APSTIPRINU
SIA „XYX999”
Valdes priekšsēdētājs

Jānis Kalējs
2013.gada 15. februārī

SIA „XYZ999” rīcības plāns elektronisko sakaru tīkla nepārtrauktas darbības nodrošināšanai

Satura rādītājs

1. Vispārīgas ziņas par komersantu

- Juridiskais nosaukums: SIA „XYZ999”
- Reģistrācijas numurs: 4000xxxxxxx
- Juridiskā adrese: Apses iela 9, Rīga, LV-1XXX, Latvija
- Pasta adrese: Bērzu iela 8, Rīga, LV-10XX, Latvija
- Tālruņa numurs: +371 67XXXXXX
- Faksa numurs: +371 671XXXXX
- Elektroniskā pasta adrese: info999@xyz999.lv
- Mājas lapa: www.yyz999.lv

2. Ziņas par struktūrvienību, kas nodrošina drošības pasākumu īstenošanu

- Struktūrvienība : IT drošības nodaļa
- Kontaktpersona: Jānis Kālis
- Tālruņa numurs: 29xxxxxx, 67xxxxxx
- Faksa numurs: 67xxxxxx
- Elektroniskais pasts: janis.kalis@xyz999.lv
- Adrese: Apses iela 9, Rīga, LV-1XXX, Latvija
- Darba režīms
  - Darba dienās no plkst. 9:00 – 17:00
- Kontaktpersonas aizvietotājs: Pēteris Upmalis
  - Tālruņa numurs: 29xxxxxx
  - Faksa numurs: 67xxxxxx
  - Elektroniskais pasts: peteris.upmalis@xyz999.lv
- 24x7 klientu apkalpošanas numurs, uz kuru var zvanīt ārkārtas situācijā: 67xxxxxx

Komentāri: Atsauce (MK Noteikumi Nr. 327 punkts 2.2).
Norādot struktūrvienību, lūgums norādīt arī atbildīgo personu, un personu, kura to aizvietos prombūtnes laikā. Ja elektronisko sakaru komersantam ir filiāles vairākos reģionos, informācija jāiesniedz par katru reģionu. Adresi nepieciešams norādīt, ja tā nesakrīt ar komersanta juridisko adresi. Darba režīms – reālais struktūrvienības vai atbildīgās personas darba laiks. Piemēram, darba režīms darba dienās darba laikā (8:00 – 17:00) vai (24x7).

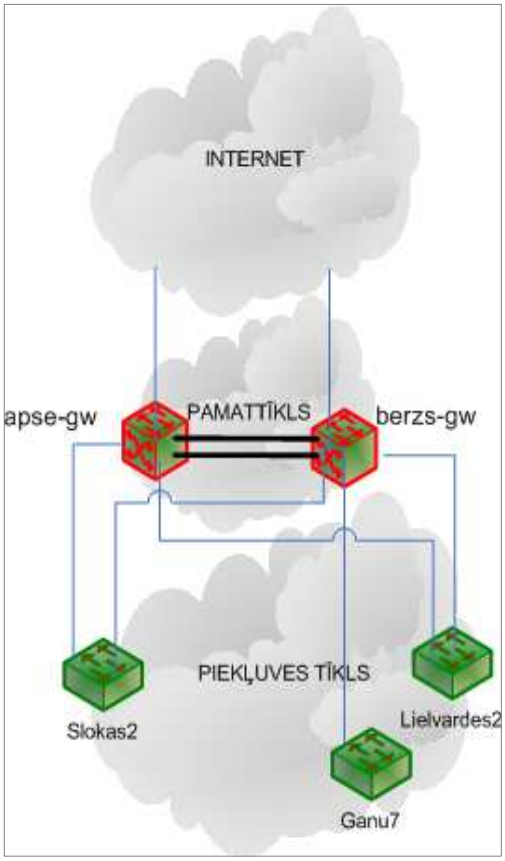
3. Elektroniskā sakaru tīkla uzbūve

Tīkla vispārējs apraksts. Ģeogrāfiskais pārklājums, izmantotās tehnoloģijas.

