daranması. Mümkün şəbəkə ünvanlarını taparaq şəbəkənin topologiyasını və şəbəkəyə mümkün giriş yollarını müəyyən etməyə cəhd edirlər.

IP-şəbəkələrdə aşağıdakı darama metodlarını ayırmaq olar:

- ICMP-darama;
- TCP-darama;
- UDP-darama.

ICMP-darama

Kompyuter sisteminin ICMP-daranması kompyuter sisteminin qovşaqlarına ayrılmış IP-ünvanlara ICMP-sorğularının göndərilməsindən və bu sorğulara cavabların analizindən ibarətdir. Çox vaxt ICMP-darama 'Echo Request' tipli sorğuların köməyi ilə həyata keçirilir. Bir sorğu göndərildikdə ***zondlama*** haqqında, (diapazondan) bir neçə IP-ünvanın ardıcıl və ya eynizamanlı zondlanması həyata keçirildikdə ***darama*** haqqında danışırlar.

Hücum obyektinin ICMP-daranması hər şeydən əvvəl onun qovşaqlarını identifikasiya etməyə (hücum obyektinə ayrılmış IP-ünvanlardan hansına hücum obyekti qovşaqlarının uyğun olduğunu aydınlaşdırmağa) imkan verir. Göndərilmiş sorğuya ICMP protokolu ilə nəzərdə tutulmuş cavabın alınması qovşağın mövcudluğunu göstərir ('Echo Request' tipli sorğulara IP-şəbəkənin qovşaqları 'Echo Reply' tipli ICMP-məlumatlarla cavab verməlidirlər).

Şəbəkəni (kompyuter sisteminin qovşaqlarını) ICMP-daraqlamanın baza aləti **ping** utilitidir ('Echo Request' tipli sorğuları tətbiq edir).

Böyük şəbəkələrin daranması üçün ping utilitinin tətbiqi onunla çətinləşir ki, bu utilit bir dəfə işə salındıqda yalnız bir IP-ünvanı emal edir. Böyük sayda şəbəkə ünvanlarının daranmasını komanda ssenarilərinin (skriptlərin) və ya çoxsaylı xüsusi utilitlərin (fping, nmap, Pinger və başqaları) köməyi ilə avtomatlaşdırmaq olar.

TCP-zondlama

Kompyuter sisteminin TCP-zondlanması (daranması) kompyuter sisteminin qovşaqlarına ayrılmış IP-ünvanlara TCP-seqmentlərin müxtəlif növlərinin göndərilməsindən ibarətdir. Baxılan kompyuter sisteminin qovşaqlarının TCP-portlarının vəziyyətini (açıq, bağlı və ya bloklanmış (şəbəkələrarası ekran ilə süzülürlər)) aşkarlamaq məqsədi ilə bu seqmentlərə alınmış cavablar analiz edilir.

Zondlama ayrıca portun vəziyyətinin aşkarlanması proseduruna deyilir. Darama haqqında ümumi məqsədlə birləşmiş (məsələn, ayrıca qovşağın açıq portlarını müəyyən etmək və ya müəyyən portlar açıq olan hər hansı IP-ünvanlar diapazonunda qovşaqları müəyyən etmək) bir neçə ardıcıl və ya eynizamanlı zondlama həyata keçirildikdə danışırlar.

TCP-seqmentin növü TCP-başlıqda qoyulmuş bayraqlarla müəyyən edilir. SYN bayrağı qoyulmuş TCP-seqmentləri SYN məlumatları, SYN və ACK bayraqları qoyulmuş TCP-seqmentləri – SYN/ACK məlumatları və s. adlandırırlar.

TCP-zondlamanın geniş yayılmış metodlarına baxaq. Qeyd edək ki, bir zondlamanın çərçivəsində məlumatlar həmişə eyni bir porta göndərilir.

Tam bağlantılı TCP-zondlama (TCP connect probe). Bağlantı qurulması prosedurunu (handshake) tam yerinə yetirməklə obyektin qovşaqlarının portlarından biri ilə TCP protokolu üzrə virtual bağlantı qurmağa cəhd edilir. Əgər bu baş tutursa, zondlayan qurulmuş bağlantını kəsir. Əgər bağlantı qurmaq mümkün olursa, port açıq hesab edilir, əks halda tədqiq olunan port bağlı və ya bloklanmış hesab edilir.

Natamam bağlantılı TCP-zondlama (TCP half-open probe) və ya SYN-zondlama (ing. TCP SYN probe). Bağlantı qurulması prosedurunun yalnız birinci fazası həyata keçirilir. Əgər SYN məlumatına cavab olaraq SYN/ACK məlumatı daxil olursa, zondlayan hələ sona kimi qurulmamış bağlantını RST məlumatı göndərməklə kəsir. Əgər SYN məlumatına cavab olaraq SYN/ACK məlumatı alınırsa, onda tədqiq olunan port bağlı hesab edilir. Əgər SYN məlumatına cavab olaraq RST/ACK məlumatı alınırsa, onda tədqiq olunan port bağlı hesab edilir.

TCP FIN-zondlama (ing. TCP FIN probe). Tədqiq olunan porta FIN məlumatı göndərilir. Əgər bu port bağlıdırsa, onda TCP protokolunun standartına (RFC 793) uyğun olaraq, cavab kimi RST məlumatı göndərilməlidir.

"Milad yolkası" metodu ilə TCP-zondlama (ing. TCP Xmax Tree probe). Tədqiq olunan porta FIN/URG/PUSH məlumatı göndərilir. Əgər bu port bağlıdırsa, onda TCP protokolunun

standartına (RFC 793) uyğun olaraq, cavab kimi RST məlumatı göndərilməlidir.

TCP sıfır-zondlama (ing. TCP null probe). Tədqiq olunan porta bayraqlar qoyulmamış TCP-seqment göndərilir. Əgər bu port bağlıdırsa, onda TCP protokolunun standartına (RFC 793) uyğun olaraq, cavab kimi RST məlumatı göndərilməlidir.

Sonuncu üç metod RFC 793-ün müvafiq tələblərini ödəməyən ƏS-ləri (məsələn, MS Windows) üçün işləmir.

Tam bağlantı qurmaqla TCP-zondlama metodunu reallaşdırmaq çox sadədir, çünki praktiki olaraq bütün şəbəkə əməliyyat sistemlərinin tətbiqi proqramlaşdırma interfeysi müvafiq altproqramlara malikdir. Eyni zamanda, bu ən az gizli metoddur: praktiki olaraq istənilən əməliyyat sisteminin qeydiyyat jurnalında müvafiq qeydiyyatlar qalır. Ondan fərqli olaraq, digər metodlar əməliyyat sistemlərinin qeydiyyat jurnallarında iz buraxmırlar (lakin hücumları aşkarlayan xüsusi vasitələrin qeydiyyat jurnallarında iz qalır), çünki bağlantı qurulmasını nəzərdə tutmurlar; buna görə belə metodları stels-zondlama (stealth-) metodları da adlandırırlar.

UDP-zondlama

Kompyuter sisteminin UDP-zondlanması kompyuter sisteminin qovşaqlarına ayrılmış IP-ünvanlara UDP-dataqramların müxtəlif növlərinin göndərilməsindən ibarətdir. Baxılan kompyuter sisteminin qovşaqlarının UDP-portlarının vəziyyətini (açıq, bağlı) aşkarlamaq məqsədi ilə bu dataqramlara alınmış cavablar analiz edilir.

TCP-seqmentlərdən fərqli olaraq UDP-dataqramlarda bayraqlar olmur. Buna görə UDP-zondlama metodları TCP-zondlama metodları kimi rəngarəngliyi ilə seçilmirlər. Əgər UDP-dataqram göndərilən port bağlıdırsa, cavab olaraq 'Port Unreachable' tipli ICMP-məlumat göndərilməlidir. Əgər bu port açıqdırsa, onun cavabı portun məhz hansı serverlə dinlənilməsindən asılıdır; bir qayda olaraq, bu halda heç bir cavab göndərilmir.

Hücum obyektinin TCP- və UDP-zondlanması (daranması) aşağıdakılara imkan verir:

- hücum obyektinin aktiv qovşaqlarını identifikasiya etmək;
- hücum obyekti qovşaqlarının kommunikasiya xidmətlərini (serverləri) identifikasiya etmək;
- hücum obyekti qovşaqlarının əməliyyat sistemlərini identifikasiya etmək.

Kommunikasiya xidmətlərinin (serverlərin) və əməliyyat sistemlərinin identifikasiyası açıq portların nömrələrinə görə həyata keçirilir. Bir qayda olaraq hər bir xidmətə müəyyən potr nömrəsi təhkim edilir. Açıq portların bəzi kombinasiyaları yalnız bu və ya digər əməliyyat sistemləri üçün xarakterikdir (məsələn, 139 nömrəli açıq TCP-portu baxılan qovşağın MS Windows ailəsindən olan əməliyyat sisteminin idarəsi altında işlədiyini göstərir).

Ən məşhur TCP- və UDP-darama vasitələrindən SATAN, nmap, netcat göstərilə bilər.

2.2.3. DoS-hücumlar

DoS-hücumlar (xidmətdən imtina hücumları) – qanuni istifadəçilərin sistemə, şəbəkəyə, tətbiqi proqrama və ya informasiyaya girişini əngəlləmək üçün yerinə yetirilən bədniyyətli hərəkətlərdir. DoS-hücumlar bir çox formalara malikdir, onlar birmənbəli (bir sistemdən işə salınan) və ya paylanmış (bir neçə sistemdən işə salınan) olurlar.

DoS-hücum insidentləri texniki və qeyri-texniki vasitələrlə yaradıla bilərlər. Qeyri-texniki vasitələrlə yaradılan DoS-hücum insidentləri, məsələn, aşağıdakı faktorlardan qaynaqlana bilərlər:

- fiziki təhlükəsizlik sisteminin pozulması nəticəsində avadanlığın oğurlanması və ya sıradan çıxarılması;
- təbii təhdidlər (yanğın, daşqın və s.) nəticəsində avadanlığa ziyan vurulması;

– ətraf mühitdə ekstremal şərait, məsələn, yüksək temperatur (nəticədə hava-kondinsioner sistemi sıradan çıxır) və s.

Texniki vasitələrlə yaradılan DoS-hücumlar iki üsulla həyata keçirilə bilər. Birinci üsulda hücum edilən kompyuterdə proqram təminatının müəyyən boşluğu istifadə edilir. Bu boşluğun köməyi ilə kompyuterdə müəyyən kritik səhv yaratmaq və sistemin iş qabiliyyətinin pozulmasına səbəb olmaq olar.

İkinci üsulda hücum edilən kompyuterə eyni zamanda böyük sayda paketlər göndərməklə həyata keçirilir. Hər bir paket müəyyən müddətə emal olunur. Əgər bu vaxt yeni paket daxil olursa, o, növbəyə qoyulur və sistemin müəyyən resurslarını zəbt edir. Buna görə də, sistemə eyni vaxtda olduqca çox sayda paket göndərilsə, onda həddindən artıq yüklənmə nəticəsində kompyuter «boğula» və ya işini tam dayandıra bilər. DoS-hücum təşkilatçılarına da məhz bu lazımdır.

DoS-hücumun bir növü olan paylanmış DoS-hücum (Distributed Denial of Service, DdoS) – çox böyük sayda kompyuterin köməyi ilə təşkil edilir, bunun sayəsində hətta İnternet-kanallarının buraxma imkanı olduqca böyük olan serverlər də bu hücuma təslim olurlar.

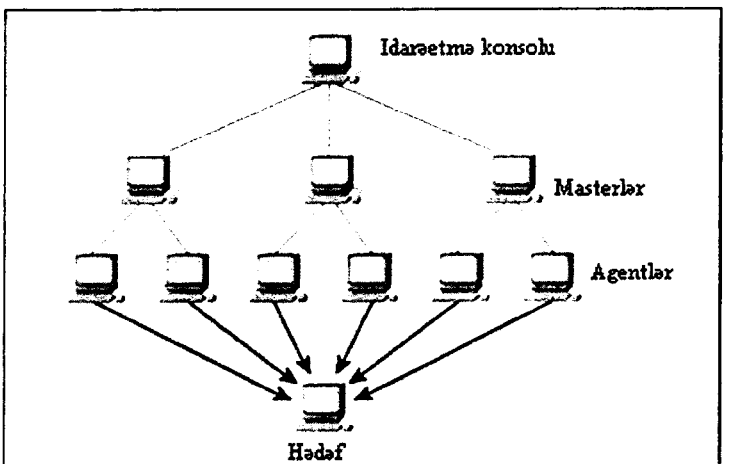
DDoS-hücumların təşkili üçün bədniyyətlilər kompyuterlərin xüsusi şəbəkəsindən – botnet-dən istifadə edirlər. Botnet (ing. botnet termini ro**bot** və **net**work – şəbəkə sözlərindən yaranmışdır) – bədniyyətliyə istifadəçinin xəbəri olmadan yoluxmuş kompyuteri məsafədən idarə etməyə imkan verən ziyankar proqramlarla – botlarla yoluxmuş kompyuterlərdən ibarət şəbəkədir. Bot istifadəçinin kompyuterində gizli quraşdırılan və bədniyyətliyə yoluxmuş kompyuterin resurslarından istifadə etməklə müəyyən əməlləri yerinə yetirməyə imkan verən proqramdır. Lazımi anda botnetin sahibinin komandasına əsasən bu proqram aktivləşir və hücum edilən serverə sorğular göndərməyə başlayır. Botnetlər spam göndərilməsi, konfidensial informasiyanın toplanması, DoS-hücumlar, fişinq hücumları üçün istifadə edilir.

DDoS-hücumlar zamanı bədniyyətlilər çox vaxt "DDoS klasteri" adlanan üçsəviyyəli arxitekturadan istifadə edirlər. Bu iyerarxik struktura aşağıdakılar daxildir (şəkil 2.1):

- idarəetmə konsolu (onlar bir neçə ola bilər) – məhz bu kompyuterdən bədniyyətli DDoS-hücumun başlaması haqqında siqnal verir;
- master-kompyuterlər – bu kompyuterlər idarəetmə konsolundan DDoS-hücum siqnalı alır və onu agentlərə ötürürlər. Hücumun miqyasından asılı olaraq bir idarəetmə konsoluna bir neçə yüzədək master-kompyuter düşə bilər.

agentlər – sorğularla hədəf-qovşağa bilavasitə hücum edirlər.

Bir qayda olaraq, həm master-kompyuterlər, həm də agent-kompyuterlər «zombi»lərdir, yəni onların sahibləri kompyuterlərinin DDoS-hücumların iştirakçıları olduqlarını bilmirlər.



Şəkil 2.1. DDoS hücumunun sxemi

Qeyd etmək lazımdır ki, bütün agentlər bir-birindən və bədniyyətlidən asılı olmadan avtonom rejimdə fəaliyyət göstərirlər. Hər bir agentin avtonom hərəkət etdiyini və hücumun aktiv komponentlərindən asılı olmadığını nəzərə alsaq, hətta bir

neçə agentin eyni zamanda neytrallaşdırılması belə bütün hücumu tamam dayandıra bilməz, çünki bu agentlərin sayı masterlərin köməyi ilə daim artırılır. Bundan başqa, masterlərin və agentlərin sayı heç nə ilə məhdud deyil.

DDoS-hücumların bir növü olan paylanmış dolayı DoS-hücumları (**Distributed Reflection DoS, DRDoS**) – İnternet şəbəkəsinin "vicdanlı" hostları vasitəsilə dolayı həyata keçirilir. DRDoS hücumunun klassik sxemi ondan ibarətdir ki, TCP-paket hücum edilən obyektin ünvanına deyil, ixtiyari hostun (reflektorun) IP-ünvanına ötürülür. Bu paketdə qayıtma ünvanı hücum obyektinin ünvanı ilə əvəz edilir. Əgər birinci paketdə mənbənin ünvanı olaraq hücum obyektinin ünvanı göstərilsə, SYN-bayrağı olan TCP sorğusuna cavab verəcək server bu ünvana SYN+ACK bayraqlı bir neçə TCP-paket göndərəcək. Yalan ünvan üzrə yalan sorğulara cavab verən güclü serverlər çoxluğundan istifadə etdikdə hücum edilən obyekt paketlər axını ilə boğulacaq.

DDoS-hücumların arasında aşağıdakı növlər seçilir:

UDP flood – hədəf-kompyuterin ünvanına çox sayda UDP paketi göndərilir. Bu metod ilk DoS-hücumlarda istifadə edilirdi, hazırda o qədər də təhlükəli deyil. Bu növ hücumdan istifadə edən proqramlar asanlıqla aşkarlanırlar, çünki masterlərlə agentlər mübadilə zamanı şifrlənməmiş TCP və UDP protokollarından istifadə edirlər.

TCP flood – hədəf-kompyuterin ünvanına çox sayda TCP paketləri göndərilir.

TCP SYN flood – hədəf-kompyuterə TCP-bağlantıların qurulması üçün çox sayda sorğular göndərilir, nəticədə o, özünün bütün resurslarını qismən açılmış bu bağlantıları izləməyə sərf edir.

Smurf – hücum obyektinin adından ICMP-əks-səda paketləri əvvəlcədən seçilmiş şəbəkəyə geniş yayımla göndərilir. Genişyayımlı ICMP-əks-səda sorğuları alan kompyuterlər hücum obyektinə ICMP-əks-səda cavabı göndərir. Beləliklə, bir paket göndərməklə bədniyyətli həm hücum obyektinə, həm də

genişyayımlı əks-səda sorğunu alan şəbəkəyə münasibətdə böyük həcmdə trafik yaradır.

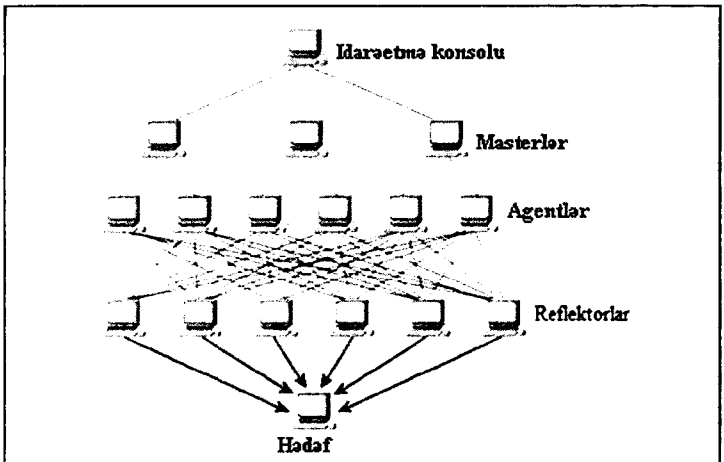
ICMP flood – mövcud olmayan hostların adından hücum edilən hosta çoxlu sayda ICMP-əks-səda sorğuları göndərilir. Əks-səda sorğuların mənbəyi mövcud olmayan hostlar olduğundan hücumun nəticəsində hücum obyektinin məhsuldarlığı, həmçinin rabitə kanalının buraxma qabiliyyəti aşağı düşür.

Bədniyyətlilər DDoS-hücumların bu növlərini kombinasiya edə bilərlər, bu hücumlar daha təhlükəli və çətin aradan qaldırılırlar. Onlara TFN və TFN2K misal göstərilə bilər, onlar xakerdən yüksək hazırlıq səviyyəsi tələb edir. DDoS-hücumların təşkili üçün proqramlardan biri də Stacheldracht ("tikanlı məftil") adlanır, ən müxtəlif hücum növləri və genişyayımlı pinq-sorğular seli təşkil etməyə imkan verir, masterlərlə agentlər arasındakı mübadilə şifrlənir.

Təəssüf ki, DDoS-hücumlardan mühafizənin universal metodları mövcud deyil. DDoS-hücumlardan mühafizə metodları hücumun növündən asılıdır. Lakin bəzi ümumi qaydalara əməl edilməsi DDoS-hücum risqlərini azalda və ya onun nəticələri ilə maksimal effektiv mübarizə aparmağa imkan verə bilər. Bir sıra belə tədbirlər mövcuddur: arzu olunmaz aktivliyi başlamağa imkan verən səbəblərin aradan qaldırılması, boşluqların aradan qaldırılması, bir-birindən asılı olmayan bir neçə serverin və güzgü saytın istifadə edilməsi, həm texniki, həm də hüquqi xarakterli tədbirlər daxil olmaqla DoS-hücum təşkilatçılarına aktiv cavab təsirlərinin göstərilməsi və s.

Marşrutizatorlarda və şəbəkə ekranlarında anti-spufinq və anti-DoS funksiyalarının savadlı konfiqurasiyası DoS hücumların təhlükəsini azaltmağa şərait yaradır. Bu funksiyalar yarıaçıq kanalların sayını məhdudlaşdırır və sistemi izafi yükləməyə imkan vermir.

DDoS-hücumların aşkarlanması üçün DDOSPing, Zombie Zapper, find_ddos kimi xüsusi proqram alətlərindən istifadə etmək olar.



Şəkil 2.2. DRDoS hücumunun sxemi

Müasir IDS/IPS sistemləri DDoS-hücumları aşkarlamağa imkan verir, lakin bu sistemlər daha yüksək səviyyəli rabitə operatoru ilə bağlantını mühafizə etmir. Bundan başqa, bu sistemlərin məhsuldarlığı hücumun öhdəsindən gəlməyə kifayət etmir.

Şəbəkə ekranlarında əvvəlcədən müəyyən edilmiş qaydalara əsasən DDoS-hücumların aşkarlanması və qarşısının alınması mexanizmləri var, lakin onlar çox sayda saxta İP-ünvandan bir nöqtəyə yönəlmiş DDoS-hücumların qarşısını ala bilmir.

DDoS-hücumların qarşısını almaq üçün operatorlar BlackHole ("qara deşik") texnologiyasından istifadə edirlər, bu zaman kliyentin ünvan fəzasında hücum edilən ünvanlar operatorun şəbəkəsində tam bloklanır (bağlanır). Bu metodu da uğurlu adlandırmaq olmaz, çünki hücum trafiki ilə yanaşı "xoşniyyətli" paketlər də atılır. Bədniyyətli faktiki olaraq operatorun köməyi ilə öz əsas məqsədinə çatır – hücum edilən resursa giriş bağlanır. Bundan başqa, BlackHole-da marşrutlama getdikcə daha incə olan müasir hücumlarla mübarizə üçün optimallaşdırılmayıb.

İzafi resursların tətbiqi – yükün istənilən pik artımı ilə bacaran əlavə buraxma zolağının və ya ehtiyat şəbəkə

qovşaqlarının alınması iqtisadi cəhətdən həmişə özünü doğrultmur. Bədniyyətliyə bu əlavə resursları tükətmək üçün yalnız hücumun miqyasını artırmaq gərəkdir.

2.2.4. Kibercasusluq

Kibercasusluq – təşkilatın və ya dövlətin maraqlarını pozmaq üçün informasiyanın oğurlanmasıdır. Korporativ sistemlərə icazəsiz girişlər bir çox halda kibercasusluq məqsədləri daşıyır.

Son dövrlər ABŞ və Çin hökümətləri müntəzəm olaraq bir-birini milli informasiya sistemlərindən strateji informasiyanın oğurlanmasına yönəlmiş gizli əməliyyatlar aparmaqda günahlandırırlar.

Toronto Universitetində 10 ay ərzində aparılmış tədqiqatlar nəticəsində 2009-cu ildə aşkarlanmış GhostNet kod adlı kibercasusluq şəbəkəsinə dünyanın 103 ölkəsindən 1295 kompyuter daxil idi. Bu kompyuterlərin təxminən üçdə biri xarici işlər nazirliklərində, səfirliklərdə, beynəlxalq təşkilatlarda, xəbər agentliklərində və qeyri-hökumət təşkilatlarında yerləşirdi. GhostNet əsas diqqətini Şərqi və Cənubi-Şərqi Asiya ölkələrinə, həmçinin Dalay Lamanın Hindistan, Brussel, London və Nyu-Yorkdakı ofislərinə yönəltmişdi. Çinə məxsus olduğu iddia edilən bu şəbəkə son iki il ərzində qurulmuşdu və hər həftə şəbəkəyə 10-dan çox yeni kompyuter əlavə edilirdi. GhostNet təkcə kompyuterləri axtararaq e-məktubları ələ keçirmirdi, yoluxdurulmuş kompyuterdə veb-kamera və mikrofonları işə salaraq ətrafdakı bütün danışıqları da yaza bilirdi.

SANS İnstitutunun tədqiqatları göstərir ki, son illər kibercasusluq dövlətlərarası münasibətlər çərçivəsindən çıxır və korporativ biznes dünyasına nüfuz edir. İşgüzar dairələrin və dövlət sektorunun getdikcə daha çox nümayəndəsi iqtisadi casusluğun obyektlərinə çevrilir. Bu hadisənin təhlükəsi artmaqdadır, çünki belə hücumların qurbanı ola biləcəklərini heç vaxt düşünməyən insanlar çox rahat hədəf olurlar və onların çoxu müdafiə olunmağa qətiyyən hazır deyillər.

Həm dövlət, həm də özəl sektoru təmsil edən "böyük resurslara malik" təşkilatlar tərəfindən maliyyələşdirilən kibercasusluq geniş yayılmağa başlayır. Bu, təşkilat rəhbərliyinin işgüzar danışıqlar zamanı müəyyən üstünlüklər qazanmaq istəyi ilə izah olunur. Kibercasusluq biznesin ən müxtəlif sahələrinə nüfuz edir və yeni məhsula aid gizli məlumatlardan tutmuş korporativ maliyyə durumuna kimi geniş məsələləri əhatə edir.

Şirkətlər potensial tərəfdaşlarla hələ münasibətlərin yaradılması prosesində xakerləri işə qoşurlar və onlar danışıqlar zamanı böyük əhəmiyyət daşıyan informasiyanı təşkilatların informasiya sistemlərindən oğurlayırlar.

Oğurlanmış biznes-məlumatların özəl sektor nümayəndələrinin maraqları üçün istifadə edilməsinə baxmayaraq, korporativ kibercasusluq fəaliyyəti bir çox halda dövlət "sponsorları" tərəfindən ciddi dəstəklənir. SANS bildirir ki, çox zaman kibercasusluq istiqamətlənmiş fişinqdən ibarət olur, onun məqsədi tez inanan əməkdaşları guya onlara tanış şəxslərdən gəlmiş e-məktublara cavab verməyə sövq etməkdir.

Ziyankar proqramlarla əlaqələndirilmiş belə məktubların məzmunu həqiqi sənədlərə çox oxşar olur, buna görə də istifadəçinin onları açması ehtimalı çox böyükdür. Belə məktublar tərtib olunarkən əməlləri gizlətmək və antivirus sistemlərdən yan keçmək üçün çox vaxt Microsoft Office paketində aşkarlanmış yeni boşluqlardan istifadə edirlər (onları "zero day" boşluqları adlandırırlar).

SANS İnstitutunun mütəxəssislərinə görə, "Kibercasusluğun biznes-məqsədlər güdən belə növü çoxlarının düşündüyündən də geniş yayılıb. Bunun real təsdiqləri var, şirkətlərin çoxu baş verənlər haqqında, nəhayət, kimsə məlumatların oğurlanmasını aşkarladıqda hüquq-mühafizə orqanlarından xəbər tuturlar".

Məlumatların insayderlər (şirkətin öz əməkdaşları) tərəfindən oğurlanması hallarının artacağı da proqnozlaşdırılır. İnsayderlər tərəfindən təhdidlərin artması amillərindən biri onunla əlaqədardır ki, bu halda hücumu həm təşkilatın lokal şəbəkəsində yerləşərək daxildən, həm də bədniyyətliyə məlum zəif yerlərdən istifadə etməklə xaricdən etmək olar.

Mobil qurğuların tətbiqi genişləndikcə, ənənəvi təhlükəsizlik perimetrləri getdikcə daha qeyri-müəyyən olur, bu qurğuların köməyi ilə əməkdaşlar korporativ şəbəkəyə öz iş yerlərindən kənarda da qoşula bilərlər. SANS ekspertlərinin fikrinə görə, son dövrlər əməkdaşların informasiyanı təşkilatdan çıxarması və qazanc məqsədi ilə onu satması üçün bir çox yeni üsullar meydana çıxmışdır.

Cəmiyyətin kibercasusluğa münasibətini aşkarlamaq məqsədi ilə Sophos təhlükəsizlik şirkətinin keçirdiyi sorğuda iştirak edənlərin üçdə ikisi bildirmişdir ki, kibercasusluq zəruridir, dövlətin iqtisadi və siyasi vəziyyətlərini dəstəkləməyə kömək edir.

Respondentlərin dörddə biri bildirir ki, xarici şirkətlərin şəbəkələrinin sındırılması və şəbəkələrdə ziyankar proqram təminatının quraşdırılması yolu ilə dövlətlərin bir-birini güdməsinə icazə vermək lazımdır. Respondentlərin yarıdan çoxu öz ölkəsinin digər ölkənin veb-saytına DDoS-hücum təşkil etməsini normal hesab edir.

2.2.5. Uyğunsuz istifadə insidentləri

Uyğunsuz istifadə – kompyuter və şəbəkə resurslarının təşkilatın informasiya təhlükəsizliyi siyasətinə və ya qanuna uyğun olmayan tərzdə istifadəsidir. Uyğunsuz istifadə resursların əyləncə və ya şəxsi qazanc üçün oğurlanmasından tutmuş resursların cinayət törətmək üçün istifadəsinə qədər uzanır. Məsələn, şəxs başqa bir şəxsi elektron məktubla hədələyir, istifadəçi proqram təminatının qanunsuz surətlərini P2P fayl paylaşımı xidməti ilə digər istifadəçilərə ötürür. Uyğunsuz istifadə insidentlərinə misal olaraq aşağıdakıları göstərmək olar:

- İnternetdən parol sındırma alətlərini və pornoqrafik materialları yükləmək;
- şəxsi biznesi reklam edən spam göndərmək;
- həmkarlarına narahatedici elektron məktublar göndərmək;
- təşkilatın kompyuterində icazəsiz veb-sayt yerləşdirmək;

- pirat materialları almaq və paylaşmaq üçün fayl və musiqi paylaşımı servislərindən istifadə etmək;
- konfidensial materialları təşkilatdan kənar yerlərə ötürmək.

Uyğunsuz istifadə insidentlərindən nisbətən daha geniş yayılmış, ciddi qanun pozuntusu pornoqrafik materialların saxlanması, istifadəsi və ötürülməsidir. Uyğunsuz istifadə insidentlərini aşağıdakı siniflərə bölmək olar:

- icazəsiz servislərdən istifadə (məsələn, veb-server, fayl paylaşımı, musiqi paylaşımı);
- uyğunsuz materiallara müraciət (məsələn, pornoqrafik materialları yükləmək, spam göndərmək);
- digər təşkilatlara qarşı hücumlar.

Adətən, uyğunsuz istifadə insidentləri informasiya təhlükəsizliyi ilə əlaqədar olmurlar. Bəzi uyğunsuz istifadə insidentləri digər təşkilatlara yönəlir, onlar müxtəlif problemlər yarada bilər. Digər təşkilatlara yönəlmiş uyğunsuz istifadə insidentlərinə misallar:

- təşkilatdan olan istifadəçi digər təşkilatın veb-saytını defeys edir (ing. deface – eybəcərləşdirmək, təhrif etmək; veb-saytın səhifəsi başqa səhifə ilə dəyişdirilir (adətən, baş səhifə dəyişdirilir, saytın qalan hissəsinə giriş bloklanır və ya saytın əvvəlki tərkibi tamam silinir));
- təşkilatdan olan istifadəçi oğurlanmış kredit kartı nömrələri ilə onlayn mağazalardan alış-veriş edir;
- üçüncü tərəf saxta e-poçt ünvanları ilə spam göndərir, bu ünvanlar təşkilata məxsus olur;
- üçüncü tərəf saxta IP-ünvanlardan paketlər generasiya etməklə digər təşkilata qarşı DoS hücumu edir, bu ünvanlar təşkilata məxsus olur.

Bu insidentləri bəzən o cəhət maraqlı edir ki, təşkilat hücumun əsas mənbəyi olmasa da, kənar təşkilatlara hücum edən tərəf kimi görünür. Belə insidentlər qısa müddətdə təhqiq olunmalı, sübutlar toplanmalı və insidentin təşkilatın şəbəkə və ya sistemlərindən başlayıb-başlamadığı müəyyən edilməlidir.

2.2.6. Hoax-proqramlar

Hoax [həuks] sözünün ingilis dilindən tərcüməsi "aldatma, hiylə, kələk (mistifikasiya)" deməkdir. Hoax-proqramların ideyası qazanc əldə etmək və ya konfidensial informasiyanı oğurlamaq məqsədi ilə istifadəçiləri aldatmaqdır. Son dövrlər bu sahənin kriminallaşması meyilləri müşahidə edilir: əvvəllər hoax-proqramlar nisbətən ziyansız hərəkətlər edirdilər – kompyuterin virusla və ya SpyWare-kodla yoluxmasını təqlid edirdilər, müasir hoax-proqramlar daha çox parolların və konfidensial informasiyanın oğurlanmasına yönəlirlər.

Hoax-proqramlar kompyuterlərə hər hansı birbaşa ziyan vurmurlar, ekrana xəbər çıxarırlar ki, belə ziyan vurulub, yaxud müəyyən şərtlərdə vurulacaq, ya da istifadəçiyə mövcud olmayan təhlükə barədə xəbərdarlıq edirlər.

Belə «pis zarafatlara», proqram müəllifinin «yumor hissindən» asılı olaraq ekrana müxtəlif qəribə məlumatlar çıxaran proqramları, məsələn, istifadəçini diskin format edildiyi xəbəri ilə «qorxudan proqramları» aid etmək olar (həqiqətdə isə disk format edilmir).

Məsələn, Hoax.DOS.INetCrack proqramı parol sındıran proqram kimi təqdim olunur. Əslində isə, heç bir parol sındırmır, bunun əvəzinə ekrana müxtəlif məlumatlar çıxarır, yaddaşda kiçik ölçülü rezident proqram yerləşdirir, bu proqram da məlumatlar çıxarır, ekranın rəngini dəyişir və bəzi hallarda da kompyuteri "asır".

Bəzi hoax-proqramlar istifadəçini inandırırlar ki, kompyuterində viruslar var və onu saxta antivirusu yükləməyə və aktivləşdirmək üçün pul ödəməyə sövq edirlər.

Hoax-proqramlar kompyuterə əsasən, bekdorların köməyi ilə və ya veb-saytda boşluğu işlətməklə yüklənirlər. (Bekdor (ing. back door, arxa qapı) – sistemə sonradan təkrar giriş əldə etmək üçün sındırılmış kompyuterlərdə bədniyyətli tərəfindən ilk giriş zamanı quraşdırılan proqram və ya proqramlar toplusudur. Qoşulma zamanı sistemə müəyyən giriş verir (bir qayda olaraq,

bunlar komanda interpretatorudur: GNU/Linux-də – Bash, Microsoft Windows NT-də – cmd))

Yalançı-antiviruslar İnternet-reklamdan, məsələn, istifadəçiləri bütün problemlərdən azad edən yeni "sehrli" məhsul haqqında məlumatlar olan reklam banerlərindən istifadə etməklə də yayılırlar. Belə "sehrli" məhsuldan imtina etmək mümkün olmur, "YES" və ya "NO" düyməsinin hər ikisi həmin proqramın gizli yüklənməsinə səbəb olur.

Kompyüterə gəlib çatan hoax-proqram gizli instalyasiya olunur (əgər istifadəçinin özü yükləyibsə, açıq instalyasiya). Bundan sonra şəraitdən asılı olaraq hərəkət edir, ekrana ya gizli təhlükə, ya da reyestrin, kitabxanaların işinin pozulması və s. barəsində məlumat çıxarır. Bundan sonra yalançı-proqram aşkarlanmış səhvləri aradan qaldırmaq və sistemi təmizləmək üçün antivirus almağı təklif edir. Ciddi proqram təminatının işi nə qədər düzgün təqlid olunsa, dələduzların yalançı antivirusa görə pul almaq şansı bir o qədər çox olur.

Yalançı antivirusu almağı qərara alan istifadəçiyə bir çox ödəniş üsulu təklif edilir – PayPal, American Express və s. Ödənişdən sonra istifadəçiyə aktivləşdirmə kodu verilir. Aldadılmasından şübhələnməməsi üçün hər iki halda kodun yoxlanması düzgün aparılır – ixtiyari kodu daxil etmək olmaz.

2.2.7. İcazəsiz giriş insidentləri

İcazəsiz giriş insidenti şəxs giriş hüququ olmayan resurslara giriş əldə etdikdə baş verir. Insidentlərin bu növü əsasən sistemə icazəsiz giriş cəhdlərindən və ya sistemin, servisin və şəbəkənin resurslarından icazəsiz istifadə hallarından ibarətdir. Adətən, icazəsiz giriş əməliyyat sistemində və ya tətbiqi proqramlarda olan boşluq istismar edilməklə, istifadəçi adlarını və parolları əldə etməklə və ya sosial mühəndislik vasitəsi ilə həyata keçirilir. Hücum edən bir boşluq vasitəsi ilə məhdud girişdən istifadə edərək nəticədə daha yüksək giriş hüquqları əldə edə bilər. Texniki vasitələrin köməyi ilə həyata keçirilən icazəzis giriş insidentlərinə aşağıdakı misallar göstərilə bilər:

- serverdə məsafədən administrator hüquqlarının ələ keçirilməsi;
- veb-saytın defeys edilməsi;
- parolların sındırılması;
- ödəniş cədvəlləri, tibbi məlumatlar, kredit kartı nömrələri kimi həssas məlumatlara baxmaq və onları kopyalamaq;
- istifadəçi adlarını və parolları tutmaq üçün kompyuterdə paket snifferindən istifadə etmək;
- pirat proqram təminatını və musiqi fayllarını yaymaq üçün anonim FTP serverdə icazə səhvlərindən istifadə etmək;
- müdafiəsiz modemə zəng edərək daxili şəbəkəyə giriş əldə etmək;
- vəzifəli şəxsin adından texniki dəstək bölməsinə zəng edərək onun e-poçt parolunu dəyişdirmək və yeni parolu öyrənmək;
- nəzarətsiz qalmış kompyuterdən icazəsiz istifadə etmək.

İcazəsiz giriş anlayışına korporativ şəbəkəyə kənardan (məsələn, e-poçt və İnternet vasitəsilə) hücumları, əməkdaşların konfidensial informasiyaya girişlərini, təşkilata məxsus verilənlərin kənar şəxslər tərəfindən oxunması və surətinin çıxarılması aid edilir. İstifadəçi tərəfindən informasiyaya öz xidməti vəzifələrini yerinə yetirmək üçün tələb ediləndən yüksək səviyyədə giriş hüququ əldə edilməsi də icazəsiz giriş insidentlərinə aid edilə bilər. İcazəsiz girişin tipik ssenariləri informasiyanın oxunması, surətinin çıxarılması, təhrif və məhv edilməsi, informasiyanın tutulması və qarşısının alınması (bloklanması), informasiyanın emalı proseslərinin əvəzlənməsi və s. ola bilər.

Qeyri-texniki vasitələrin köməyi ilə həyata keçirilən icazəzis giriş insidentinə misal fiziki mühafizə vasitələrini sıradan çıxardıqdan sonra informasiyaya icazəsiz giriş göstərilə bilər.

İcazəsiz giriş təhdidləri müasir informasiya sistemlərində ən təhlükəli təhdidlərdən biridir. Təşkilatların bir çoxunda

informasiyaya icazəsiz girişlə əlaqədar insidentlər qeydiyyata alınır.

Problem onunla mürəkkəbləşir ki, konfidensial informasiyaya icazəsiz giriş çox vaxt onun oğurlanması ilə müşaiyət edilir. Olduqca təhlükəli iki təhdidin belə kombinasiya nəticəsində təşkilata vurulan ziyan bir neçə dəfə arta bilər (oğurlanmış informasiyanın qiymətindən asılı olaraq).

2.2.8. İntellektual mülkiyyət insidentləri

Daşınan (avtomobil, mexanizm və s.), daşınmaz (torpaq, tikililər və s.) və intellektual mülkiyyəti fərqləndirirlər. İntellektual mülkiyyətin obyektləri insan intellektinin məhsulları olan hüquqi mühafizə obyektləridir.

"İntellektual mülkiyyət" anlayışı beynəlxalq hüquqi aktla – Ümumdünya İntellektual Mülkiyyət Təşkilatını (ÜİMT) təsis edən Konvensiya ilə (14 iyul 1967-ci il, Stokholm) müəyyən edilmişdir. Azərbaycan Respublikası bu Konvensiyaya 2005-ci ildə qoşulmuşdur. Konversiyada intellektual mülkiyyət aşağıdakılar aid olan hüquqlar kimi müəyyən edilir:

- ədəbi, bədii və elmi əsərlər;
- artistlərin ifaçılıq fəaliyyəti, səs yazıları, radio və televiziya verilişləri;
- insan fəaliyyətinin bütün sahələrində ixtiralar;
- elmi kəşflər;
- sənaye nümunələri;
- əmtəə nişanları, xidmət işarələri, firma adları və kommersiya işarələmələri;
- qeyri-sağlam rəqabətdən mühafizə;
- istehsalat, elm, ədəbiyyat və bədii sahələrdə intellektual fəaliyyətə aid bütün digər hüquqlar.

İnkişaf etmiş ölkələrin iqtisadiyyatı intellektual mülkiyyətə əsaslanır və onun qorunması iqtisadi inkişafın şərtlərindən biridir. 26 iyun 2000-ci ildə "Intellektual mülkiyyət üzrə Ümumdünya Bəyannaməsi" qəbul edilmişdir, burada iqtisadiyyatın və mədəniyyətin inkişafı üçün intellektual mülkiyyətin qorunmasının vacibliyi qeyd olunur.

İntellektual mülkiyyət sənaye mülkiyyətinə və müəlliflik hüquqlarına bölünür. Sənaye mülkiyyətinə ixtiralar (patentlər), əmtəə nişanları, sənaye nümunələri və əmtəənin mənşəyinin coğrafi göstəriciləri aid edilir.

İntellektual mülkiyyət bir çox təşkilat üçün əsas aktivdir, təşkilatların intellektual mülkiyyətlərinin qorunması onlar üçün həyati əhəmiyyət daşıyır, intellektual mülkiyyətlə bağlı insidentlərin cavablandırılması əhəmiyyətlidir. Məsələn, hesab olunur ki, istənilən amerikan firmasının fəaliyyətinin üçdə ikisi onun intellektual mülkiyyətidir. Maraqlıdır ki, ABŞ büdcəsində intellektual mülkiyyətin satışından əldə edilən gəlir, avtomobil satışından əldə edilən gəlirdən çoxdur.

McAfee şirkəti analitiklərinin 2010-cu ildə yerinə yetirdikləri "Kölgə iqtisadiyyatı: intellektual kapital və vacib korporativ məlumatlar kibercinayətkarların yeni valyutası kimi" adlı tədqiqat işində belə nəticəyə gəlirlər ki, kibercinayətkar ticarətinin obyekti kimi intellektual mülkiyyət □ istehsalat sirləri ("nou-hau"), marketinq planları, tədqiqatlar, məhsul nümunələri və hətta proqram təminatının ilkin kodları daha çox çəki qazanır. Bununla onlar təsbit edirlər ki, bədniyyətlilərin diqqəti və maraqları kommersiya sirri təşkil edən məlumatlara və satıla bilən digər məlumatlara doğru yönəlir.

AMEA İnformasiya Texnologiyaları İnstitutunda hazırlanmış və nəşr edilmiş "İnternet mühitində intellektual mülkiyyət hüquqlarının qorunması məsələləri" ekspress-informasiya vəsaitində İnternet mühitində intellektual mülkiyyət hüquqlarının qorunması problemlərinə və onların tənzimlənməsi məsələlərinə baxılır. Bu istiqamətdə mövcud olan müxtəlif yanaşmalar, ziddiyyətli məqamlar, beynəlxalq hüquq normaları, qabaqcıl ölkələrin təcrübəsi araşdırılır, çatışmazlıqlar təhlil edilir.

