

**Azərbaycan Milli Elmlər Akademiyası
İNFORMASIYA TEXNOLOGİYALARI
İNSTITUTU**

**Rasim Əliquliyev
Yadigar İmamverdiyev**

**İNFORMASIYA
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 aparən 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

4 23
256

249309

© «İnformasiya Texnologiyaları» nəşriyyatı, 2012

MÜNDƏRİCAT

Giriş.....	7
Fəsil 1. CERT komandalarının tarixi	8
1.1. Morris soxulcanı	10
1.2. CERT/CC-nin yaradılması	15
1.3. CIAC komandası	18
1.4. FIRST forumu	19
1.5. CERT yoxsa CSIRT?	21
1.6. Avropada ilk cavablandırma komandaları	22
1.7. EuroCERT layihəsi	25
1.8. TF-CSIRT qrupu	26
1.9. Asiya-Sakit Okean regionunda CERT-lər	28
1.10. Latin Amerikasında CERT təşəbbüsləri	28
1.11. US-CERT	30
1.12. İnsidentləri cavablandırma üzrə standartlar	32
Fəsil 2. İnformasiya təhlükəsizliyi insidentləri	35
2.1. İnsident anlayışı	37
2.2. İnsidentlərin növləri	39
2.2.1. Ziyankar proqram təminatı	40
2.2.2. Şəbəkənin daranması	45
2.2.3. DoS-hücumlar	49
2.2.4. Kibercasusluq insidentləri	55
2.2.5. Uyğunsuz istifadə insidentləri	57
2.2.6. Hoax proqramlar	59
2.2.7. İcazəsiz giriş insidentləri	60
2.2.8. İntellektual mülkiyyət insidentləri	62
2.2.9. Sosial mühəndislik insidentləri	64
2.3. İnsidentlər haqqında məlumat mənbələri	67
Fəsil 3. CSIRT modelləri	72
3.1. İnsidentləri cavablandırma komandası	74
3.2. CSIRT-in təşkilati modelləri	75
3.3. CSIRT komandalarının növləri	78
3.4. Milli CSIRT-lər.....	80
3.5. Milli CSIRT-in yaradılması modeli	82

3.6. CSIRT komandasının strukturu	84
3.7. CSIRT-in heyətlə komplektləşdirilməsi	85
3.8. CSIRT heyətinin təlimi	87
3.9. CSIRT siyasətləri	88
3.10. Keyfiyyətin qiymətləndirilməsi üsulları	92
3.11. CSIRT-in texniki infrastrukturu	94
Fəsil 4. CSIRT-in servisləri	99
4.1. Cavablandırma servisləri	101
4.2. Profilaktika servisləri	104
4.3. Təhlükəsizliyin keyfiyyətini idarəetmə servisləri	105
4.4. CSIRT servislərinin təsviri	107
4.5. Təhlükəsizlik bülletenlərinin yaradılması	110
4.6. Təhlükəsizlik bülletenlərinin formatı	113
4.7. Boşluqlar haqqında məlumatın açıqlanması	115
4.8. Boşluqlar üzrə məlumat mənbələri	117
4.9. Boşluqların qiymətləndirilməsi sistemləri	120
4.10. CVSS sistemi	122
4.10.1. Baza metrikaları.....	123
4.10.2. Zaman metrikaları.....	125
4.10.3. Mühit metrikaları.....	126
4.10.4. Metrikaların qiymətləndirilməsi düsturları.....	129
Fəsil 5. İnsidenti cavablandırma prosesləri	132
5.1. İnsidenti cavablandırma prosesləri	134
5.2. Hazırlıq prosesləri	137
5.3. İnsidentlərin emalı alqoritmi	140
5.4. İnsidentlərin aşkarlanması və analizi	142
5.5. İnsidentlərin eskalasiyası	144
5.6. İnsidentlərə prioritet verilməsi	144
5.7. İnsidentlərin lokallaşdırılması	146
5.8. İnsidentin təhqiqatı	148
5.9. İnsident sübutlarının toplanması	149
5.10. İnsidentin nəticələrinin aradan qaldırılması	152
5.11. İnsidentlərin sənədləşdirilməsi	153
5.12. İnsidentin bağlanması	154
5.13. İnsidentləri cavablandırma resursları və alətləri	155