SIA „XYZ999" piedāvā interneta pakalpojumus Rīgā. Tīkls ir veidots ar 2 centrālajiem punktiem, kas atrodas datu centros:

- Apses ielā 9, Rīga
- Bērzu ielā 8, Rīga

Centrālie punkti var savstarpēji viens otru aizvietot, katrs no tiem pieslēgts citam operatoram ar izeju uz Internet.
Pie diviem centrālajiem mezgliem pieslēgta tīkla infrastruktūra – optiskās šķiedras trases līdz mezglu punktiem - Slokas2, Lielvārdes2 un Ganu7. Visi klienti ir pieslēgti pie šiem mezglu punktiem, izmantojot optiskās šķiedras, un pēdējā jūdzē - vara kabeļu pieslēgumus. Lielākā daļa mezglu punktu pieslēgti pie abiem Centrālajiem punktiem, bet daļa tikai vienam Centrālajam punktam. Daži posmi kabeļu infrastruktūras tiek izīrēti no citiem operatoriem.
Pakalpojumu uzraudzības centrs un dažādi servisi klientiem (e-pasts, web hostings) izvietoti vienā datu centrā – Apses 9.
Tīkla shēma pievienota zemāk.



Publiski pieejami citu ESK tīkla shēmu piemēri:

- http://itserviss.lu.lv/modules/aboutlanet/tiklashema.php
- http://lix.lv/site/scheme

Komentāri: Atsauce (MK Noteikumi Nr. 327 punkts 2.3). Elektroniskā sakaru tīkla shēma var būt gan grafiskā, gan tabulārā veidā un tai ir jārada priekšstats par komersanta elektronisko sakaru tīklu.

4. Elektroniskā sakaru tīkla risku analīze

Risku novērtēšana tiek veikta vismaz vienu reizi gadā.

Pēc resursu apdraudējuma varbūtības tos iedala:

- 1 – resursi ar maza apdraudējuma varbūtību
- 2 – resursi ar vidēja apdraudējuma varbūtību,
- 3 – resursi ar liela apdraudējuma varbūtību,

Resursiem radīto kaitējumu no katra apdraudējuma iedala:

- 1 – mazs kaitējums,
- 2 – vidējs kaitējums,
- 3 – liels kaitējums.

Risku aprēķināšanu veic:

Risks= (apdraudējuma varbūtība x resursa apdraudējuma kaitējums).

R=AVxRK .

Komentāri: https://cert.lv/uploads/uploads/resursu_klasifikacija_risku_nov20111011web.pdf

4.1 Risku novērtējuma tabula

Nr	Apdraudējums	Apraksts	Apdraudējuma varbūtība (AV)	Radītais kaitējums (RK)	Aprēķinātais risks (R)
	Daba – fiziskie apdraudējumi				
1.	Ugunsgrēks	Centrālie punkti izvietoti datu centros, kas aprīkoti ar dūmu detektoriem un ugunsdzēšanas iekārtām. Pārējos Mezglu punktos nav nekāds speciāls ugunsdrošības aprīkojums. Ugunsgrēks centrālajā punktā daļēji ietekmētu pakalpojumu pieejamību. Ugunsgrēks mezgla punktā ietekmētu pakalpojumu pieejamību tiem klientiem, kas pieslēgti pie šī mezgla punkta.	1	3	3
2.	Plūdi	Centrālo un mezglu punktu aparatūra izvietota augstāk par ēkas pagrabstāvu, uzstādot aparatūras skapi, tiek ņemta vērā telpas izolācija. Plūdi centrālajā punktā daļēji ietekmētu pakalpojumu pieejamību. Plūdi mezgla punktā ietekmētu pakalpojumu pieejamību tiem klientiem, kas pieslēgti pie šī mezgla punkta.	1	3	3
3.	Zibens	Centrālo un mezglu punktu aparatūra izvietota sazemētos aparatūras skapjos, bet zibens spēriens var ietekmēt aparatūru vai	1	3	3