2.2.9. Sosial mühəndislik insidentləri

Bir çox tədqiqatçıya görə, sosial mühəndislik metodları XXI əsr xakerlərinin əsas alətlərindən biridir.

Sosial mühəndislik (ing. social engineering) – tətbiqi sosiologiyanın insanın davranışını müəyyən edən və ona nəzarəti təmin edən təşkilati strukturların məqsədyönlü dəyişdirilməsinə yönəlmiş yanaşmalar məcmusudur. İnformasiya texnologiyaları sahəsində sosial mühəndisliyi çox vaxt informasiyaya giriş əldə etməyə yönəlmiş tədbirlər kimi qəbul edirlər.

Sosial mühəndislik psixologiyanın və sosiologiyanın qanunlarına əsaslanır, digər insanları manipulyasiya etmək bacarığı ilə həyata keçirilir. Öz növbəsində, manipulyasiya insanın elementar zəifliklərinə əsaslanır: lovğalıq, şöhrətpərəstlik, qorxu, mərhəmət, qulluq göstərmə və s.

Sistemli yanaşma baxımından sosial mühəndislik ondan çıxış edir ki, orta statistik istifadəçi müəyyən ortabab xarakteristikalara malik olur. Sosial mühəndislik insana sistemin bir hissəsi kimi baxır, insan həmin sistem haqqında fundamental biliklərə malik olmur. Əks halda, sosial mühəndislik işləmir – insan onu əhatə edən mühit haqqında nə qədər çox məlumatlıdırsa, sosial mühəndislik üsullarının işləməsi ehtimalı bir o qədər azdır.

Tərs sosial mühəndisliyin (ing. reverse social engineering) məqsədi, hədəfi "kömək" üçün bədniyyətlinin özünə müraciət etməyə məcbur etməkdir. Bu məqsədlə bədniyyətli, məsələn, reklamdan: "əgər kompyuterinizdə nasazlıq olarsa, bu nömrəyə zəng edin" tipli elandan istifadə edə bilər.

Fisinq – (ing. phishing – password – parol və fishing – balıq ovu, aldatma) – İnternet dələduzluğun bir növüdür, məqsədi istifadəçilərin konfidensial məlumatlarını (parollar, kredit kartı nömrələri, PİN-kodlar və s.) ələ keçirməkdir.

Fişinq zamanı dələduzlar istifadəçini aldadıb xüsusi olaraq hazırlanmış saxta saytlara (real mövcud olan populyar saytların kopyalarına) aparırlar. İstifadəçini tovlamaq üçün həqiqi saytların sahibləri (ödəniş sistemlərinin, bankların,

provayderlərin) adından kütləvi və ya fərdi e-poçt göndərişləri istifadə edilir.

Adətən, belə məktublar hansısa hadisələr (verilənlərin itməsi, sistemdə qəzalar və s.) barədə bildirişlər şəklində gəlir, onlarla əlaqədar olaraq istifadəçi müəyyən konfidensial verilənləri təqdim etməli, yeniləməli və ya təsdiqləməlidir. Bu zaman məktubda link göstərilir, bu link servisin rəsmi veb-səhifəsinə deyil, onun dəqiq kopyasına aparır. Saxta saytda istifadəçi tərəfindən daxil edilmiş informasiya dələduzların əlinə keçir.

Fişinqə klassik misal: guya ki, ödəniş sisteminin təhlükəsizlik xidmətindən gələn elektron məktubda parolu dəyişmək xahiş edilir. Məltubda göstərilən ünvana gedən istifadəçi ödəniş sisteminin kopyası olan sayta düşür. Bu saytda öz fərdi məlumatlarını daxil edən istifadəçi öz hesabına nəzarəti faktiki olaraq bədniyyətliyə verir.

Farminq (ing. pharming) – konfidensial informasiyanın toplanması üçün təşkilatların rəsmi veb-saytlarına daxil olmağa çalışarkən istifadəçilərin xüsusi olaraq yaradılmış saxta veb-saytlara avtomatik yönləndirilməsidir. Fişinqdən daha təhlükəli dələduzluq üsuludur. Farminq zamanı çox zaman maliyyə və kommersiya təşkilatlarının veb-səhifələri saxtalaşdırılır.

Klassik fişinq sxemində əsas "zəif" nöqtə istifadəçidən asılılıqdır – o, fişerə inanacaq, yoxsa yox. Banklar, sosial şəbəkələr və digər veb-xidmətlər istifadəçiləri sosial mühəndislik metodları istifadə edilən müxtəlif dələduzluq üsulları haqqında xəbərdar edirlər. İstifadəçilərin məlumatı artdıqca onları saxta saytlara cəlb etmək çətinləşir. Buna görə də bədniyyətlilər istifadəçiləri fişinq saytlarına cəlb etmək üçün farminq mexanizmini fikirləşmişlər, burada istifadəçinin iştirakı minimuma endirilib.

Skamminq (ing. scamming) – bu gün ən populyar dələduzluq sxemlərindən biridir, istifadəçilərdən kifayət qədər məbləğdə pul qoparmağa imkan verir. Skamminqin mahiyyəti yalan məlumat olan məktublar göndərməkdən ibarətdir.

Məsələn, istifadəçiyə məktub göndərirlər ki, o, lotereyanın qalibi olmuşdur və uduşu almaq üçün göstərilən hesaba o qədər də böyük olmayan məbləğdə pul köçürmək lazımdır. İstifadəçilərə ofşor müəssisələrə və daşınmaz əmlaka pul qoymaq da tez-tez təklif edilir.

Adətən, dələduzlar istifadəçidən kiçik məbləğdə pul köçürməyi – bir neçə sentdən bir neçə dollara kimi xahiş edirlər. Bu məbləğlərin kiçikliyini nəzərə alan bəzi istifadəçilər risq edirlər və bu gün artıq dövriyyələri milyonlarla olan kiberdələduzların hesabına pul köçürürlər.

Başqa bir skamminq sxemində skammer (kişi və ya qadın) tanışlıq saytında özgələrinin fotoşəkilləri və uydurma məlumatlarla saxta anket yerləşdirir. Bundan sonra varlı adaxlı və ya gəlin seçilir. Dələduz onunla fəal yazışmaya girişir, inam münasibətləri yaratmağa çalışır və məhəbbət münasibətlərini təqlid edir. Fırıldaqçının əsas məqsədi öz qurbanını ələ almaq, onu aralarında müəyyən hisslərin yarandığına inandırmaqdır.

Bundan sonra pul qoparılması başlayır. Burada konkret vəziyyətdən asılı olaraq variantlar çox ola bilər. Məsələn, dələduz sevgilisinin yanına köçməyə razılıq verə və bunun üçün müəyyən məbləğ xahiş edə bilər. Yalnız təyyarə biletinin pulunu ödəməyi xahiş edə bilər, sonra bileti geri qaytararaq nəğd pulu götürə bilər. Qəfildən xəstələnə və müalicə xərclərini ödəməyi xahiş edə bilər. Daha çox sadə vəziyyətlərə rast gəlinir, skammer öz tərəfdaşından telefon hesablarını ödəməyi xahiş edir, ödəniş edildikdən sonra yazışmalar kəsilir və növbəti qurban axtarışı başlayır.

Vişinq (ing. vishing) – fişinqin bir növüdür, parollar, bank kartlarının nömrəsi və s. kimi konfidensial məlumatların oğurlanması üçün Wardialers (nömrəyə avtomatik zəng edən) istifadə etməkdən və İnternet-telefoniyanın (VoIP) imkanlarından istifadə etməkdən ibarətdir.

Secure Computing-in məlumatına əsasən Wardailer konfiqurasiya edilir, müəyyən nömrəni yığır və zəngə cavab zamanı aşağıdakılar baş verir:

- Wardialer istifadəçini onun kartı ilə bağlı dələduzluq əməlləri barəsində xəbərdar edir və müəyyən nömrəyə dərhal zəng etməyi təklif edir;
- bu nömrəyə zəng edən istifadəçiyə kompyuter səsi ilə bildirilir ki, məlumatları yoxlamaq üçün telefon klaviaturasından kartın nömrəsi daxil edilməlidir;
- nömrə daxil edilən kimi vişer bədniyyətli məqsədlər üçün zəruri olan bütün məlumatlara (telefon nömrəsi, tam adı, ünvan) sahib olur;
- sonra bu zəngdən istifadə edərək əlavə informasiya da toplamaq olar: PİN-kod, kartın istifadə müddəti, bank hesabının nömrəsi, təvəllüd və s.

2.3. İnsident haqqında məlumatların mənbələri

İnsidentlər haqqında bir çox mənbədən məlumat almaq olar, daha geniş yayılan mənbələr informasiya təhlükəsizliyi üzrə proqram təminatı, loq-fayllar, açıq informasiya və insanlardır. Aşağıda bu mənbələrin hər biri haqqında məlumat verilir.

Müdaxilələrin aşkarlanması sistemləri (Intrusion Detection System, IDS). IDS-məhsullar şübhəli hadisələri identifikasiya etməyə və onlara aid müvafiq verilənləri qeydiyyata almağa xidmət edirlər, verilənlərə aşkarlanmış hücumun tarixi və zamanı, hücumun növü, başlanğıc və son IP-ünvanlar, istifadəçinin adı (əgər mümkün və məlumdursa) və s. aiddir. IDS-məhsulların bir çoxu şübhəli aktivliyi aşkarlamaq üçün siqnaturalardan istifadə edirlər; yeni hücumların aşkarlana bilməsi üçün sinaturalar yenilənməlidir. IDS proqram təminatı tez-tez səhv pozitivlər (*false positives*) – həqiqətdə olmayan şübhəli aktivlik barəsində həyəcan siqnalları generasiya edir. Analitik IDS həyəcan siqnallarının düzgünlüyünü yazıya alınmış və ya digər mənbələrdən alınmış əlaqədar verilənləri diqqətlə analiz edərək yoxlaya bilər. Mühitlərin bir çoxunda IDS-lərin bir neçə növü yerləşdirilməlidir (host, şəbəkə, naqilsiz şəbəkə IDS-

ləri, müdaxilələrin qarşısının alınması sistemləri – Intrusion Prevention System (IPS)).

Antivirus, anticasus və antispam proqram təminatı. Antivirus və anticasus proqram təminatı ziyankar kodların müxtəlif növlərini aşkarlayır və onların hostları yoluxdurmasının qarşısını alır. Antivirus və ya anticasus proqram təminatı ziyankar kodu aşkarladıqda, adətən, həyəcan siqnalları generasiya edir. Hazırki antivirus və anticasus proqram məhsulları ziyankar kodları onların siqnaturaları yeniləndikdə aşkarlaya və qarşısını ala bilir. Bu yenilənmə işi böyük təşkilatlarda güc yetməyən iş ola bilər. Bunun öhdəsindən gəlməyin bir yolu antivirus və anticasus proqram təminatının mərkəzləşdirilmiş şəkildə yenilənməsini və idarə edilməsini təşkil etməkdir. Aşkarlama imkanı müxtəlif olduğundan bəzi təşkilatlar bir neçə istehsalçının məhsulundan istifadə edir. Antivirus proqram təminatı ən azı iki səviyyədə qurulmalıdır: şəbəkə perimetrində (məsələn, şəbəkə ekranları, e-poçt serverləri) və host səviyyəsində (məsələn, işçi stansiyaları, fayl serverləri, kliyent proqram təminatı). Antivirus proqram təminatının casus proqramları aşkarlama imkanı yetərli olmadıqda anticasus proqram təminatı istifadə edilməlidir; anticasus proqram təminatı da antivirus proqram təminatı kimi iki səviyyədə yerləşdirilir.

Antispam proqram təminatı spamı aşkarlamaq və onların istifadəçilərin poçt qutularına düşməsinin qarşısını almaqdır. Spamda ziyankar proqramlar, fişinq-hücumları və digər ziyankar kontent ola bilər, buna görə də antispam proqram təminatının həyəcan siqnalları hücum cəhdlərini göstərə bilər.

Faylların tamlığını yoxlayan proqram təminatı. İnsidentlər vacib fayllarda dəyişikliklərə səbəb ola bilərlər; faylların tamlığını yoxlayan proqram təminatı belə dəyişiklikləri aşkarlaya bilər. Onlar seçilmiş fayllar üçün nəzarət cəmini hesablamaq üçün kriptoqrafik heş funksiyalardan istifadə edirlər. Əgər faylda dəyişiklik edilibsə, onda yenidən hesablanmış nəzarət cəmi çox böyük ehtimalla köhnə nəzarət cəmi ilə üst-üstə düşməyəcək.

Nəzarət cəmlərini müntəzəm olaraq hesablayıb əvvəlki qiymətlərlə müqayisə edərək fayllarda dəyişiklik edildiyini aşkarlamaq olar.

Monitorinq xidməti. Bəzi təşkilatlar özlərinin onlayn servislərinin, məsələn, veb, DNS (Domain Name System) və FTP serverlərinin monitorinqini həyata keçirirlər, bunun üçün üçüncü tərəfin xidmətindən də istifadə edilə bilər. Monitorinq xidməti hər *x* dəqiqədən bir hər bir servisə avtomatik qoşulmağa cəhd edir. Əgər servisə qoşulmaq mümkün olmursa, məonitorinq xidməti müəyyən edilmiş üsullarla, məsələn, telefon zəngi, e-poçtla və s. təşkilata xəbər verir. Bəzi monitorinq xidməti müəyyən resurslarda, məsələn, veb-səhifədə dəyişiklikləri aşkarlaya və məlumat verə bilər. Monitorinq xidməti əsasən istismar fəaliyyəti baxımından faydalıdır, bununla yanaşı DoS-hücumlar və serverlərin dayanması ilə bağlı insidentlər üçün də məlumat mənbəyi ola bilər.

Loq-fayllar

Əməliyyat sistemlərinin, servislərin və tətbiqi proqramların loq-faylları. Əməliyyat sistemlərinin, servislərin və tətbiqi proqramların loq-faylları (xüsusən, auditlə əlaqəli verilənlər) insident baş verdikdə böyük qiymətə malik olurlar. Loqlar hansı uçot yazısı ilə sistemə girildiyi və hansı əməliyyatların yerinə yetirildiyi kimi qiymətli məlumatlar verə bilər. Bundan başqa, loqlar bir hadisədə neçə hostun daranmasını müəyyən etmək üçün hadisələrin agreqasiyasında da yardımçı ola bilər. Təəssüf ki, bir çox insidentlər zamanı loqlarda sübutlar olmur, çünki hostlarda ya loq yazılması imkanı bağlanıb, ya da düzgün konfiqurasiya edilməyib. İnsidentlərin effektiv emalına şərait yaratmaq üçün təşkilatlar bütün sistemlərdə loq yazılmasının baza səviyyəsini, kritik sistemlərdə isə yüksək baza səviyyəsini tələb etməlidirlər. Bütün sistemlərdə audit qoşulu vəziyyətdə olmalı və audit hadisələri, xüsusən də administratorluq səviyyəsindəki fəaliyyət loqlarda yazılmalıdır. Bütün sistemlərdə loq yazılmasının düzgün işlədiyi və loq standartlarına əməl

edilməsi periodik olaraq yoxlanmalıdır. Əlavə olaraq, loqlar düzgün rotasiya edilməli və saxlanmalıdırlar. Saxlanma zamanı loqlarda dəyişiklik edilmədiyini aşkarlamaq üçün loq-faylların tamlığı yoxlanmalıdır. Hadisə məlumatlarının korrelyasiyası yolu ilə loq-fayllar analiz üçün istifadə edilə bilər. Hadisə məlumatlarından asılı olaraq insidenti bildirmək üçün həyəcan siqnalı generasiya edilə bilər. Loq-faylların mərkəzləşdirilmiş yazılmasını həyata keçirmək üçün informasiya təhlükəsizliyi hadisələrinin idarə edilməsi (Security Event Management (SEM) və Security Information and Event Management (SIEM)) üzrə müxtəlif proqram təminatı mövcuddur.

Şəbəkə qurğularının loqları. Adətən, şəbəkə ekranları və routerlər kimi şəbəkə qurğularının loqları insidentlərin haqqında ilkin mənbələr kimi istifadə edilmir. Çox vaxt bu qurğular bloklanmış giriş cəhdlərinin loq-fayla yazılmasına konfiqurasiya edilirlər, lakin aktivliyin təbiəti haqqında az informasiya verirlər. Buna baxmayaraq, onlar trendlərin aşkarlanmasında (məsələn, konkret porta giriş cəhdlərinin sayında əhəmiyyətli artım) və digər qurğuların aşkarladığı hadisələrin korrelyasiyasının müəyyən edilməsində əhəmiyyətli ola bilərlər.

Açıq mənbələrdən olan məlumatlar

Yeni boşluqlar və eksploytlar haqqında məlumatlar. Yeni boşluqlar və eksploytlar haqqında daim məlumatlı olmaq bəzi insidentlərin baş verməsinin qarşısını ala, onların aşkarlanması və analizində kömək edə bilər. NVD bazasında boşluqlar haqqında informasiya toplanır. US-CERT, CERT®/CC kimi bəzi təşkilatlar brifinqlər, veb-postinqlər, e-poçt göndəriş siyahıları vasitəsi ilə periodik olaraq yeni boşluqlar və təhdidlər haqqında informasiya ilə təmin edirlər.

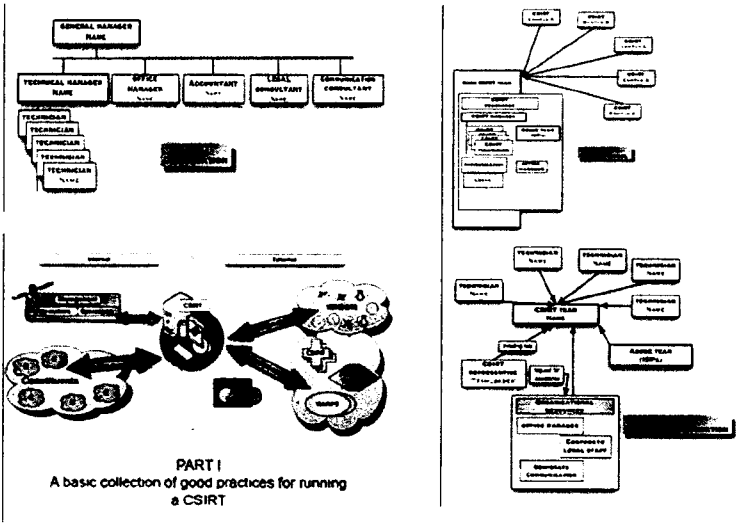
Digər təşkilatlarda olan insidentlər haqqında məlumatlar. Digər təşkilatlarda baş vermiş insidentlər haqqında hesabatlar qiymətli informasiya verə bilər. Bir sıra veb-səhifələr və göndəriş siyahıları var ki, insident cavablandırma komandaları və təhlükəsizlik üzrə ekspertlər qarşılaşdıqları insidentlər və

hücumlar haqqında təcrübələrini burada paylaşırlar. Bəzi təşkilatlar digər təşkilatlarda loqları və IDS həyəcan siqnallarını qəbul edir, onların konsolidasiyasını aparır və analiz edir.

İnsanlar

Təşkilat daxilindəki insanlar. İstifadəçilər, sistem administratorları, şəbəkə administratorları, informasiya təhlükəsizliyi əməkdaşları və təşkilat daxilindəki digər insanlar insidentlərin əlamətləri haqqında məlumat verə bilərlər. Belə məlumatların hamısının həqiqiliyini yoxlamaq vacibdir. Təkcə adi istifadəçilər insidentin baş verdiyini müəyyənləşdirəndə çətinlik çəkmirlər, bəzən hətta ən yaxşı texniki ekspertlər də səhv edə bilərlər. Yanaşmalardan bir belə məlumat verən şəxslərdən bu məlumatların dəqiqliyinə onların nə qədər əmin olmasını soruşmaqdır. Təqdim olunan informasiya ilə birlikdə bu qiymətləndirmənin də qeydiyyata alınması insidentin analizi zamanı, xüsusən də ziddiyyətli məlumatlar aşkarlandıqda əhəmiyyətli kömək edə bilər.

Digər təşkilatlardan olan insanlar. Digər təşkilatlardan olan insanlardan az sayda insident bildirişləri alınsa da, onlara ciddi yanaşmaq lazımdır. Buna klassik misal, sistemdə ciddi boşluq aşkarlayan və bu haqda təşkilata birbaşa məlumat verən və ya açıq mənbələrdə bildirən şəxs ola bilər. Başqa misal, digər təşkilatın əlaqə yaradaraq təşkilatdan kiminsə ona hücum etdiyini bildirməsidir. Kənar istifadəçilər də insidentlər, məsələn, veb-saytın defeys edilməsi və ya servisin əlyetməz olması haqqında məlumat verə bilərlər. Digər insident cavablandırma komandaları da insidentlər haqqında məlumat göndərə bilərlər. Burada kənar təşkilatların insidentlər haqqında məlumat verməsi üçün müvafiq mexanizmlərin olması və təlim görmüş heyətin bu mexanizmləri diqqətlə monitorinq etməsi vacibdir; bunu telefon nömrəsi və e-poçt ünvanını müəyyən etmək və məlumatları lazımi servis strukturuna yönləndirməklə etmək olar.



FƏSİL 3

CSIRT MODELLƏRİ

CSIRT MODELLƏRİ

- **CSIRT-in təşkilati modelləri**
- **CSIRT komandalarının növləri**
- **Milli CSIRT**
- **Milli CSIRT-in yaradılması mərhələləri**
- **CSIRT komandasının strukturu**
- **CSIRT-in texniki infrastrukturu**
- **İnsidentləri cavablandırma siyasəti**

FƏSİL 3 CSIRT MODELLƏRİ

3.1. İnsidentləri cavablandırma komandası

İnformasiya təhlükəsizliyi insidentlərinin cavablandırılması təşkilatın bir çox bölmələrinin əməkdaşlarının iştirakını tələb edən mürəkkəb və kompleks prosesdir. ISO/IEC TR18044 standartına uyğun olaraq informasiya təhlükəsizliyi insidentlərinin təhqiqatı üzrə xüsusi komanda – CSIRT komandası yaratmaq zəruridir. Bu komandanın əsas məqsədləri aşağıdakılardır:

- insidentlərin uçotu, cavablandırılması və analizi üçün təşkilatın ixtisaslı heyətlə təmin edilməsi;
- insidenti cavablandırma prosesinin zəruri əlaqələndirmə və idarəetmə ilə təmin edilməsi;
- rəhbərliyin və maraqlı şəxslərin lazımi səviyyədə məlumatlandırılmasının təmin edilməsi;
- insidentin nəticələrinin həm maddi sahədə, həm də təşkilatın nüfuzunun qorunması üçün maksimal azaldılmasının təmin edilməsi.

İnsidenti cavablandırma prosesinin təşkili aşağıdakı məqsədləri güdür.

- icazəsiz hərəkətlərin qarşısını almaq və insident baş verdikdə təşkilatın iş qabiliyyətini ən qısa müddətdə bərpa etmək;
- informasiya təhlükəsizliyi insidenti faktını təsdiq və ya təkzib etmək;
- informasiya təhlükəsizliyi insidentlərinin lokallaşdırılması və nəticələrin aradan qaldırılması;
- baş vermiş insident haqqında müfəssəl hesabat və faydalı tövsiyələr təqdim etmək. Kompyuter insidentləri haqqında dəqiq informasiyanın toplanması və saxlanması

üçün şərait yaratmaq. Oxşar insidentlərin gələcəkdə tez aşkarlanmasını və/və ya qarşısının alınmasını təmin etmək ("keçilmiş dərslərin" analizi, informasiya təhlükəsizliyi siyasətinin dəyişdirilməsi, informasiya təhlükəsizliyi sisteminin modernləşdirilməsi və s. yolu ilə);

- baş vermiş sübutların saxlanmasını və bütövlüyünü təmin etmək. Günahkar şəxslərin və onların motivasiyalarının müəyyən edilməsi, onların məsuliyyətə cəlb edilməsi imkanının təmin edilməsi. Bədniyyətliyə(lərə) qarşı mülki və cinayət işlərinin qaldırılması üçün şərait yaratmaq;
- İT-sistemin iş nizamının pozulmasını və verilənlərin korlanmasını minimumlaşdırmaq. İT-sistemin konfidensiallığının, tamlığının və əlyetərlik pozulması nəticələrini minimumlaşdırmaq;
- təşkilatın nüfuzunu və aktivlərini mühafizə etmək;
- insidenti cavablandırma prosesi haqqında təşkilat əməkdaşlarını təlimatlandırmaq.

3.2. CSIRT-in təşkilati modelləri

CSIRT üçün beş əsas təşkilati model mövcuddur. Müxtəlif şərtlər, məsələn, ətraf mühit, maliyyə imkanları və insan resursları nəzərə alınmaqla təşkilat üçün ən əlverişli CSIRT modeli seçilməlidir:

1. Təhlükəsizlik xidməti modeli (mövcud IT-heyətdən istifadə etməklə);
2. Daxili paylanmış CSIRT modeli;
3. Daxili mərkəzləşdirilmiş CSIRT modeli;
4. Hibrid paylanmış və mərkəzləşdirilmiş CSIRT modeli;
5. Koordinasiya CSIRT modeli.

Təhlükəsizlik xidməti modeli

Təhlükəsizlik xidməti modeli CSIRT üçün tipik model hesab edilmir. O, mahiyyətcə, CSIRT-in ümumi qəbul edilmiş modelinə ziddir. Bu modeldə informasiya təhlükəsizliyi

insidentlərinin emalına məsul olan mərkəzləşdirilmiş təşkilat yoxdur. Bunun əvəzinə, insidentlərin emalı üzrə məsələlər sistem və şəbəkə administratorları və ya təhlükəsizlik xidmətinin digər mütəxəssisləri tərəfindən həll edilir.

Daxili paylanmış CSIRT modeli

Bu modeli *paylanmış CSIRT* modeli də adlandırırlar. Bu modeldə CSIRT-in şəxsi heyəti CSIRT administratorundan və təşkilatın digər bölmələrinin əməkdaşlarından ibarətdir. CSIRT administratoru ümumi idaretməyə və hesabat verməyə məsuldur. Bu modeldə CSIRT rəsmən tanınmış təşkilatdır, insidentlərə verilən cavabların idarə edilməsinə görə cavabdehlik daşıyır. Xidmət təşkilatın çərçivəsində qurulduğuna görə onu "daxili" hesab edirlər.

Daxili paylanmış CSIRT modeli təhlükəsizlik xidməti modelindən aşağıdakılarla fərqlənir:

- insidentləri cavablandırma üzrə daha formal siyasətin, prosedurların və proseslərin mövcudluğu;
- təhlükəsizlik təhdidləri və cavablandırma strategiyaları məsələləri üzrə bütün təşkilatla əlaqənin müəyyən üsulu;
- insidentləri cavablandırma üzrə məsələlərin həlli üçün məxsusi təyin edilmiş CSIRT menecerinin və komanda üzvlərinin mövcudluğu.

Komandaya hüquqi və texniki sahələrdə ekspertlər və məsləhətçilər daxil olmalıdır. Komandanın tərkibinə təşkilatın aşağıdakı bölmələrinin nümayəndələrinin daxil edilməsi tövsiyə edilir:

- informasiya təhlükəsizliyi xidməti: əlaqələndirmə, inzibati, ekspert və texnoloji fəaliyyəti təmin edir;
- informasiya texnologiyaları xidməti: ekspert və texnoloji fəaliyyəti təmin edir;
- kadrlar xidməti: inzibati və prosedur fəaliyyətini təmin edir;
- hüquq xidməti: ekspert və normativ-hüquqi fəaliyyəti təmin edir;

- profil bölmələrin biznes-menecerləri: inzibati ekspert və texnoloji fəaliyyətin təmin edilməsi üçün müvəqqəti əsaslarla cəlb edilirlər;

xarici ekspertlər: məsləhət, ekspert və texnoloji fəaliyyəti təmin edirlər.

Mərkəzləşdirilmiş daxili CSIRT modeli

Mərkəzləşdirilmiş daxili CSIRT modelində CSIRT komandası mərkəzdə yerləşmiş təşkilatın həyat fəaliyyətinə nəzarət edir və dəstək verir. CSIRT bütün insidentlərin hesabatlılığı, analizi və cavablandırılması üzrə ümumi cavabdehlik daşıyır. Beləliklə, komandanın iştirakçıları digər işləri yerinə yetirə bilməzlər və bütün vaxtlarını xidmətə işləməklə və bütün insidentləri cavablandırmaqla keçirirlər. Bundan başqa, CSIRT meneceri yuxarı rəhbərliyə: baş informasiya menecerinə (Chief Information Officer, CIO), baş təhlükəsizlik menecerinə (Chief Security Officer, CSO) və ya baş risk menecerinə (Chief Risk Officer, CRO) hesabat verir.

Paylanmış və mərkəzləşdirilmiş hibrid CSIRT modeli

Model "hibrid CSIRT" kimi də məlumdur. Mərkəzləşdirilmiş CSIRT bütün təşkilata nəzarət edə və dəstək verə bilmədiyi hallarda, komandanın bəzi üzvləri təşkilatın bölmələri/sahələri/filialları üzrə paylanaraq öz cavabdehlik sərhədləri çərçivəsində xidmətin səviyyəsini, mərkəzləşdirilmiş CSIRT-də nəzərdə tutulduğu kimi təmin edirlər.

Mərkəzləşdirilmiş qrup yuxarı səviyyə verilənlərinin analizini, bərpaetmə metodlarını və təhlükələrin azaldılması strategiyalarını təmin edir. O, paylanmış xidmətin əməkdaşlarına insidentlərə, boşluqlara və zədələrdə cavab zamanı dəstək verir. Paylanmış qrupun üzvləri hər bir sahədə strategiyanı həyata keçirirlər və öz sahələrində ekspertizanı təmin edirlər.

Koordinasiya CSIRT-i modeli

Koordinasiya CSIRT-i hibrid CSIRT-də paylanmış xidmətlərin funksiyalarını gücləndirir. Koordinasiya CSIRT-i modelində hibrid CSIRT xidmətlərinin əməkdaşları şəbəkəyə qoulma, coğrafi sərhədlər və s. kimi xarakteristikalar üzrə müstəqil CSIRT-lərdə qruplaşdırılır. Onlar mərkəzləşdirilmiş CSIRT sistemi üçün uyğun gəlir. Bu model təşkilatın daxili fəaliyyəti üçün, eləcə də xarici təşkilatlarla sıx əməkdaşlıq və dəstək üçün tətbiq edilə bilər.

Koordinasiya və yardım üzrə fəaliyyətə məlumat mübadiləsi, nəticələrin yüngülləşdirilməsi strategiyalarının təmini, insidentlərin cavablandırılması, bərpaetmə metodları, tendensiyaların tədqiqi və insidentlərin fəaliyyət məlumat xarakterlərinin analizi, boşluqlar üzrə məlumat bazalarının, təhlükəsizlik alətləri üçün informasiya mərkəzlərinin yaradılması, məsləhətlər və məlumatlar verilməsi üzrə xidmətlər daxildir.

3.3. CSIRT komandalarının növləri

Hazırda CSIRT-in aşağıdakı tətbiq sektorlarını müəyyən etmək olar:

- akademik;
- dövlət;
- hərbi;
- milli;
- kritik infrastruktur;
- kommersiya;
- daxili;
- kiçik və orta biznes;
- ticarət.

Akademiya sektorunda CSIRT

Akademiya sektorunda CSIRT diqqəti elmi-tədqiqat institutlarına, onların ərazi infrastrukturlarına və universitetlərə, elm və təhsil təşkilatlarına xidmətlər göstərilməsinə yönəldir.

Belə CSIRT-lərin tipik kliyentləri elmi-tədqiqat institutlarının əməkdaşları və universitetlərin tələbələridir.

Dövlət sektorunda CSIRT

Dövlət sektorunda CSIRT dövlət və hökumət təşkilatlarına, bəzi ölkələrdə isə vətəndaşlara da (Belçika, Macarıstan, Niderland, Böyük Britaniya və Almaniya) xidmətlər göstərir.

Hərbi sektorda CSIRT

Hərbi sektorda CSIRT hərbi idarələrə və müdafiə sferasının ehtiyacları üçün istifadə edilən IT infrastrukturlara xidmətlər göstərir. Onun kliyentləri hərbi idarələrin və fəaliyyət növünə görə yaxın təşkilatların əməkdaşlarıdır.

Milli CSIRT

Milli səviyyədə işləyən CSIRT informasiya təhlükəsizliyi üzrə əsas əlaqələndirici şəxs kimi çıxış edir. Bəzi hallarda dövlət CSIRT-i də əlaqələndirici şəxs rolunu oynayır (UNIRAS, Böyük Britaniya).

Adətən, bu növ CSIRT-in kliyentləri aydın seçilmirlər, çünki CSIRT bütün ölkə miqyasında vasitəçilik rolunu oynayır.

Kritik infrastruktur üçün CSIRT

Bu sektorda CSIRT-in əsas hədəfi kritik informasiyanın və/və ya infrastrukturun mühafizəsidir. Əksər hallarda bu növ CSIRT-lər kritik infrastrukturların mühafizəsi üzrə dövlət agentlikləri ilə sıx əməkdaşlıq edirlər. Bu CSIRT ölkənin bütün kritik IT sektorlarını əhatə edir və bu ölkənin vətəndaşlarını qoruyur.

Kommersiya sektorunda CSIRT

Kommersiya sektorunda CSIRT kliyentlərə kommersiya əsasında xidmətlər göstərir. İnternet provayderin cavab qrupu əsasən istifadəçilərin İnternet şəbəkəsində sui-istifadələrinin qarşısını almaq üçün xidmətlər (Dialup, ADSL) və digər xidmətlər göstərir.

Daxili CSIRT

Daxili CSIRT yalnız onu yaradan təşkilata xidmətlər göstərir. Bu növ CSIRT digər CSIRT növləri ilə müqayisədə daha funksional (korporativ) hesab edilir. Telekommunikasiya şirkətlərinin və bankların çoxunda öz daxili CSIRT-ləri var. Adətən, bu CSIRT-lər digərlərinə xidmət göstərmirlər. Onun kliyentləri IT-departament və təşkilatın əməkdaşlarıdır.

Kiçik və orta biznesdə CSIRT

Belə CSIRT-lər öz biznesinə və tərəfdaşlarına xidmətlər göstərir. Onun kliyentləri kiçik və orta biznesin əməkdaşları, yaxud istifadəçilərin xüsusi qrupudur, məsələn, "Şəhər sakinlərinin və bələdiyyələrin Assosiasiyası".

Ticarət sektorunda CSIRT

Ticarət sektorunda CSIRT bu və ya digər istehsalçının məhsulunun dəstəklənməsini hədəfə alır. Çox vaxt onun məqsədləri boşluqların aradan qaldırılmasına və boşluqların məhsuldakı potensial mənfi təsirlərinin azaldılmasına yönəlir. Bu CSIRT-in kliyentləri bu və ya digər məhsulun sahibləridir.

3.4. Milli CSIRT-lər

Hazırda dünyada yetkinliyin müxtəlif mərhələrində olan 30-50 milli CSIRT mövcuddur. Onların çoxu Amerika, Asiya və Avropadadır, bir neçəsi son dövrlər Yaxın Şərqdə yaradılıb. Milli CSIRT-lərə misal olaraq US-CERT (ABŞ), CCIRC (Kanada), JRCERT/CC (Yaponiya), CNCERT/CC (Çin), KrCERT/CC (Cənubi Koreya) və s. göstərilə bilər. Milli CSIRT-lərin siyahısı əlavə 3-də göstərilir.

Milli CSIRT bir və ya bir neçə ölkəyə təsir edən böyük miqyaslı və/və ya kritik informasiya təhlükəsizliyi insidentlərinin cavablandırılması ilə məşğul olurlar.

Kritik informasiya təhlükəsizliyi insidentləri iqtisadiyyata, kritik infrastruktura, dövlətin fəaliyyətinə və milli təhlükəsizliyə təsir göstərə bilərlər. Təbiətlərinə görə, bu insidentlər çox zaman bir deyil, bir neçə təşkilata təsir edir.

Mövcud milli CSIRT komandaları daha çox milli komandaların yaradılmasında maraqlıdır:

- dünya miqyasında kiberhücumları dayandırmaq və ya hüquq-mühafizə fəaliyyətinə cəlb etmək;
- daha çox ölkədə daha çox insana özlərini İnternetdə necə mühafizə olunmağı öyrətmək;
- ziyankar fəaliyyəti daha erkən, kaskad yaratmadan müəyyən etmək və neytrallaşdırmaq.

Milli CSIRT-lərin şəbəkəsini yaratmaq üçün standartların və servislərin aşağıdakı minimum çoxluğu gözlənilməlidir:

- Milli CSIRT-in mənsub olduğu dövlətin məsuliyyətinin təyin edilməsi;
- əməkdaşlıq edən komandalar arasında informasiya paylaşımının prinsipləri haqqında razılaşma;
- digər milli CSIRT-lərdən informasiyanın alınması və alınan informasiyanın ölkə daxilində müvafiq qurumlar arasında yayılması üçün məsuliyyətlər;
- informasiyanın digər milli CSIRT-lərlə paylaşımı üzrə avtorizasiya;
- insidentlər və təhdidlər üçün digər milli CSIRT-lərə yardımın koordinasiyası;

Kommunikasiya və kooperasiyada həssas təhlükəsizlik məsələlərində inamı təmin edən cəhətlərə aiddir:

- sensitiv informasiyanın paylaşımı üçün təhlükəsiz infrastruktur;
- maraqlı tərəflərlə təhükəsiz kommunikasiya saxlamaq imkanı;
- ekspertlərə və qərar qəbul edənlərə sərəncam vermək imkanı;
- informasiya sızmalarının qarşısını almaq prosedurları;
- seçilmiş auditoriyaların qabaqcadan məlumatlandırma infrastrukturu;
- procedures to guard against information leakage;
- kritik informasiyanı yaymaq üçün yaxşı məlum açıq interfeys;
- böyük audensiyaya tez zamanda müraciət etmək imkanı.

3.5. Milli CSIRT-in yaradılması modeli

CSIRT-in yaradılmasını aşağıdakı mərhələlərdə həyata keçirmək tövsiyə olunur: maarifləndirmə; planlaşdırma; reallaşdırma; istismar; əməkdaşlıq.

Mərhələ 1 – CSIRT-in yaradılması haqqında sponsorların maarifləndirilməsi. Bu məlumatlandırma mərhələsidir, bu mərhələdə insidentlərə cavabvermə qurumunun yaradılmasında iştirak edənlər CSIRT-in qurulmasının nələri əhatə etməsini öyrənirlər: – qəbul edilməli olan qərarlar, CSIRT-in oynayacağı rol (məsələn, insidentlər haqqında xəbərvermə və cavablandırma üçün mərkəz kimi), qarşıya çıxa bilən əsas problemlər (idarəetmə və şəxsi heyət, etibarlı kommunikasiyanın və koordinasiyanın səmərəli proseslərinin yaradılması və s.).

Mərhələ 2 – CSIRT-in planlaşdırılması. Birinci mərhələdə əldə edilmiş bilik və informasiyanın əsasında ikinci mərhələdə CSIRT-in layihələndirilməsi və planlaşdırılması həyata keçirilir. Bu mərhələdəki fəaliyyətin konturlarını qısaca göstərək:

- CSIRT üçün tələblərin çevrəsini (komandanın əməliyyatlarına təsir edəcək qanun və normativ aktları, mühafizə ediləcək mühüm resursları, məlumat veriləcək insidentləri, ölkə üzrə əlaqələndirilmiş cavabvermədəki boşluqları və s.) müəyyən etmək;
- CSIRT-in necə fəaliyyət göstərəcəyinə baxışların işlənməsi (məqsədlərin, xidmət göstəriləcək icmanın, icma və komanda arasında kommunikasiya interfeyslərinin, göstəriləcək xidmətlər çoxluğunun, təşkilatı modelin, fiziki yerləşmə nöqtəsinin, şəxsi heyətin, avadanlıq və infrastrukturun müəyyən edilməsi, büdcə, maliyyələşdirmə təkliflərinin, layihə planlarının və ya biznes əməliyyatları planlarının işlənməsi).

Mərhələ 3 – CSIRT-in reallaşdırılması. Bu mərhələdə əvvəlki iki mərhələdə əldə edilən informasiayadan CSIRT qurulması üçün istifadə edilir. Əsas addımlara daxildir:

- maliyyənin əldə edilməsi (planlaşdırma mərhələsində müəyyən edilmiş mənbələrdən);
- CSIRT-in yaradılması haqqında geniş elan vermək;
- əlaqələndirmə və kommunikasiya mexanizmlərinin formalaşdırılması;
- CSIRT üçün təhlükəsiz informasiya sistemləri və şəbəkə infrastrukturunun qurulması;
- CSIRT-in şəxsi heyəti üçün istismar qaydalarının və prosedurlarının işlənməsi;
- CSIRT-in öz istifadəçiləri ilə qarşılıqlı əlaqəsi üçün proseslərin reallaşdırılması;
- kadrların işə götürülməsi, CSIRT şəxsi heyəti üçün müvafiq təlim və təhsilin verilməsi.

Mərhələ 4 – CSİRT-in istismarı. İstismar mərhələsində CSIRT insidentləri idarəetmənin əsas vasitələrinə malik olur və komanda fəal şəkildə insidentlər haqqında məlumatları qəbul edir və insidentlərə cavabverməni əlaqələndirir. Bu mərhələdə görülən əsas işlər:

- CSIRT-in göstərdiyi müxtəlif xidmətlərin fəal yerinə yetirilməsi;
- CSIRT-in əməliyyatlarının səmərəsinin qiymətləndirilməsi üçün mexanizmlərin işlənməsi və həyata keçirilməsi;
- qiymətləndirmənin nəticələrinə görə CSIRT-in təkmilləşdirilməsi;
- məqsədlərin, xidmətlərin və şəxsi heyətin inkişaf etdirilməsi.

Mərhələ 5 – Əməkdaşlıq. CSIRT öz əməliyyatlarını davam etdirir və parallel olaraq əsas sponsorlarla, tərəfdaşlarla və digər CSIRT-lərlə etibarlı münasibətləri inkişaf etdirir. Müəyyən zaman müddətində yetkinləşən komanda insidentlərin idarə edilməsində geniş təcrübə toplayır və qlobal CSIRT cəmiyyətində etibarlı tərəfdaşa çevrilir. Bu mərhələdəki fəaliyyətə daxildir:

– digər CSIRT-lərlə, tərəfdaşlarla, icmalarla verilənlər və informasiya mübadiləsində iştirak;
– CSIRT-lər cəmiyyətinə dəstək üçün qlobal "müşahidə və xəbərdarlıq" fəaliyyətində iştirak;
– treninqlər, seminarlar, konfranslar yolu ilə CSIRT-in fəaliyyət keyfiyyətini yaxşılaşdırmaq;
– kritik infrastrukturun təhlükəsizliyi və mühafizəsi üçün ən yaxşı praktika sənədlərinin, cavabvermə strategiyalarının və planlarının işlənməsi;
– ölkədə təşkilati CSIRT-lərin yardılmasını dəstəkləmək və belə CSIRT-lər üçün ən yaxşı praktika modellərini işləmək. Komanda bu CSIRT-lərin qiymətləndirilməsi (hətta sertifikatlaşdırılması və akkreditasiyası) xidmətlərini göstərə bilər.