Fəsil 6. CSIRT komandalarının beynəlxalq əməkdaşlığı ...	164
6.1. Trusted Introducer	166
6.2. NATO CIRC	168
6.3. APCERT	170
6.4. Avropa dövlət CERT-ləri qrupu	171
6.5. ENISA	172
6.6. SANS İnstitutu	173
6.7. TI-də qeydiyyat proseduru	174
6.8. FIRST-ə üzvlük proseduru	176
6.9. FIRST üzvlük yoxlaması	177
Fəsil 7. RFC 2350	191
7.1. Sənəd haqqında məlumat	193
7.2. Əlaqə məlumatları	194
7.3. Nizamnamə	195
7.3.1. Missiya.....	195
7.3.2. Kliyətlər.....	196
7.3.3. Sponsor-təşkilatlar və yuxarı təşkilatlar.....	196
7.3.4. Səlahiyyətlər.....	197
7.4. Qaydalar	197
7.4.1. İnsidentlərin növləri və dəstək səviyyəsi.....	198
7.4.2. Əməkdaşlıq, qarşılıqlı əlaqə və informasiyanın açıqlanması.....	198
7.4.2.1. Cavablandırma komandaları	199
7.4.2.2. Provayderlər	200
7.4.2.3. Hüquq-mühafizə orqanları	200
7.4.2.4. Mətbuat.....	200
7.4.2.5. Digərləri	201
7.4.3. Kommunikasiya və autentifikasiya	201
7.5. Servislər	202
7.5.1. İnsidentin cavablandırılması	202
7.5.1.1. İnsidentin təsnifatı	202
7.5.1.2. Cavablandırmanın koordinasiyası	203
7.5.1.3. Problemlərin həlli	204
7.5.2. Profilaktika hərəkətləri	204
7.6. Bildiriş formaları	204

7.7. İmtinalar	205
Əlavə 1. İxtisarlər	206
Əlavə 2. Milli CERT-lərin siyahısı	212
Əlavə 3. FIRST üzvlərinin siyahısı	214
Əlavə 4. İnsident barəsində bildiriş forması	215
Ədəbiyyat	216

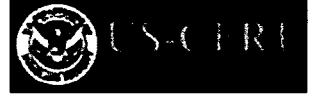
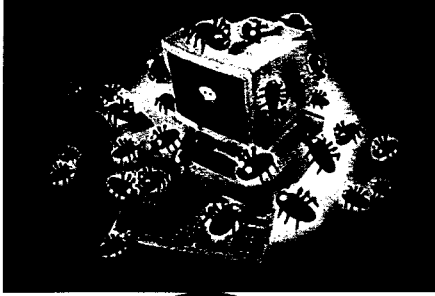
Giriş

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 Kompüter 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 kompüter 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 kompüter 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

CERT

1

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 əvvəl 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 vurmeyən 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 mənə 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 çıx 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 yükləndikdə 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 bilirlər. 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 kompyutərə 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 sürətlərinin 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 yarıda 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 Laboratories-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 məhrum etmə və 250 min dollar cərimə gözləyirdi, lakin məhkəmə yüngülləşdirici şərtləri nəzərə alaraq onu 3 il azadlıqdan şərti məhrum etmə, 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 Berkliyə 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 fəvqəladə vəziyyətə qarşı ən ağıllı tədbir isə CERT-in yaradılması oldu.

1.2. CERT/CC-nin yaradılması

«Morris soxulcanı insidenti»nin cavablandırılması zamanı ən problemlı 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 signalı 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, Kompüter 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;
- kompüter 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 bilirlər.

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 cavablandırma 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 Advisory 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://lnl.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 təhlükəsizlik 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 bildiren digər qısaltmalar da var:

Cədvəl 1.2. İnsidentləri cavablandırma qrupları

CERT	Computer Emergency Readiness Team, Kompüter Qəzalarına Hazırlıq Komandası
CSIRT	Computer Security Incident Response Team, Kompüter təhlükəsizliyi insidentlərini cavablandırma qrupu
CSIRC	Computer Security Incident Response Capability, Kompüter təhlükəsizliyi insidentlərini cavablandırma mərkəzi
CIRC	Computer Incident Response Capability, Kompüter insidentlərini cavablandırma mərkəzi
CIRT	Computer Incident Response Team, Kompüter 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 Incident 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 iş 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-ışləməyəcəyini müəyyən etmək üçün RARE (Réseaux Associéspour la Recherche Européene) CERT Task Force tərəfindən 1993-cü ilin ortalarında birillik tədqiqat layihəsi başlandı. 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 koordinasiya 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, kommertiya 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 çağırırdı. EuroCERT-in fəaliyyəti ilə əldə edilən bütün hədəflər bir daha yoxlandı, bütün iştirakçılar həmin hədəflərə aşağıdakı yanaşma ilə razılaşırdılar.