		radīt bojājumus tās daļām. Pakalpojumu pieejamība var tikt ietekmēta daļēji.			
	Vide – tehniskie apdraudējumi				
4.	Elektrības pārtraukums Centrālajā punktā	Centrālajos punktos aparatūra izvietota datu centros, kur tiek nodrošināts UPS un dīzeļģenerators. Elektrības pārtraukums abos centrālajos punktos vienlaicīgi izraisītu visu pakalpojumu nepieejamību. Elektrības pārtraukums vienā centrālajā punktā (kur izvietoti serveri) daļēji ietekmētu pakalpojumu pieejamību.	1	3	3
5.	Elektrības pārtraukums Mezgla punktā	Mezglu punktos tiek nodrošināts UPS. Ja elektrības padeve netiek atjaunota 1 stundas laikā, traucēta pakalpojumu sniegšana klientiem, kas pieslēgti pie attiecīgā Mezgla punkta.	3	2	6
6.	Kabeļu vai aparatūras bojājums/zādzība Centrālajā punktā	Centrālajos punktos tiek nodrošināta datu centra apsardze, signalizācija un ieeja datu centrā tiek žurnalēta. Tīši bojājumi un zādzība maz iespējama, bet to nodarītais kaitējums ietekmētu visu pakalpojumu pieejamību.	1	3	3
7.	Kabeļu vai aparatūras bojājums/zādzība Mezgla punktā	Mezglu punktos aparatūra tiek izvietota slēdzamos skapjos. Kabeļu/aparatūras zādzība vai tīša bojāšana ietekmētu pakalpojumu pieejamību klientiem, kas pieslēgti pie attiecīgā Mezgla punkta.	3	3	9
8.	Aparatūras neprognozēta pārslodze	Aparatūras pārslodze tiek kontrolēta no tīkla vadības sistēmas, atbildīgajām personām saņemot ziņojumus uz e-pastu un sms, ja kāda iekārta nav pieejama vai pamanītas novirzes no normālā stāvokļa. Var ietekmēt visu pakalpojumu pieejamību.	2	3	6
9.	Programmatūras kļūdas	Tiek veikta programmatūras atjaunošana vismaz 1 reizi gadā vai tiklīdz tas nepieciešams. Programmatūras kļūdas var būtiski ietekmēt daļu vai visu pakalpojumu pieejamību.	2	3	6
	Cilvēki – nekompetence, kļūdas, u.tml. apdraudējumi				
10.	Konfigurācijas kļūda pamattīklā	Konfigurācijas kļūda pamattīklā ietekmētu daļēji vai visu pakalpojumu pieejamību visiem klientiem. Konfigurācijas izmaiņas pamattīklā tiek ieplānotas ārpus darba laika un iepriekš brīdinot klientus. Visas konfigurāciju izmaiņas tiek žurnalētas un pieejama iepriekšējās konfigurācijas kopija.	3	3	9
11.	Konfigurācijas kļūda piekļuves tīklā	Konfigurācijas kļūda piekļuves tīklā var ietekmēt daļēji vai visu pakalpojumu pieejamību klientiem, kas pieslēgti pie attiecīgā Mezgla punkta.	3	2	6
12.	Darbinieku kaitnieciska darbība	Visas izmaiņas tiek žurnalētas, bijušo darbinieku konti tiek dzēsti, pieejas paroles regulāri mainītas. Darbinieku kaitnieciska	1	3	3

		darbība var ietekmēt daļēji vai visu pakalpojumu pieejamību visiem klientiem.			
	Drošības apdraudējumi [1]				
13.	Kompromitētas iekārtas	Nesankcionēta piekļuve tīkla iekārtām vai serveriem var izraisīt daļēju vai pilnīgu pakalpojumu nepieejamību visiem klientiem.	1	3	3
14.	Piekļuves lieguma uzbrukumi (DoS, DDoS)	Notiekot DoS vai DDoS uzbrukumam pamattīklam, var būt traucēta pakalpojumu pieejamība visiem klientiem. Atbildīgajai personai jārīkojas pēc iekšējās instrukcijas.	2	3	6
15.	Pikšķerēšana	Mēģinājumi iegūt informāciju no klientiem neietekmē pakalpojumu pieejamību	3	1	3
16.	Ielaušanās mēģinājumi	Ielaušanās mēģinājumi var daļēji ietekmēt serveru, tīkla iekārtu noslogojumu un pakalpojumu pieejamību	1	3	3
17.	Mēstules	Mēstuļu izsūtīšana caur XYZ999 pasta serveriem var tos noslogot un padarīt nepieejamus citiem klientiem. XYZ999 pasta serveru IP adreses var iekļūt melnajos sarakstos un e-pastu izsūtīšana kļūt daļēji vai pilnīgi bloķēta uz vairākām stundām vai dienām.	3	2	6
18.	Ļaundabīgs kods	Ļaundabīga koda izplatīšana var ietekmēt pakalpojumu pieejamību atsevišķiem klientiem. Ja kāds no XYZ999 serveriem ir uzlauzts un uz tā tiek uzlikts ļaundabīgs kods izplatīšanai, tas var ietekmēt XYZ999 reputāciju, kā arī XYZ999 IP adrešu apgabali var nonākt dažādos melnajos sarakstos un var kļūt nepieejami dažādi pakalpojumi.	2	2	4
19.	Robottīkli	Ar kaitīgu kodu inficēta iekārta var inficēt citus šī tīkla lietotājus un ietekmēt pakalpojumu pieejamību atsevišķiem klientiem.	2	2	4
20.	Citi: Vīrusu infekcija Zādzība, krāpšana Bērnu pornogrāfija Autortiesību pārkāpumi Personas datu pārkāpumi	Zemas prioritātes incidentiem ir maza ietekme uz pakalpojumu pieejamību, atbildīgā persona rīkojas pēc iekšējās instrukcijas.	 3	1	3