3.6. CSIRT komandasının strukturu

CSIRT-in əlverişli təşkilati strukturu sahib-təşkilatın və kliyentlərin mövcud strukturundan çox asılıdır. O, həmçinin daimi əsaslarla və ya konkret məsələ üçün cəlb olunan ixtisaslı ekspertlərin əlyetən olmasından da asılıdır.

Tipik CSIRT komandası daxilində aşağıdakı rolları ayırırlar:

Rəhbərlik:
– baş menecer (komandanın rəhbəri).

Şəxsi heyət:
– ofis meneceri;
– mühasib;
– kommunikasiyalar üzrə məsləhətçi;
– hüquq məsləhətçisi.

Operativ texniki qrup:
– texniki qrupun rəhbəri;
– CSIRT-servisləri göstərən texniklər (insident emalçıları);
– analitiklər (artefakt analitiki, boşluqlar üzrə analitik);
– "birinci reagent" – hotline, service/help desk əməkdaşı;

- ekspertlər (informasiya təhlükəsizliyi, şəbəkə üzrə mütəxəssislər – qismən məşğulluq);
- digər heyət.

Kənar məsləhətçilər:

– zəruri olduqda cəlb olunurlar.

CSIRT-in yaradılmasının xüsusilə başlanğıc mərhələsində ştatda hüquqşünasın olması olduqca faydalıdır. Bu xərcləri artırsa da, son nəticədə vaxta qənaət etməyə və hüquqi problemlərdən yan keçməyə kömək edir.

Kliyent qrupları arasında kvalifikasiyanın səviyyəsindən və müxtəlifliyindən asılı olaraq CSIRT yaxşı media-profilə malik olduqda qrupda kommunikasiyalar üzrə ekspertin olması çox vacibdir. Belə ekspert çətin texniki məsələləri kliyentlər və ya media-tərəfdaşlar üçün daha anlaşıqlı olan məlumatlara tərcümə etməklə məşğul olur. Kommunikasiyalar üzrə mütəxəssis kliyentlərlə texniki ekspertlər arasında əks-əlaqəni də təmin edir, bununla da bu iki qrup arasında "tərcüməçilik" və "vasitəçilik" xidməti göstərir.

3.7. CSIRT-in heyətlə komplektləşdirilməsi

Hansı servislərin göstəriləcəyi və dəstək səviyyəsi qərara alındıqdan və təşkilati model seçildikdən sonra növbəti addım lazımi sayda kvalifikasiyalı əməkdaşların tapılmasıdır.

Tələb olunan texniki heyətin sayını dəqiq söyləmək mümkün deyil, lakin praktikada özünü yaxşı göstərmiş aşağıdakı ədədləri nəzərə almaq olar..

CSIRT-lərin gündəlik insident emalı məhsuldarlığı müxtəlifdir:

– 38% CSIRT – gündə 1-3 insident;
– 18% CSIRT – gündə 4-8 insident;
– 18% CSIRT – gündə 15-dən çox insident;
– 10% CSIRT – ildə təxminən 50 insidenti idarə edir.

CSIRT-in tam yüklənmiş bir "texniki" əməkdaşı gün ərzində 1 yeni "ortabab" insident və 20 açılmış və təhqiq olunan insident

emal edə bilər. Bir insanın stress şəraitində işləmə vaxtını da nəzərə almaq lazımdır.

- Yalnız iki əsas servisin göstərilməsi – məsləhət bülletenlərini yaymaq və insidentlərin emalı üçün: tam məşğul olan minimum 4 əməkdaş lazımdır;
- CSIRT servislərinin tam spektri – iş saatlarında və sistemlərə xidmət üçün: tam məşğul olan 6-8 əməkdaş tələb edilir;
- CSIRT servislərinin hamısı – 24x7 rejimdə tam komplekt olunmuş növbə (işdənkənar vaxtda 2 növbə): təxminən, tam məşğul olan minimum 12 əməkdaş tələb edilir;

Bu ədədlərə xəstəlik, məzuniyyət, bayramlar və s. hallar üçün ehtiyatlar da daxildir, müxtəlif saat qurşaqları da nəzərə alınmalıdır. Həmçinin əmək müqavilələrinin şərtlərini də nəzərə almaq zəruridir. Əgər heyət qeyri-iş saatlarında işləyəcəksə, bu işdənkənar vaxt üçün əlavə əmək haqqı ödənilməsinə səbəb olacaq. Eyni zamanda, nəzərə alınır ki, müxtəlif vaxtlarda müxtəlif sayda insident baş verir və insanları bir "cəbhədən" digərinə keçirmək olar.

Aşağıda CSIRT qrupunun texniki ekspertlərinin əsas kompetentlik sahələrinin qısa icmalı verilir.

Şəxsi qabiliyyətlər

- çeviklik, yaradıcılıq və yaxşı komanda ruhu;
- güclü analitik vərdişlər;
- mürəkkəb texniki məsələləri sadə dillə izahetmə qabiliyyəti;
- konfidensiallığa və metodiki işə yaxşı münasibət;
- yaxşı təşkilatçılıq qabiliyyətləri;
- stresə dayanıqlıq;
- yaxşı danışıq və yazı vərdişləri;
- ağılın həssaslığı və öyrənmək istəyi.

Texniki vərdişlər

- İnternet-texnologiyaları və protokolları yaxşı bilmək;
- Linux və Unix sistemləri bilmək (kliyentlərin avadanlığından asılı olaraq);
- Windows sistemləri bilmək (kliyentlərin avadanlığından asılı olaraq);
- şəbəkə avadanlığını bilmək (marşrutizatorlar, kommutatorlar, DNS, proxy, e-poçt və s.);
- İnternet tətbiqi proqramlarını bilmək (SMTP, HTTP(s), FTP, telnet, SSH və s.);
- təhlükəsizlik təhdidlərini bilmək (DDoS, fişinq, Deface hücumları, sniffinq və s.);
- risklərin qiymətləndirilməsini və praktiki tətbiqlərini bilmək.

Əlavə qabiliyyətlər

- 24x7 rejimində və ya "çağırış üzrə" rejimdə (servis modelindən asılı olaraq) işləmək həvəsi;
- yola, əlyetənliyə maksimal vaxt (qəza halında ofisdə əlyetənlik, qəza yerinə çatmaq üçün yola maksimal vaxt);
- təhsil səviyyəsi;
- kompyuter təhlükəsizliyi sahəsində iş təcrübəsi.

3.8. CSIRT heyətinin təlimi

CSIRT heyətinin treninqinə həsr olunmuş iki əsas mənbə var: TRANSITS və CERT/CC kursları.

TRANSITS layihəsi CSIRT qruplarının yaradılmasını tezləşdirmək, mövcud CSIRT-lərin effektivliyini artırmaq üçün təcrübəli CSIRT heyətinin çatışmazlığı problemini həll etmək məqsədilə hazırlanmışdı. Bu məqsəd CSIRT-servislərin yaradılması ilə əlaqəli təşkilati, əməliyyat, texniki, marketinq və hüquq məsələləri (yeni) CSIRT-lərin şəxsi heyətinə öyrətmək üçün xüsusi təlim kurslarının təşkili ilə əldə edilmişdir.
TRANSITS-ə aşağıdakılar daxil idi:

- təlim kursları üçün hazırlanmış, düzəlişlər edilmiş və yenilənmiş modullardan ibarət materiallar;
- kurs materialların öyrənildiyi təlim seminarlarının təşkili;
- (yeni) CSIRT heyətinin, xüsusilə Avropa İttifaqına daxil olmuş ölkələrdən olan heyətin bu təlim kurslarında iştirakının mümkünlüyü;
- təlim kursunun materiallarının yayılması və onlardan istifadəyə zəmanət.

CERT/CC kursları. Kompyuter və şəbəkə infrakstrukturunun mürəkkəbliyi, həmçinin müdriyyətin tələbləri şəbəkə təhlükəsizliyinin düzgün idarə edilməsini çətinləşdirir. Şəbəkə və sistem administratorlarının kifayət sayda mütəxəssislərə və hücumlardan mühafizədə və ziyanın minimumlaşdırılması üçün təhlükəsizliyin təmin edilməsində təcrübələri yoxdur. Nəticədə kompyuter təhlükəsizliyinin pozulması insidentlərinin sayı artır. Kompyuter təhlükəsizliyi insidenti baş verdikdə tez və effektiv cavab vermək tələb edilir. Təşkilat insidenti nə qədər tez aşkarlayıb, analiz etsə və cavabını versə, ziyanın həcmi də o qədər az olar və bərpaetməyə xərclər də azalar. CSIRT-in formalaşdırılması tez insidentlərə tez cavab verilməsininin təmini, gələcək insidentlərin qarşısının alınmasını kömək üçün ən yaxşı yoldur.

CERT/CC menecerlər və texniki heyət üçün CSIRT-ə həsr edilmiş aşağıdakı sahələrdə kurslar təklif edir:

- CSİRT-in yaradılması;
- CSİRT-in menecmenti;
- insidentlərin emalının əsasları;
- insidentlərin əlavə emalı (texniki heyət üçün).

3.9. CSIRT siyasətləri

CSIRT-in fəaliyyətinin əsas elementləri servislər, siyasətlər, prosedurlar və keyfiyyətə nəzarətdir.

İnformasiya təhlükəsizliyi insidentlərinin idarə edilməsi prosesinin mərhələləri aşağıdakılardır:

– siyasətlər (hansı məqsədlərə nail olmaq istəyirik);
– proseslər (məqsədlərə çatmaq üçün nə etmək lazımdır);
– prosedurlar (bunu kim, nə vaxt və harada etməlidir);
– təlimatlar (bunu necə etməlidir);
– insanlar və alətlər (bunu nəyin vasitəsi ilə etməlidir).

Siyasət – təşkilatda qəbul edilmiş, sənədləşdirilmiş rəhbəredici prinsiplərdir. Siyasət daxili (CSIRT-in daxili istifadəsi üçün) və xarici (kliyentlər üçün), həmçinin konkret servis üçün (məsələn, zərərçəkmiş kliyentin identifikasiyası üçün) ola bilər.

İnformasiya təhlükəsizliyi insidentlərinin cavablandırma sahəsində siyasət təşkilatın xüsusiyyətləri, fəaliyyət profili nəzərə alınmaqla işlənir.

CSIRT-də aşağıdakı siyasətlər olmalıdır:

- Terminlər və təriflər;
- İnformasiyanın/insidentin klassifikasiyası siyasəti (insidentlərin kateqoriyalaşdırılması, prioritetləşdirilməsi və eskalasiyası daxil olmaqla);
- Daxil olan zənglər siyasəti;
- İnformasiyanın açıqlanması siyasəti;
- CSIRT-in təhlükəsizlik siyasəti;
- Mətbuatla ünsiyyət siyasəti;
- Digər CSIRT-lərlə koordinasiya siyasəti;
- Mürəkkəb kontaktlarla ünsiyyət siyasəti;
- İdentifikasiya edilməmiş abonentlərlə ünsiyyət siyasəti;
- Boşluqların idarə edilməsi siyasəti;
- Xəbərdarlıqların hazırlanması siyasəti.

Siyasəti işləyib hazırlamazdan əvvəl siyasətin hansı kriteriyaları ödəməli olduğunu (Cədvəl 3.1) və onda hansı məcburi bəndlərin olmasını başa düşmək lazımdır (Cədvəl 3.2).

"Birdəfə və həmişəlik" hazırlanmış ideal siyasətlər yoxdur. Bəzi hallarda siyasətlər CSIRT və ya onun ayrı-ayrı servisləri işə başladıqdan sonra yaradıla bilərlər.

Siyasətin misallarla müşaiyət edilməsi yaxşı prkatika hesab edilir.

Cədvəl 3.1. Yaxşı siyasətin atributları

Atribut	Təsviri
Rəhbərlik tərəfindən bəyənilmə və dəstəklənmə	Missiya kimi, siyasət də rəhbərlik tərəfindən dəstəklənməsə, onun icrası mümkün deyil
Aydınlıq	Nəzərdə tutulan auditoriyanın istənilən üzvü siyasətdən nədən bəhs etdiyini başa düşməlidir. Jarqonlardan qaçmaq, qısa cümlələrdən istifadə etmək lazımdır.
Qısalıq	Yaxşı siyasət – qısa siyasətdir. Uzun siyasət ya pisdir, ya da ona çoxlu sayda prosedur daxildir, idarəetməni (siyasəti) operativ fəaliyyətlə (prosedurla) qarışdırır.
Zərurilik və kafilik	Siyasət müəyyən situasiyada hərəkətlər üçün zəruri olan hər şeyi daxil etməlidir, lakin lazım olandan çox və prosedurlarda təsvir ediləndən artıq nəsə daxil etməməlidir.
Praktiklik	Gözəl, lakin mənasız frazalardan qaçmaq lazımdır (məsələn, "mühafizəliliyin yüksək səviyyəsinin təmin edilməsi")
Gerçəkləşdirmə	Siyasət mövcud resurslar nəzərə alınmaqla gerçəkləşdirilə bilən olmalıdır.
İcra edilmə	Əgər siyasət icra edilmirsə, onda o faydasızdır. Əgər siyasət məxfidirsə, onda istifadəçilər necə biləcəklər ki, onu yerinə yetirmək lazımdır.

Cədvəl 3.2. Siyasətin məzmunu

Bölmə	Təsviri
Missiya ilə əlaqə	Siyasət missiyanın yerinə yetirilməsinə necə kömək edir?
Rollar	Siyasətin (və ya onun ayrı-ayrı hissələrinin) həyata keçirilməsində iştirak edən insanlar dəqiq müəyyən edilməlidir.
Məsuliyyət	İştirakçıların vəzifələri və məsuliyyətləri (harada mümkündürsə) müəyyən edilir.
Qarşılqlı əlqə	İştirakçılar arasında qarşılıqlı əlaqə təsvir edilir. Məsələn, mətbuatla ünsiyyət zamanı ünsiyyət kanalı (telefon və ya şəxsən), sualların siyahısı, həmçinin nəşr olunmazdan öncə məcburi razılaşdırma müəyyən edilir.
Prosedurlar	Siyasəti təmin edən prosedurlar göstərilir.
Əlaqələr	Digər servislərlə və siyasətlərlə əlaqələr müəyyən edilir.
Dəstək	Siyasətin dəstəklənməsi və yenidən baxılması proseduru və məsul şəxs müəyyən edilir.
Terminlər, təriflər və ixtisarlar	CSIRT-in yeni üzvlərinin başa düşməsi və eyni dildə ünsiyyəti üçün bütün zəruri terminlər və ixtisarlar müəyyən edilir.

Siyasətin hazırlanması ilə iş bitmir, onun praktikada gerçəkləşdirilə bilməsini də qiymətləndirmək zəruridir.

Siyasəti işə salmazdan öncə, onun bütün tezislərinin praktikada tətbiq edilən olmasını yoxlamaq lazımdır. Siyasəti hazırlayan şəxslər onu yoxlayanlarla eyni olmamalıdır. Maraqların münaqişəsini və qeyri-obyektivliyi istisna etmək lazımdır. Siysətin digər siyasətlərlə də uyğunluğunu yoxlamaq zəruridir. Ən pis ssenarilər və insanların real davranışı olan pilot layihə işə salınmalıdır. "Həmsöhbətlərlə həmişə mehriban olun" məsləhətini çox aqressiv opponentlər üzərində yoxlamaq lazımdır.

Siyasətdə edilən istənilən dəyişiklik təsdiq edilməzdən əvvəl yoxlanılmalıdır, siyasətin "işləmə qabiliyyəti" müntəzəm olaraq yoxlanmalıdır. Siyasətin aktual vəziyyətdə saxlanması üçün məsul şəxsin olması zərurdir.

3.10. Keyfiyyətin qiymətləndirilməsi üsulları

Aydındır ki, servislər kataloqunun, informasiya axınları matrisinin, siyasət və prosedurların mövcudluğu CSIRT servislərini keyfiyyətli səviyyədə göstərmək üçün yetərli deyil. Keyfiyyətə nəzarət tələb olunur.

Praktikada keyfiyyətə nəzarəti çox vaxt həyata keçirmirlər. Standart formalar – insidentlərin prioritetləşdirilməsi və rəhbərlik tərəfindən şikayətlərin olmamasıdır. Keyfiyyət göstəricilərinin müəyyən edilməsi "yuxarıdan aşağıya", missiyadan başlamalıdır. Orada "vaxtında", "çevik", "bütün mümkün ssenarilər" kimi keyfiyyət göstəriciləri ola bilər.

Hər bir servis, siyasət, prosedur, öz keyfiyyət göstəricilərinə malik ola bilər:

- servisin fəaliyyət sferasından olan hadisələrə (boşluq, insident) cavab müddəti;
- hadisənin prioriteti;
- hadisə üçün təqdim edilən informasiyanın səviyyəsi (qısamüddətli prespektiv);
- hadisə üçün təqdim edilən informasiyanın uzunmüddətli prespektivdə səviyyəsi (hesabat, anons, icmal, ...);
- konfidensiallıq səviyyəsi;
- açılmış və bağlanmış insidentlərin sayı;
- "kömək istəyən zənglərin" sayı (zənglər, e-poçt məlumatları, veb ilə məlumatlar);
- insidenti orta cavablandırma müddəti (müxtəlif prioritetlər üçün);
- insidentlərin prioritetlər üzrə paylanması;
- trendlər (müxtəlif kəsiklər üzrə insidentlərin sayının artması/azalması).

Keyfiyyət göstəricilərinin siyahısı müəyyən edildikdən sonra onları ölçülən konkret qiymətlərlə əlaqələndirmək lazımdır.

Keyfiyyət parametri	Qiymət
Boşluq haqqında məlumatı cavablandırma müddəti	Kritik olmayan bütün boşluqlar üçün CSIRT birinci məlumat anından iki gün müddətində tövsiyələr buraxacaq.
Yüksək prioritetli insidenti cavablandırma müddəti	Hər bir yüksək prioritetli insident 2 saat müddətində təsdiq olunmalıdır. Analiz insident barəsində məlumat alındıqdan sonra birinci saat müddətində başlayır.
Aşağı prioritetli insidenti cavablandırma müddəti	Hər bir aşağı prioritetli insident 4 saat müddətində tanınmalıdır. Analiz insident haqqında məlumat aldıqdan sonra ilk 48 saat ərzində başlayır.

Keyfiyyətə nəzarət sistemi statik deyil. Bir parametrin qiyməti digər parametrlərin qiymətinə təsir edə bilər (məsələn, krizis zamanı cavablandırma müddəti adi insidentdə olduğundan dəfərlə kiçik ola bilər). Keyfiyyət parametrlərinin qiymətləri çevik ola bilərlər (məsələn, prioritet olmayan bütün insidentlərin 95%-i 5 gün müddətində emal olunacaq). Zəruri olduqda, maraqlı tərəfləri keyfiyyət parametrlərinin qiymətlərinin dəyişməsi barədə xəbərdar etmək gərəkdir.

Keyfiyyətə nəzarət sisteminə göstəricilərin yoxlanılması da daxil olmalıdır. Trivial olmayan bu məsələ keyfiyyət göstəricilərinin ölçülməsi və müvafiq hesabatların hazırlanması üzrə prosedurlar və alətlər toplusunu nəzərdə tutmalıdır. Yoxlanılma tezliyi də vacibdir. Çox az-az – CSIRT-in iş keyfiyyəti aşağı düşə bilər, tez-tez ölçüldükdə CSIRT-in vaxtını alır və resurslar tələb edir.

Yoxlama zamanı ümumi səhv – prosedurların mürəkkəb olmasıdır. Keyfiyyətin yoxlanılması prosedurları olduqca uzunmüddətlidir, səhv üçün potensial imkanlar var. Yoxlama məqsədə çevrilir (çoxları unudur ki, yoxlamanın vəzifəsi keyfiyyət sisteminin işinə kömək etməkdir, ona mane olmaq deyil). Yoxlama prosedurlarının sayı minimum olmalı, onlar şəffaf və anlaşıqlı olmalıdırlar.

CSIRT əməkdaşları yoxlamaların nə üçün lazım olduğunu başa düşməlidirlər. Bu, yoxlama zamanı mümkün münaqişələrin qarşısını alardı. Keyfiyyət göstəricilərini dəyişdirərkən yoxlama prosedurlarını da dəyişmək lazımdır. Məsələn, insident haqqında məlumat verən kliyentlə əlqənin yoxlanmasına baxaq. İlkin keyfiyyət göstəricisi belədir: "Kliyentin insident haqqında məlumatına cavab siqnal alındığı andan 2 saat müddətində olmalıdır". Fərz edək ki, e-poçt ilə avtomatik cavab sistemi tətbiq edilib və cavab dərhal göndərilir. Bu halda göstəricini belə dəyişmək lazımdır. "İnsident haqqında məlumat alındıqdan sonra dərhal avtomatik cavab göndərilir. CSIRT əməkdaşlarının şəxsən cavabı siqnal alındıqdan sonra 2 saat müddətində olmalıdır."

Keyfiyyət göstəriciləri siyahısının kliyentlərə elan olunmasına gəlincə, keyfiyyət göstəricilərinin bir hissəsini seçmək və onları elan etmək olar.

Prosedurlar, yoxlamalar və öz işini yerinə yetirmək zərurəti arasında balans lazımdır. CSIRT prosedurları problemin həllinə kömək edə bilmədikdə və ya CSIRT üzvləri öz işini keyfiyyətlə yerinə yetirmədikdə nə etmək lazımdır? Bu halda eskalasiya proseduru, həmçinin məsuliyyət haqqında müddəa olmalıdır, onlar CSIRT-in standart prosedurlarına müqabildirlər. Oxşar tədbir öz vəzifələrini yerinə yetirməyən kliyentlərə qarşı da olmalıdır. Belə kliyentləri CSIRT-dən çıxarmaq və ya onlara xidmət səviyyəsini aşağı salmaq olar.

3.11. CSIRT-in texniki infrastrukturu

CSIRT-in texniki infrastrukturunun əsas elementlərini komandanın göstərdiyi xidmətlərin siyahısından çıxış edərək müəyyən edirlər. CSIRT texniki infrastrukturuna daxildir:

- CSIRT kompyuter sistemləri, kompyuter şəbəkələri, daxili və xarici mühafizə mexanizmləri.
- CSIRT və insident məlumatlarının saxlanması üçün verilənlər bazaları və verilənlərin analizi alətləri.
- CSIRT alətləri və tətbiqi proqramları.

- Təhlükəsiz e-poçt və səs kommunikasiyası üçün mexanizmlər və tətbiqi proqramlar.
- CSIRT və verilənlərin fiziki yerləşməsi və təhlükəsizliyi
- CSIRT-in ofisi və ofis avadanlığı.

Aşağıda AZ-CERT misalında CSIRT-in texniki infrastrukturu analiz edilir. FIRST Site Visiting Document-də zəruri texniki resursların siyahısını aydınlaşdırmaq üçün faydalı mənbədir.

Telefon və faks. Hər şeydən əvvəl kliyentlərlə, digər CSIRT-lə, rəhbərliklə və s. telefon rabitəsi tələb edilir. Komandanın 24x7 rejimində əlaqə saxlamaq imkanında olmalı, iş günü olmayan vaxtlarda kimin zənglərə cavab verəcəyini müəyyən etməlidir: komandanın üzvü, başqa əməkdaş və ya səs poçtu. Sonradan analiz etmək üçün daxil olan zənglərin qeydiyyata alınması çox vacibdir.

Bəzi təşkilatlar kommunikasiya vasitəsi kimi faksdan istifadəyə üstünlük verə bilər. Bunadan başqa şəbəkə və ya poçt serveri işləmədikdə faksdan istifadə etmək olar.

İnternet bağlantısı. Təbii olaraq, komandanın İnternet bağlantısı olmalıdır. İdealda, komanda ayrıca İnternet-bağlantıya malik olmalıdır.

Elektron poçt CSIRT-in ən çox istifadə edilən kommunikasiya vasitəsi e-poçtdur. AZ-CERT e-poçt sistemi kimi pulsuz yayılan Mozilla Thunderbird poçt kliyentindən istifadə edir. İstifadəçilərin insidentlər haqqında məlumat vermələri üçün sadə, asan yadda qalan poçt ünvanı seçilir məsələn, info@cert.az.

Veb-sayt. Veb-sayt yəqin ki, informasiya təhlükəsizliyi üzrə xəbərdarlıqları yaymaq və kliyentlərlə informasiyanı bölüşmək üçün ən səmərəli üsuldur. Ümumdünya hörümçəyinin populyarlığını nəzərə alaraq indi CSIRT komandasının öz veb-saytına malik olması məcburidir. Komanda öz veb-saytının təhlükəsizliyinə xüsusi fikir verməlidir, onun sındırılması kliyentlərin komandaya inamını itirməsinə səbəb ola bilər.

Kompyuter avadanlığı. Komandanın ölçülərindən və göstərdiyi xidmətlərdən asılı olaraq komandaya müxtəlif kompyuter avadanlığı tələb edilir. Onlar elə seçilməlidir ki, kliyentlərə keyfiyyətli xidmət göstərilsin. İnsidentlərin emalı adətləri üçün komandaya serverlər (veb-server, verilənlər bazası serveri, IDS, şəbəkə skaneri və s.) zəruridir. Gündəlik iş üçün komandanın hər bir üzvü ayrıca fərdi kompyuterlə və ya dizüstü kompyuterlə təmin edilməlidir, çünki konfidensial informasiya olan sistemlərdən ortaq istifadə məsləhət görülmür.

Şəbəkə infrastrukturu. Trafikin dinlənilməsi riskini minimal etmək üçün komanda təşkilatın qalan şəbəkəsindən izolə edilmiş lokal şəbəkəyə (LAN) malik olmalıdır. Şəbəkələrin izolə edilməsi fiziki (marşrutizator və ya şəbəkə ekranı istifadə edilməklə) və ya məntiqi (VLAN-ın köməyi ilə) həyata keçirilə bilər.

Naməlum proqram təminatını test etmək üçün komandanın ayrıca testetmə şəbəkəsi olmalıdır. Test şəbəkəsini də qalan bütün şəbəkələrdən izolə etmək lazımdır (fiziki və ya məntiqi). Həmçinin ziyankar və ya digər proqramların CSIRT sistemlərində test edilməsi zamanı CSIRT heyətinə tələbləri müəyyən edən siyasət də işlənməlidir.

Kommunikasiyaların təhlükəsizliyi. Elekrton poçt əvəzedilməz kommunikasiya vasitəsidir, lakin onu asanlıqla saxtalaşdırmaq olar. Kommunikasiyaların təhlükəsizliyi üçün AZ-CERT komandası Gnu PG (GNU Privacy Guard) proqram təminatından istifadə edir.

Enigmail proqramının köməyi ilə GnuPG Mozilla ThunderBird poçt kliyentində məlumatları şifrləmək və autentifikasiyası üçün işləyir. GnuPG General Public License lisenziyası ilə inkişaf etdirilir, GNU layihəsinin bir hissəsidir və Almaniya hökuməti tərəfindən dəstəklənirdi. GPG-PGP (Pretty Good Privacy) kriptoqrafik proqram təminatına alternativdir, GnuPG-nin hazırki versiyaları PGP və digər OpenPGP – sistemləri ilə uyardır.

İnsidentlərin emalı üçün alətlər. CSIRT komandasına CSIRT məlumatlarını saxlamaq, analiz etmək və izləmək, loqları, faylları və artefaktları analiz etmək, (IP-)ünvanları və əlaqə məlumatlarını müəyyən etmək, sistemləri daramaq, müdaxilələri aşkarlamaq, şəbəkələrin monitorinqi, təhlükəsiz kommunikasiya üçün alətlər lazımdır.

İnformasiya təhlükəsizliyi insidentlərinin emalı proseslərini izləmək üçün xüsusi proqram təminatı istifadə edilir. Onlardan biri RTIR (request Tracker for Incident Response) pulsuz yayılır. RTIR proqramı JANET-CERT (Böyük Britaniya elm və təhsil şəbəkəsinin CERT komandası) komandası tərəfindən işlənilib, dünyada və Avropada bir çox CERT komandası tərəfindən istifadə edilir. İnsidentlərin izlənilməsi üçün digər həllər də mövcuddur: AIRT (Application for Incident Response Teams), OTRS (Open Ticket Request System), SIRIOS (System for Incident Response in Operational Security) və s.

Clearing House of Incident Handling Tools (CHIHT) pilot saytında CSIRT komandalarının istifadə etdikləri geniş yayılmış alətlərə çox sayda istinadlar tapmaq olar. Onlar iki istiqamət üzrə qruplaşdırılıb. Alətlərin birinci qrupu insidentlərin təhqiqatına aiddir (sübutların toplanması, insident sübutlarının tədqiqi, sübutların emalı, insidentdən sonra sistemin bərpası). İkinci qrupun CSIRT-in gündəlik işində istifadə edilən alətlər təşkil edir (insidentin izlənməsi, insidentlərin arxivi, məsafədən təhlükəsiz girişin təmini, boşluqların aşkarlanması və insidentlərin qarşısının alınması üçün preventiv alətlər).

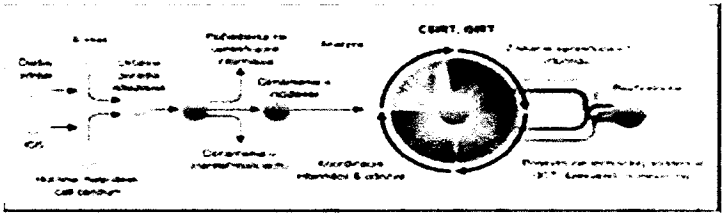
CSIRT-in fiziki təhlükəsizliyi. Fiziki mühafizə tələblərinə daxildir:

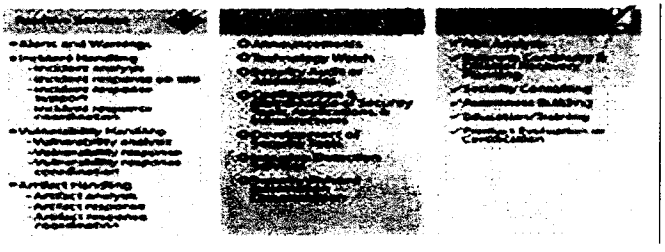
- serverlər və verilənlər bazaları üçün mühafizəli otaqlar;
- CSIRT-in əməliyyatlarını müzakirə etmək və insidentlərin təhqiqatını aparmaq üçün mühafizəli və səskeçirməyən otaqlar;
- qeyri-elektron verilənlərin və yazıların saxlanması üçün seyf;

- mühafizəli kommunikasiya mexanizmləri, məsələn, mühafizəli telefonlar, fakslar və e-poçt.
- CSIRT heyətinin təşkilatın qalan hissələrində fiziki izolyasiya edilməsi.

Verilənlərin ehtiyat surətçıxarması. Verilənlərin ehtiyat surətlərinin çıxardılması da informasiya təhlükəsizliyi mexanizmidir, onlar təhlükəsizlik qaydalarının pozulmasına qarşı son müdafiə xəttidir. Verilənlərin ehtiyat surətçıxarması üçün çoxsaylı alətlər mövcuddur, məsələn, UNIX və Linux istifadəçiləri üçün tar, dump, dd və s. dd alətindən Windows istifadəçiləri də istifadə edə bilərlər. Norton Ghost tipli alətlər İntel platformasında binar ehtiyat surətlər yaza bilər.

Ehtiyat surətlər üçün daşıyıcı kimi tərpənməz disklər, DVD, CD-disklər, ZIP-qurğular və lentlərin müxtəlif növləri istifadə edilə bilər. Ehtiyat surətçıxarmanın şəbəkə aələtləri də yaxşı həll ola bilər.





FƏSİL 4

CSIRT SERVİSLƏRİ

CSIRT SERVİSLƏRİ

- **Cavablandırma servisləri**
- **Profilaktika servisləri**
- **Təhlükəsizliyin keyfiyyətini idarəetmə servisləri**
- **Təhlükəsizlik bülletenlərinin formatı**
- **Boşluqlar haqqında məlumatların açıqlanması**
- **Boşluqların qiymətləndirilməsi sistemləri**
- **CVSS sistemi**

FƏSİL 4 CSIRT SERVİSLƏRİ

CSIRT-in öz kliyentlərinə göstərə biləcəyi servislərin sayı olduqca çoxdur, lakin hələlik mövcud CSIRT-lərin heç biri bu servislərin hamısını təqdim etmir. Buna görə də təqdim ediləcək servislərin seçilməsi çox vacib məsələdir. Aşağıda CERT/CC tərəfindən nəşr edilmiş "Handbook of CSIRT" kitabında təsvir olunmuş bütün məlum CSIRT servisləri haqqında qısa məlumat verilir.

CSIRT komandasının göstərdiyi servisləri cavablandırma servisləri, profilaktika servisləri və təhlükəsizlik sisteminin keyfiyyətinin idarə edilməsi servisləri kimi üç sinifə bölmək olar.

Cavablandırma servisləri insidentlərin emalına və potensial ziyanın azaldılmasına, profilaktika servisləri isə məlumatlılığın artırılması və treninqlər vasitəsi ilə insidentlərin qarşısının alınmasına yönəlib. Təhlükəsizlik sisteminin keyfiyyətinin idarə edilməsi servisi məsləhət və təhsil tədbirlərindən ibarətdir və uzunmüddətli məqsədlər güdür.

4.1. Cavablandırma servisləri

Cavablandırma servisləri CSIRT-in əsas servisləridir. Bu servislərə aşağıdakılar daxildir:

1) **Xəbərvermə və xəbərdarlıq** – bu servislər təhlükəsizlik boşluğu, müdaxilə, kompyuter virusu və ya aldatma kimi problemlərin həlli üçün məlumat verilməsini və cavablandırma metodlarının təqdim edilməsini nəzərdə tutur.

2) **İnsidentlərin emalı** – bu servis insident bildirişlərinin alınmasını, nizamlanmasını və cavablandırılmasını, insidentlərin

və hadisələrin analizini və prioritetinin müəyyən edilməsini özündə birləşdirir. Konkret cavab tədbirlərinə aşağıdakılar daxildir:

- **İnsidentin analizi** – bütün əlyetən informasiyanın və təsdiqləyici sübutların, insident və ya hadisə ilə əlaqəli artefaktların ekspertizası. Belə analizin məqsədi bu insidentin miqyasını, insidentin vurduğu ziyanın dərəcəsini, insidentin təbiətini və əlyetən cavablandırma metodlarını və strategiyalarını müəyyən etməkdir.
- **Maddi sübutların toplanması** – sistemdəki dəyişikliklərin müəyyən edilməsi və risq yaratmış hadisələrin bərpasına (rekonstruksiyasında) kömək etmək üçün risqə məruz qalmış sistemdə sübutların toplanması, saxlanması, sənədləşdirilməsi və analizi.
- **Axtarış və izləmə** – bədniyyətlinin zədələnmiş sistemə və onunla əlaqəli şəbəkəyə necə giriş əldə etməsi izlənir və ya axtarılır. Baxılan fəaliyyətə "çağırılmamış qonağın" mənşəyinin izlənməsi və ya bədniyyətlinin girdiyi sistemlərin aşkarlanması daxildir.

3) **İnsidentlərin yerində cavablandırılması** – CSIRT kliyentlərə insidentdən sonra özünə gəlmək üçün bilavasitə yerində kömək göstərilməsini təmin edir.

4) **İnsidentləri cavablandırma üzrə dəstək** – CSIRT insidentdən sonra bərpa zamanı hücum qurbanlarına telefon, elektron poçt, faks və ya sənədlərin köməyi ilə yardım və rəhbərlik edir.

5) **İnsidenti cavablandırmanın koordinasiyası** – İnsidentə cəlb edilmiş tərəflər arasındakı cavablandırma üzrə işlər koordinasiya edilir. Bura, bir qayda olaraq, hücumun qurbanı, hücum zamanı cəlb edilmiş digər tərəflər, həmçinin hücumun analizi zamanı köməyə ehtiyacı olan istənilən tərəflər daxildir. Bura qurbana İT-dəstək göstərən ISP və digər CSIRT-lər kimi tərəflər də daxil ola bilər.

6) **Boşluğun aşkarlanması zamanı hərəkətlər** – aparat vasitələrinin və proqram təminatının boşluğu haqqında məlumatların alınmasını, boşluğun təsirlərinin analizini, boşluğun aşkarlanması və aradan qaldırılması üçün cavablandırma strategiyasının işlənməsini nəzərdə tutur.

- **Boşluğun analizi** – aparat vasitələrinin və ya proqram təminatının boşluğunun texniki analizinə və ekspertizasına aiddir. Belə analizə misal boşluğun mənşəyini müəyyən etmək üçün sazlayıcı istifadə edilməklə ilkin koda baxılması və ya test sistemində problemin təkrarlanması cəhdi ola bilər.
- **Boşluğun cavablandırılması** – boşluqların "yumşaldılması" və aradan qaldırılması üçün müvafiq tədbirlərin müəyyən edilməsini nəzərdə tutur. Baxılan servis yenilənmələrin və yamaqların quraşdırılması yolu ilə cavablandırmanın həyata keçirilməsini nəzərdə tutur. Bura nəticələrin yumşaldılması strategiyaları, boşluq barəsində məlumatlandırma, tövsiyələr və xəbərdarlıqlar da daxildir.
- **Boşluğu cavablandırmanın koordinasiyası** – CSIRT təşkilatın müxtəlif bölmələrini və kliyentləri boşluq haqqında məlumatlandırır və təhlükəni azaltmaq və ya aradan qaldırmaq barəsində məlumat verir, CSIRT boşluğu uğurla cavablandırma strategiyalarını da klassifikasiya edir. Tədbirlərə boşluğun analizi və ya boşluq haqqında məlumatlar, müxtəlif tərəflərin etdiyi texniki analizin ümumiləşdirilməsi daxildir. Bu servisə boşluqlar və müvafiq cavab tədbirləri haqqında məlumatlar olan dövlət və ya özəl arxivin və ya biliklər bazasının aparılması da daxil ola bilər.

7) Artefakt servisləri – bu servislər kompyuter virusları, troya atları, soxulcanlar, skriptlər və istifadə edilmiş digər alətlərlə əlaqədar artefaktların analizi, cavablandırılması, koordinasiyası və emalından ibarətdir. Bu servislərə ziyankar proqram

təminatının sonrakı yayılmasının qarşısını almaq üçün istehsalçılar və digər maraqlı tərəflər arasında yekun informasiyanı yaymaq da daxildir.

- **Artefaktın analizi** – CSIRT sistemdə tapılmış istənilən artefaktın texniki ekspertizasını və analizini yerinə yetirir. Artefaktları fərdi kompyuterdə, lokal şəbəkədə, İnternetdə, e-poçtda, vebdə, mobil qurğularda, idarə edilməyən qurğularda, ilkin kodlarda, kontentdə tapmaq olar.
- **Artefaktın cavablandırılması** – artefaktların aşkarlanması və sistemdən silinməsi üçün lazımi tədbirlərin müəyyən edilməsi daxildir.
- **Artefaktın cavablandırılmasının koordinasiyası** – artefakta aidiyyəti olan digər tədqiqatçılarla, CSIRT-lərlə, provayderlərlə və digər təhlükəsizlik ekspertləri ilə nəticələrin analizinin və cavablandırma strategiyalarının mübadiləsi və ümumiləşdirilməsi aiddir.

4.2. Profilaktika servisləri

Profilaktika servisləri hər hansı insident və ya hadisə aşkarlanana kimi kliyentlərin təhlükəsizlik infrastrukturunun və proseslərinin yaxşılaşdırması üçün təqdim edilir. Bu servislərə aşağıdakılar aiddir:

1) Xəbərdarlıq – onlara həyəcan siqnalları, boşluqlar barəsində bülletenlər, təhlükəsizlik üzrə məsləhətlər və s. aiddir. Bu xəbərdarlıqlar kliyentlərə ortamüddətlidən uzunmüddətli təsirə kimi yeni işləmələr barəsində məlumatlar verirlər, məsələn yeni aşkarlanmış boşluqlar və bədniyyətlinin alətləri kimi. Xəbərdarlıqlar kliyentlərə öz sistemlərini və şəbəkələrini yeni aşkarlanmış problemlərdən onlar istifadə edilənə kimi mühafizə etməyə imkan verirlər.

2) Texnologiyaların izlənməsi – gələcək təhdidlərin müəyyən edilməsinə kömək etmək üçün yeni texniki işləmələrin, bədniyyətlilərin fəaliyyətinin və əlaqəli tendensiyaların

müşahidəsini və monitorinqini nəzərdə tutur. Bu servisin nəticəsi təhlükəsizliyin orta və uzunmüddətli məsələlərinə yönəlik hərhansı rəhbər prinsiplər və ya tövsiyələr ola bilər.

3) Təhlükəsizliyin qiymətləndirilməsi və auditi – bu servis təşkilatın təhlükəsizlik infrastrukturunun təşkilatda müəyyən edilmiş tələblərə və ya tətbiq edilən digər sahə standartlarına əsasən ətraflı xülasəsini və analizini təqdim edir.

4) Təhlükəsizlik vasitələrinin, tətbiqi proqramların, infrastrukturun və servislərin sazlanması və xidmət göstərilməsi – bu servis vasitələri, tətbiqi proqramları və ümumi hesablama infrastrukturunu təhlükəsiz sazlama və xidmət üzrə müvafiq göstərişlər verir.

5) Təhlükəsizliyin təmin edilməsi üzrə vasitələrin yaradılması – bu servisə kliyentlərin istəkləri nəzərə alınmaqla yeni vasitələrin, proqram təminatının, plaqinlərin və yamaqların yaradılması daxildir, bu vasitələr təhlükəsizliyin təmin edilməsi məqsədi ilə yaradılır və yayımlanır.

6) Müdaxilələrin aşkarlanması üzrə servislər – bu servisi göstərən CSIRT müdaxilələrin aşkarlanması sistemlərinin (Intrusion Detection Systems, IDS) jurnallarına baxır, onları analiz edir və özlərinin hərəkət zonasında baş vermiş hadisələrin cavablandırılmasına başlayırlar.

7) Təhlükəsizliklə əlaqəli informasiyanın yayılması – bu servis kliyentlərə təhlükəsizliyin yüksəldilməsində kömək edən faydalı informasiya toplusu təqdim edir.

4.3. Təhlükəsizliyin keyfiyyətini idarəetmə servisləri

Təhlükəsizliyin keyfiyyətini idarəetmə servisləri – insidentləri, boşluqları və hücumları cavablandırma nəticəsində alınmış bilikləri təqdim etməyə yönəlirlər. Belə servislərə aiddir:

1) Risklərin analizi – real təhdidlərin qiymətləndirilməsi, informasiya resursları üçün risqlərin real kəmiyyət və keyfiyyət

qiymətləndirilməsi, cavablandırma strategiyasının və mühafizənin qiymətləndirilməsi üzrə CSIRT-in imkanlarının təkmilləşdirilməsini nəzərdə tutur.

2) Biznes-proseslərin fasiləsizliyinin və qəzalardan sonra bərpaetmənin planlaşdırılması – biznes-proseslərin fasiləsizliyi və kompyuter təhlükəsizliyi sisteminə hücumlar nəticəsində törədilmiş qəzalardan sonra bərpaetmə lazımi planlaşdırma ilə təmin edilir.

3) Təhlükəsizlik üzrə məsləhət – CSIRT biznes-əməliyyatların həyata keçirilməsi üçün praktiki məsləhətlər və tövsiyələr də verə bilər.

4) Məlumatlılığın yüksəldilməsi – CSIRT kliyentlərə zəruri olan təhlükəsizlik metodları və siyasətləri üzrə informasiyanın və tövsiyələrin aşkarlanması və verilməsi yolu ilə təhlükəsizlik məsələlərində məlumatlılıq səviyyəsini yüksəltməyə çalışır.