- 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.

- Incident 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 komandalının üzvləri trening materialları çoxluğunun yekun versiyasını yeni insident cavablandırma heyəti üçün kurs yaratdılar. Layihədə CSIRT təlimi üçün təqdimatlar və materiallar toplanmışdır. Bu treninglər Avropa İttifaqı tərəfindən dəstəklənir və yeni CSIRT üzvləri treningdə nominal ödənişlə iştirak edə bilirlər.

Bu qrupun digər faydası müxtəlif komandalın 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 fondlarındanadır. 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 kommertiya təşkilatları ilə təmas nöqtəsidir.

Brazilyada CSIRT təşəbbüsləri 1995-ci ilin mayında Internet İdarəetmə Komitəsinin (Internet Steering Committee – CGI.br) yaradılması ilə başlanmışdır. CGI.br dövlət, akademik, biznes və qeyri-hökumət 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 infrastrukturunu, 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 işlənilib 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 fəvqəladə hallara hazırlığı yoxlamaq məqsədilə mütəmadi olaraq (iki ildə bir dəfə) Cyber Storm təlimlərini keçirir;
- kibertəhlükəsizlik üzrə ildə bir dəfə informasiya-təhsil ayлығы 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 tərəfdaşdır. 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 rəqləşdirilməsini həyata keçirir. Bu sistem daxil olan informasiyanı süzgəcdən keçirir və zəruri olduqda avtomatik rejimdə bütün istifadəçilərə həyəcan signalı göndərir.

- kiberhəyəcan signalı – 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 icməldir.

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 tənəkmilləşdirilməsi 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 Incident Response Teams (CSIRTs);

- State of the Practice of Computer Security Incident 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/SEL-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 gözlənilir” 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 uyurluğu 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 istifadəsi, 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

İNFORMASIYA TƏHLÜKƏSİZLİYİ İNSİDENTLƏRİ

İNFORMASIYA TƏHLÜKƏSİZLİYİ İNSİDENTLƏRİ

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

FƏSİL

İNFORMASIYA

2

TƏHLÜKƏSİZLİYİ

İNSIDENTLƏRİ

2.1. İnsident anlayışı

“İnformasiya təhlükəsizliyi insidenti” anlayışının müxtəlif təriflərinə 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 ardıcılığına 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 bədniiyyətli (təşkilatın əməkdaşı da ola bilər) belə sənədləri mütləq görəcək.

İnformasiya texnologiyaları inkişaf etdikcə və onların tətbiq sahələri genişləndikcə informasiya sistemində nəzərə alınmayan 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 cavablandığı 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 darlanması, 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 **malicious** – ziyankar və **software** – 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 mənfəət 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 başvuru İnternet-resursların siyahısı, axtarış sorğuları və sonrakı reklam kampaniyalarında istifadə edilə bilən digər verilənlər (çox vaxt Spyware ilə Adware bir məhsulda olur).

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

Snoopware (ing. snoop – özgəsinin işlərinə qarışan adam və software – 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 bədniiyyətliyə 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, keyloqqlər, 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 sisteme administrator kimi daxil olurlar, bunun hesabına bədniiyyətinin 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 mərmə və **software** – proqram təminatı) kompyutərə 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 bədniiyyətli 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 gizləncə idarə edilməsidir. Adətən, BackDoor yoluxmuş kompyuterdən faylları köçürməyə və əksinə, fayl və proqramları yoluxmuş kompyutərə 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 yetirilərk 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 açma 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 komandalara 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 olduğdan və istehsalçılar onları bağladıqdan sonra bədiyyətlilər 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 konfigurasiyası 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 həddlərini müəyyən etmək zəruridir. Məsələn, təşkilatın bütün kompüter şəbəkəsi, yoxsa onun yalnız müəyyən segmenti (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 obyektini 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 süzülülər)) 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 danışirlar.

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. adlandırirlar.