4.2 Risku mazināšanas pasākumi.

[1] https://cert.lv/section/show/90

Tiek izvēlēti aprēķinātie riski, kuru vērtība pārsniedz 6 un kuriem ir nepieciešams veikt risku mazināšanas pasākumus. Tie riski, kam aprēķinātā vērtība zem 6, tiek pieņemti, jo pašreiz netiek uzskatīti par būtiskiem. Zemāk aprakstīti risku mazināšanas pasākumi, paredzētais ieviešanas termiņš un atbildīgā persona par izpildīšanu.

Nr.	Apdraudējums	Riska mazināšanas pasākums	Aprēķinātais risks	Ieviešanas termiņs	Izpildītājs
1.	Elektrības pārtraukums Mezgla punktā	• Ne retāk kā vienu reizi gadā jāveic pārbaude, vai visos Mezglu punktos elektrības padeve tiek uzraudzīta; Neuzraudzītās iekārtas jāpieslēdz monitoringa sistēmai. • Regulāri jātestē un jāatjaunina UPS baterijas atbilstoši iekšējai procedūrai; • Jānoslēdz līgums un jāsaskaņo dīzeļģeneratora uzstādīšana Mezglu punktos elektropadeves traucējumu gadījumos.	6	01.01.2013	J. Kālis
2.	Kabeļu vai aparatūras bojājums/zādzība Mezgla punktā	• Pārbaudīt un regulāri atjaunot dokumentāciju par izvietotajām iekārtām un kabeļiem Mezglu punktos. • Uzstādīt signalizāciju/apsardzi,. • Pārbaudīt un atjaunot rezerves iekārtu pieejamību noliktavā. • Pārbaudīt termiņus līgumiem par svarīgāko tīkla iekārtu (tīkla iekārtas, kas izvietotas Centrālajos punktus) nomaiņu.	9	1.1.2013	J.Kālis
3.	Aparatūras neprognozēta pārslodze	• Pārbaudīt, vai visas iekārtas tiek uzraudzītas un tiek izsūtīti e-pasti/sms par novirzēm no normas.	6	1.1.2013	J. Kālis
4.	Programmatūras kļūdas	• Pārbaudīt, vai programmatūra atjaunināta uz visām iekārtām atbilstoši iekšējai procedūrai;	9	1.1.2013	J. Kālis
5.	Konfigurācijas kļūda pamattīklā	• Pārbaudīt, vai visu iekārtu iepriekšējās konfigurācijas kopijas tiek uzglabātas; • Pārbaudīt, vai visu iekārtu žurnālfaili tiek uzglabāti un pieejami pārskatīšanai; • Pārbaudīt termiņus līgumiem par svarīgāko tīkla iekārtu (tīkla iekārtas, kas izvietotas Centrālajos punktus) nomaiņu.	9	1.1.2013	J. Kālis
6.	Konfigurācijas	• Pārbaudīt, vai visu iekārtu	6	1.1.2013	J. Kālis

	kļūda piekļuves tīklā	iepriekšējās konfigurācijas kopijas tiek uzglabātas; • Pārbaudīt, vai visu iekārtu žurnālfaili tiek uzglabāti un pieejami pārskatīšanai.			
7.	Piekļuves lieguma uzbrukumi (DoS, DDoS)	• Izstrādāt iekšējo procedūru, kā rīkoties DoS/DDoS gadījumā.	6	1.1.2013	J. Kālis
8.	Mēstules	• Uzstādīt kontroles mehānismu e-pasta serveros, lai identificētu mēstuļu sūtītājus; izstrādāt iekšējo procedūru mēstuļu sūtītāju bloķēšanai;	6	1.1.2013	J. Kālis

Komentāri: Ja uzņēmumā izstrādāts iekšējais dokuments, kas ietver elektroniskā sakaru tīkla riska analīzi, Rīcības plānā var uzrādīt vispārīgi, kādas risku grupas apskatītas un atsaukties uz uzņēmumu iekšējo dokumentu, ko pēc CERT.LV uzaicinājuma jāuzrāda.