5) Təhsil/Təlim – bu servis insidentlər haqqında bildirişlərin tərtibi üzrə əsas prinsiplər, müvafiq cavablandırma metodları, insidentləri cavablandırma vasitələri, insidentlərin qarşısının alınması metodları kimi mövzular üzrə kadrların təhsilini və hazırlanmasını, həmçinin kompyuter təhlükəsizliyi insidentlərinin aşkarlanması, bildirilməsi və cavablandırılması üzrə zəruri olan digər məlumatların təqdim edilməsini nəzərdə tutur. Tədris metodlarına konfranslar, kurslar və öyrədici proqramlar daxildir.

6) Məhsulların qiymətləndirilməsi və ya sertifikatlaşdırılması – CSIRT vasitələrin, tətbiqi proqramların və digər servislərin köməyi ilə məhsulun təhlükəsizliyini və onun CSIRT və ya təşkilat tərəfindən qəbul edilən praktiki təhlükəsizlik səviyyələrinə uyğunluğunu təmin etmək üçün məhsulun qiymətləndirilməsini yerinə yetirə bilər.

Kliyentlərə göstəriləcək CSIRT servislərinin düzgün seçilməsi çox vacib addımdır. Servislərin seçilməsi təşkilatın servisləri keyfiyyətli göstərmək üçün resurslarından, informasiya

təhlükəsizliyi ilə əlaqəli digər bölmələrin mövcudluğundan, CSIRT ekspertlərinin kvalifikasiyasından asılıdır. Servislərin necə göstəriləcəyi: iş vaxtı, qarşılıqlı əlaqə metodları, informasiyanın yayımlanması, servislərin təşkilatda necə inkişaf etdiriləcəyi də əhəmiyyət daşıyır.

Müxtəlif servislərin prioritetləri müxtəlifdir. Adətən, cavablandırma servisləri profilaktika servislərindən və ya informasiya təhlükəsizliyinin keyfiyyətinin idarə edilməsi servislərindən daha yüksək prioritetə malikdir.

CSIRT-lərin əksəriyyəti "Məlumatlandırma və xəbərdarlıq" baza servislərinin göstərilməsindən başlayır, "Elanlar" göndərirlər və öz kliyentlərinə "İnsidentlərin emalı" servisini göstərirlər. Adətən, bu baza servisləri ictimai maraq səviyyəsini və diqqəti kliyentlər tərəfindən müəyyən edirlər və ən əsas servislər hesab edilirlər.

"Pilot" kliyentlər adlanan kiçik qrupun yaradılması, müəyyən zaman müddətində (pilot müddətində) baza servislərinin göstərilməsi və göstərilən servislərin keyfiyyəti haqqında onların fikir və rəylərinin öyrənilməsi tövsiyə olunur.

Maraqlı tərəf olan "pilot" kliyentləri, adətən, konstruktiv rəylər bildirilər və onların ehtiyaclarına adaptasiya olunmuş zəruri servislərin siyahısını hazırlamağa kömək edirlər.

4.4. CSIRT servislərinin təsviri

CSIRT-in hər bir servisi təsvir edilməli və bu təsvir bütün maraqlı tərəflərə əlyetən olmalıdır. Hər bir servis üçün iki təsvirin olması tövsiyə edilir:

- xarici auditoriya üçün – servisin kimə göstərildiyi, servisin göstərilməsi üçün necə müraciət edilməsi və CSIRT-dən gözləntilər təsvir edilir;
- daxili auditoriya üçün – xarici auditoriya üçün təsvir təkrar edilir, servisin göstərilməsi üzrə ətraflı tövsiyələr verilir və servisin idarə edilməsi təkrarlanır.

İstənilən CSIRT servisi iki ölçü ilə – məntiqi və texniki istiqamətlərdə təsvir edilməlidir. CSIRT servislərinin təsvir faktorları Cədvəl 4.1-də göstərilir.

Servisin məqsədi CSIRT-in missiyasından irəli gəlir, o da öz növbəsində informasiya təhlükəsizliyi şöbəsinin və ya CSIRT üzərində yüksəkdə duran başqa infrastrukturun missiyasından irəli gəlir.

Cədvəl 4.1. CSIRT servislərinin təsvir faktorları

Faktor	**Təsviri**
Məqsəd	Servisin məqsədi
Tərif	Servisin tətbiq sahəsinin təsviri
Funksiyalar	Servisin funksiyalarının təsviri
Əlyetənlik	Servisin kliyentlərə əlyetən olduğu şərtlər (kimə, nə vaxt və necə)
Keyfiyyət zəmanətləri	Servisin parametləri və kliyentlər üçün məhdudiyyətlər
Qarşılıqlı əlaqə və informasiyanın açıqlanması	Komandalar və kliyentlər, digər komandalar və ya jurnalistlər kimi üçüncü tərəflər arasında qarşılıqlı əlaqə. İnsident haqqında informasiyanın açıqlanması strategiyası da daxildir.
Digər servislərlə interfeys	Baxılan servislə CSIRT-in digər servisləri arasında informasiya axınları
Prioritetlər	Servis daxilində funksiyaların və servisin digər servislərə nəzərən prioritetlərinin təsviri

Servisin gerçəkləşdirilməsini təsvir etməzdən əvvəl mövcud resurslarla əlaqədar bütün məhdudiyyətləri başa düşmək, göstərilən xidmətlərin miqyasını və dərinliyini təsvir etmək vacibdir. Servis məqsədlə, resurslarla (maliyyə, insan, texniki), CSIRT heyətinin təcrübəsi və kvalifikasiyası ilə, səlahiyyətlərlə, xarici aləmlə əlaqələri ilə məhdudlana bilər.

Hər bir CSIRT servisinin öz funksiyaları çoxluğu var. Məsələn, insidentlərin emalı servisinə 4 funkisya daxildir:

sistemləşdirmə, emal, xəbərdaretmə və əks-əlaqə. Funksiyalar bölməsində funksiyanın məqsədi, gerçəkləşdirmə detalları və müvafiq prosedurlara istinadlar, funksiyalara prioritet verilməsi kriteriyaları, göstərilən xidmətlərin səviyyələri, keyfiyyət kriteriyaları göstərilir. Gerçəkləşdirmə detallarında fuksiyanın necə işə düşməsi, istifadə edilən kommunikasiya formaları, funksiyanın işləməsi üçün tələb edilən verilənlər (giriş və çıxış) göstərilir.

Əlyetənlik bölməsində kimin hansı şərtlərdə servisə giriş əldə etməsi, servisin hansı vaxtlarda əlyetən olması (müxtəlif servislər, servisin müxtəlif səviyyələri, insidentlərin müxtəlif növləri/prioritetləri, kliyentlərin müxtəlif növləri müxtəlif zamanlarda) göstərilir. Servisin göstərilməsi şərtləri aşağıdakılardır:

- insident haqqında müəyyən forma üzrə doldurulmuş bildiriş;
- kliyentin həqiqiliyinin yoxlanması prosedurunun mütləq yerinə yetirilməsi.

Keyfiyyət zəmanətləri bölməsində kliyentlərin servisin keyfiyyəti barədə gözləntiləri (müxtəlif kliyentlər, müxtəlif funksiyalar, müxtəlif zamanlar, müxtəlif prioritetlər üçün müxtəlif keyfiyyət), CSIRT-in hansı müddətdə kliyentin sorğusuna cavab verəcəyi göstərilir.

Qarşılıqlı əlaqə və informasiyanın açıqlanması bölməsində CSIRT-lə insident iştirakçıları arasında baş verən qarşılıqlı əlaqələr, CSIRT-in zərərçəkən tərəfdən nə gözləməsi, zərərçəkənin CSIRT-ə təqdim etdiyi fayllarla, sənədlərlə və materiallarla necə davranılacağı göstərilir (onlar CSIRT-dən kənara veriləcəkmi, əgər veriləcəksə, necə qorunacaqlar?).

Digər servislərlə interfeys bölməsində verilmiş servislə digər servislər arasında hansı qarşılıqlı əlaqələrin baş verməsi, qarşılıqlı əlaqə kriteriyaları göstərilir. Bütün servislər üçün ümumi olan funksiyaların mövcudluğu sualına cavab verilir. Məsələn, çox vaxt sistemləşdirmə funksiyası bütün servislər üçün ümumi olur.

CSIRT servisləri arasında informasiya axınları. Təklif edilən servislərin spektrindən asılı olmadan onların bir-biri ilə necə əlaqəli olmasını başa düşmək zəruridir. Xüsusi halda, aşağıdakıları müəyyən etmək zəruridir:

- hansı servislər digər servislərin informasiyasından asılıdır və ya digər servislərə informasiya verirlər;
- hansı servislərin ortaq informasiya mənbəyi var və ya CSIRT-in hər hansı funksiyaları üçün ümumidirlər;
- hansı servislər hər hansı şərtdən asılı olan (konfidensiallıq, qanunvericilik) informasiyanı emal edirlər;
- hansı servislər CSIRT-dən kənara informasiya verirlər.

İnformasiya axınlarının başa düşülməsi resursları optimallaşdırmağa və mövcud informasiyanı effektiv istifadə etməyə imkan verir. Müxtəlif servislər informasiyanı müxtəlif cür emal edirlər. Bir sıra hallarda informasiya axını məhdudlaşdırıla və ya hətta bloka alına bilər. Məsələn, informasiyanın açıqlanması siyasəti, qanunvericiliyin tələbləri, konfidensiallığın tələbləri, müqavilə şərtlərinin yoxluğu və s. Bu ssenari CSIRT işə başladıqdan sonra deyil, işə başlayana qədər həll edilməlidir.

4.5. İnformasiya təhlükəsizliyi bülletenlərinin yaradılması

Həyəcan siqnallarının, bülletenlərin, xəbərdarlıqların və elanların yaradılması eyni sxem üzrə aparılır:

- informasiyanın toplanması;
- informasiyanın vacibliyinin və mənbəyinin yoxlanması;
- toplanmış informasiya əsasında risqin qiymətləndirilməsi;
- informasiyanın yayımlanması;

Aşağıda bu iş sxemi ətraflı izah edilir.

Addım 1. Boşluq haqqında informasiyanın toplanması

CSIRT servisləri üçün giriş məlumatları verən mənbələrin iki əsas növü var:

- informasiya sisteminin boşluqları haqqında məlumatlar;

– insidentlər haqqında məlumatlar.

Fəaliyyət növündən və IT-infrastrukturdan asılı olaraq, boşluqlar haqqında açıq və qapalı çoxsaylı mənbələr mövcuddur:

– açıq və qapalı e-poçt göndərişi siyahıları;
– istehsalçıların boşluqlar haqqında məlumatları;
– veb-saytlar;
– İnternetdə məlumatlar;
– boşluqlar haqqında informasiya verə bilən ictimai və şəxsi əlaqələr (FIRST, TF-CSIRT, CERT/CC, US-CERT, ...).

Bütün bu məlumatlar informasiya sisteminin spesifik boşluqları haqqında bilik səviyyəsini artırır.

Addım 2. İnformasiyanın vacibliyinin və mənbəyinin yoxlanması

İdentifikasiya. Boşluq haqqında məlumatın mənbəyi həmişə yoxlanılmalıdır və kliyentə istənilən informasiyanın yayımlanmasından əvvəl mənbəyə etibar edib-etməməyi müəyyənləşdirmək lazımdır. Əks halda, insanlar səhvən narahat edilə bilərlər, bu biznes-proseslərdə lazımsız proseslərə gətirib çıxara və son nəticədə CSIRT-in nüfuzuna ziyan vura bilər.

Aktuallıq. Kliyentlərdə quraşdırılmış avadanlığın və proqram təminatının icmalı boşluq haqqında məlumatın aktuallığını müəyyən etmək üçün istifadə edilə bilər: "Kliyent baxılan proqram təminatından istifadə edirmi?", "Kliyent üçün bu informasiya aktualdırmı?".

Təsnifat. Alınmış bəzi informasiya "xidməti istifadə üçün" qrifi ilə nişanlana bilər (məsələn, insidentlər haqqında digər komandalardan daxil olan hesabatlar). Bütün informasiya göndərənin tələblərinə və öz informasiya təhlükəsizliyi siyasətinə uyğun olaraq emal edilməlidir. Yaxşı bir qayda var: "Əgər yayımlanma üçün nəzərdə tutulduğuna əmin deyilsiniznizsə, informasiyanı yaymayın, əgər şübhələnirsizsə, göndərəndən yayımlamaq üçün icazə alın".

Addım 3. Riskin qiymətləndirilməsi

Boşluğun riskinin və (mümkün) nəticələrinin qiymətləndirilməsi üçün bir çox metodlar var. Riski boşluğun istifadəsinin potensial mümkünlüyü kimi müəyyən etmək olar. Bir neçə vacib faktoru sadalayaq:

- Boşluq geniş məlumdurmu?
- Boşluq yayılıbmı?
- Boşluqdan istifadə etmək asandırmı?
- Boşluğu məsafədən istifadə etmək asandırmı?

Bu suallar boşluğun ciddiliyini anlamağa imkan verir.

Aşağıdakı düstur riskin qiymətləndirilməsinə sadə yanaşma ola bilər:

Nəticələr = Risq × Potensial ziyanlar

Potensial ziyanlar aşağıdakılar ola bilər:

- verilənlərə icazəsiz giriş;
- xidmətdən imtina (DoS);
- giriş hüququnun əldə edilməsi və ya artırılması və s.

Bu suallara cavab verərək, bülletenə potensial risq və nəticələr barəsində məlumat verən ümumi reytinq əlavə etmək olar. Çox zaman, Aşağı, Orta və Yüksək kimi sadə terminlər istifadə edilir.

Addım 4. İnformasiyanın yayımlanması

CSIRT kliyetlərin arzusundan və özünün kommunikasiya strategiyasından asılı olaraq bir neçə yayılma metodu arasından seçim edə bilər.

- veb-sayt;
- elektron poçt;
- bülletenlər;
- arxivlər və hesabatlar.

CSIRT-in yayımladığı təhlükəsizlik bülletenləri həmişə eyni struktura malik olmalıdır. Bu oxunaqlığı artırır və oxucu bütün vacib informasiyanı tez tapa bilir.

4.6. Təhlükəsizlik bülletenlərinin formatı

İstifadəçilərin və administratorların informasiya təhlükəsizliyi problemləri barəsində vaxtında məlumatlandırılması istehsalçılar və CSIRT komandaları üçün vacib məsələdir. Bunu həyata keçirmək üçün geniş yayılmış üsul "təhlükəsizlik bülletenləri"nin buraxılmasıdır. 2000-ci illərin əvvəlində təhlükəsizlik bülletenləri üçün müxtəlif formatlar istifadə edilirdi, bülletenlər müxtəlif struktura, terminologiyaya, dəqiqliyə malik idilər və bu müxtəlif mənbələrdən alınmış bülletenlərin öyrənilməsi, analizi, müqayisəsi zamanı bir çox çətinliklər yaradırdı.

Buna görə də 2002-2004-cü illərdə təhlükəsizlik bülletenlərinin tərtibi və mübadiləsi üçün bir sıra standartlar işləndi. Təhlükəsizlik bülletenlərinin ümumi formatı oxucuların, bülleten müəlliflərinin və naşirlərinin ehtiyaclarını əks etdirməli, əməkdaşlığa və təkrar istifadəyə imkan verməli, proseslərin avtomatlaşdırılmasını dəstəkləməli, asanlıqla genişləndirilə bilməlidir. Aşağıda onlar qısa təsvir olunur.

CAIF (Common Announcement Interchange Format) – təhlükəsizlik elanlarının saxlanması və emalı üçün XML-əsasında yaradılmış formatdır. Təhlükəsizliyə aid məsələnin əsas aspektlərini təsvir etmək üçün zəruri elementlərin baza, lakin müfəssəl toplusunu təqdim edir. Standartın yaradılması layihəsi 2002-2004-cü illərdə Ştutqart Universitetinin CERT komandası (RUS-CERT) tərəfindən icra edilmişdir (http://cert.uni-stuttgart.de/projects/caif/). Elementlər toplusunu müvəqqəti, ekzotik və ya yeni tələbləri əks etdirmək üçün asanlıqla genişləndirmək olar. Bir sənəd daxilində bir neçə problemi təsvir etməklə yanaşı, format informasiyanı oxucuların bir neçə qrupu üçün qruplaşdırmağa, sənəddə bir neçə dildə mətn verməyə imkan verir. CAIF elanları təcililik meyarına görə həyəcan, xəbərdarlıq, məsləhət, məlumat və digər xarakterli ola bilər, təfsilatına görə qısa, tam, annotasiya və s. olmaqla boşluğun təsvirinə, yamaq haqqında bildirişə, nəzərə çatdırma məlumatına həsr oluna bilər.

EISPP (European Information Security Promotion Program) – 2002-2004-cü illərdə Avropa İttifaqının 5-ci Çərçivə Proqramı (5th Framework Programme) daxilində yerinə yetirilib (http://www.eispp.org/). Layihənin məqsədi – kiçik biznesə təhlükəsizlik üzrə müntəzəm informasiya, ilk növbədə boşluqlar və təhdidlər haqqında mümkün xəbərdarlıqlar almaqda kömək etmək idi. İnformasiya təhlükəsizliyi məlumatları ilə işləmək müəyyən kvalifikasiya tələb edir ki, bu da kiçik biznes təşkilatlarında çox zaman çatışmır. Layihənin müsbət nəticələrinə xəbərdarlıqlar üçün EISPP Common Advisory Format standartının işlənməsini aid etmək olar.

DAF (Deutsches Advisory Format) formatı hazırda CSIRT-lər tərəfindən təhlükəsizlik bülletenlərinin yaradılması və müxtəlif komandalar arasında mübadiləsi üçün standart kimi istifadə edilir. DAF – Almaniya CERT-Verbund-un təşəbbüsüdür və EISPP Common Advisory Format əsasında xüsusi olaraq alman CERT-lərinin ehtiyacları üçün hazırlanmışdır, CERT-Bund, DFN-CERT, PRESECURE və Siemens-CERT kimi komandalar tərəfindən təkmilləşdirilir və dəstəklənir.

Təhlükəsizlik bülletenində ən azı aşağıdakı informasiya olmalıdır.

Bülletenin adı
.....
Nömrə ..... Təsirlənən sistemlər - ..... - ..... Əməliyyat sistemi və onun versiyası ..... Risq (Yüksək-Orta-Aşağı) ..... Nəticələri/potensial itkilər (Yüksək-Orta-Aşağı) ..... Boşluğun İdentifikatoru: (CVE, Vulnerability bulletin ID) .....
Boşluğun xülasəsi ..... Təsirləri ..... Çözümlər ..... İstinadlar

4.7. Boşluqlar haqqında məlumatın açıqlanması

Kompyuter sistemlərində boşluqlar layihələndirmə, reallaşdırma və istismar zamanı buraxılan səhvlər nəticəsində meydana çıxır. Boşluqların xeyli hissəsini istehsalçı məhsulun yaradılması, test edilməsi və müşaiyət edilməsi gedişində aşkarlanır, lakin onların bir hissəsi müstəqil tədqiqatçılar tərəfindən aşkarlanır. Boşluğu aşkarlayan şəxs məqsədlərindən, mənəvi dəyərlərindən və digər amillərdən asılı olaraq müxtəlif davranış strategiyaları seçə bilər.

Boşluğun aşkarlanması, düzəlişlərin hazırlanması və boşluğun aradan qaldırılması prosesi qarşılıqlı əlaqədə olan üç tərəfin: tədqiqatçının, istehsalçının və istifadəçinin maraqlarında münaqişə yaradır. İnformasiya təhlükəsizliyi boşluqları haqqında məlumatların açıqlanması metodları informasiya təhlükəsizliyi ictimaiyyəti arasında mübahisələrə səbəb olur.

Keçən əsrin sonlarında istehsalçıların dəstəklədiyi əsas siyasət açıqlamama (ing. non-disclosure) siyasəti idi, onu çox vaxt «susmaq yolu ilə təhlükəsizlik» (ing. security through obscurity) adlandırırdılar. Buna əks olaraq, bəzi mütəxəssislər boşluq tapılan kimi onun haqqında məlumatın əlyetər mənbələrdə tam açıqlanmasını (ing. full-disclosure) təkidlə tələb edirlər. Ümid edilir ki, bu yanaşma istehsalçıların təhlükəsizlik sahəsində fəallığını artıracaq və zəruri düzəlişlər olduqda istifadəçilərə boşluğu müstəqil aradan qaldırmağa imkan verəcək.

Lakin tam açıqlama siyasətinin tənzimlənməyən istifadəsi ciddi ziyan vura bilər, çünki bədniyyətlilər boşluqlar haqqında məlumatları, bir qayda olaraq, istifadəçilərdən və administratorlardan daha fəal istifadə edirlər.

Digər bir yanaşma bunu nəzərə alaraq, daha böyük riskə məruz qalan istifadəçilərə boşluq haqqında məlumat verilməsini, tam məlumatın isə yalnız müəyyən gecikmə ilə nəşr edilməsini və ya heç nəşr edilməməsini məsləhət görür. Gecikmə məlumatlandırılan istifadəçilərə boşluğu aradan qaldırmağa imkan verə bilər, lakin məlumat almayanlar baxımından riski artıra bilər.

Boşluq haqqında məlumatın açıqlanması üzrə bir sıra siyasətlər mövcuddur: Rain Forest Puppy (RFPolicy), CERT/CC Vulnerability Disclosure Policy, OIS Guidelines (Organization for Internet Safety). RFPolicy siyasətinə əsasən boşluğu aşkarlayan şəxs bu barədə istehsalçıya e-poçtla müvafiq məlumat göndərir. Məktubda açıqlama tarixi bildirilir və razılaşdırmaq tələb edilir ki, istehsalçının düzəliş buraxmağa və ya boşluqdan qorunmaq üçün məsləhətlər verməyə imkanı olsun. İstehsalçı, öz növbəsində həmin şəxslə əlaqə saxlamalı və onu problemin

aradan qaldırılması gedişi haqqında məlumatlandırmalıdır. Əgər beş gün başa çatdıqdan sonra istehsalçı susursa, hansısa üsullarla öz istifadəçilərini çaşdırırsa və ya nəzakətsiz dialoqa girirsə, onda xaker təkrar məktub göndərir. Daha beş iş günü gözlədikdən sonra xakerin boşluq haqqında məlumatı öz resursunda və ya digər açıq resurslarda yerləşdirmək hüququ var.

Qeyd etmək lazımdır ki, RFPolicy siyasətinin tələbləri kifayət qədər kəskindir, digər siyasətlərdə bu tələblər bir qədər yumşaldılır, məsələn, CERT/CC boşluq haqqında məlumatın açıqlanması üçün 45 gün, OIS Guidelines isə 30 gün vaxt qoyur.

4.8. Boşluqlar üzrə məlumat mənbələri

CSIRT komandası informasiya texnologiyalarının inkişafını, proqram və aparat təminatında aşkarlanmış boşluqları daim izləməlidir. İnformasiya təhlükəsizliyi boşluqları üzrə müxtəlif tezliklə məlumatlar nəşr edən onlarla veb-saytlar və göndəriş siyahıları mövcuddur. Bir sıra şirkətlər boşluqlar üzrə verilənlər bazasından pullu abunə xidmətləri də təklif edirlər (məsələn, Secunia şirkəti, secunia.com). Bu mənbələrin izlənməsi CSIRT komandası üçün xeyli çətinliklər törədir. Aşağıda informasiya təhlükəsizliyi boşluqları üzrə mötəbər mənbələr barəsində məlumat verilir.

SecurityFocus (http://www.securityfocus.com) – 1999-cu ildə fəaliyyətə başlayan SecurityFocus informasiya təhlükəsizliyi ictimaiyyətininin bilik və təcrübəsinin paylaşımı məqsədi ilə yaradılmışdı, hazırda informasiya təhlükəsizliyinin təmin edilməsi məsələlərinin geniş spektri üzrə məşhur informasiya mərkəzinə çevrilmişdir.

SecurityFocus veb saytı informasiya təhlükəsizliyi ictimaiyyətini maraqlandıran bir neçə əsas sahəyə diqqət yönəldir:

- BugTraq – müxtəlif platformalarda və servislərdə aşkarlanmış informasiya təhlükəsizliyi insidentlərinin ətraflı müzakirəsi üçün böyük həcmli göndəriş siyahısıdır. Əməliyyat sistemləri üzrə bölmələr, o cümlədən, Windows sistemlər üçün BugTraq göndəriş siyahısı mövcuddur.

–Boşluqlar bazası (www.securityfocus.com/vulnerabilities) – informasiya təhlükəsizliyi peşəkarlarını bütün platformalar və servislərdə aşkarlanmış boşluqlar haqqında ən yeni məlumatlarla təmin edir.

–Göndəriş siyahıları (Mailing Lists) – informasiya təhlükəsizliyi ictimaiyyətinin dünyadakı bütün üzvlərinə informasiya təhlükəsizliyinin müxtəlif məsələlərini müzakirə etməyə imkan verir. Hazırda 31 göndəriş siyahısı var və onların çoxu müzakirələri mövzu üzərində saxlamaq və spama yol verməmək üçün moderatorlar tərəfindən nizamlanır.

–İnsidentlər arxivi (http://www.securityfocus.com/incidents) – insidentlərin real zamanda xəbər verilməsi və müzakirəsi üçün açıq forumdur. Hücumlar və insidentlər barəsində kömək və tövsiyə xahiş etmək olar.

– İnsidentlərlə iş alətləri (http://www.securityfocus.com/tools) – annotasiya və reytinqi göstərilməklə informasiya təhlükəsizliyi alətlərinin daim artırılan geniş arxivi dəstəklənir, axtarış imkanları var.

Boşluqların tezaurusu üzrə baza. Boşluqların tezaurusu (Common Vulnerabilities and Exposures, CVE) – bütün məlum boşluqların vahid tezaurusudur, boşluqların adlandırılmasının vahid qaydalarını müəyyən edir, bütün maraqlanan şəxslərin Internet ilə çıxışı üçün açıqdır (cve.mitre.org). CVE boşluqların sistemləşdirilməsinə iddia etmir.

CVE-nin meydana çıxması müxtəlif mənbələrdə, o cümlədən şəbəkə skanerlərində (məsələn, Internet Scanner və CyberCop Scanner) eyni boşluğun müxtəlif cür adlandırılması ilə əlaqədar idi. CVE müxtəlif şəbəkə skanerlərinin imkanlarının müqayisəsi məsələsini olduqca asanlaşdırır. Eyni CVE-dən istifadə edən skanerlər üçün onların aşkarladıqları boşluqların siyahısını tutuşdurmaq kifayətdir. Əgər skanerlər boşluqları adlandırmaq üçün müxtəlif işarələmə sistemindən istifadə edirsə, onların müqayisəsi məsələsi olduqca çətinləşir.

Hazırda şəbəkə skanerləri istehsalçılarının çoxu, o cümlədən Symantec, NAI, ISS, Cisco və başqaları öz məhsullarında boşluqları adlandırmağın standart üsulu kimi CVE-ni dəstəklədiklərini bəyan edirlər.

CVE indeksinin (CVE Entry) alınması prosesi boşluğun aşkarlanmasından başlayır. Boşluğa CVE namizədi statusu və müvafiq nömrə (CVE candidate number) verilir. Nömrədə il və unikal indeks göstərilir, məsələn, CAN-199-0067. CVE namizədi qısa təsvir edilir və müvafiq istinadlarla əlaqələndirilir. CVE Editorial Board tərəfindən namizədin müzakirəsi keçirilir və ona CVE indeksinin verilib-verilməməsi haqqında qərar qəbul edilir. Namizəd təsdiqlənəndən sonra "CAN" önlüyü "CVE" ilə əvəzlənir.

CVE indeksi aldıqdan sonra məlumat saytda yerləşdirilir, CVE indeksinə əsasən boşluğun təsvirini və onun aradan qaldırılması haqqında məlumatları tez tapmaq olar.

OSVDB verilənlər bazası (http://osvdb.org/). 2002-ci ilin avqustunda Black Hat və Defcon konfranslarında proqram və aparat təminatındakı boşluqlar haqqında məlumatlar yayımlayan müstəqil və açıq mənbə kimi Open Source Vulnerability DataBase (OSVDB) verilənlər bazasının yaradılması qərarlaşdırıldı.

Hazırda OSVDB layihəsi çərçivəsində 200-ə yaxın könüllü mütəxəssis tərəfindən boşluqlar üzrə mərkəzləşdirilmiş verilənlər bazası yaradılıb, bazaya giriş açıqdır və axtarış vasitələri var. OSVDB mümkün qədər çox məhsul əhatə etməyə çalışır. OSVDB verilənlər bazasını müvafiq OSVDB-lisenziya imzalamaqla pulsuz yükləmək olar. Verilənlər bazasında hər bir boşluğa unikal OSVBD ID nömrəsi verilir.

NVD verilənlər bazası (http://nvd.nist.gov/). 2005-ci ildə Milli Standartlar və Texnologiyalar İnstitutu tərəfindən Vahid Boşluqlar Bazası (National Vulnerability Database, NVD) istifadəyə verildi. NVD-yə informasiya təhlükəsizliyi üzrə yoxlama vərəqləri bazası, proqram təminatı və konfiqurasiyalar üzrə boşluqlar bazası, məhsul siyahıları və təhülkəsizliyin

yoxlanması üzrə metrikalar daxildir. NVD saytında US-CERT məlumatları, o cümlədən boşluqlar haqqında qeydlər və texniki həyəcan siqnalları da yerləşdirilir.

NVD ABŞ hökümətinə boşluqlar üzrə əlyetən bütün resursları vahid bazada birləşdirir, CVE standartına əsaslanır və ona tam uyğundur. NVD veb-saytında axtarış, statistika, NVD məlumatlarının bazadan XML formatında yüklənməsi xidmətləri var, onlardan qeydiyyatdan keçmədən və pulsuz istifadə etmək olar.

NVD statistika mexanizmi konkret məhsullarda və ya konkret boşluq növlərində aşkarlama reytinqində olan dəyişiklikləri qiymətləndirməyə imkan verir, zamana görə boşluqların trendi üzrə statistika generasiya edir. Müəyyən məhsulları və istehsalçıları da izləmək olar.

14 iyul 2011-ci il tarixində NVD repozitarisində 46958 boşluq, 177 yoxlama siyahısı, 212 US-CERT həyəcan siqnalı, US-CERT-in boşluqlar haqqında 2511 qeydi, 6057 OVAL sorğusu vardı (OVAL – Open Vulnerability and Assessment Language). Həmin vaxt CVE-nin nəşr sürəti gündə 10 boşluq idi.

4.9. Boşluqların qiymətləndirilməsi sistemləri

Boşluğun risk dərəcəsi, bir qayda olaraq boşluq aşkarlanan sistemin istehsalçısı və ya informasiya təhlükəsizliyi vasitələri istehsal edən (boşluq skanerləri, IDS sistem və s.) şirkət tərəfindən müəyyən edilir. Bu zaman yol hərəkəti qaydalarında olan işıqfor sxemi istifadə edilir: aşağı dərəcədə risk (yaşıl), orta dərəcədə risk (sarı) və yüksək dərəcədə risk (qırmızı). Bəzən əlavə olaraq riskin dördüncü dərəcəsi – kritik boşluqlar da daxil edilir.

Belə yanaşmadan istehsalçıların əksəriyyəti istifadə edir. Məsələn, Microsoft proqram təminatı yenilənmələri haqqında elanlarında boşluqların kritikliyinin dörd səviyyəsindən istifadə edir.

Bu sadə yanaşma administratorun tələblərini həmişə ödəmir. Boşluğun risk dərəcəsi zaman keçdikcə dəyişə bilər. İstifadəsinin detalları yalnız istehsalçı şirkətin mütəxəssislərinə məlum olan

kritik boşluqla istismar proqramı əlyetən olan boşluq arasındakı fərq böyükdür.

Boşluğun istifadə edilməsi ehtimalı ilə əlaqədar faktorları nəzərə almaq üçün standart "işıqfor" modelinə əlavə şərtlər daxil etmək lazımdır. Məsələn, SANS İnstitutu boşluqların analizi zamanı (SANS Critical Vulnerability Analysis) o boşluqlara kritik səviyyə verir ki, bu boşluqdan istifadə edən, hamıya əlyetən və ya istismarı xüsusi vərdişlər tələb etməyən proqram mövcud olsun. Əks halda, hətta potensial olaraq çox təhlükəli boşluq kritik yox, yüksək səviyyəyə malik olacaq. SANS metodikasında istismarın sadəliyi ilə yanaşı, boşluğa həssas sistemlərin yayılması da nəzərə alınır.

Microsoft şirkətinin PSS qrupu ziyankar proqram təminatı ilə bağlı riskin qiymətləndirilməsi metodikasında boşluğu aradan qaldıran yenilənmənin mövcudluğu, hücum edənin istifadə edə biləcəyi hücum vektorlarının sayı, boşluğa həssas sistemlərin yayılması nəzərə alınır. Məsələn, "kritik təhlükəli soxulcan" yenilənmə olmayan Microsoft proqram təminatındakı lağım vasitəsilə, geniş yayılmış sistemlərdə iki və daha artıq hücum vektorundan istifadə etməklə yayılmalıdır.

US-CERT-in istifadə etdiyi metodikada boşluğa aşağıdakı kriteriyalardan asılı olaraq qiyməti 0-180 arasında olan risk dərəcəsi müəyyən edilir.

- boşluq haqqında informasiya nə dərəcədə əlyetəndir?
- boşluqdan istifadə halları qeydə alınıbmı?
- şəbəkə üçün kritik İnternet-qovşaqlara təhlükə varmı?
- şəbəkənin boşluğa həssas qovşaqlarının sayı.
- boşluqdan istifadənin nəticələri necədir?
- boşluqdan istifadə nə dərəcədə asandır?
- boşluqdan istifadənin şərtləri necədir?

Təəssüf ki, kriteriyalar arasında onların mümkün çəkiləri və nəticədə alınan risq dərəcəsi formal müəyyən edilməyib, bu eyni boşluğun qiymətləndirilməsində ziddiyyətlər üçün geniş meydan verir. Bundan başqa, sadalanmış metodikalar konkret iş üçün yox, bütövlükdə İnternet üçün riskin qiymətini verir.

Yuxarıda qeyd edilənləri ümumiləşdirərək boşluğun qiymətləndirilməsi metodikasına tələbləri aşağıdakı kimi ifadə etmək olar:

- boşluğun risk dərəcəsinin boşluğun istismarı imkanından asılı olaraq qiymətləndirilməsi imkanı olmalıdır;
- metodikanın tətbiqinin nəticəsi risklərin analizi zamanı istifadə üçün yararlı olan ədədi qiymət olmalıdır;
- metodikanın konkret informasiya sisteminə adaptasiyası imkanı olmalıdır;
- qiymətləndirmə zamanı istifadə edilən parametrlər minimum müxtəlif yozuma malik olmalıdır;
- yekun qiymətin hesablanması mexanizmi sadə və anlaşıqlı olmalıdır.

4.10. CVSS sistemi

Boşluqları ümumi qiymətləndirmə sistemi (Common Vulnerability Scoring System, CVSS) – IT-boşluqların menecerlər, tətbiqi proqramların və informasiya təhlükəsizliyi vasitələrinin istehsalçıları, tədqiqatçılar və istifadəçiləri üçün anlaşıqlı, şəffaf və ümumi qəbul edilmiş qiymətləndirmə üsuludur. CVSS qiymətləndirmə sistemi 3 metrikadan ibarətdir:

- baza metrikası (Base Score Metrics);
- zaman metrikası (Temporal Score Metrics);
- mühit metrikası (Environmental Score Metrics).

Hər bir metrika 0-dan 10-a kimi intervalda olan ədəddən (qiymətdən) və vektordan – qiymətin hesablanması üçün istifadə edilən kəmiyyətlərin qısa mətn təsvirindən ibarətdir. Baza metrikası boşluğun əsas xarakteristikalarını əks etdirir. Zaman metrikası boşluğun zamanla dəyişən xarakteristikalarına, mühit metrikası – boşluğun istifadəçinin mühiti üçün unikal xarakteristikalarına uyğundur.

4.10.1. Baza metrikaları

Boşluğun baza metrikalarına zamana görə dəyişməyən aşağıdakı parametrlər daxildir.

Giriş vektoru (Access Vector, AV) boşluğun necə aşkarlanmasını və istifadə edilə bilməsini müəyyən edir. Mümkün variantlar belə seçilib:

- Lokal (L) – boşluğun aşkarlanması və istifadə edilməsi üçün bədniyyətlinin boşluğa həssas sistemə fiziki girişi və ya lokal uçot yazısı olmalıdır;
- Şəbəkə seqmenti (Adjacent Network, A) – boşluq yalnız boşluğa həssas sistemin yerləşdiyi şəbəkə seqmentində aşkarlana və istifadə edilə bilər;
- Şəbəkə (N) – boşluq açıq şəbəkədən (İnternet) aşkarlana və istifadə edilə bilər.

İstifadənin çətinliyi (Access Complexity, AC) boşluq vasitəsi ilə sistemə giriş əldə edildikdən sonra hücumun nə qədər çətin olmasını müəyyən edir. CVSS üç səviyyə müəyyən edir:

- Yüksək (H) – boşluqdan yararlanmaq üçün hücum edən yüksək kvalifikasiyaya malik olmalı, sistem haqqında əhəmiyyətli informasiyaya malik olmalı, sosial mühəndisliyin mürəkkəb metodlarından istifadə etməli və ya hücumun gerçəkləşdirilməsinin qeyri-standart vasitələrini (yollarını) ixtira etməlidir;
- Orta (M) – hücum edən tərəf müəyyən avtorizasiya səviyyəsində sistemlər və ya istifadəçilər qrupu ilə məhduddur, uğurlu hücumun başlanması üçün müəyyən iformasiya toplanmalıdır, hücum kiçik miqyasda sosial mühəndislik tələb edir, boşluğa həssas konfiqurasiya defolt deyil və geniş yayılmayıb;
- Aşağı (L) – boşluqdan istifadə çətin deyil – konfiqurasiya defoltdur, xüsusi hüquqlar tələb edilmir (məsələn, anonim istifadəçi), istifadəçilər dairəsi genişdir, çətin nəzarət edilir, kiçik qabiliyyət və az iformasiya toplamaq tələb edilir.

Autentifikasiya (Authentication, Au) boşluqdan istifadə etmək imkanı əldə edənə qədər bədniyyətlinin neçə autentifikasiya və avtorizasiya səviyyəsindən keçəcəyini müəyyən edir. CVSS üç səviyyə təklif edir:

- Çox (Multiple, M) – bir neçə autentifikasiya və avtorizasiya tələb edilir;
- Yeganə (Single, S) – bir avtorizasiya tələb edilir;
- Heç (None, N) – autentifikasiya və avtorizasiya yoxdur.

Konfidensiallığa təsir (Confidentiality Impact, CI) boşluqdan istifadə edən uğurlu hücumun sistemin və verilənlərin konfidensiallığına təsirini göstərir. CVSS üç səviyyə müəyyən edir:

- Heç (None, N) – təsir yoxdur;
- Qismən (Partial, P) – konfidensiallığın qismən itirilməsi (kritik verilənlərə giriş imkanı məhduddur);
- Tam (Complete, C) – konfidensiallığın tam itirilməsi (məxfi sənədlərin və kritik verilənlərin itirilməsi və ya üstünün açılması).

Tamlığa təsir (Integrity Impact, II) boşluqdan istifadə edən uğurlu hücumun sistemin və verilənlərin tamlığına təsirini göstərir. CVSS üç səviyyə müəyyən edir:

- Heç (None, N) – təsir yoxdur;
- Qismən (Partial, P) – tamlığın qismən itirilməsi (sistemdə və ya onun ayrı-ayrı modullarının konfiqurasiyasının bir hissəsində dəyişikliklər mümkündür, verilənlərin bir hissəsində dəyişikliklər edilə bilər və s.);
- Tam (Complete, C) – tamlığın tam itirilməsi (vacib verilənlərin əvəzlənməsi, bütün sistemin konfiqurasiyasında və proseslərində dəyişiklik).

Əlyetənliyə təsir (Availability Impact, AI) boşluqdan istifadə edən uğurlu hücumun sistemin əlyetənliyinə təsirini göstərir. CVSS üç səviyyə müəyyən edir:

- Heç (None, N) – təsir yoxdur;

- Qismən (Partial, P) – qismətən əlyetən deyil (sistemin və ya onun hissələrinin məhsuldarlığının bir qədər düşməsi, sistemin işində və resursun əlyetənliyində qısa fasilələr müşahidə edilir);
- Tam (Complete, C) – sistemin əlyetənliyi tam pozulub (DoS-hücumu, resurslar əlyetən deyil, prosessor tam yüklənib və s.).

4.10.2. Zaman metrikaları

Boşluğun zamana görə dəyişən xarakteristikalarını qiymətləndirən zaman istismarın mümkünlüyü (Exploitability), boşluğun aradan qaldırılması imkanının varlığı (Remediation Level) və boşluq haqqında informasiyanın səhihliyi (Report Confidence) kimi parametrlər istifadə edilir.

İstismarın mümkünlüyü (Exploitability, E) boşluğun cari vəziyyətini və giriş əldə edərək boşluğu istismar etməyə imkan verən kodun mövcudluğunu müəyyən edir. CVSS bir neçə səviyyə müəyyən edir:

- Təsdiqlənməmiş (Unproven, U) – boşluq təsdiqlənməyib və boşluğu istismar etməyə imkan verən kod yoxdur;
- Konsepsiyanın isbatı (Proof of Concept, POC) – boşluğu bəzi sistemlərdə istismar etməyə imkan verən kod mövcuddur, lakin onu modifikasiya etmədən hücum üçün istifadə etmək olmaz;
- Funksional (Functional, F) – boşluğu əksər sistemlərdə istifadə etməyə imkan verən kod mövcuddur, boşluğun tam və ya qismən texniki təsviri müəyyən şəxslərə əlyetəndir;
- Yüksək (High, H) – boşluğu istismar etməyə imkan verən bir çox kod variantı mövcuddur, yaxud boşluqdan istifadə etmək üçün eksployt lazım deyil, boşluğun texniki detalları geniş məlumdur;
- Müəyyən edilməyib (Non Determined, ND) – parametri nəzərə almamaq üçün istifadə edilir.

Müalicə səviyyəsi (Remediation Level, RL) boşluğu aradan qaldıran yenilənmənin mövcudluğunu müəyyən edir. CVSS beş səviyyə müəyyən edir:

- Rəsmi yenilənmə (Official Fix, OF) – boşluğu tam bağlayan rəsmi yenilənmə var;
- Müvəqqəti yenilənmə (Temporary Fix, TF) – boşluğu qismən bağlayan müvəqqəti yeniləmə var;
- Dolayı həll (Workaround, W) – qeyri-rəsmi, müvəqqəti dolayı həll var;
- Əlyetməz yenilənmə (Unavailable, U) – yenilənmə yoxdur və ya onu tətbiq etmək mümkün deyil;
- Müəyyən edilməyib (Not Defined, ND) – parametri nəzərə almamaq üçün istifadə edilir.

Hesabatın səhihliyi (Report Confidence, RC) boşluq haqqında alınmış məlumatların və texniki məlumatların səhihlik dərəcəsini müəyyən edir. CVSS dörd səviyyə müəyyən edir:

- Təsdiqlənməmiş (Unconfirmed, UC) – boşluq istehsalçı (vendor) tərəfindən rəsmən təsdiqlənməyib, təsdiqlənməmiş bir məlumat və ya bir-birinə zidd olan bir neçə məlumat var;
- Müstəqil təsdiqlənmiş (Uncorroborated, UR) – boşluq bir neçə qeyri-rəsmi mənbə (müstəqil təhlükəsizlik şirkətləri və elmi təşkilatlar) tərəfindən təsdiqlənib;
- Təsdiqlənmiş (Confirmed, C) – boşluq istehsalçı tərəfindən rəsmən təsdiqlənib, yaxud boşluqdan istifadə edən işlək proqram mövcuddur;
- Müəyyən edilməyib (Not Defined, ND) – qiymətləndirmədə parametri nəzərə almamaq üçün istifadə edilir.