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 alınarsa, onda tədqiq olunan port bağlı hesab edilir. Əgər SYN məlumatına cavab olaraq RST/ACK məlumatı alınarsa, 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.

“Mülad yolması” 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 obyektini qovşaqlarının kommunikasiya xidmətlərini (serverləri) identifikasiya etmək;
- hücum obyektini 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 port 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-darəmə 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 bilər. Qeyri-texniki vasitələrlə yaradılan DoS-hücum insidentləri, məsələn, aşağıdakı faktorlardan qaynaqlana bilər:

- 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-kondisioner sistemi sıradan çıxır) və s.

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

İkinci üsulda hücum edilən kompüterə 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 göndərsə, onda həddindən artıq yüklənmə nəticəsində kompüter «boğula» və ya işini tam dayandıra bilər. DoS-hücum təşkilatçılarında məhz bu lazımdır.

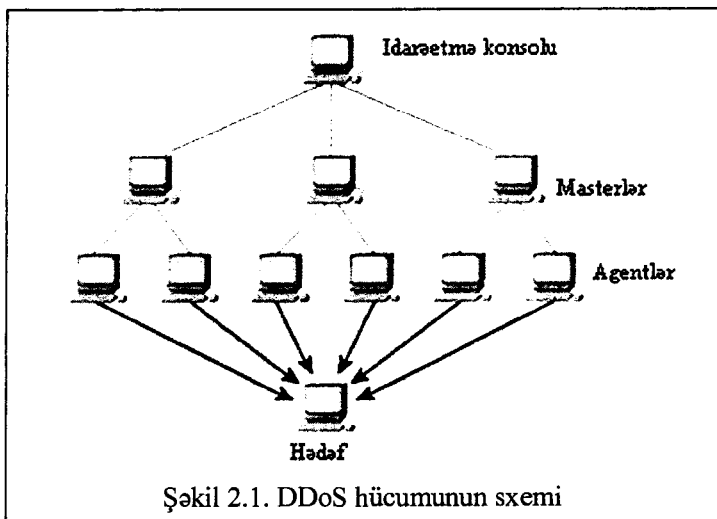
DoS-hücumunun bir növü olan paylanmış DoS-hücum (Distributed Denial of Service, DDoS) – çox böyük sayda kompüterin köməyi ilə təşkil edilir, bunun sayəsində hətta İnternet-kanallarının buraxma imkanı olduqca böyük olan serverlər də bu hücumla təslim olurlar.

DDoS-hücumların təşkili üçün bədniyyətli kompüterlərin xüsusi şəbəkəsindən – botnet-dən istifadə edirlər. Botnet (ing. botnet termini **robot** və **network** – şəbəkə sözlərindən yaranmışdır) – bədniyyətli istifadəçinin xəbəri olmadan yoluxmuş kompüterini məsafədən idarə etməyə imkan verən ziyankar proqramlarla – botlarla yoluxmuş kompüterlərdən ibarət şəbəkədir. Bot istifadəçinin kompüterində gizli quraşdırılan və bədniyyətli yoluxmuş kompüterin resurslarından istifadə etməklə müəyyən əməlləri yerinə yetirməyə imkan verən proqramdır. Lazımı 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 bədiyyətlilər çox vaxt “DDoS klasteri” adlanan üçsəviyyəli arxitekturdan istifadə edirlər. Bu iyerarxik struktura aşağıdakılar daxildir (şəkil 2.1):

- idarəetmə konsolu (onlar bir neçə ola bilər) – məhz bu kompyuterdən bədiyyətli 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.



Qeyd etmək lazımdır ki, bütün agentlər bir-birindən və bədiyyətliyədən 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 dolay DoS-hücumları (**Distributed Reflection DoS, DRDoS**) – İnternet şəbəkəsinin “vicdanlı” hostları vasitəsilə dolay 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 göstərsə, SYN-bayrağı olan TCP sorğusuna cavab verəcək server bu ünvanı 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. Genişyayimli ICMP-əks-səda sorğuları alan kompyuterlər hücum obyektinə ICMP-əks-səda cavabı göndərir. Beləliklə, bir paket göndərməklə bədniiyyətli həm hücum obyektinə, həm də