5. Reaģēšanas kārtība uz drošības incidentiem[2]

5.1. Informācija par incidentiem var tikt saņemta no
  5.1.1. CERT.LV
  5.1.2. tīkla uzraudzības sistēmas, kur definēti sliekšņi, kas ziņo par notikumu ārpus normas (Cacti, NFSen, Zabbix, Nagios, Firewall, IDS/IPS u.c.)
  5.1.3. citiem avotiem (piemēram, klientiem)

5.2. Par incidentiem dežūrējošais administrators apkopo informāciju (žurnālfailus, NetFlow datus, serveru (vai datoru) *Image* failus) vēlākai analīzei vai nodošanai CERT.LV/tiesībsargājošam iestādēm.
CERT.LV kontaktinformācija : +371 67085858, cert@cert.lv

5.3. Reaģēšanas kārtība uz drošības incidentu[3]

1. *Incidenta veids* – Mērķtiecīgi servisa atteices uzbrukumi (DoS, DDoS, skanēšana, ievaijonamību skanēšana) **no** XYZ999 IP adresēm uz internetu.
   1.1. *Incidenta īss apraksts* – dežurējošais administrators saņem informāciju par incidentu, ja no kādas XYZ999 IP adreses notiek mērķtiecīgi uzbrukumi uz internetu kādam citam interneta lietotājam Latvijā vai ārpus Latvijas. Šādos gadījumos iespējams gan, ka IP adreses īpašnieks to dara ļaunprātīgi, gan arī, ka viņa dators ir ticis uzlauzts un tiek izmantots.
   1.2. Dežurējošā administratora rīcība:–
      1.2.1. Reģistrēt incidentu *ticketing* sistēmā;
      1.2.2. Identificēt uzbrukuma cēloņus izmantojot pakalpojumu uzraudzības sistēmas (NetFlow datus, ugunsmūra datus u.c.).
      1.2.3. Sazināties ar klientu, noskaidrot, kas notiek, pieprasīt pārtraukt uzbrukumu.
      1.2.4. Ja klients nav sasniedzams, bet uzbrukums turpinās, atslēgt klienta piekļuvi XYZ999 tīklam[4]. Klienta Piekļuve XYZ999 tīklam jāatslēdz 1 stundas laikā (pēc CERT.LV pieprasījuma vai IPS iniciatīvas), neietekmējot citu lietotāju piekļuvi tīklam. Ja nepieciešams, slēgt piekļuvi uz laiku līdz 24 stundām.
      1.2.5. Ja incidents būtiski ietekmējis XYZ999 tīkla darbību (izraisot pārtraukumu vairāk kā 24 stundas) vai, ja informācija par incidentu tika saņemta no CERT.LV, informēt CERT.LV par veiktajām darbībām un problēmas risinājumu.
      1.2.6. Reģistrēt veiktās darbības *ticketing* sistēmā.
2. *Incidenta veids* - Mērķtiecīgi servisa atteices uzbrukumi (DoS, DDoS, skanēšana, ievaijonamību skanēšana) **uz** XYZ999 IP adresēm no interneta
   2.1. *Incidenta īss apraksts* – dežurējošais administrators saņem informāciju par incidentu, ja uz XYZ999 tīklu notiek mērķtiecīgi uzbrukumi (skanēšana, ievaijonamību skanēšana) no interneta
   2.2. Dežurējošā administratora rīcība:–
      2.2.1. Reģistrēt incidentu *ticketing* sistēmā;
      2.2.2. Identificēt uzbrukuma cēloņus, izmantojot pakalpojumu uzraudzības sistēmas (NetFlow datus, ugunsmūra datus u.c.).

[2] MK Noteikumi Nr. 327 punkts 2.5
[3] Biežāk sastopamie piemēri
[4] MK noteikumi Nr. 327, III nodaļa

2.2.3. Izfiltrēt datu plūsmas anomālijas uz attiecīgās iekārtas vai sazināties ar *upstream* piegādātājiem, lai veiktu datu plūsmas bloķēšanu.
2.2.4. Ja incidents būtiski ietekmējis XYZ tīkla darbību[5] (izraisot pārtraukumu vairāk kā 24 stundas) vai, ja informācija par incidentu tika saņemta no CERT.LV, informēt CERT.LV par veiktajām darbībām un problēmas risinājumu.
2.2.5. Reģistrēt veiktās darbības *ticketing* sistēmā.