4.10.3. Mühit metrikaları

Mühit metrikaları – boşluğun uğurlu istifadəsinin şirkətə, onu əhatə edən mühitə və maraqlı tərəflərə təsirini qiymətləndirməyə imkan verən parametrlərdir.

Boşluğun uğurlu istifadəsi nəticəsində **potensial ziyan** (Collateral Damage Potential, CDP) – maddi və qeyri-maddi aktivlərə, nüfuza, insanların həyatına ziyan vurulması ehtimalını göstərir. CVSS altı səviyyə müəyyən edir:

- Heç (None, N) – əməkdaşların həyatına, fiziki aktivlərə, məhsuldarlığa və gəlirə ziyan potensialı yoxdur;
- Aşağı (Low, L) – boşluğun uğurlu istismarı nəticəsində təşkilatın fiziki aktivlərinə, məhsuldarlığına və gəlirinə yüngül ziyan vurula bilər;
- Orta-aşağı (Low-Medium, LM) – boşluğun uğurlu istismarı nəticəsində təşkilatın fiziki aktivlərinə, məhsuldarlığına və gəlirinə orta ziyan vurula bilər;
- Orta-yüksək (Medium-High, MH) – boşluğun uğurlu istismarı nəticəsində təşkilatın fiziki aktivlərinə, məhsuldarlığına və gəlirinə əhəmiyyətli ziyan vurula bilər;
- Yüksək (High, H) – boşluğun uğurlu istismarı nəticəsində təşkilatın fiziki aktivlərinə, məhsuldarlığına və gəlirinə çox böyük ziyan vurula bilər;
- Müəyyən edilməyib (Not Defined, ND) – qiymətləndirmədə parametri nəzərə almamaq üçün istifadə edilir.

Aydındır ki, hər bir təşkilat özü üçün "yüngül, orta, əhəmiyyətli və çox böyük ziyan" anlayışlarının dəqiq mənalarını müəyyən etməlidir.

Hədəflərin sıxlığı (Target Distribution, TD) – baxılan boşluğa həssas hədəflərin varlığını və əlyetənliyini qiymətləndirir. CVSS beş səviyyə müəyyən edir:

- Heç (None, N) – hədəf sistemlər yoxdur və ya yalnız qapalı laborator şəraitdə mövcuddur;
- Aşağı (Low, L) – mövcud mühitdə bir neçə potensial hədəf sistem var, lakin onların əlyetənliyi məhduddur. Bütün mühitin 1%-25%-i risk altındadır;
- Orta (Medium, M) – istifadə edilən sistemlərin çox hissəsi boşluğa həssasdır və əlyetəndirlər. Bütün mühitin 26%-75%-i risk altındadır;

- Yüksək (High, H) – mövcud mühitdə sistemlərin, demək olar, hamısında baxılan boşluq var və hücum üçün əlyetəndirlər. Bütün mühitin 76% - 100%-i risk altındadır.
- Müəyyən edilməyib (Not Defined, ND) – qiymətləndirmədə parametri nəzərə almamaq üçün istifadə edilir.

Təhükəsizlik tələbləri (CR, IR, AR) konfidensiallığın, tamlığın və əlyetənliyin pozulmasının təşkilata və onun əməkdaşlarına nə dərəcədə təsir etmələrini müəyyən edir. CVSS dörd səviyyə müəyyən edir.

- Aşağı (Low, L) – konfidensiallığın | tamlğın | əlyetənliyin itirilməsi təşkilata və onun əməkdaşlarına minimal dərəcədə təsir edir;
- Orta (Medium, M) – konfidensiallığın | tamlğın | əlyetənliyin itirilməsi təşkilata və onun əməkdaşlarına orta ağırlıqda təsir edir;
- Yüksək (High, H) – konfidensiallığın | tamlğın | əlyetənliyin itirilməsi təşkilata və onun əməkdaşlarına ciddi nəticələrə səbəb olur;
- Müəyyən edilməyib (Not Defined, ND) – qiymətləndirmə parametrini nəzərə almamaq üçün istifadə edilir.

CVSS vektorunda hər bir metrika qısaldılmış ad və qoşa nöqtədən ":" sonra verilmiş qısaldılmış qiymət ilə verilir. Vektorda bu metrikalar əvvəlcədən müəyyən edilmiş sırada sadalanır, onlar bir-birindən "/" işarəsi ilə ayrılır. Əgər zaman və mühit metrikaları istifadə edilmirsə, bu "ND" (Not Defined) qiyməti ilə verilir. Baza, zaman və mühit vektorları cədvəl 4.1-də göstərilir.

Cədvəl 4.1. CVSS vektoru

Metrika	Vektor
Baza	AV:[L,A,N]/AC:[H,M,L]/Au:[M,S,N]/C:[N,P,C]/I:[N,P,C] /A:[N,P,C]
Zaman	E:[U,POC,F,H,ND]/RL:[OF,TF,W,U,ND]/RC:[UC,UR,C, ND]
Mühit	CDP:[N,L,LM,MH,H,ND]/TD:[N,L,M,H,ND]/CR:[L,M,H ,ND] /IR:[L,M,H,ND]/AR:[L,M,H,ND]

Məsələn, baza metrikasının qiymətləri "Giriş vektoru: Aşağı, İstifadənin çətinliyi: Orta, Autentifikasiya: Heç, Konfidensiallığa təsir: None, Tamlığa təsir: Qismən, Əlyetənliyə təsir: Tam" olan boşluğun baza vektoru: "AV:L/AC:M/Au:N/C:N/I:P/A:C" olacaq.

4.10.4. Metrikaların qiymətləndirilməsi düsturları

Metrikaların alınmış qiymətlərinin hər birinə CVSS sənədində göstərildiyi qaydalara əsasən müvafiq ədədi qiymətlər verilir və həmin sənəddə verilmiş düsturlara əsasən qiymətləndirmə aparılır.

Baza metrikası üçün aşağıdakı tənliklərdən istifadə edilir:

```
BaseScore = round_to_1_decimal(((0.6*Impact)+
    (0.4*Exploitability)-1.5)*f(Impact))

Impact = 10.41*(1-(1-CI)*(1-II)*(1-AI))

Exploitability=20*AV*AC*Au

f(impact)= 0 if Impact=0, 1.176 otherwise.
```

`round_to_1_decimal` funksiyası onluq kəsrdə vergüldən sonra bir onluq rəqəmə qədər yuvarlaqlaşdırma aparır. Baza metrikalarının mümkün qiymətləri Cədvəl 4.2-də göstərilir.

Cədvəl 4.2. Baza metrikalarının mümkün qiymətləri

CI/ II /AI	*Ad*	*None*	*Partial*	*Complete*
	Qiymət	0	0,275	0,66
AV	*Ad*	*Local*	*Adj.network*	*Network*
	Qiymət	0,395	0,646	1
AC	*Ad*	*High*	*Medium*	*Low*
	Qiymət	0,35	0,61	0,71
Au	*Ad*	*Multiple*	*Single*	*None*
	Qiymət	0	0,56	0,704

Zaman metrikası üzrə düstur BaseScore ilə zaman metrikası qiymətlərini birləşdirir və 0-10 arasında olan TemporalScore qiymətini hesablayır. Bu qiymət BaseScore-dən böyük və onun 33 %-dən kiçik olmayacaq. TemporalScore düsturu belədir:

```
TemporalScore = round_to_1_decimal(BaseScore*E*RL*RC)
```

Zaman metrikalarının mümkün qiymətləri Cədvəl 4.3-də göstərilir.

Cədvəl 4.3. Zaman metrikalarının mümkün qiymətləri

E	*Ad*	*U*	*POC*	*F*	*High*	*ND*
	Qiymət	0,85	0,9	0,95	1,00	1,00
RL	*Ad*	*OF*	*TF*	*W*	*U*	*ND*
	Qiymət	0,87	0,90	0,95	1,00	1,00
RC	*Ad*	*UC*	*UR*	*C*	*ND*	
	Qiymət	0,90	0,95	1,00	1,00	

Mühit metrikası üzrə düstur TemporalScore ilə zaman metrikası qiymətlərini birləşdirir və 0-10 arasında olan EnvironmentalScore qiymətini hesablayır. Bu qiymət TemporalScore-dan böyük olmayacaq. EnvironmentalScore aşağıdakı kimidir:

```
EnvironmentalScore =
round_to_1_decimal((AdjustedTemporal+(10-
AdjustedTemporal)*CDP)*TD).
```

Burada AdjustedTemporal yenidən hesablanmış TemporalScore qiymətidir, BaseScore düsturunda Impact ifadəsi AdjustedImpact düsturu ilə əvəzlənir:

```
AdjustedImpact=min(10,10.41*(1-(1-CI*CR)*(1-II*IR)*(1-
                    AI*AR)))
```

Mühit metrikalarının mümkün qiymətləri Cədvəl 4.4-də göstərilir.

Cədvəl 4.4. Mühit metrikalarının mümkün qiymətləri

CDP	*Ad*	*N*	*L*	*LM*	*MH*	*H*	*ND*
	Qiymət	0	0,1	0,3	0,4	0,5	0
TD	*Ad*	*N*	*L*	*M*	*H*	*ND*	
	Qiymət	0	0,25	0,75	1,00	1,00	
CR/IR/AR	*Ad*	*L*	*M*	*H*	*ND*		
	Qiymət	0,5	1,0	1,51	1,0		

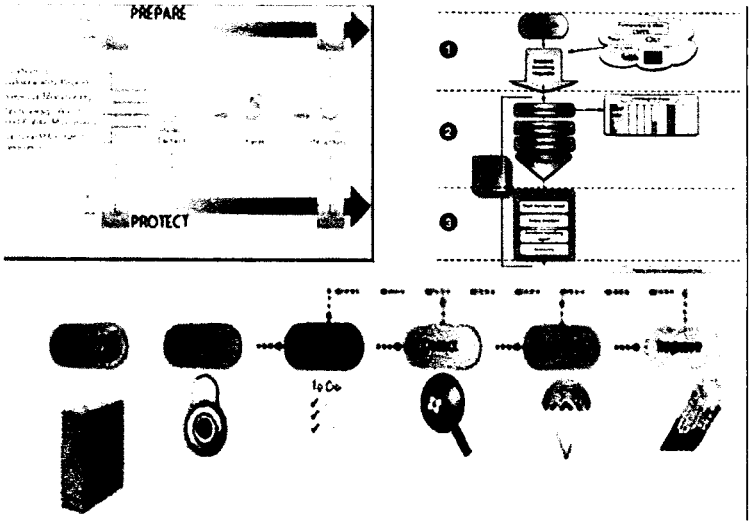
US-CERT-in həftəlik Kibertəhlükəsizlik bülletenində Milli Standartlar və Texnologiyalar İnstitutunun (NIST) dəstəklədiyi NVD boluqlar bazasında qeydə alınmış yeni boşluqların icmalı verilir. NVD bazası US-CERT tərəfindən dəstəklənir. Dəyişikliklər edilmiş və ya yenilənmiş məlumatlar NVD veb-saytında əks olunur.

Boşluqlar CVE boşluq adlandırma standartına əsaslanan və CVSS standartında müəyyən edilən ciddilik səviyyələrinə uyğun olaraq təşkil edilir. Ciddilik ballara uyğun olaraq aşağıdakı kimi Yüksək, Orta və Aşağı səviyyələrə bölünür.

Yüksək – boşluqların CVSS baza hesabı 7.0-10.0 olarsa, boşluqlar Yüksək ciddilik səviyyəsi ilə nişanlanır.

Orta – boşluqların CVSS baza hesabı 4.0-6.9 olarsa, onlar Orta ciddilik səviyyəsi ilə nişanlanır.

Aşağı – boşluqların CVSS baza hesabı 0.0-3.9 olarsa, onlar Aşağı ciddilik səviyyəsi ilə nişanlanır.



FƏSİL 5

İNSİDENTLƏRİ CAVABLANDIRMA PROSESLƏRİ

İNSİDENTLƏRİ CAVABLANDIRMA PROSESLƏRİ

- **İnsidentləri cavablandırma prosesinin mərhələləri**
- **İnsidentlərin aşkarlanması və analizi**
- **İnsidentlərə prioritet verilməsi**
- **İnsidentin aradan qaldırılması**
- **İnsident sübutlarının toplanması**
- **İnsidentlərin təhqiqatı**
- **İnsidentlərin sənədləşdirilməsi**
- **İnsidentləri cavablandırma alətləri**

FƏSİL 5 İNSİDENTLƏRİ CAVABLANDIRMA PROSESLƏRİ

5.1. İnsidenti cavablandırma prosesləri

İnformasiya təhlükəsizliyi insidenti çox vaxt kompleks və çoxtərəfli problemin təzahürü olur. Bu insidentlərin cavablandırılmasına düzgün yanaşma – strukturlaşdırılmış proses yanaşmasından istifadə etməkdir. İnformasiya təhlükəsizliyi insidentlərinin idarə edilməsi üzrə normativ sənədlərdə və metodikalarda belə yanaşmaların müxtəlif nümunələri təklif edilir.

İnsidentlərin idarə edilməsi üzrə ilk işlərdən biri 1990-cı ildə meydana çıxmışdır. Bundan sonra bu və ya digər dərəcədə insidentlərin idarə edilməsinə proses yanaşmasını təsvir edən çox sayda işlər ortaya çıxdı, bu işlərdə proseslərin sayı 5-11 arasında dəyişir. Məsələn, insidentlərin idarə edilməsi üçün Karneqi Mellon Universitetinin və SANS İnstitutunun təklif etdikləri proses modellərinə daxil olan proseslər Cədvəl 5.1-də sadalanır:

Cədvəl 5.1. İnsidentləri cavablandırma prosesləri

Karneqi Mellon Universitetinin təklif etdiyi model	SANS İnstitutunun təklif etdiyi model
1. Hazırlıq	1. Hazırlıq
2. İnfrastrukturun mühafizəsi	2. İdentifikasiya
3. İnsidentlərin aşkarlanması	3. Lokallaşdırma
4. İnsidentlərin sistemləşdirilməsi	4. Səbəblərin aradan qaldırılması
5. Cavablandırma	5. Bərpaetmə
	6. Dərs çıxarma

CSIRT-in vəzifələrindən və strukturundan asılı olaraq bu proseslərin hamısı praktikada realizə edilmir.

Ümumi xüsusiyyət kimi qeyd etmək olar ki, yanaşmaların heç də hamısı hazırlıqdan başlamır, heç də hamısı dərs çıxarmır, hesabatların hazırlanması insidentlərin idarə edilməsi həyat tsiklinin müxtəlif yerlərində həyata keçirilir.

Karneqi Mellon Universitetinin təklif etdikləri proses modellərinə daxil olan proseslərin qısa təsviri aşağıdakı kimidir.

Hazırlıq prosesi aşağıdakıları əhatə edir:

- insidentlərin idarə edilməsi və ya CSIRT-in potensialının planlaşdırılması və həyata keçirilməsi;
- bu potensialın saxlanması və dəstəklənməsi;
- mövcud potensialın çıxarılmış dərslər və CSIRT-in fəaliyyətinin müntəzəm qiymətləndirilməsi əsasında təkmilləşdirilməsi;
- "uğurlu" insidentdən sonra insidentlərin idarə edilməsi üzrə mövcud tədbirlərin dəyişdirilməsi və yeni tədbirlərin tətbiq edilməsi;
- infrastrukturun mühafizəsinin yaxşılaşdırılması üzrə tədbirlərin işlənməsi (sonrakı prosesə ötürülür).

İnfrastrukturun mühafizəsi prosesinə daxildir:

- insidentləri və ya insidentlərin meydana çıxması üçün potensial imkanları (boşluqları) dayandıran və ya qarşısını alan dəyişikliklərin həyata keçirilməsi;
- "ölümdən sonrakı" analiz və digər proses yaxşılaşdırma mexanizmlərinin nəticəsi olan infrastrukturun mühafizəsinin təkmilləşmələrinin tətbiqi;
- şəbəkə monitorinqi və proaktiv darama, həmçinin risklərin analizi yolu ilə hesablama infrastrukturunun qiymətləndirilməsi;
- cari insidentlər, aşkarlanmış boşluqlar və qiymətləndirmə zamanı aşkarlanmış digər təhlükəsizlik hadisələri haqqında bütün informasiyanın İnsidentlərin aşkarlanması prosesinə ötürülməsi.

İnsidentlərin aşkarlanması prosesinə daxildir

- insidentlərin aşkarlanması və onlar haqqında məlumat verilməsi;
- insidentlər haqqında məlumatların qəbulu;
- IDS, şəbəkə monitorinqi və texnologiyaların izlənməsi funksiyaları kimi indikatorların proaktiv monitorinqi;
- təşkilatda təhdidlərin, risklərin və zərərli davranışların meydana çıxmasını göstərən indikatorların analizi;
- bütün şübhəli hadisələrin İnsidentlərin sistemləşdirilməsi prosesinə ötürülməsi;
- baxılan prosesdən kənara çıxan hadisələrə yeni təyinatın verilməsi;
- növbəti mərhələyə keçməyən hadisələrin emalının dayandırılması.

İnsidentlərin sistemləşdirilməsi prosesinə aşağıdakılar daxildir:

- insidentlərin klassifikasiyası və korrelyasiyası;
- insidentlərə prioritetlərin verilməsi;
- insidentlərə müvafiq insident emalı prosedurları təyin edilir;
- müvafiq verilənlər və informasiya Cavablandırma prosesinə ötürülür;
- insidentlərin idarə edilməsi prosesinə aid olmayan hadisələr mümkün olduqda müvafiq sahələrə yönləndirilir;
- cavablandırma prosesinə ötürülməyən və ya digər sahələrə yönləndirilməyən bütün hadisələr bağlanır.

Cavablandırma prosesinə aşağıdakılar daxildir:

- hadisələrin analizi;
- cavablandırma strategiyasının planlaşdırılması;
- insidentlərin qarşısını alan, aradan qaldıran və ya yüngülləşdirən, zərər çəkmiş sistemləri təmir və bərpa edən hərəkətlər daxil olan texniki, inzibati və hüquqi cavablandırma hərəkətlərinin koordinasiyası və həyata keçirilməsi;
- kənar tərəflərlə kommunikasiya;

– insidentlərin idarə edilməsi prosesinə aid olmayan hadisələr mümkün olduqda müvafiq sahələrə yönləndirilir;
– cavablandırma dayandırılır;
– öyrənilmiş dərslər və insident məlumatları "ölümdən sonrakı" analiz üçün Hazırlıq prosesinə ötürülür.

5.2. Hazırlıq prosesləri

İnformasiya təhlükəsizliyi insidentinin baş verməsi faktına hazırlıq xarakteri daşıyan Hazırlıq mərhələsi insidentlərin cavablandırılması üzrə fəaliyyətin təşkili və reqlamentlərin formalaşdırılması üçün nəzərdə tutulub. İnsidentlərin baş verməsi vəziyyətinə təşkilatın hazırlanması üçün (onun nəticələrini minimumlaşdırılması və təşkilatın iş qabiliyyətinin tez bərpa edilməsi) addımlar atılır. Bu mərhələ ən vaciblərdən biridir, mümkün insidentlərin emalında uğur bu mərhələdən asılıdır.

Hazırlığın əsas mərhələləri aşağıdakılar ola bilər:
– CSIRT komandasının formalaşdırılması: insan resurslarının və maddi resursların ayrılması;
– insidentləri cavablandırma sxeminin işlənməsi;
– müvafiq təşkilati sənədlərin işlənməsi və təsdiqi;
– CSIRT heyətinin təlimi;
– insidentləri cavablandırma üzrə seçilmiş sxemin test edilməsi.

Hazırlıq mərhələsinin məqsədi informasiya təhlükəsizliyi sisteminin möhkəm fundamentini yaratmaq və inkişaf etdirməkdir. Bura texniki və qeyri-texniki komponentlər daxildir. Ən mürəkkəb, lakin ən vacib mərhələdir, ən yaxşı metodlar tətbiq edilməlidir. Miqyaslı hücumu dəf edərkən ən yaxşı metodların və proseslərin tətbiqi haqqında düşünmək gecdir.

Təşkilatın rəhbərliyi təşkilat daxilində informasiya təhlükəsizliyi insidentlərini cavablandırma prosedurlarının tətbiq edilməsi üçün zəruri şəraitin yaradılmasına yardım etməlidir:
– insidentləri cavablandırma siyasətinin işlənməsi;
– insidentin emal prosedurlarının işlənməsi;

- təhqiqat prosesində informasiyaya müraciətin hüquqi aspektlərinin tənzimlənməsi;
- insidenti cavablandırma komandasınınn strukturunun təsdiq edilməsi;
- insidenti cavablandırma komandasının profil mütəxəssislərlə (hüquqşünaslar, kadrlar şöbəsi, informasiya təhlükəsizliyi xidməti və s.) təşkilatdaxili təmasların yoluna qoyulması (təşkil edilməsi);
- insidenti cavablandırma komandasının məsuliyyət sahəsinin müəyyən edilməsi, təlimi və texniki təchizatı.

İnsidentləri cavablandırma prinsiplərinin və prosedurlarının sənədləşdirilməsi təşkilatdaxili qarşılıqlı əlaqənin təmin edilməsi və dövlət hakimiyyəti orqanlarında təsəvvürün formalaşması məqsədini güdür:

- insidenti cavablandırma prosesində ətraflı təhqiqat və ya cavablandırma prosedurunu məntiqi sonluğa çatdırmaq üçün kənar təşkilatlarla əlaqəyə girmək tələb oluna bilər (KİV, hüquq-mühafizə orqanları, üçüncü şəxslər tərəfindən zərərçəkənlər).
- insidentin təhqiqatı ilə əlaqəli konfidensial informasiyanın qeyri-mütənasib açılması halında belə hərəkətlərdən gələn ziyan informasiya təhlükəsizliyi insidentinin özünün vura bildiyi ziyanla eyni miqyaslı ola və ya onu aşa bilər.
- qeyri-mütənasib açıqlama probleminin tənzimlənməsi üçün əlaqə nöqtəsi (POC – Point Of Contact) yaradılır, onun strukturu və səlahiyyətləri insidenti cavablandırma siyasətinin formalaşdırılması mərhələsində razılaşdırılır və informasiya mübadiləsi iştirakçıları üçün hüquqi təsbit edilmiş etibar mühiti yaradır.
- insidenti cavablandırma nəticələri barəsində təşkilatın öz əməkdaşlarının və tərəfdaşlarının məlumatlandırılması.

CSIRT komandası yatarmaq və funksiyaları əvvəlcədən bölmək lazımdır. Komanda üzvlərinin zəruri kvalifikasiyaya malik olmasına çalışmaq lazımdır. Öz imkanlarını dəqiq başa

düşmək, insidentlərin idarə edilməsi üzrə alətləri hazırlamaq lazımdır.

Düşməni öyrənmək, tanımaq zəruridir. Bədniyyətlinin motivlərini, onun texniki imkanlarını və üsullarını başa düşmək lazımdır.

İnformasiya təhlükəsizliyi insidentlərini cavablandırmaya hazırlıq mərhələsi insidentlər barəsində informasiyanın toplanması və analizi, komandaların təlimi ilə yanaşı, insident cavablandırma üçün zəruri alətlərin hazırlanmasını əhatə edir:

- cavablandırma komandası əməkdaşlarının əlaqə məlumatları;
- texniki xidmət bölməsinin telefonları;
- şübhəli hərəkətlər barəsində məlumat vermək üçün açıq və anonim rabitə kanalı;
- əməkdaşların mobil telefonlarının nömrələri;
- cavablandırma komandası üzvləri arasında informasiya mübadiləsinin mühafizəsi üçün kriptoqrafik vasitələr;
- təhlükəsiz danışıq otağı;
- sübutların və insidentləri cavablandırma nəticələrinin saxlanması üçün verilənlər bazaları.

Alətlərin tərkibinə verilənlərin toplanması üçün proqram təminatı və aparat təminatı vasitələri daxil olmalıdır:

- insidenti cavablandırma nəticələrinin saxlanması üçün kompyuter sistemləri;
- insidenti cavablandırma komandası üzvlərinin rahat işi üçün mobil kompyuterlər;
- insidentin mümkün inkişafının analizi üçün sınaq laboratoriyası;
- təmiz disket, CD və DVD dəstləri;
- disk sisteminin vəziyyətinin analizi üçün proqram təminatı;
- şəbəkə trafikinin analizi üçün snifferlər və protokol analizatorları;
- təşkilatda istifadə edilən bütün əməliyyat sistemlərinin yükləmə diskləri;

– təhqiqat gedişində sübutedici bazanın toplanması üçün diktofonlar, rəqəmsal foto- və video-kameralar kimi əlavə qurğular.

İnsidentləri cavablandırma komandası universal mobil alətlər toplusuna (ing. jump kit) malik olmalıdır. Təşkilat insidentləri cavablandırma komandasının alətlərini aktual vəziyyətdə saxlamaq üçün maliyyə əsaslarını təmin etməlidir.

Yoxlama siyahıları. İnsidenti cavablandırma prosesində faydalı təcrübə yoxlama siyahılarının (ing. check lists) istifadəsidir. Bu təcrübə eyni vaxtda cavablandırılan insidentlərin sayı çox (onlarla) ola bilən orta və iri təşkilatlarda tətbiq edilə bilər. Yoxlama siyahısının strukturu ixtiyari ola bilər, siyahı cavablandırma komandasının ekspertləri tərəfindən təşkilatda insidentləri cavablandırma üzrə aparılan tədbirlər nəzərə alınmaqla işlənir.

5.3. İnsidentlərin emalı alqoritmi

İnformasiya təhlükəsizliyi insidentlərinin emalı üzrə hərəkətlərin ümumi alqoritmi aşağıdakı kimi ola bilər:

1. İnsidenti identifikasiya etmək və onun həqiqətən də baş verdiyinə əmin olmaq.
2. IT-infrastrukturun insidentə qarışmış sahəsini lokallaşdırmaq.
3. İnsidentə qarışmış obyektlərə girişi məhdudlaşdırmaq.
4. Təşkilatın rəhbərliyinə insidentin baş verməsi haqqında məlumat vermək.
5. Məsləhət üçün lazımi mütəxəssislər cəlb etmək.
6. İnsidentin təhqiqatı üzrə qrup yaratmaq və sübutların toplanması və sistemlərin bərpası üzrə işlər planı tərtib etmək. İnsidenti cavablandırma gedişində həyata keçirilən bütün hərəkətləri protokollaşdırmaq.
7. Sübutların saxlanmasını və lazımınca sənədləşdirməsini təmin etmək
   7.1. İşləyən sistemdən enerjidən asılı informasiyanı götürmək.

7.2. Real vaxtda davam edən insident barəsində informasiya toplamaq.
7.3. Elektrik şəbəkəsindən açmaq.

8. Üçüncü müstəqil tərəfin iştirakı ilə sübut bazası olan informasiya daşıyıcılarının götürülməsini və möhürlənməsini həyata keçirmək, həmçinin obrazların və digər informasiyanın götürülməsini sonrakı analiz və saxlamaq üçün!
   8.1. İnformasiya daşıyıcıları ilə bütün əməliyyatları protokolla sənədləşdirmək.
   8.2. İnformasiya olan obyektlərin, götürülən verilənlərin və onların saxlandığı yerlərin müfəssəl siyahısını tutmaq.
   8.3. Prosesi fotovideokamera ilə sənədləşdirmək.
   8.4. Möhürlənmiş obyektləri protokollarla birgə etibarlı yerdə daşıyıcıların tədqiqata və ya hüquq-mühafizə orqanlarına verilənədək saxlamaq
9. Maddi sübutlar saxlandıqdan və sənədləşdirildikdən sonra informasiya sistemlərinin işini bərpa etmək
10. Tədqiqat aparılan zaman informasiya mənbələrinin sübutlarının dəyişməzliyini təmin etmək. Yalnız kopyalarla işləmək.
11. Təhqiqat aparılarkən maraqlı tərəflərlə və xarici təşkilatlarla (informasiya təhlükəsizliyi və insidentlərin cavablandırılması ilə məşğul olan təşkilatlarla) düzgün qarşılıqlı əlaqəni təmin etmək
12. Təhqiqat başa çatdıqdan sonra müvafiq hesabat tərtib etmək və gələcəkdə oxşar insidentlərin baş verməsi risklərinin azaldılması üzrə tövsiyələr üzərində işləmək.
13. Hüquq-mühafizə orqanlarına müraciət edilən zaman insidentin ətraflı təsvirini toplanmış sübutların təsvirini və onların analizinin nəticələrini təqdim etmək.

5.4. İnsidentlərin aşkarlanması və analizi

İnformasiya təhlükəsizliyi insidentləri müxtəlif mənbələrdən törəyə bilərlər. İdealda, təşkilat ziyankar aktivliyin istənilən təzahürünə hazır olmalıdır. Lakin praktikada bunu həyata keçirmək mümkün olmur.

Cavablandırma komandası təşkilatda baş vermiş hər bir insidenti təsnifatlaşdırmalı və təsvir etməlidir, eyni zamanda risklərin analizi nəticəsində güman edilən mümkün insidentləri təsnif etməli və təsvir etməlidir.

Mümkün təhdidlər və onlarla əlaqəli mümkün insidentlər haqqında tezaurusu genişləndirmək üçün İnternetin daim təzələnən açıq mənbələrindən istifadə etmək yaxşı praktikadır.

İnformasiya təhlükəsizliyi insidentlərinin baş verməsi haqqında güman üç əsas faktora əsaslanmalıdır:

- informasiya təhlükəsizliyi insidenti haqqında məlumat bir neçə mənbədən eyni vaxtda daxil olur (istifadəçilər, IDS, jurnal faylları);
- IDS çoxsaylı təkrarlanan hadisələr haqqında siqnal verir;
- jurnal fayllarının analizi administratora insident hadisəsinin baş verməsi imkanı haqqında nəticə çıxarmağa əsas verir.

Ümumi halda, insidentlərin əlamətlərini iki əsas kateqoriyaya bölürlər: insidentin hal-hazırda baş verməsi haqqında məlumatlar və insidentin yaxınlarda baş verəcəyi haqqında məlumatlar.

Aşağıda baş vermiş insidentin bəzi əlamətləri sadalanır:

- IDS buferin dolmasını qeydə alır;
- antivirus proqramının xəbərdarlığı;
- istifadəçilər İnternetə çıxış zamanı sürətin olduqca kiçik olmasını bildirirlər;
- sistem administratoru adları oxunmaz faylların mövcudluğunu qeydə alır;
- şəbəkə administratoru şəbəkə trafikinin kəskin artmasını qeydə alır;

- istifadəçilər poçt yeşiklərində çoxsaylı təkrarlanan məlumatların olması haqqında xəbər verirlər;
- host audit jurnalında konfiqurasiyanın dəyişməsi haqqında qeyd edir;
- tətbiqi proqram jurnal faylında çoxsaylı uğursuz avtorizasiya cəhdlərini qeydə alır.

İnformasiya təhlükəsizliyi üçün mənbə ola bilən hadisələrə misallar:

- KİV-də eksploytların yeni növünün meydana çıxması haqqında məlumatlar;
- kompyuter cinayətkarları sizin təşkilata müharibə elan edilməsini açıq bəyan edirlər.

Bədniyyətlilər sistemdə öz fəaliyyətlərinin izini qoymamaq üçün hər şey etməyə çalışırlar. İnsident əlamətlərində serverin konfiqurasiya faylında kiçik əhəmiyyətsiz dəyişiklik və ya ilk baxışda e-poçt istifadəçisinin standart şikayəti var. İnsident hadisəsinin baş verməsi haqqında qərar qəbul etmək insidenti cavablandırma komandasının ekspertlərinin səriştəsindən çox asılıdır, operatorun təsadüfi səhvini informasiya sisteminə məqsədyönlü bədniyyətli təsirdən fərqləndirmək zəruridir. İnformasiya təhlükəsizliyi insidentinin "boş-boşuna" emalı faktı özü informasiya təhlükəsizliyi insidentidir, çünki komandanın ekspertlərini vacib problemlərdən yayındırır. Təşkilatın rəhbərliyi bu hala fikir verməli və komanda ekspertlərinə müəyyən hərəkət sərbəstliyi verməlidir.

İnsidentin analizi prosesində komandanın informasiya sisteminin analizi üçün zəruri olan bütün resurslara giriş imkanı olmalıdır:

- əməliyyat sistemi portlarının vəziyyəti;
- əməliyyat sisteminin, tətbiqi proqramların, protokolların, IDS sistemlərinin işinin sübutları, antivirusların siqnaturaları;
- şəbəkənin ən vacib qurğularının iş jurnalları (veb-serverlər, e-poçt serverləri, FTP-serverlərin iş protokolları);
- tətbiqi proqramların fəaliyyət jurnalları;

– kriptoqrafik vasitələrin jurnalları;
– jurnal fayllarının analizi üçün, o cümlədən administrator hüquqları ilə əməliyyat sistemlərinə giriş;
– əməliyyat mühitlərində yüklənən yenilənmələr haqqında məlumatlar;
– ehtiyat surət yaratma reqlamentləri və ehtiyat daşıyıcıların test edilməsi haqqında informasiya.

5.5. İnsidentlərin eskalasiyası

İnsidentlərin eskalasiyası – insidentlərin cavablandırılması zamanı əlavə biliklərin və ya səlahiyyətlərin cəlb edilməsi mexanizmidir.

İnsidentlərin eskalasiyası müxtəlif səbəblərdən meydana çıxır:
– CSIRT heyəti baxılan insidentin öhdəsindən gələ bilmir;
– insident barəsində əlaqədar auditoriyaya necə məlumat veriləcəyi aydın deyil;
– yeni resurslar tələb edilir;
– insident CSIRT-in məsuliyyət zonasında deyil;
– vacib şəxsdən insidentlə əlaqəsi olmayan məlumat alınıb və s.

Funksional (üfüqi) və *iyerarxik* (şaquli) eskalasiyanı fərqləndirirlər. Funksional eskalasiya – insidentin cavablandırılmasına texniki dəstək əməkdaşlarının cəlb edilməsidir. İyerarxik eskalasiya – insidentin cavablandırılması üçün daha çox səlahiyyət lazım olduqda (təşkilat daxilində) daha yüksək səlahiyyətli əməkdaşların cavablandırmaya cəlb edilməsidir. İnsidentin cavablandırılması prosesində digər bölmələrdən də mütəxəssislərin cəlb edilməsi mümkündür.

5.6. İnsidentlərə prioritet verilməsi

Bir neçə insidenti eyni zamanda emal edərkən resursların çatışmaması şəraitində insidentlərə prioritet verilməsi çox vacibdir. Təkcə insidentlərin prioriteti yox, servis daxilində funksiyanın prioriteti də vacibdir.

İnformasiya təhlükəsizliyi insidentlərinə prioritet verilməsini müxtəlif kriteriyalara görə aparmaq olar. İnformasiya

təhlükəsizliyi insidentlərinə prioritet verilməsi üçün hücum edilən resursun kritiklik dərəcəsinin və həmin resursa insidentin təsirinin kritiklik dərəcəsinin müəyyən edilməsi prinsipi əsas götürülür. Resursun populyarlığı – resursa tələbatın səviyyəsi, insidentin növü, hücumun məqsədi, bədniyyətlinin kvalifikasiyası/hücumun mürəkkəbliyi və s. də nəzərə alınmalıdır. İnformasiya təhlükəsizliyi insidentlərinə prioritet verilməsi zamanı insidentin potensial mümkün effektləri də nəzərə alınır, yəni cavablandırma komandası təkcə baş vermiş insident faktına deyil, gələcəkdə baş verə biləcək nəticələrə və potensial təhdidlərə də baxır.

Belə kriteriyalar üzrə qiymətləndirmə metodika şəklində tərtib olunmalı və informasiya təhlükəsizliyi insidentlərini cavablandırma siyasətinə tərkib hissə kimi daxil edilməlidir. Belə metodikanın əlverişli təsvir forması matris şəklində göstərilmədir.

Adətən, sadəlik üçün informasiya təhlükəsizliyi insidentlərinin prioritetinin qiymətləndirilməsi üçün aşağıdakı kriteriyalardan istifadə edilir (şəkil 5.1):

- təsir dərəcəsi – servisin normal səviyyəsindən kənarlaşma dərəcəsi, insidentin toxunduğu istifadəçilərin və ya biznes-proseslərin sayı və onların keyfiyyətinə insidentlərin təsiri ilə ifadə olunur;
- təcililik səviyyəsi – insidentin cavablandırılmasında (SLA-da nəzərdə tutulmuş) yolverilən gecikmə müddəti.

Təsir dərəcəsi və təcililik səviyyəsi əsasında insidentlərin prioritetlərini cədvəl 5.1-də göstərildiyi kimi müəyyən etmək olar.

Cədvəl 5.1. İnsidentlərə prioritet verilməsi matrisi

		Təsir dərəcəsi		
		Yüksək	Orta	Aşağı
Təcililik	Yüksək	Kritik	Yüksək	Orta
	Orta	Yüksək	Orta	Aşağı
	Aşağı	Orta	Aşağı	Planlı

İnsidentin prioritetləri üçün kritik (5), yüksək (4), orta (3), aşağı (2) və planlı (1) qiymətlərdən istifadə edirlər.

Kritik prioritetli insidentlər 1 saat, **Yüksək** prioritetli insidentlər 8 saat, **Orta** prioritetli insidentlər 24 saat, **Aşağı** prioritetli insidentlər 48 saat ərzində cavablandırılmalıdır. **Planlı** prioriteti verilmiş insidentin cavablandırma müddəti plana uyğun olaraq müəyyən edilir.

5.7. İnsidentlərin lokallaşdırılması

İnsidentlərin aşkarlanması, analizi və klassifikasiyasından sonra onun yayılmasının qarşısının alınması – insidentin lokallaşdırılması çox vacib mərhələdir. Yayılmaya əks-təsirlər üzrə hərəkətlər bir çox cəhətdən cavablandırma komandasının əvvəlki mərhələləri nə qədər keyfiyyətli aparmasından asılıdır. Təşkilatın bölmələrinin qarşılıqlı təsiri, düzgün təsnifat və

mümkün nəticələrin analizinin dərinliyi həlledici rol oynayır və cavablandırma vaxtını əhəmiyyətli dərəcədə azaldır. İnsidentlərin yayılmasına əks təsirlərə hazırlığın ən yaxşı təcrübəsi əvvəlcədən hazırlanmış hərəkətlər ssenarisi, risklərin analizini aparmaq və insidentlərin əsas siniflərinin hər biri üzrə hadisələrin təsnif olunmasıdır.

İnsidentin yayılmasına əks-təsir proseduru hər bir konkret insident üçün ayrıca qurulur və onun tipindən asılı olur. Əks-təsir strategiyasının meyarları formalaşdırılmalı və cavablandırma komandasının bütün üzvlərinə əlyetən olmalıdır. Strategiyanın müəyyən edilməsi meyarlarına aşağıdakı əsas bəndlər aiddir:

- aktivin potensial mümkün zədələnməsi və ya oğurlanması;
- insidentin sübutlarının saxlanması zərurəti;
- aktivin əlyetənliyi;
- əks-təsirin həyata keçirilməsi üçün tələb olunan zaman və resurslar;
- strategiyanın təsir müddəti (həftə, ay, kvartal və s.).

Bəzi hallarda bədniyyətlini öyrənmək və insidentin zəruri sübutlarını toplamaq üçün təsirə salınmış saxlama (nəzarət edilən) strategiyası tətbiq edilə bilər, onun mahiyyəti bədniyyətlinin hərəkətlərinin aşkarlanması, analizi, klassifikasiyası və izlənməsindən ibarətdir. Bu metodikanın yüksək effektivliyi ilə yanaşı, yüksək riski də var, çünki bədniyyətli nüfuzdan düşmüş aktivdən təşkilatın digər aktivlərinə hücum üçün meydança kimi istifadə edilə bilər. Nəzarət edilən saxlama təşkilatda yüksək ixtisaslı ekspertlər komandasının olması şərtində mümkündür və yaxşı işlənmiş insidentləri cavablandırma siyasətinin mövcudluğu. Korporativ heterogen paylanmış informasiya sistemlərində aktivlərin vahid prosesdə iştirakı faktorunu nəzərə almaq lazımdır, yəni hostlar arasındakı əlaqələri və əlyetənliyin pozulmasının bütövlükdə informasiya sisteminin fəaliyyətinə təsiri. Bu halda standart cavablandırma prosedurları ilə yanaşı İT-idarəetmə məsələləri, sistemlərin ehtiyatlarının yaradılması səviyyələri daxil olmaqla öyrənilməsi zəruridir. Əks halda, cavablandırma komandası gücsüz olacaq.

5.8. İnsidentin təhqiqatı

İnformasiya təhlükəsizliyi insidentlərinin təhqiqatı müəyyən etməlidir ki: kim, nə, nə vaxt, harada, necə və nə üçün insidentə cəlb edilibdir. Təhqiqatın aparılmasının vahid metodikası mövcud deyil, lakin ümumi halda təhqiqat gedişində aşağıdakı hərəkətlər yerinə yetirilir:

- sübutların toplanması və onların analizi;
- günahkarların aşkarlanması və onların məsuliyyət dərəcəsinin müəyyən edilməsi;
- insidentin baş verməsinə imkan verən səbəblərin müəyyən edilməsi;
- insidentlərin qarşısının alınması üçün tədbirlərin görülməsi üzrə tövsiyələrin işlənməsi;
- təhqiqat materiallarının saxlanılması və mühafizəsi.

Təhqiqata serverlərin, şəbəkə qurğularının yoxlanması və sübutların toplanması, həmçinin qeyri-texniki xarakterli ənənəvi tədbirlər daxildir. Onu iki mərhələyə bölmək olar: verilənlərin toplanması və onların kriminalistik analizi. Təhqiqatın birinci mərhələsinin gedişində toplanmış informasiya sonradan insidentin cavablandırılması strategiyasının yaradılmasına xidmət edir. Analiz mərhələsində kimin, nəyin, necə, nə zaman, harada və nə üçün insidentə cəlb olunması müəyyən olunur.

Toplanmış verilənlərin analizinə iş protokolları fayllarının, konfiqurasiya fayllarının, İnternet-brauzerlərinin tarixçələrinin (cookie-lər daxil olmaqla), elektron poçt məlumatlarının və qoşma faylların, quraşdırılmış proqramların, qrafiki faylların və s. analizini əhatə edir. Proqram təminatının analizini aparmaq, açar sözlərlə axtarış, insidentin vaxtını və tarixini yoxlamaq zəruridir. Kriminalistik analizə həmçinin "aşağı" səviyyədə analiz də daxil ola bilər – silinmiş faylların və sahələrin, itirilmiş klasterlərin, boş yaddaşın axtarışı, həmçinin xarab edilmiş daşıyıcılardan bərpa edilmiş verilənlərin analizi (məsələn, qalıq maqnitlənməyə əsasən).

İnsidentləri təhqiq edərkən verilənlərin toplanması "Disk Duplicate" proqram təminatının köməyi ilə yerinə yetirilə bilər.

O, tərpənməz disklərin dəqiq surətlərini çıxarmağa imkan verir ("sektor sektora"). Alınmış verilənlərin analizi üçün istifadəçilərin kompyuterlərinin emulyasiyası üçün xüsusi vasitələr, məsələn, "VMware Virtual Machine" istifadə edilə bilər. Tərpənməz disk fəzalarının analizi "Encase Enterprise Edition" xüsusi proqram məhsulu və ya Vogon International şirkətinin ekspert vasitələri istifadə edilməklə aparıla bilər. Bu iki məhsul informasiya təhlükəsizliyi insidentlərinin təhqiqatı zamanı dünyada ən yaxşı vasitə hesab olunur. Bir sıra hallarda kompyuter insidentlərinin izlərini aşkar etmək məqsədi ilə şirkətin lokal şəbəkəsinə "qulaq asılması" üçün cürbəcür proqram-aparat kompleksləri (çox vaxt şəbəkə snifferləri istifadə edilir), cürbəcür proqram-tələlər (HoneyPot) və s. istifadə edilə bilər.