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

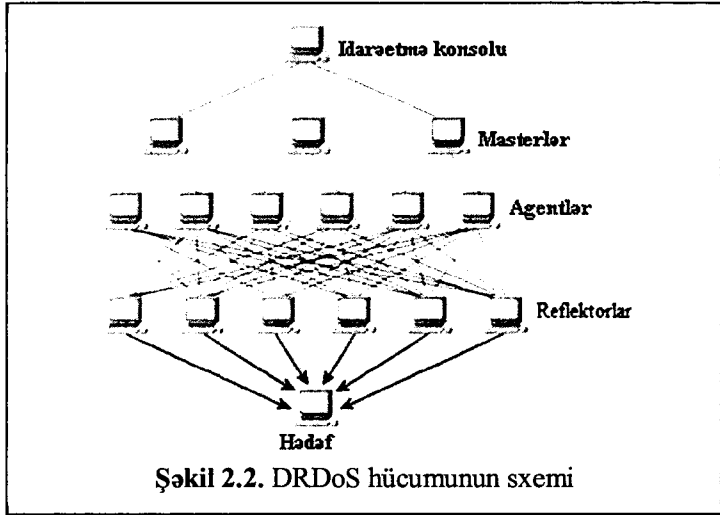
ICMP flood – mövcud olmayan hostların adından hücum edilən hosta çoxlu sayda ICMP-əks-səda sorğuları göndərilir. Əks-səda sorğuların mənbəyi mövcud olmayan hostlar olduğundan hücumun nəticəsində hücum obyektinin məhsuldarlığı, həmçinin rabitə kanalının buraxma qabiliyyəti aşağı düşür.

Bədənyyətli 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 genişyaymlı ping-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 risklərini 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.

Mərsutizatorlarda və şəbəkə ekranlarında anti-spufinq və anti-DoS funksiyalarının savadlı konfigurasiyası 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.



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 IP-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. Bədniiyyətli 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. Bədniiyyətliyə 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 hökumətləri müntəzəm olaraq bir-birini milli informasiya sistemlərindən strateji informasiyanın oğurlanmasına yönəlmiş gizli əməliyyatlar aparmaqda günahlandırır.

Toronto Universitetində 10 ay ərzində aparılmış tədqiqatlar nəticəsində 2009-cu ildə aşkarlanmış GhostNet kod adlı kibercasusluq şəbəkəsinə dünyanın 103 ölkəsindən 1295 kompüter daxil idi. Bu kompüterlərin 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 yönəlmişdi. Çinə məxsus olduğu iddia edilən bu şəbəkə son iki il ərzində qurulmuşdu və hər həftə şəbəkəyə 10-dan çox yeni kompüter əlavə edilirdi. GhostNet təkcə kompüterləri axtararaq e-məktubları ələ keçirmirdi, yoluxdurulmuş kompüterdə veb-kamera və mikrofonları işə salaraq ətrafdakı bütün danışmaları 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 qətiyyənlə 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 perimetrleri getdikcə daha qeyri-müəyyən olur, bu qurğuların köməyi ilə əməkdaşlar korporativ şəbəkəyə öz iş yerlərindən kənar da qoşula bilirlər. 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 dördüdə biri bildirir ki, xarici şirkətlərin şəbəkələrinin sındırılması və şəbəkələrdə ziyankar proqram təminatının quraşdırılması yolu ilə dövlətlərin bir-birini güdməsinə icazə vermək lazımdır. Respondentlərin yarısından 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 sürətlərini 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 yönəliirlər.

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 qərribə 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 inandırır 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 yüklənilir. (Bekdor (ing. back door, arxa qapı) – sistemə sonradan təkrar giriş əldə etmək üçün sındırılmış kompyuterlərdə bədniiyyətli 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 icazəsis giriş insidentlərinə aşağıdakı misallar göstərilə bilər:

- serverdə məsafədən administrator hüquqlarının ələ keçirilməsi;
- veb-saytın defeqs 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;
- pırat 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 sürətinin 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, sürətinin 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 icazəsiz giriş insidentinə misal fiziki mühafizə vasitələrini sıradan çıxarıqdan sonra informasiyaya icazəsiz giriş göstərilə bilər.

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

informasiyaya icazəsiz girişlə əlaqədar insidentlər qeydiyyatda alınır.

Problem onunla mürəkkəbləşir ki, konfidensial informasiyaya icazəsiz giriş çox vaxt onun oğurlanması ilə müşayiət 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 “İntellektual 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 obyekt 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, bədnüvətlilərin 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.