İnsidentlərin təhqiqatı zamanı buraxılan klassik səhvlər aşağıdakılardır:

- sistemin işi təcili bərpa edilir və bu zaman izlər və sübutlar məhv edilir;
- insident informasiya texnologiyaları şöbəsi tərəfindən ört-basdır edilir;
- əgər günahkarların günahı aşkar olunsa da, onları heç kim axtarmır (İnternetdə xakerləri tutmaq real deyil) ;
- insidentin təhqiqatına aşağı ixtisaslı heyət cəlb edilir;
- gələcəkdə insidentlərin profilaktikası və idarə edilməsi üzrə tədbirlər görülmür.

5.9. İnsident sübutlarının toplanması

İnformasiya təhlükəsizliyi insidentlərinə aid sübutların toplanması bədniyyətlinin təşkilata və ya ayrıca əməkdaşlara ziyan vurulması məqsədi ilə etdiyi hərəkət faktlarının toplanması prosedurudur. Sübutların toplanmasını zəruri edən səbəblər qəsdən və ya bilməyərəkdən törədilmiş hərəkət və ya hərəkət cəhdinə görə (təşkilata ziyan vurulmasına yönəlmiş) şəxslərin və ya şəxslər qrupunun məsuliyyətə cəlb edilməsi üçün qanuni əsasların əldə edilməsi, əməlləri törətmiş şəxslərin məsuliyyətə

cəlb edilməsi üçün faktların toplanmasıdır. Digər səbəb □ boşluğun analizi və informasiya təhlükəsizliyi insidentinin nəticələrinin aradan qaldırılması üçün təkliflərin formalaşdırılmasıdır.

İnsident sübutlarının toplanması metodologiyasına aşağıdakılar daxildir:

– hazırlıq;
– insidentin sənədləşdirilməsi;
– siyasətlərin yoxlanılması;
– sübutların toplanması strategiyası;
– sübutların toplanması prosesinin başlanması;
– sübutların toplanması.

Hazırlıq prosesində alətlər – proqram təminatı (məsələn, EnCase və ya Sysinternals) və zəruri avadanlıq hazır vəziyyətə gətirilir, şübhəli sistemlər üçün sübutların toplanılması siyasətinin mövcudluğu yoxlanılır və ya bu siyasət yaradılır.

İnsidentin sənədləşdirilməsi zamanı insidentin profilinə aşağıdakılar daxil edilir:

– insidentin qeydə alınma vaxtı;
– insidentin baş vermə vaxtı;
– insidentin kim və ya nə tərəfindən qeydə alınması;
– əlaqədar proqram təminatı və ya avadanlıq;
– əlaqə saxlamaq üçün şəxs;
– şübhəli resursun kritiklik dərəcəsi;
– mənbənin identifikasiyası (yerləşdiyi yer, ID, hostun adı, MAC-ünvan, IP-ünvan və s.);
– kömək üçün müraciət edən əməkdaşların fərdi verilənləri;
– hər bir sübutun zamanı və vaxtı;
– sübutlarn saxlandığı resursun yerləşmə yeri.

Sübutların toplanması gündəliyində insidentin təhqiqatı zamanı edilən hər şey qeydə alınır. Eyni zamanda sübutların toplanması nəticələri də qeydiyyata alınır.

Siyasətlərin yoxlanması zamanı əsas məsələ sübutların toplanması üçün səlahiyyətlərin olub-olmamasını aydınlaşdırmaqdır.

Sübutların toplanması strategiyasında hansı informasiyanın toplandığı, verilənlərin tipi, sübutların toplanması üçün alətlər, sübutların toplanması nəticələrinin saxlanacağı yer, hansı giriş hüquqlarının tələb edildiyi, periferiya qurğularının növləri, şəbəkəyə qoşulma və s. aydınlaşdırılır.

Verilənlər operativ yaddaşda (RAM), daimi yaddaşda, fləş-yaddaşlarında, Zip, Jazz, Firewire (IEEE 1394), optik və maqnit daşıyıcılarında, "qeyri-standart" qurğularda, smartfonlarda, iPod (və digər pleyerlərdə), Xbox, PSP, USB-saatlarda və s. saxlana bilər.

İnformasiya daşıyıcıları üzrə nəzərə almaq lazımdır ki, onlar qidalanmanın kəsilməsinə, elektromaqnit və işıq təsirlərinə, yüksək və aşağı temperatura, yüksək nəmişliyə, statik elektrikə qarşı həssasdırlar. Onları etibarlı yerdə tədqiq etmək və saxlamaq lazımdır. Bəzi qurğular yuxu rejiminə gedə və sonra parol istəyə bilərlər.

Sübutların olduğu/saxlandığı yerlərin bir çoxu daimi elektrik mənbəyi tələb edir. Onlar kəsildikdə sübutlar itə bilər. Fərdi kompyuterdə sistemi ani olaraq söndürmək və sonra sistemin surətini yaratmaq və onu analiz etmək tövsiyə edilir. Ani söndürmə zamanı UPS olmadığına əmin olmaq və elektrik şəbəkəsindən ayırmaq lazımdır.

Sübutların toplanması prosesinə başlanması mərhələsi etibarlı yüklənməni, ötürmə və saxlama metodlarını, nəticələrin tamlığını, analiz mühitinin dəyişməzliyini əhatə edir.

Sübutların toplanması zamanı bütün hərəkətlər (vaxt, zaman, daxil edilən komandaların tarixi) qeydiyyata alınır. Bütün komandaların və alətlərin işə salınma vaxtı izlənir (loqların sonrakı analizi üçün). Analiz edilən sistemin tipindən – əməliyyat sistemi, tətbiqi proqram, verilənlər bazasını idarəetmə sistemi (VBİS), şəbəkə avadanlığı, mobil qurğular, printerlər və s. çıxış edərək bütün zəruri məlumatlar toplanır.

İnformasiya təhlükəsizliyi insidentinə aid sübutların toplanması proseduru daxili reqlament şəklində işlənməli və cavablandırma komandasının hər bir üzvünün və insidentin təhqiqatına cəlb edilmiş bölmələrin mütəxəssislərinin diqqətinə çatdırılmalıdır.

Pozucunun identifikasiyası. İnsidentin təhqiqatı gedişində pozucunu identifikasiya etmək cəhdi heç də həmişə uğurlu olmur. İnsidentlərin yayılmasına əks-təsir prosedurunun uğuruna baxmadan bədniyyətlinin "şəxsiyyətinin" müəyyən edilməsi üçün bir neçə insidentin təhqiqatı, faktların qarşılaşdırılması, hücum edənin "dəst-xəttinin" analizi tələb edilə bilər. İstənilən halda, əgər təhdid daxili pozucudan gəlmirsə və insident təşkilat əməkdaşlarının əlbir olmasına gətirib çıxaran hadisələrin mürəkkəb zənciri deyilsə, onda cavablandırma komandası ekspertlərinin hərəkətləri bu reqlamentin predmeti olan tədbirlərin həyata keçirilməsinə yönəlməlidir. Əks halda, insidentin təhqiqatına daxili təhlükəsizliyin müvafiq xidmətləri qoşulmalıdır. Burada insident sübutlarının toplanması və analizi mühümdür.

5.10. İnsidentin nəticələrinin aradan qaldırılması

İnformasiya təhlükəsizliyi insidentlərinin nəticələrinin aradan qaldırılması proseduru daxili reqlament şəklində tərtib olunmalıdır və təşkilatın informasiya sisteminin fəaliyyət xüsusiyyətlərindən və bədniyyətlinin tətbiq etdiyi hücum üsulundan birbaşa asılıdır. İnsidentin nəticələrinin aradan qaldırılması prosesində komanda üzvlərinin hərəkətləri həm texniki mütəxəssislərlə (sistemə xidməti həyata keçirən), həm də informasiyaları bədniyyətlinin obyektinə çevrilmiş bölmələrin rəhbərləri ilə razılaşdırılmalıdır.

Praktikada insident nəticələrinin aradan qaldırılması zamanı komanda üzvlərinin effektiv hərəkətlər toplusunu birqiymətli müəyyən edə bilən universal metodika yoxdur. Bərpaetmənin miqyasları müxtəlif ola bilər: virusla yoluxmuş faylların müalicəsindən və istismar mühitinin ehtiyat surətlərdən bərpasından tutmuş məhkəmədə təşkilatın nüfuzunun müdafiəsinə qədər. Hazırda ən yaxşı təcrübə təşkilatda daim qüvvədə olan kollegial idarəetmə orqanı ilə dəstəklənən fəaliyyətin bərpası planının mövcudluğudur.

İnsidenti cavablandırma komandasının ekspertləri öz diqqətlərini həqiqətən də təhqiq olunan insidentlə əlaqəsi olan

informasiyanın toplanmasına və saxlanmasına yönəltməlidirlər, oxşar və ya analoji şəraitə deyil. Əks halda baxılan insidentin təcrübəsi faydasız olacaq.

5.11. İnsidentlərin sənədləşdirilməsi

İnformasiya təhlükəsizliyi insidentlərinin sənədləşdirilməsi sübutların toplanması və sonrakı konsolidasiyası üçün zəruridir. Bədniyyətli təsirin bütün faktları və sübutları sənədləşdirilməlidir. Təsirin *texnoloji sübutları* və *əməliyyat sübutları* fərqləndirilir. Texnoloji sübutlara verilənlərin toplanması və analizinin texniki vasitələrindən alınmış (snifferlər, IDS) informasiya, əməliyyat sübutlarına isə heyətin dindirilməsi prosesində toplanmış verilənlər və dəlillər, Service Desk-ə müraciət sübutları, Call Center-ə zənglər aid edilir.

İnformasiya təhlükəsizliyi insidentlərinin sənədləşdirilməsi üşün tipik praktika insidentin cavablandırılması jurnalının aparılmasıdır, onun standart formatı yoxdur və cavablandırma komandası işləyib hazırlayır. Bu jurnalın vacib sahələrinə aiddir:

- cavablandırmanın cari statusu;
- insidentin təsviri;
- insidentin emalı zamanı cavablandırma komandasının yerinə yetirdiyi hərəkətlər;
- cavablandırma aktorlarının siyahısı (onların funksiyaları və məşğulluq faizləri göstərilir);
- insidenti cavablandırma gedişində toplanmış sübutların siyahısı (mənbələr mütləq göstərilir);
- insidenti cavablandırma iştirakçılarının şərhləri;
- sonrakı hərəkətlərin təsviri və prosesin vəziyyəti (məsələn, "Call Center-ə sorğunun nəticələri gözlənilir" və s.).

İnsidentin təhqiqatı gedişində bütün sübutlar icazəsiz girişlərdən mühafizə olunmalıdır, çünki məlumatlarda informasiya sisteminin əsaslı boşluqları haqqında məlumatlar ola bilər.

5.12. İnsidentin bağlanması

Nəticələri və səbəbləri yetərli şəkildə aradan qaldırılmış informasiya təhlükəsizliyi insidentlərini bağlamaq olar. Əgər insident bağlanıbsa, onda bu barədə bütün maraqlı tərəfləri məlumatlandırmaq zəruridir.

İnsidentləri müxtəlif səbəblərdən bağlamaq olar:

- yeni viruslar haqqında məlumatlar analiz üçün heç nə vermir;
- CSIRT tərəfindən texniki dəstək daha tələb edilmir.

İnsidentin bağlanması prosesi bir neçə mərhələdən ibarətdir, onların gedişində tətbiq edilmiş həllərin effektivliyi, insident haqqında qeydiyyatın dəqiqliyi və dolğunluğu yoxlanır.

İnsidentin aradan qaldırılması üzrə həll tətbiq edildikdən sonra tətbiq edilmiş həlli yoxlamaq zəruridir. Adətən, belə yoxlama həlli tətbiq edən qrup tərəfindən yerinə yetirilir. Zəruri olduqda, həllin yoxlanması üçün kliyent ilə də əlaqə saxlanır. İnsidenti bağlayarkən, insidentə verilmiş ilkin kateqoriyanın düzgünlüyünü yoxlamaq lazımdır. Əgər insidentin kateqoriyası düzgün təyin edilməyibsə, onda qeydiyyat yazısında düzgün kateqoriyanı göstərmək lazımdır. Əgər insident haqqında yazıda informasiya çatışmırsa, onda zəruri informasiya əlavə edərək insident haqqında yazının dolğunluğunu təmin etmək lazımdır. İnsidentin bağlanması prosesinin sonuncu mərhələsində insidentin təkrar baş verməsi ehtimalı müəyyən edilir və uyğun bağlanış kateqoriyası göstərilir.

Qeyd etmək lazımdır ki, informasiya təhlükəsizliyi insidenti bağlandıqdan sonra informasiya təhlükəsizliyi insidenti üzrə hesabat forması doldurula və lazımi instansiyaya təqdim oluna bilər.

İnsidentlə əlaqədar hadisələr, müraciətlər və ya dəyişikliklər olduqda insident bağlanmır və insidentin əlavə emalı tələb edilir. Məsələn, əgər insidentlə əlaqəli məhkəmə işi bağlanmırsa, onda insident də bağlanmır.

Vacib yeni informasiya aldıqda insidenti yenidən açmaq və ya başqa insidentlə birləşdirmək olar. Əgər bu əvvəlki təhqiqatın davamı deyilsə, yeni insindet açmaq daha yaxşı olardı.

5.13. İnsidentləri cavablandırma resursları və alətləri

CSIRT komandasına CSIRT məlumatlarını saxlamaq, analiz etmək və izləmək, loqları, faylları və artefaktları analiz etmək, (IP-) ünvanları və əlaqə məlumatlarını müəyyən etmək, sistemləri daramaq, müdaxilələri aşkarlamaq üçün şəbəkələrin monitorinqi, təhlükəsiz kommunikasiya üçün alətlər lazımdır.

Zəruri texniki bazanın yaradılmasında CSIRT-lərə dəstək vermək məqsədi ilə Clearing House of Incident Handling Tools (CHIHT) pilot saytı yaradılmışdır. Saytda CSIRT komandalarının istifadə etdikləri geniş yayılmış alətlər haqqında çox sayda istinadlar tapmaq olar. Onlar iki istiqamət üzrə qruplaşdırılıb. Alətlərin birinci qrupu insidentlərin təhqiqatına aiddir (sübutların toplanması, insident sübutlarının tədqiqi, sübutların emalı, insidentdən sonra sistemin bərpası). Alətlərin ikinci qrupunu CSIRT-in gündəlik işində istifadə edilən alətlər təşkil edir (insidentin izlənməsi, insidentlərin arxivi, məsafədən təhlükəsiz girişin təmini, boşluqların aşkarlanması və insidentlərin qarşısının alınması üçün preventiv alətlər).

İnsidentlərin izlənməsi alətləri

AIRT (Application for Incident Response Teams) – son istifadəçilərə xidmət göstərən CSIRT qrupları üçün nəzərdə tutulub. Windows, Unix, Mac platformalarında əlyetəndir (http://www.uvt.nl/infolab/airt/). CERT.LV, SURFnet-CERT, UvT CERT tərəfindən istifadə edilir.

Jitterbug – vebə əsaslanan, açıq kodlu izləmə sistemidir. Problemlər haqqında veb-formalar və ya e-poçt ilə məlumat vermək olar, autentifikasiya edilmiş istifadəçilər onları klassifikasiya edə, şərhlər əlavə edə və sistem daxilində məlumatlara cavab verə bilərlər. Veb-səhifədə müxtəlif nümayiş və informasiya materialları vardır. Windows, Unix, Mac

platformalarında əlyetəndir (http://samba.anu.edu.au/cgi-bin/jitterbug).

RT (Request Tracker) – sorğuları izləmək üçün pulsuz sistemdir. RT-ni müxtəlif cür konfiqurasiya etmək olar. RT e-poçtla göndərilən insident məlumatını avtomatik qeydiyyata alır və bu məlumatı göndərən istifadəçiyə bilet verir (göndərir), məlumatları verilənlər bazasında saxlayır. Unix platformasında əlyetəndir (http://www.fsck.com/projects/rt/). CERT Polska, CERT.PT tərəfindən istifadə edilir.

RTIR (Request Tracker for Incident Response) – JANET-CERT tərəfindən Request Tracker sisteminin xüsusi olaraq insidentlərin cavablandırılması sahəsi üçün işlənilmiş variantıdır. Unix platformasında əlyetəndir (http://www.bestpractical.com/rtir/ index.html). ACOnet-CERT, CERT Polska, CERT.PT, SWITCH-CERT tərəfindən istifadə edilir.

Sübutların toplanması alətləri

İnsident səhnəsindən sübutların toplanması üçün aşağıdakı alətlər istifadə edilir.

Encase – sübutların toplanması və analizi üçün ABŞ Maliyyə Nazirliyinin gizli xidməti; FTB və MTA-nin ehtiyacları üçün yaradılmışdı, hazırda açıq satışda olan kommersiya alətidir. Disklərin obrazının yaradılmasından təhqiqatın aparılmasına və son hesabatın yaradılmasına kimi bütün mərhələləri yerinə yetirir. İnformasiyanın müxtəlif fayl sistemlərində (FAT 12, FAT 16, FAT 32, NTFS), müxtəlif əməliyyat sistemlərində (Linux, Unix, MAC), daşıyıcılarda (RAID, CD-ROM, DVD-R, Yaz, Zip, IDE, SCSI və s.) axtarışını və analizini həyata keçirir.

Diskin obrazı yaradıldıqdan sonra, Encase silinmiş fayllar və boş disk sahələri də daxil olmaqla obrazda axtarış apara bilər, bu zaman sistemin özünün axtarış aləti və ya makrodil istifadə edilir.

Paralel port və ya şəbəkə platasından kompyuteri ilkin analiz etməyə (iz buraxmadan) imkan verir. Avtomatlaşdırma üçün

makrodili vardır. Standart gizli izləri (swap-faylları, "zibil qutusunu" və s.) axtarır, lakin loq faylları analiz etmir. Hesabat hazırlama sistemi inkişaf edib. Müstəntiq qeydlər və şərhlər edə bilər.

Fstat – fstat komandası sistemdə açıq faylların siyahısını verir, bundan gözlənilməyən loq-faylları (məsələn, paket snifferlərinin yaratdığı) müəyyən etmək üçün istifadə etmək olar.

Netcat – istənilən port nömrəli TCP və ya UDP şəbəkə bağlantıları yaradır, oradan verilənləri qəbul edir və məlumatları göndərir. Onu çox vaxt digər komandalarla birlikdə skriptlərdə istifadə edirlər. Bu proqramı şəbəkənin və ya trafikin test edilməsi üçün paket axınları yaratmaq və ya tutmaq üçün istifadə etmək olar. Həmçinin, boşluğu olan serverləri aşkarlamaq üçün şəbəkələri daramaq, şəbəkə ekranlarını test etmək, proksi qurmaq üçün də istifadə etmək olar.

sockstat – sockstat komandası sistemdə açıq soketlərin siyahısını verir, bundan gözlənilməyən bağlantıları (məsələn, paket snifferlərinin yaratdığı) müəyyən etmək üçün istifadə etmək olar.

The Coroner's Toolkit (TCT) – Weitse Venema və Dan Farmer tərəfindən yazılmış proqramlar toplusudur, sındırılmış Unix sistemlərinin "ölümdən sonrakı" analizi üçün istifadə edilə bilər. Veb-saytda alətin praktiki vəziyyətlərdə istifadəsinə aid nümunələr verilib.

Sysinternals utilitləri – Sysinternals istifadəçilərə Microsoft Windows mühitinin idarə edilməsi, diaqnostikası, nasazlıqların aradan qaldırılması və monitorinqi üçün fayl və disk utilitləri, şəbəkə utilitləri, proses utilitləri, təhlükəsizlik utilitləri, sistem haqqında məlumat utilitləri və müxtəlif utilitlər adı altında çox sayda pulsuz utilitlər təqdim edir.

Sysinternals saytı (əvvəllər «ntinternals» kimi də məşhur idi) 1996-cı ildə Mark Russinovich və Bryce Cogswell tərəfindən yaradılmışdı və «Winternals Software LP» şirkətinə məxsus idi. 18 iyul 2006-cı ildə «Winternals» şirkətini bütün məhsulları ilə

birlikdə Microsoft şirkəti almışdır və indi Sysinternals □ Microsoft Technet veb-saytının bir hissəsidir (http://technet.microsoft.com/en-us/sysinternals).

2011-ci ilin yanvarında Microsoft utilitlərin Mark Rusinoviç və Bryus Koqsvell tərəfindən yaradılmış kodlarını Microsoft Technet saytından yığışdırdı. Microsoft öz hərəkətlərini onunla əsaslandırırdı ki, bu ilkin kodlara giriş Windows ƏS-in digər komponentlərinin dəstəklənməsində problemlər yarada bilər.

İnsidentlərin təhqiqatı üçün alətlər

AbuseHelper - CERT və Sui-istifadələri aşkarlama komandaları (ing. Abuse team) üçün alətlər toplusudur. AbuseHelper ilə müxtəlif mənbələrdən məlumat toplamaq, onları müxtəlif əlamətlər (məsələn, AS nömrələri və ya ölkə kodları) əsasında birləşdirmək, hesabatları müxtəlif formatlarda yaratmaq olar. Windows, Unix, Mac platformalarında əlyetəndir (http://www.abusehelper.org/). CERT-EE, CERT-FI, CERT.LV, BELNET CERT tərəfindən istifadə edilir.

InterNIC – axtarış aparıla bilən Whois verilənlər bazası saxlayır, ona sorğu verməklə IP-ünvanlar blokunun sahibini müəyyən etmək olar. Verilənlər bazasının .com, .edu və s. kimi yüksək səviyyə domenlərinin əksəriyyəti haqqında informasiyaya girişi var.

RIPE (Reseaux IP Europeens) – Avropada, Yaxın Şərqdə, Şimali Afrikada və Asiyanın müəyyən hissələrində IP-ünvanlar və Avtonom sistem nömrələri (Autonomous System, AS) verir. Onun veb-saytında axtarış aparıla bilən Whois verilənlər bazası saxlanır, ona sorğu verməklə IP-ünvanlar blokunun sahibini müəyyən etmək olar. Whois protokolu ilə whois.ripe.net istifadə edilməklə birbaşa Whois serverinə sorğu göndərmək olar.

APNIC (Asia Pacific Network Information Centre) – Asiya-Sakit Okean coğrafi regionunda IP-ünvanlar və AS nömrələri verir. Onun veb-saytında axtarış aparıla bilən Whois verilənlər bazası saxlanır, ona sorğu verməklə IP-ünvanlar blokunun

sahibini müəyyən etmək olar. Whois protokolu ilə whois.apnic.net istifadə edilməklə birbaşa Whois serverinə sorğu göndərmək olar.

ARIN (American Registry for Internet Numbers) – Şimali və Cənubi Amerika, Karib ölkələri və Böyük Səhradan cənubdakı 48 Afrika ölkəsi üçün IP ünvanlar və AS nömrələri verir. Veb-saytda Whois verilənlər bazasında axtarış aparmaq, IP-ünvan blokunun sahibini müəyyən etmək olar. Whois protokolu ilə birbaşa whois.arin.net istifadə edilməklə Whois serverinə sorğu da göndərmək olar.

BGP Ranking – İnternet Servis Provayderinin təhlükəsizlik ranqını hesablamaq üçün (Internet Service Provider, ASN) pulsuz proqram təminatı və pulsuz xidmətdir.

Dig (Domain Information Groper) – DNS ünvan məlumatlarını sorğulamaq üçün istifadə edilən komandadır, nslookup utilitinə alternativdir.

Host – bu komandanın köməyi ilə müxtəlif Internet mənbələrindən hostlar barəsində ünvan və ad məlumatlarını toplamaq olar.

Norman sandbox – Hazırda yeni viruslar populyar tətbiqi proqramlarda tapılan boşluqları istismar etməklə getdikcə daha sürətlə yayılır. Siqnaturaya əsaslanan ənənəvi antivirus alətləri yeni viruslarla mübarizə üçün yetərli deyil. Norman SandBox texnologiyası yeni və məlum olmayan viruslardan qorunmaq üçün təklif edilmiş proaktiv həlldir.

Whois – bu servis IP-ünvanın sahibini müəyyən etməyə imkan verir. IP-ünvan statik və ya dinamik ola bilər (bədniyyətli provayderin şəbəkəsində və ya İnternet-kafedə ola bilər). Bədniyyətli bir neçə aralıq proksi-server üzərindən işləyə bilər. Bədniyyətli heç bir şeydən xəbəri olmayan istifadəçinin kompyuterində quraşdırılmış ziyankar proqram təminatı vasitəsilə işləyə bilər (birbaşa və ya bota komandalar göndərməklə).

Traceroute – bu servis bədniyyətliyədək olan yolu izləməyə, o cümlədən, marşrutlama cədvəllərinin icazəsiz dəyişməsini başa düşməyə imkan verir.

Traceroute circl – CSIRT operatorlarının fəaliyyətini dəstəkləmək üçün traceroute proqramının genişlənməsidir. Adətən, CSIRT komandası IP-ünvanlar əsasında insidentləri emal etməli olur. Bu alət bütün tranzit IP-ünvanlar üçün sui-istifadə kontaktlarını avtomatik göstərir, hər bir hop üçün CSIRT kliyenturasını göstərir və ya RBL-i axtarır (RBL – Realtime BlackList və ya DNSBL – onlayn qara siyahı).

Nslookup – DNS servisindən informasiya sorğulamaq üçün istifadə edilən komandadır. Onu adları və IP-ünvanları axtarmaq üçün, eləcə də DNS-lə əlaqədar problemlərin və ya ad serverinin keşi çərçivəsində informasiyanın korlanması cəhdlərinin diaqnostikası üçün istifadə etmək olar.

Tcpdump – Ethernet trafikinin analizatorudur (ing. TCP və dump – zibillik, yükü boşaltmaq). Kommersiya və pulsuz çoxlu analizator var, lakin tcpdump daha geniş yayılıb və baha deyil. Linux və BSD daxil olmaqla UNIX distrubutivlərinin çoxuna daxildir. Proqramın Windows üçün variantları da var, məsələn, windump. Tcpdump şəbəkə interfeysindən keçən TCP/IP paketlərinin məzmununu çıxış qurğusuna (adətən, fayl və ya ekrana) çıxarır. Tcpdump-ın işləməsi üçün o, şəbəkə platasını dinləmə rejiminə (ing. promiscuous mode) keçirməlidir. Bu, o deməkdir ki, şəbəkə platası yalnız ona ünvanlanmış trafiki deyil, bütün Ethernet trafikini tutacaq. Proqramı yerinə yetirmək üçün root hüququ və qurğuya birbaşa giriş olmalıdır. Proqram iki əsasa hissədən ibarətdir: paketləri ələ keçirən hissə (libcap (Linux) və pcap (Windows) kitabxanalarına müraciət) və tutulmuş paketlərin göstərilməsi (ilkin kod səviyyəsində modulyardır və yeni protokolu dəstəkləmək üçün yeni modul əlavə etmək kifayətdir).

Top – Linux ƏS-də işə salınmış proseslərin siyahısını göstərmək üçün istifadə edilir, proseslərin statusu real vaxt rejimində

göstərilir (*top – atop, htop, iotop, iftop, dnstop və s. utilitlərindən ən sadəsi və geniş yayılanıdır). Top utiliti prosesin sistem resurslarından istifadəsini göstərir, məsələn, əgər proses olduqca çox yaddaş istifadə edirsə, onu siyahının əvvəlində tapmaq olar.

Nmap ("Network Mapper") şəbəkənin tətqiqi və təhlükəsizliyin yoxlanması üçün açıq kodlu utilitdir (http:/nmap.org). Böyük şəbəkələrin sürətli daranması üçün yaradılmasına baxmayaraq, məhdud məqsədlər üçün də yaxşı işləyir. Nmap şəbəkədə əlyetən hostları, onların təklif etdikləri xidmətləri (tətbiqi proqramın adını və versiyasını), onların istifadə etdikləri əməliyyat sistemlərini (ƏS-nin versiyasını), istifadə edilən şəbəkə ekranını və s. müəyyən etməyə imkan verir. Nmap təhlükəsizliyin yoxlanması üçün istifadə edilir, lakin şəbəkə və sistem administratorları onu adi məsələlərin həllində də faydalı hesab edirlər. Şəbəkənin srtukturuna nəzarət edilməsi, servislərin işə salınması cədvəllərinin idarə edilməsi, hostun və ya servisin iş müddətinin uçotu və s.

Nessus – informasiya təhlükəsizliyi sistemlərində məlum boşluqların avtomatik axtarışı üçün proqramdır. Proqram kliyent-server arxitekturasına malikdir, bu darama imkanlarını olduqca genişləndirir. (http://www.nessus.org).

Nessus hər şeydən əvvəl portların daranması üçün istifadə edilir və onlardan istifadə edən servisləri müəyyən edir. Boşluqlar bazası əsasında servislərin yoxlanması da həyata keçirilir. Boşluqların test edilməsi üçün NASL dilində (Nessus Attack Scripting Language) yazılmış xüsusi plaqinlər istifadə edilir. Boşluqlar bazası həftədə yenilənir, kommersiya abunəçiləri üçün yeddi gün gözləmədən yeni plaqinləri yükləmək imkanı var.

Kliyent hissəsi həm Unix, həm də Windows sistemlərdə, server isə yalnız Unix sistemlərdə işləyə bilər. Kliyentlə server arasında ünsiyyət TCP üzərindən işləyən xüsusi Nessus protokolu – NTP ilə aparılır.

WireShark – şəbəkə analizatorudur (köhnə adı Ethereal-dır, 2006-cı ilin yayından yeni ad ilə tanınır). Lokal şəbəkənin trafikini və ya diskdəki əvvəlcədən hazırlanmış dampdan real rejimdə analiz edir. Wiresharkın son versiyaları VoIP səs trafikini analiz edir, həmçinin IPSec, ISAKMP, Kerberos, SNMPv3, SSL/TLS, WEP və WPA/WPA2 protokollarını deşifrləyə bilir. gzip-lə sıxılmış verilənlər də real rejimdə açılır. Sniffer təkcə Ethernetdə deyil, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Realy, FDDI şəbəkələrdə də işləyir.

AirSnort – naqilsiz lokal şəbəkələrdə (Wtreless LAN) şifrləmə açarlarını bərpa edən alətdir. AirSnort trafiki passiv monitorinq edir və kifayət qədər paket toplandıqdan sonra şifrləmə açarını hesablayır.

hping – komanda ilə işləyən TCP/IP paket analizatorudur. İnterfeysi ping (8) Unix komandasından qaynaqlanır, lakin təkcə ICMP exo-sorğularının göndərilməsi ilə kifayətlənmir. TCP, UDP, ICMP və RAW-IP protokollarını dəstəkləyir, traceroute rejimi var, qapalı kanallar arasında faylları ötürmək və bir çox digər xüsusiyyətləri var.

TripWire – faylların tamlığını yoxlayır (OSSEC, AIDE və Samhain də oxşar funksiyaları təklif edir). Kommersiya və açıq kodlu versiyaları mövcuddur, onların arasında əhəmiyyətli fərqlər var. Kommersiya versiyası bir çox platformanı, o cümlədən Windows-u dəstəkləyir. Kommersiya versiyası proqramın verilənlər bazalarını və konfiqurasiyaları idarə etmək üçün yaxşı interfeysə malikdir.

Sistemə soxulduqda hakerlərin ən sevimli üsullarından biri əsas faylları troyan versiyaları ilə əvəz etməkdir. Tripwire ilk dəfə işə salındıqda bütün faylların (və ya konfiqurasiyada göstərilənlərin) heş-kodlarını hesablayır və verilənlər bazası yaradır. Bundan sonra Tripwire-ni periodik işə salmaq və heş-kodları müqayisə etmək olar, əgər onlar üst-üstə düşmürsə, deməli, faylda dəyişiklik edilib.

Snort – şəbəkə IDS-dir (müdaxilələrin aşkarlanması sistemi), IP-şəbəkələrdə trafikin real vaxt rejimində analizini apara bilir. Protokolların analizini, kontentdə axtarışı, bufer daşması, gizli port daramaları, CGI hücumlar, SMB zondları, ƏS-nin tipini və versiyasını müəyyən etmək cəhdləri kimi bir sıra hücumları aşkarlaya bilir.

Argus (Audit Record Generation and Utilisation System) – şəbəkə monitorinqi sistemidir, şəbəkədə tranzaksiyaların vəziyyətini izləməyə imkan verir. İnformasiya standart formatda yazılır, yazıları analiz edərək anomaliyaları, müdaxilələrin əlamətlərini axtarmaq olar.

FƏSİL 6

CSIRT KOMANDALARININ BEYNƏLXALQ ƏMƏKDAŞLIĞI

CSIRT KOMANDALARININ BEYNƏLXALQ ƏMƏKDAŞLIĞI

- **Trusted Introduser**
- **NATO CIRC**
- **APCERT**
- **ENISA**
- **SANS İnstitutu**
- **TI-də qeydiyyat və akkreditasiya**
- **FIRST-ə üzvlük tələbləri**

FƏSİL 6 CSIRT KOMANDALARININ BEYNƏLXALQ ƏMƏKDAŞLIĞI

Hazırda dünyada informasiya təhlükəsizliyi insidentlərinin cavablandırılması üçün yaradılmış bir sıra beynəlxalq CSIRT-lər və əlaqədar təşkilatlar mövcuddur. CSIRT-lər lokal hücumlara cavab verə və özlərinin digər funksiyalarını yerinə yetirə bilərlər, beynəlxalq hücumlar isə beynəlxalq CSIRT-lərin diqqət mərkəzindədir.

6.1. Trusted Introducer

CSIRT əməkdaşlığına TF-CSIRT-in sərgilədiyi yeni yanaşmanın daha bir uğurlu nəticəsi Trusted Introducer (TI, Etibarlı Vasitəçi) olmuşdur. Bu qrup Avropa CSIRT-lərinin vahid kataloqunun aparılmasını öz üzərinə götürmüşdür. Kataloqla yanaşı, TI akkreditasiya xidməti və 2010-cu ildən CSIRT-lərin sertifikasiyası xidməti də göstərir. Avropa CSIRT-lərinin praktikada infrastruktur və texniki xidmət nəzərdə tutan kataloqu TI-dən əvvəl mövcud idi (1995-1997-ci illərdə DFN-CERT, 1998-1999-cu illərdə EuroCERT tərəfindən istismar edilirdi). Hazırda TI bu dəstək infrastrukturunu tam təmin etmək imkanındadır.

TI xidmətinə doğru ilk addım 2000-ci ilin əvvəlində aparılmış analiz olmuşdu. Analizə TERENA tərəfindən nəzarət edilmişdi.

Bu analizin nəticələri olan hesabatda TI təsvir edilir: "müəyyən edilmiş miqyas (CSIRT-lər) çərçivəsində yeni komandalara elə səviyyəyə qalxmağa imkan verəcək ki, digər

komandalar onlarla informasiya paylaşımını və insidentlər üzərində onlarla birgə işləməyi nisbətən asan görəcəklər (başqa sözlə, onlara etibar edəcəklər), artıq mövcud olan komandalara isə həmin səviyyəni təmin etmək üçün TI yoxlanıla bilən obyektiv tələblərə əsaslanmalıdır."

Komandalar arasında müzakirələrin əksəriyyəti TI prosesinin bir hissəsi kimi sertifikatlaşdırmanın, yoxsa akkreditasiyanın yerinə yetirilməsi barəsində idi. Komandaların çoxu sertifikatlaşdırmanın həqiqətən də zəruri olmasına əmin deyildilər və çoxları fikirləşirdi ki, irəli sürülən tələblərin çoxu həmin vaxt yaxşı aydınlaşdırılmamışdı, əldə edilə bilən hədəfləri qarşıya qoymaqla akkreditasiyanın yerinə yetirilməsi qəbul edildi.

Hesabatın müsbət əks-sədasına əsaslanaraq CSIRT-komandalar beynəlxalq əməkdaşlığa TI yanaşmasını həyata keçirməyə başladılar. TI xidməti 1 sentyabr 2000-ci ildən işə başladı, ilkin maliyyələşdirməni TERENA edirdi, bir il işlədikdən sonra akkreditasiya edilmiş komandaların üzvlük haqları ilə maliyyələşməyə keçildi.

IRT-obyektlər. Akkreditasiya edilmiş CSIRT komandalarına TI-nin təqdim etdiyi xidmətlərdən biri IRT-obyektlərin saxlandığı verilənlər bazasına girişdir.

IP-ünvan üzrə əlaqə məlumatlarının axtarışı insidentlərin cavablandırılması komponentlərindən biridir. Adətən, RIPE NCC, Inter NIC, APNIC, LatNIC kimi regional IP-reyestrlərin verilənlər bazaları istifadə edilir. Burada IP-ünvanlar blokuna xidmət edən təşkilat və ya ISP barəsində əlaqə məlumatları olur. IRT-obyektlərin verilənlər bazası TF-CSIRT və RIPE NCC Database Group-un birgə işinin məhsuludur. Məqsəd – müəyyən IP-ünvan fəzası üçün əlaqə məlumatlarının axtarışını təşkil etməkdir.

IRT-obyekt insident halında və ya informasiya təhlükəsizliyi məsələləri üzrə kiminlə əlaqə yaratmaq barədə informasiyanı bazaya əlavə etməyə imkan verir.

Verilənlər bazasına IRT-obyekti daxil etmək hüququ IP-ünvanlar qrupuna xidmət edən təşkilata və ya TI-yə məxsusdur. Verilənlər bazasının yoxlanılması və bazaya xidmət isə TI-nin səlahiyyətindədir.

6.2. NATO NCIRC

NATO özünün CERT mərkəzinin yaradılması işlərinə Praqa (2002) və İstanbul (2004) sammitlərində alınmış qərarlara uyğun olaraq başladı, onu Kompyuter İnsidentlərini Cavablandırma üzrə NATO Koordinasiya Mərkəzi (NATO Computer Incident Response Capability, NCIRC) adlandırdılar (http://www.ncirc.nato.int/).

NCIRC-in xidmətlərinə aşağıdakılar daxildir:

- NATO çərçivəsində kompyuter təhlükəsizliyi insidentlərinə cavab kimi texniki və qanunvericilik dəstəyi xidmətləri;

Mərkəzləşdirilmiş xidmətlər:

- profilaktika tədbirləri (bülletenlər, proqram təminatının yenilənməsi və s.);
- cavab tədbirləri (insident və IDS dəstəyi və cavablar);
- qanunvericilik dəstəyi (məhkəmə, istintaq, siyasətin təkmilləşdirilməsi).

NCIRC-in strukturu 3 səviyyədən ibarətdir:

- ***birinci səviyyə***: NCIRC-in koordinasiya mərkəzi;
- ***ikinci səviyyə***: NCIRC-in texniki mərkəzi, həmçinin NCIRC ilə qarşılıqlı əlaqədə olan dövlət və qeyri-dövlət CERT-ləri;
- ***üçüncü səviyyə***: NATO sistem və şəbəkə mərkəzləri/administratorlar.

NCIRC-in xidmətlərinin NATO-nun qapalı şəbəkəsində (təxminən 25000 işçi stansiya), NATO-nun açıq şəbəkələrində (o cümlədən İnternet), milli şəbəkələr üçün şlüzlərdə istifadə edilməsi nəzərdə tutulur.

Kompyuter insidentlərini cavablandırma potensialı çərçivəsində əsas xidmətlərə aşağıdakılar daxildir:

- pozuntularla mübarizədə kömək;

- boşluqlar və təhdidlər haqqında məlumatlar;
- riskin qiymətləndirilməsi (onlayn/yerində)
- konsaltinq xidmətləri (elmi və məhkəmə ekspertizası);
- onlayn verilənlərin toplanması və monitorinqi (IDS, antiviruslar, şəbəkə ekranları);
- onlayn dəstək (avtomatik yenilənmə) ;
- insidentlərin analizi (oflayn) və təhlükəsizliyin test edilməsi.

Bəzi hallarda sistemin funksiyaları tam, bəzilərində isə qismən avtomatlaşdırılıb.

NATO CERT-inin yaradılması prosesinə yardım etmək üçün hər altı aydan bir NATO ölkələrinin nümayəndələri NCIRC təhlükəsizlik seminarlarında görüşürlər. Bu seminarların məqsədləri aşağıdakılardır:

- NATO çərçivəsində və NATO ölkələri ilə kompyuter təhlükəsizliyi insidentlərinin emalı üzrə korporativ biliklərin təkmilləşdirilməsi və paylaşımı;
- Məlumat kitabı – "CIRC fəaliyyətlərinin konseptual və əməliyyat arxitekturasını müəyyən etmək üçün əsas sənəd" hazırlamaq;
- Diqqəti üç spesifik istiqamətə yönəltməli:
  - texniki ekspertiza və spesifik kompyuter insidentlərinin və IDS hadisələrinin analizi üçün standart əməliyyat prosedurları;
  - məhkəmə ekspertizası;
  - kibertəhlükəsizlik təlimləri.

Bu iclaslarda həm hərbi, həm də mülki və dövlət CERT-lərinin (GovCERT.NL, UNIRAS, CERTA, NOR-CERT, CERT Polska) mütəxəssisləri iştirak edirlər. NCIRC seminarlarının başqa bir nəticəsi bu seminarlarda tapılmış həllər əsasında bəzi ölkələrdə yeni dövlət CERT-lərinin yaradılmasıdır.

6.3. APCERT

Kompyuterdə fövqəladə hallara cavab üzrə Asiya-Sakit Okean qrupu (Asiya Pacific Computer Emergency Response Team, APCERT) bu regionda təhlükəsizlik məsələləri üzrə məlumatlılığı yüksəltmək və insidentlərə cavab potensialının gücləndirilməsi üçün təhlükəsizlik üzrə ekspertlərin şəbəkə cəmiyyəti kimi 2003-cü ilin fevralında yaradılmışdı. Asiya-Sakit Okean ölkələrinin CSIRT-komandalarının ilk konfransı 2002-ci ildə Yaponiyada keçirilmişdi. Bir il sonra Taypeydə konfrans zamanı APCERT yaradıldı, burada 14 Asiya-Sakit Okean CSIRT-i iştirak edirdi. 2011-ci il 1 avqust tarixinə APCERT-də 19 daimi üzv və 8 assosiativ üzv var idi.

APCERT iştirakçıları etiraf edirlər ki, hazırda kompyuter təhlükəsizliyi sahəsində insidentlər olduqca çoxdur və onların bir təşkilat və ya bir ölkə daxilində idarə edilməsi çətindir, daha effektiv cavablandırma APCERT-in digər üzvləri ilə əməkdaşlıq əsasında həyata keçirilə bilər. FIRST-də olduğu kimi, APCERT-də də ən vacib anlayış informasiya mübadiləsi və bir-biri ilə qarşılıqlı əlaqə üçün iştirakçılar arasında inam münasibətləridir. Beləliklə, APCERT-in tədbirləri aşağıdakılara yönəlib:

- Asiya-Sakit Okean regional və beynəlxalq əməkdaşlığın genişləndirilməsi;
- böyükmiqyaslı və regional şəbəkələrdə təhlükəsizlik sahəsində insidentlərlə mübarizə tədbirlərinin birgə işlənməsi;
- təhlükəsizlik sahəsində texnologiya, informasiya, o cümlədən kompyuter virusları, istifadə edilmiş skriptlər və s. haqqında informasiya mübadiləsinin yaxşılaşdırılması;
- ümumi problemlər üzrə birgə tədqiqatların effektivliyinin yüksəldilməsi;
- informasiya təhlükəsizliyi insidentlərin effektiv cavablandırılması üzrə regionda digər CERT-lərə kömək göstərilməsi;

– regional informasiya təhlükəsizliyi və insidentləri cavablandırma ilə bağlı hüquqi məsələlər üçün tövsiyələrin və həllərin təklif edilməsi.

6.4. Avropa dövlət CERT-ləri qrupu

Avropa dövlət CERT-ləri qrupu (European Government CERTs Group, EGC) Avropa ölkələrində CSIRT-lə əlaqədar qeyri-rəsmi komitədir, 2001-ci ilin noyabrında yaradılmışdır. Hazırda aşağıdakı CERT komandaları onun üzvləridir:

Finlandiya	CERT-FI	www.ficora.fi/suomi/tietoturva/cert.htm
Fransa	CERTA	www.certa.ssi.gouv.fr
Almaniya	CERT-BUND	www.bsi.bund.de/certbund/index.htm
Macarıstan	CERT-Hungary	www.cert-hungary.hu/
Niderland	GOVCERT.NL	www.govcert.nl
Norveç	NorCERT	www.cert.no
İspaniya	CCN-CERT	www.ccn-cert.cni.es/
İsveç	SITIC	www.sitic.se
Birləşmiş Krallıq	CSIRTUK	www.cpni.gov.uk
Birləşmiş Krallıq	GovCertUK	www.govcertuk.gov.uk

EGC-nin funksiyaları aşağıdakılardır:

– irimiqyaslı və regional şəbəkələrdə təhlükəsizlik sahəsində insidentlərlə mübarizə üçün tədbirlərin birgə işlənməsi;
– təhlükəsizlik sahəsində insidentlərlə, ziyankar kodun istifadəsindən yaranan təhdidlərlə və boşluqlarla əlaqəli informasiya və texnologiya mübadiləsinə yardım edilməsi;
– EGC qrupunun daxilində birgə istifadə edilə bilən bilik və təcrübə sahələrinin müəyyən edilməsi;
– iştirakçılar üçün maraq kəsb edən mövzular üzrə birgə elmi-tədqiqatlar və işləmələr üçün sahələrin müəyyən edilməsi;

– Avropa ölkələrində dövlət CSIRT-lərinin formalaşmasına kömək göstərilməsi.

Boşluqları və insidentləri cavablandırmanın beynəlxalq aspektlərini nəzərə alaraq EGC komandaları digər CERT təşəbbüsləri ilə də əməkdaşlıq edirlər. Məsələn, bütün EGC komandaları FIRST-in və TF-CSIRT-in üzvləridir və onların Avropada və dünyada işlərini dəstəkləyirlər. EGC komandaları ENISA-nın fəaliyyətində, xüsusilə Avropada dövlət CERT-lərinin yaradılması məsələsində yaxından iştirak edirlər və ENISA-nın nəticələrinə töhfələr verirlər.

EGC veb saytı www.egc-group.org-dır. EGC sədri rotasiya qaydası ilə təyin edilir və EGC-qrupu üçün təmas nöqtəsi kimi xidmət edir. Əlavə olaraq, hər bir EGC üzvü ilə fərdi təmas yaratmaq olar. Media ilə təmaslar üzv təşkilatlar tərəfindən fərdi idarə edilir.

6.5. ENISA

CSIRT mövzusu üzrə elmi-metodiki işlərin əsas mənbələri üç təşkilatdır: CERT/CC Koordinasiya Mərkəzi, SANS (SysAdmin, Audit, Network, Security) İnstitutu və ENISA (European Network and Information Security Agency, Avropa Şəbəkə və İnformasiya Təhlükəsizliyi Agentliyi).

ENISA Agentliyinin məqsədi şəbəkə və informasiya təhlükəsizliyi (ŞİT) sahəsində mədəniyyətin formalaşdırılması yolu ilə Avropa İttifaqında ŞİT-in yüksəldilməsidir. ENISA 2004-cü ilin yanvarında Nazirlər Şurası və Avropa parlamenti tərəfindən "yüksək texnologiya" cinayətlərinə cavab vermək üçün yaradılmışdı. Agentlik aşağıdakı vəzifələri yerinə yetirir:

– ENISA və Avropa İttifaqı üzvləri arasında ŞİT-in təmin edilməsi məqsədi ilə dəstək göstərilməsi;
– maraqlı tərəflər arasında davamlı informasiya mübadiləsinə kömək göstərilməsi;
– ŞİT-lə əlaqəli olan funksiyaların koordinasiyasının yaxşılaşdırılması.

ENISA 2005-2010-cu illərdə "CERTs in Europe" adlı beş seminar təşkil etmişdi. Yeni CSIRT komandalarının yaradılmasını dəstəkləmək üçün ENISA 2006-cı ildə "CSIRT yaradılması üzrə addımbaaddım rəhbərlik" adlı sənəd işləmişdir və 20 dildə, o cümlədən rus dilində əlyetəndir. Bu sənəd CSIRT yaradılması prosesini həm texniki, həm də biznes-proseslərin idarə edilməsi baxımından ətraflı təsvir edir. ENISA Agentliyi bir sıra digər açıq istifadəli sənədlər də işləmişdir:

- CSIRT-in istismarı üzrə yaxşı təcrübələrin baza toplusu (A basic collection of good practices for running a CSIRT);
- CSIRT-komandasının treninqi üçün çalışma materialları toplusu (CERT Exercises Handbook və CERT exercises toolset);
- Dövlət/milli CSIRT komandaları üçün baza imkanları (Baseline capabilities of national / governmental CERTs);
- İnsidentlərin idarə edilməsi üzrə praktiki rəhbərlik (Good Practice Guide for Incident Management);
- İnsidentlərin emalı üzrə geniş yayılmış alətlərinin icmalı (Clearinghouse for Incident Handling Tools veb-saytı).

6.6. SANS İnstitutu

SANS (SysAdmin, Audit, Network, Security) İnstitutu 1989-cu ildə təhsil-tədqiqat müəssisəsi kimi yaradılmışdır, informasiya təhlükəsizliyi sahəsində mütəxəssislərin hazırlanması və sertifikatlaşdırılması ilə məşğul olur. SANS İnstitutu təhlükəsizlik məsələləri üzrə çoxsaylı informasiya və təhsil materialları hazırlayır, dəstəkləyir və pulsuz yayımlayır, mütəxəssislərin treninqi və sertifikatlaşdırılması (Global Information Assurance Certification (GIAC) Program: GSEC (GIAC Security Essentials Certification), GIAC Specialist, GIAC Security Expert) xidmətləri göstərir. Hazırda onun proqramlarından 165 000-dan çox informasiya təhlükəsizliyi mütəxəssisi yararlanmışdır.

SANS İnstitutunun göstərdiyi informasiya xidmətlərinə daxildir:

- Internet Storm Center – İnternetdə erkən xəbərdarlıq sistemi;
- boşluqların həftəlik xülasəsi (@RISK);
- yeniliklərin həftəlik xülasəsi (NewsBites);
- 1200-dən çox orijinal elmi tədqiqat məqaləsinin, metodiki tövsiyələrin daxil olduğu onlayn kitabxana (oxu zalı) və s.

SANS İnstitutunun onlayn oxu zalında insidentlərin idarə edilməsi mövzusu üzrə maraqlı məqalələr tapmaq olar. 1990-cı illərin ortalarında SANS "Kompyuter təhlükəsizliyi insidentlərinin addımbaaddım emalı" adlı sənəd hazırlamışdır. Bu sənədin 2.3.1 versiyasında insidentlərin emalının 6 ardıcıl prosesi təklif edilir: hazırlıq, identifikasiya, lokallaşdırma, səbəblərin aradan qaldırılması, bərpaetmə, dərs çıxarma. İnsidentlərin 8 növü üçün xüsusi hərəkətlərin təsviri verilir (zərərli kod, skanlama, DoS, qanunsuz istifadə, şpionaj, mistifikasiya, icazəsiz giriş, intellektual hüquq). SANS İnstitutu "SANS Security 504 Hacker Techniques, Exploits and Incident Handling" adlı kurs da təklif edilir.

6.7. TI-də qeydiyyat proseduru

Trusted Introducer (TI) Avropada CSIRT-lər və ya CERT-lər üçün inam şəbəkəsidir. İnsidentlərin emalı xidmətləri göstərən istənilən CSIRT komandası TI-də qeydiyyatdan keçməyə dəvət olunur. Qeydiyyatdan keçdikdən ("siyahıya düşdükdən") sonra komandanın məlumatları TI tərəfindən ictimaiyyətə təqdim olunur.

Qeydiyyatdan keçmək üçün aşağıdakı addımları yerinə yetirmək lazımdır.

1. "Siyahıya düşmək" forması doldurulur.
2. Doldurulmuş forma TI-yə göndərilir.
3. TI məktubu aldığını təsdiqləyəcək və sizə əlavə suallar verəcək, həmçinin TI soruşacaq ki, sizin "siyahıya düşmək" sorğunuzu dəstəkləyən TI-akkreditasiyalı

komanda tanıyırsınızmı (sizi dəstəkləyən ən azı iki komanda lazımdır).

Əgər məktuba cavab gəlməsə, o zaman SMS nömrəsindən istifadə etmək lazımdır: +447771533788.

Nömrə yalnız SMS üçündür, zəng etmək olmaz.

Sizin göndərəcəyiniz qısa ismarıcda aşağıdakı məlumatlar olmalıdır:

- sizin adınız;
- təşkilatın adı;
- sizinlə əlaqə üçün e-poçt ünvanı;
- sizinlə əlaqə üçün nömrə;
- mövzu adı və ya qısa təsvir;
- natamam ismarıclara baxılmaya bilər.

4. TI kifayət qədər informasiyaya malik olduqdan sonra akkreditasiyalı komandalar cəmiyyəti ilə sizin "siyahıya düşmək" sorğunuzu məsləhətləşəcək və buna 2 həftə vaxt verəcək. Bu məsləhətləşmə prosesi gizlidir və sizə yalnız binar nəticə (HƏ/YOX tipli) göndəriləcək. Yaxşı halda 2 həftə içində akkreditasiyalı 2 komanda sizin sorğunuzu dəstəkləyəcək və heç kim etiraz etməyəcək – bu halda sizin sorğunuzun nəticəsi müsbət (POSITIVE) olacaq. Bütün digər hallarda, TI müsbət və ya mənfi (NEGATIVE) nəticə haqqında qərara gəlmək üçün məsələni TI Review Board şurasına çıxaracaq.

5. Yuxarıdakı addımlardan sonra sizə sorğunuzun nəticəsi haqqında binar formada məlumat veriləcək:
   Nəticə POSITIVE olarsa, CSIRT həmin andan "siyahıya düşəcək". Bundan sonra siz akkreditasiya üçün dərhal müraciət edə bilərsiniz.
   Nəticə NEGATİVE olarsa, sorğunuz rədd edilir, dəqiq bir il keçdikdən sonra siz yenidən müraciət edə bilərsiniz. (Qeyd: 3 rəddən sonra komandaya siyahıya düşmək üçün sorğu göndərməyə icazə verilmir.)

6.8. FIRST-ə üzvlük proseduru

1. Sponsorluq üçün 2 tam FIRST-üzvü tapılır. Onları tapmaq üçün yaxşı fürsət illik FIRST konfranslarında iştirak etməkdir.
2. Sponsorlar ərizə veriləcəyi barədə FIRST Katiblik Xidmətinə (FIRST Secreteriat Services, FSS) xəbər verirlər. FSS "çoban"ın – FIRST üzvlük komitəsinin üzvünün adını bildirəcək, bu şəxs ərizə verən komandaya və sponsorlara bütün proses ərzində kömək edəcək.
3. Əlavə A doldurulur. Bu zaman hər hansı problem olsa, sponsorlar və çoban kömək edəcək. Ərizəçi komanda öz üzvlərindən birini FIRST-təmsilçi (Representative, rep) kimi bildirməlidir. Rep bütün komandanı təmsil edəcək, xüsusilə FIRST-in Böyük İllik Toplantısında (Annual Grand Meetings, AGM). Ərizəçiyə ən azı iki müxtəlif pgp-açarı tələb olunur: rep-in şəxsi açarı və bütün komanda üçün bir açar (team-açar).
4. Ərizəçi pgp-açarlarını (rep-açar və team-açar) sponsorlara imzaladır.
5. FIRST-ə birləşmək haqqında ərizə məktubu yazılır, burada komandanın FIRST-ə verəcəyi fayda göstərilir.
6. Sponsorlardan biri Ərizəçi-komandanı ziyarət edir. Tələblərlə tanış olmaq üçün Ruefle R. və Rajnovic D. tərəfindən hazırlanmış "Sayt ziyarəti sənədi" israrla tövsiyə edilir (FIRST Site Visit Requirements and Assessment, version 1.0).
7. Sponsorların hər ikisi təqdimat və Ərizəçi-komandanın tam FIRST üzvlüyü üçün tövsiyə məktubu yazırlar. Sayt ziyarəti gerçəkləşdirən sponsor bunu öz məktubunda qeyd etməlidir, sayt ziyarəti üzrə müfəssəl hesabatın olması yüksək qiymətləndirilir.
8. Sponsorlardan biri bütün paketi (Əlavə_A, 3 məktub, pgp-açarlar) imzalanmış və şifrlənmiş e-poçt ilə first-sec@first.org-a göndərir.

9. FIRST üzvlük komitəsi ərizəni nəzərdən keçirir. Əgər problemlər aşkarlanmasa, üzvlük komitəsi ərizəni qəbul etməyi tövsiyə edir.
10. Tam ərizə üzvlüyə qəbul tövsiyəsi ilə birlikdə FIRST-üzvlərin hamısına və FIRST İdarəetmə Komitəsinə (ing. Steering Committee) baxılmaq üçün göndərilir. Ən azı bir həftədən sonra İdarəetmə Komitəsi ərizə üzrə səsvermə keçirir.

6.9. FIRST üzvlük yoxlaması

1. Ümumi məsələlər

1.1. Müəyyən edilmiş kliyentura **(Məcburi)**

CSIRT kliyenturasının başa düşülməsi komandaya onların nəyə ehtiyacları olduğunu müəyyən etməyə, hansı aktivlərin mühafizə edilməli olduqlarını və CSIRT-lə qarşılıqlı əlaqələrin necə olacağını müəyyən etməyə kömək edir. Bu informasiyadan istifadə etməklə hansı servisləri təklif etməyi və bu servisləri göstərmək üçün CSIRT-in hansı təşkilati modelinin əlverişli olacağını müəyyən etmək olar.

Kliyenturanın müəyyən edilməsi CSIRT işə başladıqda işin miqyasını da imkan verir. O hansı sorğuların emal ediləcəyini, hansı sorğuların digər CSIRT-lərə və digər müvafiq tərəflərə ötürüləcəyini müəyyən etməyə imkan verir. Hər bir komanda aydın müəyyən edilmiş kliyenturaya malik olmalıdır. Əgər başqa komanda ilə üst-üstə düşürsə, bu aydınlaşdırılmalıdır və kliyenturaya aydın olmalıdır ki, nə vaxt hansı komandaya müraciət etsin.

1.2. Missiya bəyanatı və ya nizamnamə **(Məcburi)**

RFC 2350-də təsvir edildiyi kimi missiya CSIRT-in məqsədlərini və funksiyalarını aydın, birqiymətli şəkildə izah etməlidir. O, komandanın əsas hədəflərinin qısa siyahısını da verməlidir.

Missiya ayrıca məram bəyanatı sənədində, yaxud CSIRT-in nizamnaməsində və ya oxşar sənəddə yerləşdirilməlidir.

Missiya CSIRT-in əsasında qurulduğu fomal sənəddir. Bu sənəd yalnız CSIRT-i təsis etmir, həm də onun bəyənilmiş əməliyyatlarını və hakimiyyətini də təsvir edir.

Bu yuxarı rəhbərliyin dərkənarı və ya oxşar sənəd də ola bilər. Bu 1.2 bəndində adı çəkilmiş missiya və ya nizamnamənin hissəsi ola bilər və ya 1.3-də adı çəkilmiş rəhbərliyin elanı ola bilər.

1.3. Yaradılması, effektiv başlama tarixi və elan sənədi **(Məcburi)**

Komandanın əməliyyatlara başladığı effektiv başlama tarixi qeydiyyata alınmalıdır. Bu komandanın rəsmən öz mövcudluğuna başlaması vaxtıdır. Bu 1.5 bəndində müzakirə edilən yaradılma sənədinə və ya oxşar sənədə bir hissə kimi daxil edilə bilər.

Komandanın uğurlu olması üçün kliyentura onun mövcudluğundan xəbərdar olmalıdır və CSIRT-lə necə təmasa keçməyi və qarşılıqlı əlaqədə olmağı başa düşməlidir. CSIRT əməliyyata başladıqda bu kliyenturaya elan olunmalı və kliyentura ilə interfeys təsvir edilməlidir.

1.4. Kliyentura üçün göstərilən servislərin müəyyən edilmiş və elan edilmiş çoxluğu **(Məcburi)**

Servislərin müəyyən edilmiş çoxluğuna malik olmalıdır, onlar kliyentura üçün hansı hərəkətlərin, funksiyaların və son nəticələrin yerinə yetirildiyini izah edirlər. Bura həmçinin CSIRT və onun kliyenturası arasında razılaşdırılmış servis səviyyələrinin tərifləri də daxil edilməlidir.

Servislərin bu siyahısı kitabça, veb-sayt və ya digər oxşar mexanizm vasitəsilə kliyenturaya asanlıqla əlyetən olmalıdır.

Servislərin siyahısı CSIRT-in kliyentura üçün nəyi təmin etdiyini və təmin etmədiyini müəyyən edir. Bu həm CSIRT heyəti, həm də kliyentura üzvlərinin CSIRT-in malik olduğu rollar və məsuliyyətlər barədə gözləntilərini yerbəyer etməyə kömək edir.

Belə siyahının verifikasiyası CSIRT-in servislərini və məramlarını sənədləşdirən istənilən kitabçalarda və ya istənilən belə sənədlərdə, nizamnamələr, əməliyyat konsepsiyaları və sorğu kitabları daxil olmaqla tapıla bilər.
Bu tələbləri qarşılamaq üçün təkcə servislərin bu siyahısı müəyyən edilməməlidir, həm də kliyenturaya elan edilməlidir.

1.5. Maliyyələşdirmə modeli **(Məcburi)**
CSIRT-in uzunmüddətli stabilliyini təmin etmək üçün müvafiq maliyyələşdirmə modeli olmalıdır. Bu model komandanın fasiləsiz əməliyyatlarını və CSIRT servislərinin kliyenturaya fasiləsiz çatdırılmasını təmin etmək üçün CSIRT-ə maliyyə mənbələri verməlidir. Əgər servislər və ya abunələr üçün kliyenturadan hər hansı ödəniş alınırsa, bunlar kliyenturaya açıq bildirilməlidir. Təkcə işə salınma xərcləri deyil, uzunmüddətli istismar, heyət və avadanlıq xərcləri üçün də müvafiq maliyyələşdirmə olmalıdır. Müvafiq büdcə və ya maliyyə planı və ya istənilən forma qəbul edilməlidir.

1.6. Təşkilati ev **(Məcburi)**
CSIRT-in təşkilati evi komandanın baş təşkilat və ya kliyentura çərçivəsində mövqeyini göstərir. Daxili CSIRT öz şöbəsində, təhlükəsizlik qrupunda, IT və telekommunikasiya şöbəsində yerləşə bilər.
CSIRT CIO-ya, CEO-ya və ya digər şöbə müdirinə hesabat verməlidir və ya onun özünün ayrıca meneceri olmalıdır.
Koordinasiya CSIRT-i geniş kliyentura üçün mərkəzləşdirilmiş şöbə və ya özünün məxsusi təşkilatında yerləşə bilər. Milli komandaların çoxu dövlət təşkilatlarında yerləşir, digərləri isə tədqiqat şəbəkəsi və ya universitetlə əlaqələndirilə bilər.
CSIRT-in təşkilati evi təşkilatın sxeminə və diaqramına və ya rəhbərliyin hər hansı elanına baxmaqla yoxlanıla bilər.

1.7. Komandanın təşkilati strukturu **(Operativ)**

Komandanın təşkilati strukturu əsasən CSIRT-in heyət üzvlərini, onların rollarını və məsuliyyətlərini və baş təşkilat və ya kliyentura daxilində onların müvafiq yerləşmələrini təsvir edir. Bütün komanda üzvləri eyni şöbədə yerləşməyə bilərlər, onlar uzaqda yerləşə bilərlər və ya onlar resursu paylaşa bilərlər.

Komandanın təşkilati strukturunun təsvirinə CSIRT-in ola bilsin ki, bölündüyü altbölmə və altqruplar da daxil ola bilər. Məsələn, burada xüsusi treninq komandası və ya boşluğun emalı komandası ola bilər. Bu təşkilati təsvir CSIRT-in komanda liderini və bütün əsas və əlavə heyətini müəyyən etməlidir.

2. Siyasət

Bu bölmədə insidentin, boşluğun, artefaktın və sayt məlumatının mühafizə olunduğuna və təhlükəsizliyinə əmin olmaq üçün CSIRT-in malik olmalı olduğu müxtəlif siyasətlər təhlil edilir.

Bütün bu siyasətlər yazılı siyasətin sənədlərini təhlil etməklə və digər müvafiq prosedurlarla yoxlana bilər. Yoxlanmanı həm də heyətlə söhbət etməklə, onların siyasəti bildiyini və başa düşdüyünü aydınlaşdırmaq üçün etmək olar.

2.1. İnformasiyanın klassifikasiyası **(Məcburi)**

Bu siyasət CSIRT-in və uyğun kliyenturanın təsis etdikləri informasiya klassifikasiyasını təsvir etməlidir.

Klassifikasiya həssas, konfidensial və açıq informasiyanı fərqləndirməlidir.

Klassifikasiya siyasəti elektron və kağız formada istənilən informasiyaya tətbiq edilməlidir.

Bu siyasət FIRST komandalarından alınmış istənilən informasiyanın necə klassifikasiya (kateqoriyalaşdırma) ediləcəyini göstərməlidir.

2.2. İnformasiyanın mühafizəsi **(Məcburi)**

Bu siyasət informasiyanın müxtəlif növlərinin necə saxlanmasını və qorunmasını təsvir etməlidir. Burada hansı informasiyanın CSIRT avadanlığı çərçivəsində qalması və informasiyanın leptoplarda və digər mobil qurğularda necə emal edilməsi göstərilməlidir.

2.3. Yazıların saxlanması **(Məcburi)**

Bu siyasət müxtəlif sinfə aid informasiyanın CSIRT tərəfindən hansı müddətdə qorunub saxlandığını müəyyən etməlidir. Burada informasiyanın necə saxlandığı və mühafizə edildiyi, arxiv kopyalarının necə emal edildiyi, nəql edildiyi və arxivləşdirildiyi də təsvir edilməlidir.

Bu siyasət elektron və kağız formasında olan istənilən informasiyaya tətbiq edilməlidir.

2.4. Yazıların məhv edilməsi **(Məcburi)**

Bu siyasət klassifikasiya əsasında informasiyanın (elektron və ya kağız) necə məhv edildiyini təsvir etməlidir. Bu sərt disklər, portativ saxlama qurğuları və s. kimi mühitin necə məhv edilməli olduğunu təsvir etməlidir ki, həssas informasiya sızmasın və icazəsiz şəxsə əlyetən olmasın. Bu siyasət informasiyanın kağız formada necə və kim tərəfindən doğranmasını da təsvir etməlidir.

2.5. İnformasiyanın yayılması **(Məcburi)**

Bu siyasətin iki məqsədi var: müxtəlif daxili və xarici qruplarla paylaşıla bilən informasiyanın növünü müzakirə etməli və informasiyanın hansı metodlarla paylaşılmasını təsvir etməlidir.

Ən yüksək səviyyədə informasiyanın yayılması siyasəti hansı informasiyanın daxili və xarici qruplara, təşkilatlara açıqlana bildiyini təsvir edir. Onlar informasiyanın açıqlanmalı olmayan spesifik növlərini klassifikasiya ilə göstərir və hansı növ informasiyanın həssas və ya konfidensial hesab edilməsini hədəfləyir.

Bu siyasət CSIRT üçün çox vacibdir, çünki komandaların çoxu onların etibarlılığı əsasında yaşaya bilir. Bütün CSIRT heyətinin informasiyanın açıqlanması qaydalarını bilməsi tələb edilir, onlar nəyi deməyi və kimə deməyi bilməlidirlər. Kliyentura da bilməlidir ki, onlar insident və ya hücumlar haqqında CSIRT-ə məlumat verdikdə konfidensiallığın hansı səviyyəsinə ümüd edə bilərlər.

2.6. İnformasiyaya giriş **(Məcburi)**

Bu siyasət göstərməlidir ki, hansı növ və sinif informasiya CSIRT heyətinin üzvləri, baş və ya sahib təşkilat üzvləri, kliyentura üzvləri və xarici təşkilat tərəfindən baxıla və müraciət edilə bilər. İnformasiyanın, xüsusən də həssas və konfidensial informasiyanın müxtəlif səviyyələri ola bilər, bu giriş üçün daha yüksək səviyyədə avtorizasiya tələb etməlidir.

Bu siyasət kimdə giriş hüquqlarını dəyişmək hüququnun olmasını və kimin giriş prosesinə xidmətə görə məsuliyyət daşıdığını da təfsilatı ilə bildirməlidir. Müxtəlif növ informasiyaya baxa bilən avtorizasiyalı heyətin siyahısını aktual saxlamaq tövsiyə edilir.

2.7. CSIRT sistemlərinin düzgün istifadəsi **(Məcburi)**

Bu, əsasən yolverilən istifadə siyasətidir, gündəlik əməliyyatlar zamanı CSIRT heyətinin CSIRT avadanlığını və sistemlərini necə istifadə etdiyini ətraflı təsvir edir.

Komandanın istifadə etdiyi bütün avadanlıq icazəsiz girişlərə qarşı mühafizə edilməlidir.

İşlək vəziyyətdə olan və ya konfidensial məlumatlar ekranda olan kompyuterlər müşaiyətsiz buraxılmamalıdır. Əgər mümkündürsə, kompyuterlərdə icazəsiz aparat (məsələn, keylogger) və proqram təminatını (məsələn, keylogger, troyan, viruslar) müəyyən etmək üçün periodik yoxlamalar aparılmalıdır.

Bu siyasət və müvafiq prosedurlar təsvir etməlidir:

- sistemlərin yolverilən istifadəsi:
  - fərdi fəaliyyət üçün sistemlər istifadə edilə bilərmi?
  - CSIRT sistemlərindən hansı saytlara qoşulmaq və qoşulmamaq olar?
  - CSIRT sistemlərində şəxsi proqram təminatı yüklənə və quraşdırıla bilərmi?
- CSIRT sistemlərində verilənlərin hansı tezliklə və hansı növ ehtiyac kopyaları yaradılır?
- brauzerlər daxil olmaqla, proqram təminatı üçün təhlükəsizlik konfiqurasiyaları;
- hansı növ virus və spyware yoxlanması və hansı tezliklə aparılıb?
- proqram təminatı yenilənmələri və yamaqları necə quraşdırılır?
- uzaqdakı CSIRT servislərinə və sistemlərinə məsafədən girişin düzgün metodu.

Bu siyasət siyasətə əməl edilmədikdə baş vurulan intizam hərəkətlərini də göstərməlidir.

2.8. Kompyuter təhlükəsizliyi hadisələrinin və insidentlərinin tərifi **(Məcburi)**

Bildirişi qiymətləndirmək üçün müəyyən kriteriya olmalıdır ki, onun insident olub-olmadığı və kateqoriyası müəyyən edilsin. Bu kriteriya CSIRT-in kliyenturası çərçivəsində kompyuter təhlükəsizliyi insidentinin tərif edilməsinə əsaslanır. Bu tərifdən istifadə edərək insidentlərin müxtəlif kateqoriyaları müəyyən edilməlidir. İnsidentlərin korrelyasiyası və kombinasiyası üçün metodlar və kriteriyalar da müəyyən edilməlidir.

2.9. İnsidentlərin emalı siyasəti **(Məcburi)**

İnsident bildirişi insident emalında yalnız birinci addımdır. Mərkəzi bildiriş nöqtəsi heç də həmişə insidenti tədqiq edən və cavablandırılan həmin qrup deyil. İnsidentin emalı siyasəti kimin hansı növ kompyuter təhlükəsizliyi insidentin emalı üçün məsul olduğunu və cavabın gerçəkləşdirilməsi üçün digər sahələrdən kimlərin köməyə cəlb oluna biləcəyini müəyyən etməlidir.

2.10. Digər komandalarla kooperasiya **(Məcburi)**

Bu siyasət digər komandalarla formal və qeyri-formal əməkdaşlığa qoşulmaq üçün CSIRT tərəfindən izlənən prosesi müəyyən etməlidir. Hansı növ razılaşmaların, NDA (Non Disclosure Agreement, açıqlamama haqqında müqavilə) və SLA (Service Level Agreement, servis səviyyəsi barədə razılaşma) tələb olunduğunu və hansı növ informasiyanın mübadilə edilə bilməsini təsvir etməlidir. Bu siyasət informasiyanın yayılması siyasətini dəstəkləməli və hansı növ informasiyanın digər komandalarla paylaşıla bilməsini təsvir etməlidir.

2.11. Digər siyasətlər

CSIRT-in yaratdığı və ya baş/sahib təşkilatın müəyyən etdiyi, CSIRT-in əməliyyatlarına və ya onun FIRST üzvlüyünə təsir edən istənilən digər siyasət təhlil edilməlidir.

3. İş yeri və mühit

Öz işini effektiv yerinə yetirməsi üçün komanda müvafiq infrastruktura malik olmalıdır.

CSIRT-in iş yeri, mühiti və infrastrukturuna daxildir:

fiziki yerləşmə və CSIRT heyəti və verilənlərin təhlükəsizliyi;

heyətin ofis və ev avadanlığı;

CSIRT şəbəkələri, routerlər, şəbəkə ekranları və IDS-lər kimi daxili/xarici mühafizələr:

- insidentlərin emalını və göstərilən digər servisləri dəstəkləmək üçün CSIRT və tətbiqi proqramları;
- CSIRT və insident informasiyasını saxlamaq üçün verilənlər bazaları, verilənlər repozitariləri, verilənlərin analizi alətləri;
- təhlükəsiz e-poçt və səs kommunikasiyaları üçün mexanizmlər və ya tətbiqi proqramlar.

Komandanın fəaliyyət göstərdiyi otaqlar minimal təhlükəsizlik tələblərinə cavab verməlidir ki, informasiya adekvat qorunsun. Komandanın heyəti müəyyən səviyyədə məxfiliyə malik olmalıdır ki, komanda üzvü olmayan əməkdaşlar və ya təşkilatın qonaqları onların bilməli olmadıqları informasiyanı asanlıqla öyrənə bilməsinlər.

Əgər komanda səpələnibsə, bütün yerləşmə yerlərində eyni məxfilik və mühafizə səviyyəsi təmin edilməlidir. Lokal şəraitdən asılı olaraq dəyişikliklər ola bilər. Məsələn, qonaqları yerlə təmin etməyən ofislər qonaqlarla davranışa aid bəzi tələblərə baxmaya bilər.

3.1 Fiziki təhlükəsizlik **(Məcburi)**

Fiziki təhlükəsizlik digərləri ilə yanaşı, aşağıdakı məsələləri də əhatə edir:

- qonaqların yerləşdirilməsi siyasəti;
- komanda danışıqlarına qulaq asılması (telefon və ya başqa);
- komanda otaqlarına və avadanlıqlarına giriş (fiziki və ya başqa);
- komandanın sənədlər arxivinə giriş (kağız və elektron);

Fiziki təhlükəsizlik tələblərinə aiddir:

- CSIRT serverlərinin və verilənlər repozitarilərinin yerləşdirilməsi üçün təhlükəsiz otaqlar və ya təhlükəsizlik əməliyyatları mərkəzi (Security Operations Center, SOC);
- CSIRT fəaliyyətinin müzakirəsi və təhqiqatlar üçün təhlükəsiz və səs keçirməyən otaqlar;

- qeyri-elektron verilənlərin və yazıların saxlanılması üçün seyf;
- təhlükəsiz kommunikasiya mexanizmləri;
- CSIRT heyətinin təşkilatın digər hissələrindən fiziki ayrılması, müəyyən növ giriş kartları daxil olmaqla.

3.2 Avadanlıq

Kompyuterlər **(Məcburi)**

Gündəlik işlərini həyata keçirmək üçün komanda kompyuterlərə malik olmalıdır.

Telefonlar **(Məcburi)**

Faks

Şrederlər və digər məhvetmə mexanizmləri **(Məcburi)**

Ən azı kağız şredderlərinin olması tələb edilir.

3.3. Saxlanc **(Məcburi)**

Hər komandanın saxlanılan materialları olacaq. Materiallara kağızlar, kitablar, CD-lər, sərt disklər, kompyuterlər və digər avadanlıqlar aid ola bilər. Saxlanan materiallar təsnifatına (kitablar komanda daxilində ortaqdır, əksinə təhqiqat məlumatları konfidensialdır) və məqsədinə (məhv edilməyi gözləyən, istifadə edilməyən materiallar, yalnız indi istifadə edilməyən materiallar) görə fərqlənə bilərlər.

3.4. İnsidentin izlənməsi **(Məcburi)**

Bütün hadisələr və insidentlər izlənməlidir. Onlar mürəkkəb verilənlər bazasında, kağız jurnalda və ya fayl sistemində fayl kimi saxlana bilər. Böyük sayda insidentlər gözlənilirsə, sistem miqyaslanan olmalıdır. İzləmə sisteminə digər tələb icazəsiz girişdən mühafizə mexanizmlərinin olmasıdır. Onun audit imkanları da olmalıdır ki, ən azı, onu kimin və nə vaxt istifadə etdiyini müəyyən etmək olsun.

3.5. Şəbəkə infrastrukturu

Ayrı CSIRT lokal şəbəkəsi **(Məcburi deyil, lakin tövsiyə edilir)**

Komandanın lokal şəbəkəsi təşkilatın şəbəkəsindən ayrılmalıdır. Məqsəd komandanın trafikinə qulaq asılması risqini azaltmaqdır. Şəbəkənin ayrılması fiziki (üstünlük verilir) və ya məntiqi ola bilər. Fiziki ayrılma komandanın şəbəkəsi ilə təşkilatın qalan şəbəkəsi arasında ayırıcı qurğu cəlb etməlidir (məsələn, marşrutizator və ya şəbəkə ekranı). İdealda, komanda İnternetə məxsusi çıxışa da malik olmalıdır. Məntiqi ayrılma (məsələn, VLAN) komandanın şəbəkəsində əhəmiyyətli hadisələrin monitorinqi zamanı sayıqlığı artırmaqla kompensasiya edilməlidir.

Test şəbəkəsi **(Məcburi)**

Test şəbəkəsi naməlum proqram təminatını test etmək üçün vacibdir. Test istehsalat şəbəkəsində edilməməlidir. İstehsalat maşınlarının, hətta VMware kimi virtual maşınların belə test üçün istifadəsi tövsiyə edilmir.

İdealda, test şəbəkəsi istənilən digər mövcud şəbəkədən ayrılmalıdır. Onun İnternetə öz çıxışı da ola bilər.

İstənilən ziyankar və digər proqramın CSIRT sistemlərində test edilməsi zamanı CSIRT heyəti üçün tələbləri bəyan edən siyasət olmalıdır. Bu siyasət proqram təminatının və ziyankar proqramların harada və necə test edilməsini müəyyən etməlidir.

İnfrastrukturda əməliyyatlar **(Məcburi)**

Komandanın şəbəkə infrastrukturunu kimin istismar etdiyi müəyyən edilməlidir. Bu belə məsələləri əhatə etməlidir: DNS, poçt infrastrukturu, FTP və veb server, kompyuterlər, verilənlərin arxiv kopyaları və arxiv daşıyıcılarının idarə edilməsi. Bu siyahı tam deyil. Məqsəd icazəsiz informasiya sızmasının baş verə biləcəyi mümkün zəif nöqtələri identifikasiya etməkdir.

Əgər risk yolverilən dən yüksəkdirsə, komanda təsiri azaltmaq üçün müvafiq tədbirlər işləməli və tətbiq etməlidir. "Sayt ziyarəti"ni həyata keçirən komanda bütün təhlükəsizlik tələblərinin qarşılandığına əmin olmaq üçün infrastruktur provayderi ilə söhbət apara bilər.

Təhlükəsiz kommunikasiyadan istifadə **(Məcburi)**

Komanda təhlükəsiz kommunikasiyaların istifadəsi və ya faylların təhlükəsiz qaydada saxlanılması, arxivləşdirilməsi üçün tələblərə malik ola bilər. "Sayt ziyarəti"ni həyata keçirən şəxslər komanda daxilində hansı növ təhlükəsiz kommunikasiyanın istifadə edilməsini təhlil etməlidir.

3.6. PGP-nin istifadəsi **(Məcburi)**

FIRST icmasında kommunikasiya üçün PGP və GPG istifadə edilir, buna görə də, "Sayt ziyarətini" həyata keçirən şəxslər komanda mühitində PGP-nin necə istifadə edildiyini təhlil etməlidir.

FIRST üzvü olması üçün CSIRT PGP şifrələnməsini təmin və istifadə etməlidir.

Şifrələmə açarları ondan istifadə edəcək bütün tərəflərə paylanmalıdır. Paylanma metodu açıq açar repozitarisində yerləşdirmək (məsələn, PGP keyserver), veb-saytda yerləşdirmək və ya CD, smart-kartda göndərmək ola bilər. "Sayt ziyarəti"ni həyata keçirən şəxslər şifrləmə açarının işlənməsini yoxlaya bilər.

4. İnsidentin emalı

Bu bölmədə CSIRT-in insidentləri emal etmək üçün istifadə etdiyi metodlara, proseslərə və texnologiyalara tələblər nəzərdən keçirilir.

Bu bölmənin məqsədi CSIRT verilənlərini mühafizə etməyə və səmərəli insident emalına imkan verən formal prosedurların yerində olmasına əmin olmaqdır.

4.1. İnsident barədə necə xəbər verilir **(Məcburi)**

Kompyuter təhlükəsizliyi hadisələrini emal etmək üçün komanda hadisələr və insidentlər barəsində xəbər tutmaq metoduna malik olmalıdır. Kliyenturanın sual vermək, hadisə və insident barəsində xəbər vermək, əks-əlaqə və tövsiyələr almaq üçün komanda ilə kommunikasiya yolları olmalıdır. Ən geniş yayılan yollar: e-poçt, telefon və faksdır. Üstünlük verilən kommunikasiya kanalı yoxdur, onlardan istənilənı istifadə edilə bilər. Əsas məsələ ondadır ki, kanal komanda üçün əlverişli olsun (komandanın əməliyyat mühiti və kliyentura nəzərə alınmaqla). Kliyentura bunun nə olduğunu və necə istifadə edildiyini bilir. Bunlar İnsident Bildirişi qaydalarında (İncident Reporting Guidelines) sənədləşdirilməlidir.

İnsident Bildirişi qaydaları kliyentura üçün yazılır və bildirilməli olan insidentlərin növlərini və onların hansı qaydada bildirilməsini təsvir edir.

4.2. İnsidentin emalı prosesi **(Məcburi)**

"Sayt ziyarəti"ni həyata keçirən şəxslər komandanın hansı proseslərlə kompyuter təhlükəsizliyi insidentlərini qəbul etdiyini və cavablandırdığını yoxlamalıdır.

Bu insidentlərin necə:

Təyin edildiyini
Eskalasiya edildiyini
Bağlandığını
Dərs çıxarmaq üçün təhlil edildiyini

əhatə etməlidir.

4.3. Bildirişin alınmasının təsdiqlənməsi **(Məcburi deyil, lakin tövsiyə edilir)**

Komandanın bildirişləri necə təsdiqlədiyi komanda ilə onun kliyenturası arasında SLA razılaşmasında müəyyən edilməlidir. Qəbul edilmiş hər bir insident bildirişinə müəyyən formada təsdiqin verilməsi tövsiyə olunur. Təsdiq

şəxs tərəfindən və ya avtomatik mexanizm tərəfindən edilə bilər.

5. Əlaqə məlumatı və informasiyanın yayılması

5.1. Daxili yoxsa xarici **(Məcburi)**

Kliyentura CSIRT-lə necə təmas yaratmağı və qarşılıqlı əlaqədə olmağı bilməlidir. Bunun üçün komandanın əlaqə məlumatları müvafiq qaydada daxili və xarici istifadəçilərə elan edilməlidir. Onlar eyni qayda ilə edilə bilər, lakin bu məcburi deyil. Bəzi hallarda komanda xaricə elan edilməyi istəməyə bilər.

6. Peşəkar inkişaf

6.1 Treninq **(Məcburi)**

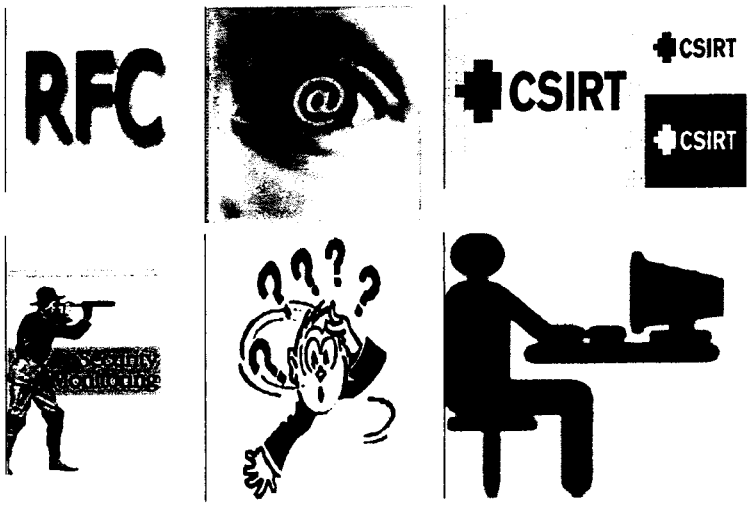
İnsidentin menecmenti dinamik sahədir. Effektiv komanda olmaq üçün üzvlər daim yeni biliklər qazanmalıdır.

Treninq planına malik olmaq yetərli deyil. İnsanlara təlim və öyrənmək üçün vaxt vermək lazımdır.

6.2 Konfranslar

Konfranslarda iştirak edilməsi yeni biliklər əldə etmək və başqa komandalarla və şəbəkələrlə əlaqə yaratmaq üçün çox vacibdir. Komandaların konfranslarda iştirak etmiş üzvlərə malik olması həvəsləndirilir.

(Məcburi) Fəal komanda hesab edilməsi üçün komandadan kimsə ən azı bir CSIRT-lə bağlı hadisə və ya konfransda iştirak etməlidir.



FƏSİL 7

RFC 2350

RFC 2350

- **Sənəd haqqında məlumat**
- **Əlaqə məlumatları**
- **Nizamnamə**
- **Qaydalar**
- **Xidmətlər**
- **Bildiriş formaları**
- **İmtinalar**

FƏSİL 7 RFC 2350

RFC 2350 hazırda CSIRT-lərin vəzifələrinə, xidmətlərinə, qarşılıqlı əlaqə üsullarına və s. tələblərin təsvir olunduğu əsas RFC (Request for Comments, müzakirə üçün sorğu) sənəddir.

RFC 2350 sənədi aşağıdakı bölmələrdən ibarətdir:

1. Sənəd haqqında məlumat
2. Əlaqə məlumatları
3. Nizamnamə
4. Qaydalar
5. Xidmətlər
6. İnsident barədə bildiriş forması
7. İmtinalar

Aşağıda bu bölmələrin məzmunu barəsində qısa məlumat verilir.