Fişinq – (ing. phishing – password – parol və fishing – balıq ovu, aldatma) – İnternet dələduzluğunun 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. Məktubda göstərilən ünvana gedən istifadəçi ödəniş sisteminin kopyası olan sayta düşür. Bu saytda öz fərdi məlumatlarını daxil edən istifadəçi öz hesabına nəzarəti faktiki olaraq bədniiyyətliyə 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 kommertiya təşkilatlarının veb-səhifələri saxtalaşdırılır.

Klassik fişinq sxemində əsas "zəif" nöqtə istifadəçidən asılılıqdır – o, fişərə inanacaq, yoxsa yox. Banklar, sosial şəbəkələr və digər veb-xidmətlər istifadəçiləri sosial mühəndislik metodları istifadə edilən müxtəlif dələduzluq üsulları haqqında xəbərdar edirlər. İstifadəçilərin məlumatı artıqca onları saxta saytlara cəlb etmək çətinləşir. Buna görə də bədniiyyətlilər 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 fotosəkilləri və uydurma məlumatlarla saxta anket yerləşdirir. Bundan sonra varlı adaxlı və ya gəlin seçilir. Dələduz onunla fəal yazışmaya girir, inam münasibətləri yaratmağa çalışır və məhəbbət münasibətlərini təqlid edir. Fırıldağının 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 nəgd pulu götürə bilər. Qəfildən xəstələmə 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-telefoniyının (VoIP) imkanlarından istifadə etməkdən ibarətdir.

Secure Computing-in məlumatına əsasən Wardailer konfigurasiya 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 bədniiyyətli məqsədlər üçün zəruri olan bütün məlumatlara (telefon nömrəsi, tam adı, ünvan) sahib olur;
- sonra bu zəngdən istifadə edərək əlavə informasiya da toplamaq olar: PIN-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 qeydiyyatı 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 aşkarlanma 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. Hazırkı antivirus və anticasus proqram məhsulları ziyankar kodları onların siqnaturaları yeniləndikdə aşkarlaya və qarşısını ala bilər. 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. Spamdə 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 kriptografik 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.

Monitoring xidməti. Bəzi təşkilatlar özlərinin onlayn servislərinin, məsələn, veb, DNS (Domain Name System) və FTP serverlərinin monitoringini həyata keçirirlər, bunun üçün üçüncü tərəfin xidmətindən də istifadə edilə bilər. Monitoring xidməti hər x dəqiqədən bir hər bir servise avtomatik qoşulmağa cəhd edir. Əgər servise qoşulmaq mümkün olmur, monitoring xidməti müəyyən edilmiş üsullarla, məsələn, telefon zəngi, e-poçtla və s. təşkilata xəbər verir. Bəzi monitoring xidməti müəyyən resurslarda, məsələn, veb-səhifədə dəyişiklikləri aşkarlaya və məlumat verə bilər. Monitoring 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 agregasiyasında da yardımçı ola bilər. Təəssüf ki, bir çox insidentlər zamanı loqlarda sübutlar olmur, çünki hostlarda ya loq yazılması imkanı bağlanıb, ya da düzgün konfigurasiya 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 signalı 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 konfigurasiya edirlər, 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.

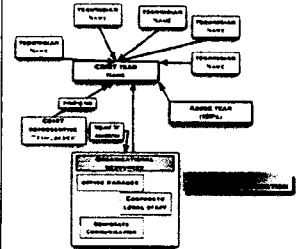
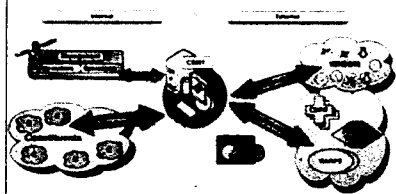
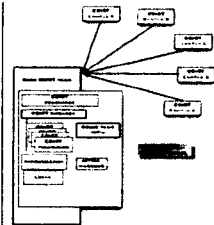
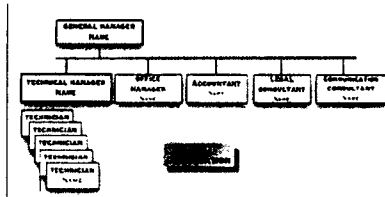
Digər təşkilatlarda olan insidentlər haqqında məlumatlar. Digər təşkilatlarda baş vermiş insidentlər haqqında hesabatlar qiymətli informasiya verə bilər. Bir sıra veb-səhifələr və göndəriş siyahıları var ki, insident cavablandırma komandaları və təhlükəsizlik üzrə ekspertlər qarşılaşdıqları insidentlər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

hücumlar haqqında təcrübələrini burada paylaşılar. 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 bilirlər. Belə məlumatların hamısının həqiqiliyini yoxlamaq vacibdir. Təkcə adi istifadəçilər insidentin baş verdiyini müəyyənləşdirəndə çətinlik çəkmirlər, bəzən hətta ən yaxşı texniki ekspertlər də səhv edə bilirlər. Yanaşmalardan bir belə məlumat verən şəxslərdən bu məlumatların dəqiqliyinə onların nə qədər əmin olmasını soruşmaqdır. Təqdim olunan informasiya ilə birlikdə bu qiymətləndirmənin də qeydiyyatı 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 defeyts edilməsi və ya servisin əlyetməz olması haqqında məlumat verə bilirlər. Digər insident cavablandırma komandaları da insidentlər haqqında məlumat göndərə bilirlər. 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.



PART I
A basic collection of good practices for running a CSIRT

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 lazımı 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. Kompüter 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, təhlükəsizliyinin və əlyətərlik 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 idarəetməyə 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 edirlər;
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, bərpəetmə 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 qoşulma, 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 tələbələrindədir.

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 infrastrukturuna 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 kliyətləri IT-departament və təşkilatın əməkdaşlarıdır.

Kiçik və orta biznesdə CSIRT

Belə CSIRT-lər öz biznesinə və tərəfdaşlarına xidmətlər göstərir. Onun kliyətləri 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 kliyətləri bu və ya digər məhsulun sahibləridir.

3.4. Milli CSIRT-lər

Hazırda dünyada yetkinliyin müxtəlif mərhələlərində 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 bilər. 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 infrastrukturunu;
- procedures to guard against information leakage;
- kritik informasiyanı yaymaq üçün yaxşı məlum açıq interfeys;
- böyük audensiyaaya 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 çıxan 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 qıscaca 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 çoxluğu, 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 informasiyadan 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 – CSIRT-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 yardımını 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 kliyətlərin mövcud strukturundan çox asılıdır. O, həmçinin daimi əsaslarla və ya konkret məsələ üçün cəlb olunan ixtisaslı ekspertlərin əlyətən 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.

Kliyənt 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 kliyəntlər və ya media-tərəfdaşlar üçün daha anlaşqlı olan məlumatlara tərcümə etməklə məşğul olur. Kommunikasiyalar üzrə mütəxəssis kliyəntlərlə 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 lazımı 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 (işdänkənar 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 işdänkənar 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 izah etmə qabiliyyəti;
- konfidensiallığa və metodiki işə yaxşı münasibət;
- yaxşı təşkilatçılıq qabiliyyətləri;
- stressə dayanıqlıq;
- yaxşı danışıq və yazı vərdişləri;
- ağılın həssaslığı və öyrənmək istəyi.

Texniki vərdişlər

- İnternet-texnologiyaları və protokolları yaxşı bilmək;
- Linux və Unix sistemləri bilmək (klientlərin avadanlığından asılı olaraq);
- Windows sistemləri bilmək (klientlərin 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” rejimində (servis modelindən asılı olaraq) işləmək həvəsi;
- yola, əlyətənliyə maksimal vaxt (qəza halında ofisdə əlyətənlik, qəza yerinə çatmaq üçün yola maksimal vaxt);
- təhsil səviyyəsi;
- kompüter təhlükəsizliyi sahəsində iş təcrübəsi.

3.8. CSIRT heyətinin təlimi

CSIRT heyətinin tədrisində 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 öyrəniləndiyi 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. Kompüter və şəbəkə infrastrukturunun mürəkkəbliyi, həmçinin müdiriyyətin 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 kompüter təhlükəsizliyinin pozulması insidentlərinin sayı artır. Kompüter 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 bərpa etməyə xərclər də azalar. CSIRT-in formalaşdırılması tez insidentlərə tez cavab verilməsinin 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 edilir:

- CSIRT-in yaradılması;
- CSIRT-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 (klientlər üçün), həmçinin konkret servis üçün (məsələn, zərərçəkmiş klientin 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 xidmətləri işə başladığından sonra yaradıla bilər.