7.1. Sənəd haqqında məlumat

İstənilən sənəd onu identifikasiya edən məlumatlardan başlamalıdır, baxılan halda bu məlumatlar xüsusi tələblərdən ibarətdir:

Komandanın iş təfərrüatları zaman keçdikcə dəyişir, buna görə RFC 2350-də son dəyişikliyin tarixi göstərilməlidir. Bundan başqa, sonrakı dəyişikliklər haqqında informasiyanın necə əldə edilməsi də məlum olmalıdır.

- son dəyişiklik tarixi; məlumatların aktuallığını yoxlamaq üçün zəruridir, çünki komandanın işinin detalları zaman keçdikcə dəyişir;
- göndəriş siyahısı; Komandanın kliyentləri komandanın detallarında dəyişikliklər barədə vaxtında məlumatlandırılmalıdır. Poçt siyahıları – yenilənmələrin çox sayda istifadəçilər arasında yayılması üçün rahat vasitədir, adətən, bu siyahılarda cavablandırma komandasının fəal

qarşılıqlı əlaqədə olan kollektivlər sadalanır. Dəyişikliklər barəsində məlumatlar komandanın elektron imzası ilə təsdiqlənməlidir.

– sənədin yerləşdimə yeri. Sənədin cari versiyası komandanın operativ informasiya xidmətləri çərçivəsində əlyetən olmalıdır. Bu halda istifadəçilər komanda haqqında asanlıqla əlavə məlumatlar ala, son dəyişiklikləri analiz edə bilərlər. Sənədin bu versiyası da elektron imza ilə təsdiqlənməlidir.

7.2. Əlaqə məlumatları

Bu bölmədə ətraflı əlaqə məlumatı göstərilməlidir, məlumatın xarakteri müxtəlif komandalar üçün çox fərqli ola bilər. Məsələn, komanda üzvlərinin adları açıqlanmaya bilər. Aşağıda yalnız lazım olduqda izahatlar verilir.

- komandanın adı;
- poçt ünvanı;
- saat qurşağı; Bu məlumat bir neçə saat qurşağına toxunan insidentin emalı zamanı faydalıdır.
- telefon nömrəsi;
- digər əlaqə üsulları (məsələn, qapalı telefon şəbəkəsində nömrə);
- elektron poçt ünvanı;
- açıq açarlar və şifrələmə üsulları; Konkret mexanizmlərin istifadəsi əlaqə saxlayan tərəfdə müvafiq proqramların açarların və s. olmasından asılıdır. Belə məlumatın göstərilməsi istifadəçilərə imkan verir ki, komanda ilə təhlükəsiz əlaqənin necə qurulmasını müəyyən edə bilsinlər.
- komandanın üzvləri;
- iş saatları; İş saatları və istirahət günlərinin qrafiki gösərilməlidir.
- digər əlaqə məlumatları; Daim işlək "qaynar xətt" mövcuddurmu? Xüsusi istifadəçilər üçün hər hansı əlaqə məlumatı mövcuddurmu?

Daha ətraflı əlaqə təqdim edilə bilər, məsələn, müxtəlif xidmətlər üçün müxtəlif əlaqə üsulları, operativ məlumat xidmətlərinin siyahısı və s. Əgər bəzi xidmətlərə (məsələn, poçt siyahısına müraciət üçün ünvanlar) giriş üçün xüsusi prosedurlar mövcuddursa, onlar bu bölmədə izah edilməlidirlər.

7.3. Nizamnamə

Hər bir cavablandırma komandası nizamnaməyə malik olmalıdır, nizamnamə komandanın nə etdiyini və nəyin əsasında etdiyini müəyyən edir. Nizamnamədə ən azı aşağıdakılar olmalıdır:

- missiya;
- kliyentlər;
- sponsorlar və yuxarı təşkilatlar;
- səlahiyyətlər.

7.3.1. Missiya

Bu bölmədə komandanın məqsədləri və vəzifələri, komanda tərəfindən müəyyən edilmiş əsas fəaliyyət növləri göstərilir. Komandanın insidentləri cavablandırma komandası sayıla bilməsi üçün o, insidentlər haqqında hesabatları dəstəkləməli, insidentlər haqqında hesabatları dəstəkləməli və insidentlərin araşdırılmasında istifadəçilərə kömək etməlidir.

Missiya qeyri-müəyyən olmamalıdır, məqsədlər aydın və anlaşıqlı ifadə edilməlidir. Missiya 3-4 cümlə ilə təsvir edilməli, rəhbərlik və maraqlı tərəflər (informasiya təhlükəsizliyi, İT-şöbə və s.) tərəfindən dəstəklənməlidir.

Missiyaya aid misallar. JA.NET CSIRT-in missiyası

- JA.NET-in və onun kliyentlərinin hal-hazırda və gələcəkdə təhlükəsizliyini və
- JA.NET-in informasiya təhlükəsizliyi siyasətinin həyata keçirilməsində təşəbbüsü öz üzərinə götürmək;
- cavablandırmanı koordinasiya etmək;
- informasiya təhlükəsizliyi resurslarını hazırlamaq;
- yüksək kvalifikasiyanın himayə edilməsi hesabına təmin etmək.

Bu missiyanın dəstəklənməsi üçün biz insidentlərin idarə edilməsinin koordinasiyasını, JA.NET kliyentləri üçün təlim və məsləhət, JA.NET-çərçivəsindən kənar müvafiq təşkilatlarda əməkdaşlığı təklif edirik.

7.3.2. Kliyentlər

Cavablandırma komandasının kliyentləri (istifadəçilər, qəyyum icmalar) bir neçə üsulla müəyyən edilə bilər. Məsələn, onlar müəyyən təşkilatın əməkdaşları və ya pullu abunəçilər ola bilərlər. Texniki terminlərlə də müəyyən etmək olar, məsələn, konkret əməliyyat sisteminin istifadəçiləri.

Kliyentlərin müəyyən edilməsi komandanın öz xidmətlərini göstərəcəyi çərçivəni verə bilər. Qaydalar bölməsində kənardan daxil olan sorğuların necə emal edilməsi izah edilməlidir.

Əgər komanda öz istifadəçilərini açıqlamaq istəmirsə, belə qərarın səbəbini izah etməlidir. Məsələn, kommunikasiya komandaları öz kliyentlərini sadalamırlar, lakin göstərirlər ki, onlar böyük istifadəçi qruplarına xidmətlər göstərirlər, onların adlarının müqavilənin şərtlərinə görə göstərilmədiyini deyirlər.

İstifadəçi icmaları kəsişə bilərlər. Məsələn, Internet-provayder istehlakçılarına cavablandırma xidməti göstərə bilər, istehlakçıların öz cavablandırma komandaları ola bilər. "Səlahiyyətlər" bölməsində belə qarşılıqlı əlaqələri izah etmək lazımdır.

7.3.3. Sponsor-təşkilatlar və yuxarı təşkilatlar

Bu bölmədə komandaya səlahiyyətlər verən təşkilatlar göstərilir. Bu məlumatlar komandanın "köklərini", "krışasını" və imkanlarını aydınlaşdırmağa imkan verir, bu isə kliyentlərlə inam münasibətlərinin yaradılması üçün zəruridir.

7.3.4. Səlahiyyətlər

Bu bölmə komandanın istifadəçilərlə qarşılıqlı münasibətlərinə əsaslanmış spesifikasiyasından əhəmiyyətli dərəcədə asılıdır. Məsələn, korporativ komandanın səlahiyyətlərini rəhbərlik müəyyən edir, ictimai komanda özünü idarəetmə əsasları ilə seçilə və məsləhətçi rolu oynaya bilər və s.

Komanda nəzarət edilən perimetr çərçivəsində bütün sistemlərin işinə qarışmaq səlahiyyətinə malik ola və ya olmaya bilər. Başqa sözlə idarəetmə oblastı ümumi halda istifadəçilər dairəsindən fərqlənir. Digər hallarda idarəetmə oblastı iyerarxik qurula bilər, bu halda həmin fakt tabe komandalar göstərməklə təsbit edilməlidir.

Səlahiyyətlərin təsviri komandanı məhkəmə iddiaları üçün həssas edə bilər, buna görə bu məsələdə hüquqşünasların köməyinə arxalanılmalıdır (hüquqi aspektlərə daha ətraflı baxıldığı 7.7 bəndində də baxmalı).

CSIRT-in səlahiyyətləri (hakimiyyəti) aşağıdakı kimi müəyyən edilə bilər:

Tam – CSIRT-in öz kliyentlərinin adından qərar qəbul etmək və istənilən hərəkətləri həyata keçirmək üçün bütün səlahiyyətləri var.

Qismən – CSIRT öz kliyentlərinə dəstəyi təmin edir və birlikdə qərar qəbul edirlər (tövsiyə edirlər, diqtə edə bilməzlər).

Yoxdur – CSIRT-in heç bir səlahiyyəti yoxdur və yalnız məsləhətçi kimi çıxış edir.

Dolayı – CSIRT öz kliynetlərinin qərar qəbul etməsinə dolayı təsir edir (məsələn, təşkilat öz filiallarına və ya rabitə operatoru öz kliyentlərinə təsir edir).

7.4. Qaydalar

Cavablandırma komandasının öz qaydalarını müəyyən etməsi çox vacibdir. Növbəti bənddə bu qaydaların istifadəçilərə çatdırılması müzəkirə edilir.

7.4.1 İnsidentlərin növləri və dəstək səviyyəsi

Bu bölmədə komandanın cavab vermək imkanı olduğu insidentlərin növləri və hər növ insident üçün göstərilən dəstəyin səviyyəsi sadalanmalıdır.

"Xidmətlər" bölməsində daha ətraflı təsvir olunur, həmçinin insidentlərə birbaşa dəxli olmayan mövzulara toxunulur.

İstifadəçilərə dəstəyin səviyyəsi bir çox faktordan asılı olaraq dəyişə bilər, onlar təsvir və izah edilməlidirlər.

Dəstəyin səviyyəsi komandanın yükündən və əlyetən informasiyasının tamlığı kimi faktorlardan asılı olaraq dəyişə bilər. Belə faktorlar təsvir olunmalı, onların təsiri isə izah edilməlidir. İnsidentlərin məlum növlərinin siyahısı bütün mümkün və ya gələcək insidentləri əhatə edə bilməz, buna görə "digər" insidentlər üçün dəstək təsvir edilməlidir.

Gələcək insidentləri mümkün edən boşluqlar haqqında əldə edilən informasiya əsasında komandanın hərəkət edib-etməyəcəyini müəyyən etmək lazımdır. Öz istifadəçilərinin maraqlarına görə belə informasiyanı nəzərə almağa razılıq cavablandırma komandasının məcburi xidməti yox, əlavə profilaktika xidməti hesab edilir.

7.4.2. Əməkdaşlıq, qarşılıqlı əlaqə və informasiyanın açıqlanması

Bu bölmədə hansı oxşar komandalarla əlaqənin sahmana salındığı izah edilməlidir. Belə qarşılıqlı əlaqənin insidentləri cavablandırma çərçivəsində baş verməsi məcburi deyil, o, texniki məsələlərdə və xidmətlərdə əməkdaşlığın möhkəmləndirilməsinə yönəldilə bilər.

Əməkdaşlıq haqqında müqavilələrin detallarını da göstərmək lazım deyil; bölmənin əsas məqsədi ondan ibarətdir ki, qarşılıqlı əlaqənin mövcud növləri və onların məqsədləri haqqında istifadəçilərdə ümumi təsəvvür yaradılsın.

Komandalar arasında müəyyən razılaşmaların qəbul edilməsi komandalararası qarşılıqlı əlaqənin sadələşməsinə gətirib çıxarır.

Bildiriş və informasiyanın açıqlanması qaydaları izah etməlidir ki, kimlər və hansı hallarda komanda bildirişlərini ala bilərlər.

Onlarda göstərilməlidir ki, digər komandanın qüvvəsi ilə iş gözlənilirmi və ya məhz bu istifadəçiyə aid olan məsələlər üzrə digər imkanın üzvü ilə birbaşa qarşılıqlı əlaqə.

Qarşılıqlı əlaqə keçirilə bilən təşkilatlar aşağıda sadalanır.

7.4.2.1. Cavablandırma komandaları

Tez-tez başqa CERT komandaları ilə qarşılıqlı əlaqə zəruri olur. Məsələn, korporativ komanda insident barəsində komandaya bildirir, o da öz növbəsində bildirişi digər ölkələrə göndərir ki, geniş miqyaslı hücumun qurbanları olan bütün informasiya sistemləri əhatə olunsun.

Komandalar arasında olan əməkdaşlıq da informasiyanın açıqlanmasına səbəb ola bilər.

Aşağıda belə açıqlanma nümunələri göstərilir, aydındır ki, siyahı tamlığa iddia etmir;

- daxili insidentlər haqqında digər komandalara göndərilmiş bildirişlər. Bu zaman təşkilatın informasiya sistemi haqqında məlumatlar açıqlanmış ola bilər (o cümlədən, mətbuatda);
- haqqında kənardan bildirişlər daxil olmuş insidentlərin cavablandırılması (bu o deməkdir ki, informasiyanın sızması artıq baş vermişdir);
- fərz olunan və ya təsdiqlənmiş xarici insidentləri göstərən və nəzarət edilən sərhədlər çərçivəsindəki müşahidələr barəsində bildiriş;
- bildirişlər əsasında xarici insidentlər haqqında cavablandırma;
- boşluqlar barəsində məlumatların provayderlərə, tərəfdaş komandalara və ya bilavasitə əlaqədar olan və olmayan təşkilatlara göndərilməsi;
- insidentlər və boşluqlar haqqında məlumatlara cavab;

– istifadəçilər, digər icmaların üzvləri, digər komandalar, hüquq-mühafizə orqanları haqqında əlaqə məlumatlarının təqdim edilməsi.

7.4.2.2. Provayderlər

Bəzi provayderlərin öz cavablandırma komandaları var, bəzilərində isə yoxdur. Əgər provayderin öz komandası yoxdursa, komanda bilavasitə provayderlə işləməlidir ki, təkmilləşmə və dəyişikliklər təklif etsin, texniki problemi analiz etsin və ya təklif olunan həlləri testdən keçirsin. Əgər provayderin məhsulları insidentə cəlb edilibsə, bu provayder cavablandırmada xüsusi rol oynayır.

7.4.2.3. Hüquq-mühafizə orqanları

Cavablandırma komandaları və istifadəçilər qüvvədə olan qanunvericiliyə əməl etməlidir, qanunvericilik müxtəlif ölkələrdə əhəmiyyətli dərəcədə fərqlənə bilər. Cavablandırma komandası hücumun texniki detalları haqqında tövsiyələr verə bilər və ya insidentin hüquqi nəticələri haqqında məsləhət istəyə bilər. Qanunvericilikdə bildirişlərin təqdim olunması və konfidensiallığa əməl edilməsi haqqında spesifik tələblər ola bilər.

7.4.2.4. Mətbuat

Mətbuatdan vaxtaşırı məlumat və şərhlər barəsində xahişlər daxil ola bilər.

Mətbuata informasiyanın verilməsi haqqında aydın qaydalar çox faydalı ola bilərdi, xüsusilə istifadəçilərin gözləntilərinin aydınlaşdırılması baxımından. Bu qaydalar bütün sualları mümkün olduqca ətraflı izah etməlidir, çünki, adətən, istifadəçilər mətbuatla təmasları çox həssaslıqla qəbul edirlər.

7.4.2.5. Digərləri

Bu bölmədə tədqiqat işləri və ya sponsor-təşkilatların qarşılıqlı əlaqəsi barəsində söhbət gedə bilər.

Komandanın əldə etdiyi və informasiya təhlükəsizliyinə aid olan istənilən informasiyanın fərz olunan statusu "konfidensialdır", lakin bu müddəaya ciddi əməl edilməsi komandanı "qara deşiyə" çevirir, bu komandanın istifadəçilər və digər təşkilatlar kimi cəlbediciliyini azalda bilər. Hansı informasiyanın kimə və ya nə vaxt bildirildiyini müəyyən etmək vacibdir. Mümkündür ki, müxtəlif komandalar informasiyanı açıqlamağı tələb edən və ya məhdudlaşdıran müxtəlif qanunvericiliyin subyektləri olsun, bu, xüsusən, komandalar müxtəlif ölkələrdən olduqda belədir. Bundan başqa, komandalar sponsor təşkilatlar tərəfindən bildirişlərə qoyulan məhdudiyyətlərə də əsaslana bilərlər. Komanda haqqında məlumatlarda bütün bu məhdudiyyətlər müəyyən edilməlidir ki, istifadəçilər və digər komandalar üçün vəziyyət aydın olsun.

İnformasiyanın açıqlanmasına maraqların münaqişəsi də mane ola bilər, xüsusilə də kommersiya; biz belə növ münaqişələrin həlli üzrə tövsiyələr vermirik.

Adətən komandalarda statistik məlumatlar toplanır. Əgər belə məlumat açıqlanırsa, onda bildirişlər və məlumatların açıqlanması siyasətində bu açıq şəkildə qeyd edilməlidir, həmçinin bu statistik məlumatları necə əldə etməyin yolları da.

7.4.3. Kommunikasiya və autentifikasiya

Kommunikasiyaların təhlükəsizliyi metodlarını müəyyən edən siyasət olmalıdır. Bu həm komandalar, həm də komandalarla istifadəçi arasındakı qarşılıqlı əlaqə üçün zəruridir. RFC 2350 sənədində açıq açarlar və onlara istinadlar, açarların heş-kodları göstərilməli və autentikliyi yoxlamaq üçün bu informasiyadan necə istifadə edilməsi və zədələnmiş informasiya ilə nə etmək lazım olduğu (məsələn, zədələnmə barədə hara müraciət etmək) göstərilməlidir.

Hazırda hər bir komandanın ən azı PGP açarına (əgər mümkündürsə) malik olması tövsiyə olunur. Əgər komandaya və istifadəçilərə kömək edirsə, digər mexanizmlər də istifadə edilə bilər (məsələn, PEM, MOSS, S/MIME). Lakin qeyd etmək lazımdır ki, komandalar və istifadəçilər qanunvericiliyə əməl etməlidirlər. Bəzi ölkələrdə güclü kriptoqrafiya qadağan olunur, yaxud kriptoqrafik texnologiyaların istifadəsinə xüsusi məhdudiyyətlər vardır. Kritik informasiyanın şifrlənməsinə əlavə olaraq onu rəqəmsal imza ilə də təchiz etmək lazımdır (Qeyd edək ki, ölkələrin əksəriyyətində rəqəmsal imza ilə məlumatların autentikliyinin təmin olunması kriptoqrafiya üzrə qadağanların təsirinə düşmür.

Əgər əlaqə telefon və faksla həyata keçirilirsə, potensial tərəfdaşlarla əvvəlcədən gizli autenti verilənləri, məsələn, parol sözləri və ya fazaları əvvəlcədən razılaşdırıla bilər. Aydındır ki, bu gizli məlumatlar açıqlanmalı deyil, lakin onların mövcudluğunu açıqlamaq olar.

7.5. Servislər

Cavablandırma komandasının göstərdiyi xidmətləri təxmini olaraq iki kateqoriyaya bölmək olar: real vaxt ərzində göstərilən xidmətlər – bilavasitə əsas vəzifə insidentlərin cavablandırılması ilə əlaqədar; köməkçi rol oynayır və real vaxt ərzində göstərilməyən profilaktika xidmətləri. İkinci kateqoriya və birincinin bir hissəsi o mənada əlavə hesab edilirlər ki, onları cavablandırma komandalarının hamısı göstərmir.

7.5.1. İnsidentlərin cavablandırılması

İnsidentlərin cavablandırılmasına, adətən, daxil olan bildirişlərin qiymətləndirilməsi ("insidentlərin klassifikasiyası") və daxil olan informasiya üzərində digər komandalarla, İnternet-provayderlər və digər təşkilatlarla birgə iş aid edilir ("cavablandırmanın əlaqələndirilməsi"). Xidmətlərin üçüncü qrupu, insidentdən sonra normal işin bərpa edilməsində lokal istifadəçilərə kömək ("problemlərin həlli") kimi əlavə

xidmətlərdən ibarət olur, onu yalnız müəyyən komandalar göstərir.

Profilaktika hərəkətlərinə daxildir:

- informasiya paylaşımı. Bu ad altında məlum boşluqlar, yamaqlar, keçmiş problemlərin həlli üsulları üzrə arxivlərin dəstəklənməsi və ya tövsiyə məqsədləri üçün göndəriş siyahılarının təşkili başa düşülür;
- təhlükəsizlik vasitələrinin verilməsi (məsələn, audit vasitələrinin);
- kadrların təlimi və hazırlanması;
- məhsulların qiymətləndirilməsi;
- təşkilatın təhlükəsizliyinin qiymətləndirilməsi, məsləhət xidmətləri.

7.5.1.1. İnsidentlərin təsnifatı

İnsidentlərin təsnifatına, adətən, aşağıdakı əməllər daxildir:

- *Bildirişlərin qiymətləndirilməsi.* Daxil olan informasiya yozumlanır, təsnif olunur vaciblik dərəcəsinə görə, davam edən hadisələrlə və aşkarlanmış meyillərlə qarşılaşdırılır.
- *Verifikasiya.* İnsidentin həqiqətən olub-olmaması və onun miqyasları müəyyən edilir.

7.5.1.2. Cavablandırmanın koordinasiyası

Cavablandırmanın koordinasiyası dedikdə, adətən, aşağıdakılar başa düşülür:

- *İnformasiyanın kateqoriyalaşdırılması.* İnsidentə aid olan informasiya (qeydiyyat jurnalları, əlaqə məlumatları və s.) məlumatın açıqlanması siyasətinə uyğun olaraq kateqoriyalara bölünür.
- *Koordinasiya.* İnformasiyanın açıqlanması siyasətinə uyğun olaraq digər tərəflərə insident haqqında məlumat verilir.

7.5.1.3. Problemlərin həlli

Adətən əlavə olan, problemlərin həlli üzrə xidmətlərə aşağıdakılar daxildir:

- Texniki dəstək (məsələn, "sındırılmış" sistemlərin analizi).
- Problemlərin aradan qaldırılması. İnsidentlərin səbəblərinin (istifadə edilmiş boşluqların) və onların nəticələrinin (məsələn, pozucu istifadəçinin seansının kəsilməsi) aradan qaldırılması.
- Bərpaetmə. Sistem və xidmətlərin təhlükəsizliyin pozulmasına qədər olan vəziyyətə qaytarılmasında kömək.

7.5.2. Profilaktika hərəkətləri

Adətən bu hərəkətlər əlavə hesab olunur. Onlara daxildir:

- İnformasiya verilməsi. Bura məlum boşluqların bazasının aparılması, yamaqların, keçmiş problemlərin həlli üsullarının və ya tövsiyə məqsədləri ilə göndəriş siyahılarının təşkili.
- Təhlükəsizlik vasitələrinin (məsələn, audit vasitələrinin) təqdim olunması.
- Məhsulların qiymətləndirilməsi
- Təşkilatın təhlükəsizliyinin qiymətləndirilməsi, konsaltinq xidmətləri.

7.6. Bildiriş formaları

İnsident barəsində məlumat vermək üçün bildiriş formalarının istifadə edilməsi həm istifadəçilərin, həm də cavablandırma komandalarının işini asanlaşdırır. İstifadəçilər bəzi vacib suallara əvvəlcədən, sakit şəraitdə cavab hazırlaya bilərlər. Komanda isə dərhal – ilk məlumatda bütün informasiyanı əldə edər ki, bu da səmərəli cavablandırma üçün zəmin hazırlayır.

Konkret komandanın məqsədlərindən və xidmətlər toplusundan asılı olaraq bir neçə forma istifadə edilə bilər. Məsələn, yeni boşluq barəsində məlumat üçün forma insident barəsində bildiriş formasından əhəmiyyətli dərəcədə fərqlənə bilər.

Daha yaxşı olardı ki, formalar CSIRT komandasının onlayn informasiya xidmətləri çərçivəsində təqdim edilsin. İstifadə qaydalarının təsviri və formalarla iş üzrə rəhbərliklə birlikdə formalara dəqiq istinadlar komandanı təsvir edən sənədlərdə göstərilməlidir. Əgər "forma üzrə bildirişlər" üçün ayrıca e-poçt ünvanları dəstəklənirsə, onları da göstərmək lazımdır.

Belə formalardan biri CERT/CC koordinasiya mərkəzinin insidentlər barəsində bildiriş formasıdır: ftp://info.cert.org/incident_reporting_form.

7.7. İmtinalar

İmtinalar cavablandırma komandalarını təsvir edən sənədlərin saziş olmamasına baxmayaraq, xidmətlərin və məqsədlərin təsvirlərindən sonradan məhkəmə sanksiyalarının mümkünlüyü meydana çıxa bilər. Buna görə də RFC 2350 sənədinin sonluğunda istifadəçilərə mümkün məhdudiyyətlər barəsində xəbərdarlıq edən müvafiq imtina (yazılı imtina) yerləşdirmək tövsiyə edilir.

Əgər RFC 2350 sənədinin orijinal versiyası başqa dilə tərcümə edilirsə, tərcümədə müvafiq imtina və orijinal istinad yerləşdirilməlidir.

"Bizim ilkin sənədi azərbaycan dilindən ingilis dilində diqqətlə tərcümə etməyə səy göstərdiyimizə baxmayaraq, biz əmin ola bilmərik ki, hər iki sənəd identik fikirləri eyni təfərrüat və korrektivlik səviyyəsində ifadə edir. İki versiya arasında fərq meydana çıxdığı bütün hallarda üstünlük azərbaycan dilindəki versiyaya verilir".

İmtinaların istifadə edilməsi və onun təmin etdiyi mühafizə qüvvədə olan qanunvericiliklə müəyyən edilir. Komanda qanunvericiliyi bilməlidir, şübhəli hallarda hüquqşünasla məsləhətləşmək tövsiyə olunur.

Əlavə 1. İxtisarlar

APCERT	Asia Pacific CERT Asiya-Sakit Okean CERT-i
BCP	Business Continuity Plan Fəaliyyətin fasiləsizliyi planı
CAIF	Common Advisory Interchange Format Təhlükəsizlik bülletenlərinin vahid mübadilə formatı
CERT	Computer Emergency Responce Team Kompyuter insidentlərini cavablandırma komandası
CERT/CC	CERT Coordinating Center CERT Əlaqələndirmə Mərkəzi
CIAC	Computer Incident Advisory Capability Kompyuter insidentləri üzrə məsləhət potensialı
CIIP	Critical Information Infrastructure Protection Kritik İnformasiya İnfrastrukturunun Mühafizəsi
CIRC	Computer Incident Response Capability Kompyuter insidentlərini cavablandırma potensialı
CIRT	Computer Incident Response Team Kompyuter insidentlərini cavablandırma komandası
CPNI	Centre for Protecting National Infrastructure (United Kingdom) Milli infrastrukturun mühafizəsi mərkəzi (Birləşmiş Krallıq)
CSIRC	Computer Security Incident Response Capability Kompyuter təhlükəsizliyi insidentlərini cavablandırma potensialı

CSIRT	Computer Security Incident Response Team Kompyuter təhlükəsizliyi insidentlərini cavablandırma komandası
CVE	Common Vulnerabilities and Exposures Boşluqların vahid tezaurusu
CVSS	Common Vulnerability Scoring System Boşluqların ümumi skorinq sistemi
DARPA	Defense Advanced Research Projects Agency Perspektiv Müdafiə Tədqiqat Layihələri Agentliyi
DDoS	Distributed Denial Of Service Paylanmış DoS
DHS	Department of Homeland Security Milli Təhlükəsizlik Nazirliyi
DLL	Dynamic Link Library Dinamik yüklənən kitabxana
DNS	Domain Name System Domen adları sistemi
DoS	Denial Of Service Xidmətdən imtina
DRDoS	Distributed Reflector Denial Of Service Paylanmış dolayı DoS
DRP	Disaster Recovery Planning Qəzasonrası bərpa planı
EGC	European Government CERTs Group Avropa Dövlət CERT-ləri Qrupu
EISPP	European Information Security Promotion Program Avropa İnformasiya Təhlükəsizliyi üzrə Maarifləndirmə Proqramı

ENISA	European Network and Information Security Agency Avropa Şəbəkə və İnformasiya Təhlükəsizliyi Agentliyi
ƏS	Əməliyyat Sistemi
FIRST	Forum of Incident Response and Security Teams İnsident Cavablandırma və Təhlükəsizlik Komandalarının Forumu
FTP	File Transfer Protocol Fayl ötürmə protokolu
HTTPS	Hypertext Transfer Protocol Secure Hipermətni təhlükəsiz ötürmə protokolu
XML	eXtended Markup Language Genişləndirilmiş nişanlama dili
ICMP	Internet Control Message Protocol İnternet idarəetmə məlumatları protokolu
IDMEF	Intrusion Detection Message Exchange Format Müdaxilələrin aşkarlanması məlumatlarını mübadilə formatı
IDS	Intrusion Detection System Müdaxilələrin aşkarlanması sistemi
IEC	International Electrotechnical Commission Beynəlxalq Elektrotexnika Komissiyası
IEEE	Institute of Electrical and Electronics Engineers Elektrotexnika və Elektronika Mühəndisləri İnstitutu
IETF	Internet Engineering Task Force İnternet standartları üzrə işçi qrupu
IHT	Incident Handling Team İnsident emalı komandası

IODEF	Incident Object Description and Exchange Format İnsident obyektlərinin təsviri və mübadiləsi formatı
IPS	Intrusion Prevention System Müdaxilələrin qarşısının alınması sistemi
IRC	Incident Response Center və ya Incident Response Capability İnsident Cavablandırma Mərkəzi
IRT	Incident Responce Team İnsidentləri cavablandırma komandası
ISO	International Organization for Standardization Beynəlxalq Standartlaşdırma Təşkilatı
ISP	Internet Service Provider İnternet xidmətləri provayderi
ITU	International Telecommunications Union Beynəlxalq Telekommunikasiya İttifaqı (BTİ)
ITU-T	ITU Telecommunication Standardization Sector BTİ Standartlaşdırma Sektoru
MIME	Multipurpose Internet Mail Extensions İnternet-poçtun çoxməqsədli genişlənməsi
MIT	Massachusetts Institute of Technology Massaçusets Texnologiya İnstitutu
MOSS	MIME Object Security Standard MIME obyektlərin təhlükəsizliyi standartı
NASA	National Aeronautics and Space Administration Aeronavtika və Kosmosun tədqiqatı üzrə Milli Agentlik

NCIRC	NATO Computer Incident Response Capability NATO Kompyuter İnsidentlərini Cavablandırma Potensialı
NIST	National Institute of Standards and Technology Milli Standartlar və Texnologiyalar İnstitutu
NSA	National Security Agency Milli Təhlükəsizlik Agentliyi
NVD	National Vulnerability Database Vahid boşluqlar bazası
PEM	Privacy Enhanced Mail Məxfiliyi gücləndirilmiş poçt
PGP	Pretty Good Privacy Yetərincə yaxşı məxfilik
RFC	Request for Comments Müzakirə üçün təkliflər (İnternet Texniki Spesifikasiyası)
S/MIME	Secure / Multipurpose Internet Mail Extensions Təhlükəsiz MIME
SCADA	Supervisory Control and Data Acquisition Dispetçer idarəetməsi və verilənlərin toplanması
SEI	Software Engineering Institute Proqram Mühəndisliyi İnstitutu
SERT	Security Emergency Response Team Təhlükəsizlik insidentlərini cavablandırma komandası
SIRT	Security Incident Response Team Təhlükəsizlik insidentlərini cavablandırma komandası
SLA	Service Level Agreement Xidmət səviyyəsi üzrə müqavilə

SMTP	Simple Mail Transfer Protocol Sadə poçt ötürmə protokolu
SOP	Standard Operating Procedure Standart istismar proseduru
SSH	Secure Shell Təhlükəsiz örtük (Shell)
TCP	Transmission Control Protocol Ötürməni idarəetmə protokolu
TERENA	Trans-European Research and Education Networking Association Trans-Avropa Elm və Təhsil Şəbəkələri Assosiasiyası
TF-CSIRT	Task Force CSIRT CSIRT işçi qrupu
TI	Trusted Introducer Etibarlı Təqdimatçı
TRANSITS	Training of Network Security Incident Teams Staff Şəbəkə təhlükəsizliyi insident komandalarının təlimi
UDP	User Datagram Protocol İstifadəçi deytaqram protokolu
VBİS	Verilənlər bazasını idarəetmə sistemi

Əlavə 2. Milli CSIRT-lər

Ölkə	CERT komandası	Veb-sayt
ABŞ	US-CERT	www.us-cert.gov
Almaniya	CERT-Bund	www.bsi.bund.de/certbund
Argentina	ArCERT	www.arcert.gov.ar
Avstraliya	AusCERT	www.aucert.org.au
Avstriya	CERT.at	www.cert.at
Böyük Britaniya	GovCertUK	www.govcertuk.gov.uk
Braziliya	CERT.br	www.cert.br
Bruney Darüssalam	BruCERT	www.brucert.org.bu
Çili	CLCERT	www.clcert.cl
Çin	CNCERT/CC	www.cert.org.cn
Danimarka	DK-CERT	www.cert.dk
Estoniya	CERT-EE	www.cert.ee
Filippin	PHCERT	www.phcert.org
Finlandiya	CERT-FI	www.cert.fi
Fransa	CERTA	www.certa.ssi.gouv.fr
Hindistan	CERT-In	www.cert-in.org.in
Honkonq	HKCERT	www.hkcert.org
İndoneziya	ID-CERT	www.cert.or.id
Pakistan	PakCERT	www.pakcert.org
İspaniya	IRIS-CERT	www.rediris.es/cert
İsveç	SITIC	www.sitic.se
İsveçrə	SWITCH CERT	www.switch.ch/cert
Kanada	CanCERT	http://www.cancert.ca/
Qətər	Q-CERT	www.qcert.org
Cənubi Koreya	KrCERT/CC	www.krcert.or.kr
Litva	LITNET CERT	cert.litnet.lt
Macarıstan	CERT-Hungary	www.cert-hungary.hu
Malayziya	MyCERT	www.mycert.org.my

Meksika	UNAM-CERT	www.cert.org.mx
Niderland	GOVCERT.NL	www.govcert.nl
Norveç	NorCERT	www.cert.no
Özbəkistan	UZ-CERT	www.cert.uz
Polşa	CERT Polska	www.cert.pl
Rusiya	CERT-RU	www.cert.ru
Səudiyyə Ərəbistanı	CERT-SA	www.cert.gov.sa
Sinqapur	SingCERT	www.singcert.org.sg
Sloveniya	SI-CERT	www.arnes.si/english/si-cert
Tayland	ThaiCERT	www.thaicert.nectec.or.th
Tunis	tunCERT	www.ansi.tn/en/about_cert-tcc.htm
Türkiyə	TR-CERT	http://www.bilgiguvenligi.gov.tr/certen/index.php
Ukrayna	CERT-UA	www.cert.gov.ua
Vyetnam	VNCERT	www.vncert.gov.vn
Yaponiya	JPCERT/CC	www.jpcert.or.jp
Yeni Zelandiya	CCIP (Centre for Critical Infrastructure Protection)	www.ccip.govt.nz

Əlavə 3. FIRST üzvlərinin siyahısı (mart, 2011-ci il)

Ölkə (CERT-lərin sayı)	**Ölkə (CERT-lərin sayı)**
Argentina (2)	Malayziya (2)
Avstraliya (3)	Meksika (1)
Avstriya (3)	Niderland (6)
Belçika (2)	Norveç (5)
Braziliya (2)	Oman (1)
Kanada (14)	Peru (2)
Çili (1)	Polşa (1)
Çin (3)	Qətər (1)
Taypey (2)	Rusiya Federasiyası (1)
Xorvatiya (2)	Sinqapur (4)
Danimarka (6)	Sloveniya (1)
Estoniya (2)	Cənubi Afrika Respublikası (1)
Avropa (1)	İspaniya (5)
Finlandiya (4)	Şri-Lanka (1)
Fransa (5)	İsveç (3)
Almaniya (17)	İsveçrə (5)
Yunanıstan (1)	Tayland (1)
Macarıstan (1)	Tunis (1)
Hindistan (1)	Ukrayna (1)
İsrail (2)	Birləşmiş Ərəb Əmirlikləri (2)
Yaponiya (18)	Birləşmiş Krallıq (18)
Cənubi Koreya (6)	ABŞ (60)
Latviya (1)	Uruqvay (1)
Litva (2)	Venesuela (1)

Əlavə 4. İnsident barəsində bildiriş forması

Xahiş olunur, bu formanı doldurub e-poçt və faksla göndərəsiniz.
**-la işarə edilmiş sətirlərin doldurulması məcburidir.*

Təşkilatın adı

1. Adı* :
2. Təşkilatın adı*:
3. Sektor:
4. Ölkə*:
5. Şəhər:
6. E-poçt ünvanı*
7. Telefon nömrəsi:
8. Digər:

Ziyan vurulmuş kompyuter(lər)

9. Kompyuterlərin sayı:
10. Host adı və IP*:
11. Kompyuterlərin funksiyalari*:
12. Saat qurşağı:
13. Avadanlıq (konfiqurasiya)
14. Əməliyyat sistemi:
15. Zədələnmiş proqram təminatı:
16. Zədələnmiş fayllar:
17. Təhlükəsizlik:
18. Host adı və IP:
19. Protokol/Port:

İnsident

20. İnsidentin nömrəsi
21. İnsidentin növü
22. İnsidentin başlanma vaxtı və metodu:
23. Daimi insidentdirmi: Hə/Yox
24. Aşkarlanma vaxtı və metodu:
25. Məlum boşluqlar:
26. Şübhəli fayllar:
27. Əks-tədbirlər:
28. Detallı təsvir*:

Ədəbiyyat

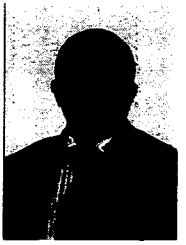
1. İmamverdiyev Y.N., Milli CERT yaradılmasına mərhələli yanaşma modeli // Riyaziyyatın tətbiqi məsələləri və yeni informasiya texnologiyaları. Respublika elmi konfransının materialları. – Sumqayıt, 26-27 noyabr, 2007, səh. 252-254.
2. İmamverdiyev Y.N., Həmzəyev R.F. AzScienceNet elm kompyuter şəbəkəsi üçün CERT-komandasının yaradılması (rus dilində) / İnformasiya cəmiyyəti problemləri, 2011, №1, səh. 15-26.
3. Əliquliyev R.M., Mahmudov R.Ş. İnternet mühitində intellektual mülkiyyət hüquqlarının qorunması məsələləri. Ekspress-İnformasiya. Bakı: İnformasiya Texnologiyaları. - 2010. - 60 s.
4. Браунли Н., Гатмэн Э. Как реагировать на нарушения информационной безопасности (RFC 2350, BCP 21) / Информационный Бюллетень Jet Info, 2000, № 5 (84), 20 с.
5. Пошаговое руководство по созданию CSIRT. По результатам WP2006/5.1(CERT-D1/D2). European Network and information Security Agency (ENISA), 2006. 86 с.
6. Alberts C., Dorofee A., Ruefle R., Killcrece G., Zajicek M. Defining Incident Management Processes for CSIRTs: A Work in Progress. Technical Report CMU/SEI-2004-TR-015, 2004, 249 p.
7. Clearinghouse of Incident Handling Tools (CHIHT) http://www.enisa.europa.eu/act/cert/support/chiht
8. Grobler M., Bryk H. Common challenges faced during the establishment of a CSIRT // Information Security for South

Africa (ISSA), 2010, 2-4 August, 2010, Sandton, Johannesburg, pp.1-6.

9. ISO/IEC 27001:2005 Information technology – Security techniques – Information security management systems – Requirements. 2005. 34 p.
10. ISO/IEC TR 18044:2004–Information technology–Security techniques–Information security incident management. 2004. 50 p.
11. Kácha P. OTRS: Tool for Security Incident Reports Management. Technical report 12/20074. Praha: CESNET, 2007, 13 p. http://www.cesnet.cz/doc/techzpravy/2007/otrs/.
12. Killcrece G, Kossakowski KP, Ruefle R, Zajicek M. Organizational models for computer incident response teams (CSIRTs). Report: CMU/SEI-2003-HB-001. Carnegie Melon University/Software Engineering Institute. 2003, 158 p.
13. Killcrece G., Kosakowsky K., Ruefle R., Zajicek M. State of the practice of Computer Security Incident Response Team (CSIRT's). Technical Report No. IA-233, Carnegie Mellon Software Engineering Institute. 2003, 291 p.
14. Killcrece G., Steps for Creating National CSIRTs. Carnegie Mellon University, 2004, 26 p.
15. Kruse W., Heiser J.· Computer Forensics – Incident Response Essentials. Addison-Wesley, 2001. 416 p.
16. Mandia K., Prosise C., Pepe M. Incident Response & Computer Forensics. 2nd edition, McGraw-Hill, 2003. 507 p.
17. Mitropoulos S., Patsos D., Douligeris C. On Incident Handling and Response: A state-of-the-art approach / Computers & Security, v.25, no.5, 2006, pp. 351-370.

18. NIST Special Publication 800-3: Establishing a Computer Security Incident Response Capability (CSIRC). – November 1991, 45 p.
19. NIST Special Publication 800-61: Computer security incident handling guide. National Institute of Standards and Technology. January 2004, 148 p.
20. NIST Special Publication 800-86 Guide to Integrating Forensic Techniques into Incident Response. – August 2006. 121 p.
21. Northcutt S. Computer Security Incident Handling: Step-by-Step (Version 2.3.1). SANS Institute, 2003, 76 p.
22. Penedo D. Technical Infrastructure of a CSIRT // International Conference on Internet Surveillance and Protection – ICISP '06, 26-28 August 2006, Cote d'Azur, France, pp.27-35.
23. RTIR: Request Tracker for Incident Response. http://www.bestpractical.com/rtir/
24. Ruefle R., Rajnovic D. FIRST Site Visit Requirements and Assessment, version 1.0, 4/2006, 22 p. http://www.first.org/membership/site-visit-V1.0.pdf.
25. Shumway R., Schultz G. Incident Response: A Strategic Guide to Handling System and Network Security Breaches. Indianapolis: New Riders Publishing, 2002. 384 p.
26. Van Wyk K., Forno R. Incident response. NY: O'Reilly. 2001, 240 p.
27. West-Brown M.J., Stikvoort D., Kossakowski K.P. Handbook for computer security incident response teams (CSIRTs). Report: CMU/SEI-98-HB-001. Carnegie Melon University/Software Engineering Institute. 1998, 222 p.

Rasim Məhəmməd oğlu Əliquliyev
AMEA-nın müxbir üzvü, professor.
AMEA İnformasiya Texnologiyaları İnstitutunun direktoru və "İnformasiya cəmiyyəti problemləri" şöbəsinin rəhbəri.
director@iit.ab.az



Yadigar Nəsib oğlu İmamverdiyev
Texnika elmləri üzrə fəlsəfə doktoru.
AMEA İnformasiya Texnologiyaları İnstitutunun şöbə müdiri.
yadigar@lan.ab.az

Texniki redaktorlar: Anar Səmidov
Zülfiyyə Hənifəyeva

Korrektor: Ləman Manahova

Kompyuter dizaynı: Rəna Gözəlova
Həsən Həsənli

Kompyuter yığımı: Həcər Əliyeva

Çapa imzalanmışdır 14.05.2012, Çap vərəqi 60x84,
Sifariş №37, sayı 100 ədəd

Azərbaycan Milli Elmlər Akademiyası
İNFORMASİYA TEXNOLOGİYALARI İNSTİTUTU
"İnformasiya Texnologiyaları" nəşriyyatı

Az1141, Bakı şəh., B.Vahabzadə, 9
Tel.: (+99412) 510 42 74 Faks: (+99412) 539 61 21
secretary@iit.ab.az, www.ikt.az