Siyasətin misallarla müşayiət edilməsi yaxşı praktikə hesab edilir.

Cədvəl 3.1. Yaxşı siyasətin atributları

Atribut	Təsviri
Rəhbərlik tərəfindən bəyanilmə və dəstəklənmə	Missiya kimi, siyasət də rəhbərlik tərəfindən dəstəklənməyə, 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 pisdır, 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 nəşə daxil etməməlidir.
Praktiklik	Gözəl, lakin mənasız frazalardan qaçmaq lazımdır (məsələn, “mühafizəçiliklə 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.
Qarşılıqlı əlaqə	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. Siyasətin 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 yoxlanılmalıdır. Siyasətin aktual vəziyyətdə saxlanması üçün məsul şəxsin olması zəruridir.

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 (çoqları 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 münafiqşələrin 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 infrastrukturunu 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 qeydiyyatına alınması çox vacibdir.

Bəzi təşkilatlar kommunikasiya vasitəsi kimi fakstan istifadəyə üstünlük verə bilər. Bundan başqa şəbəkə və ya poçt serveri işləmədikdə fakstan 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 göstərsin. İnsidentlərin emalı adətləri üçün komandaya serverlər (vəb-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. Elektron poçt əvəzəlməz 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 şifrələmək 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) kriptografik proqram təminatına alternativdir, GnuPG-nin hazırkı 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 işlənib, dünyada və Avropada bir çox CERT komandası tərəfindən istifadə edilir. İnsidentlərin izlənməsi 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).

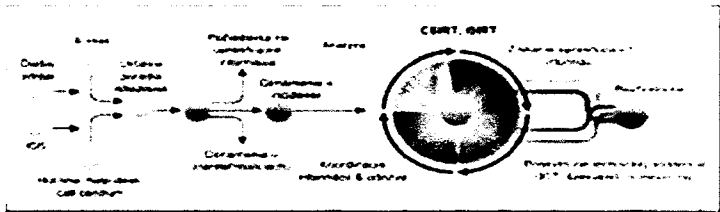
CSIRT-in fiziki təhlükəsizliyi. Fiziki mühafizə tələblərinə daxildir:

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

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



Alerts and Warnings

- Incident Handling
- Incident analysis
- Incident response
- Incident response
- Incident response

Vulnerability Handling

- Vulnerability analysis
- Vulnerability response
- Vulnerability response

Product Handling

- Product analysis
- Product response
- Product response

Communications

- Technology
- Technology
- Technology
- Technology
- Technology

Operational Security

- Operational Security
- Operational Security
- Operational Security

Policy Development

- Policy Development
- Policy Development
- Policy Development
- Policy Development

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

CSIRT

4

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 risk yaratmış hadisələrin bərpasına (rekonstruksiyasında) kömək etmək üçün riskə məruz qalmış sistemdə sübutların toplanması, saxlanması, sənədləşdirilməsi və analizi.
- **Axtarış və izləmə** – bədniiyyətlinin zədələnmiş sistemə və onunla əlaqəli şəbəkəyə necə giriş əldə etməsi izlənilir və ya axtarılır. Baxılan fəaliyyətə “çağırılmamış qonağın” mənşəyinin izlənməsi və ya bədniiyyətlinin 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 lazımı 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 yaxşılaşdırılması 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 bədniiyyətlinin 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, bədniiyyətlilərin fəaliyyətinin və əlaqəli tendensiyaların

müşahidəsini və monitorinqini nəzərdə tutur. Bu servisin nəticəsi təhlükəsizliyin orta və uzunmüddətli məsələlərinə yönəlik hər-hansı 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 servise 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 yönəliirlər. Belə servislərə aiddir:

1) Risklərin analizi – real təhdidlərin qiymətləndirilməsi, informasiya resursları üçün risklərin 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 kliyətlərə 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.

Kliyətlərə 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, “E-lanlar” göndəririlər və öz kliyətlərinə “İnsidentlərin emalı” servisini göstəririlər. Adətən, bu baza servisləri ictimai marağ səviyyəsini və diqqəti kliyətlər tərəfindən müəyyən edirlər və ən əsas servislər hesab edilirlər.

“Pilot” kliyətlər 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” kliyətləri, 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 əlyətən 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.