3. *Incidenta veids* - Pikšķerēšana (phishing)
   3.1. *Incidenta īss apraksts* – dežurējošais administrators saņem informāciju no CERT.LV gadījumos, ja uz kādas no XYZ999 adresēm ir atklāta pikšķerēšanas lapa vai arī XYZ999 adreses kā citādi ir iesaistītas mēģinājumos izkrāpt lietotāju datus (arī pikšķerēšanas e-pasti, u.tml.) Visbiežāk šādos gadījumos datora īpašnieks par pikšķerēšanas lapām vai e-pastiem nav informēts, viņa dators ir ticis uzlauzts un tiek izmantots.
   3.2. Dežurējošā administratora rīcība:
      3.2.1. Reģistrēt incidentu *ticketing* sistēmā;
      3.2.2. Pārbaudīt, vai lapa ir aktīva, izmantojot drošu, šim nolūkam sagatavotu laboratorijas vidi, piemēram, virtuālo mašīnu, kas reizi dienā tiek atgriezta "tīrā" stāvoklī. Ja šāda laboratorijas vide nav pieejama, interneta pārlūku (piemēram, atjauninātu Firefox ar papildinājumiem NoScript+FlashBlock).
      3.2.3. Sazināties ar klientu un informēt par problēmu.
      3.2.4. Ja klients nemāk/negrib noņemt šo lapu - liegt piekļuvi šai lapai – vai nu izfiltrēt tieši lapu vai bloķēt visu IP adresi.
      3.2.5. Ja klients vēlas uzzināt papildinformāciju par iespējām uzlabot sava datora drošību, sniegt klientam CERT.LV kontaktinformāciju.
      3.2.6. Pārbaudīt žurnālfailus un sadarbībā ar klientu savākt un sniegt CERT.LV informāciju par šo kaitīgo failu izvietotājiem (IP adreses, žurnālfailu kopijas utt.)
      3.2.7. Pārbaudīt vai lapa ir noņemta, informēt CERT.LV par veiktajām darbībām.
      3.2.8. Reģistrēt veiktās darbības *ticketing* sistēmā.
4. *Incidenta veids* - Robotu tīkla komandu un kontroles centrs XYZ999 IP adrešu apgabalā
   4.1. *Incidenta īss apraksts* - dežurējošais administrators saņem informāciju gadījumos, ja uz kādas no XYZ999 IP adresēm ir atklāts kāda Robotu tīkla komandu un kontroles centrs (C&C).
   4.2. *Dežurējošā administratora rīcība:*
      4.2.1. Reģistrēt incidentu *ticketing* sistēmā
      4.2.2. Sazināties ar klientu un informēt par problēmu.
      4.2.3. Ja klients nav sasniedzams vai nevēlas noņemt kaitīgo saturu, liegt piekļuvi C&C IP adresei.
      4.2.4. Ja klients vēlas uzzināt papildinformāciju par iespējām uzlabot sava datora drošību, sniegt CERT.LV kontaktinformāciju.
      4.2.5. Pārbaudīt žurnālfailus un sadarbībā ar klientu savākt un sniegt CERT.LV informāciju par šo kaitīgo failu izvietotājiem (IP adreses, žurnālfailu kopijas utt.)

[5] MK noteikumi Nr. 327, III nodaļa

4.2.6. Informēt CERT.LV par veiktajām darbībām.
4.2.7. Reģistrēt veiktās darbības *ticketing* sistēmā.

5. *Incidenta veids* – Nodarījumi no XYZ999 IP adresēm, kuru pazīmes atbilst krimināllikumā ietverto noziedzīgo nodarījumu sastāvam un kas nav apskatīti iepriekš, piemēram, bērnu pornogrāfija.
   5.1. *Incidenta īss apraksts* - dežurējošais administrators saņem informāciju gadījumos, ja uz kādas no XYZ999 IP adresēm ir atklāta lapa ar nelegālu saturu vai notiek kāds cits noziedzīgs nodarījums. Šādos gadījumos iespējams gan, ka IP adreses īpašnieks to dara ļaunprātīgi, gan arī, ka viņa dators ir ticis uzlauzts un tiek izmantots.
   5.2. Dežurējošā administratora rīcība:–
      5.2.1. Reģistrēt incidentu *ticketing* sistēmā
      5.2.2. Sazināties ar klientu un pieprasīt noņemt nelegālo saturu.
      5.2.3. Ja klients nav sasniedzams vai nevēlas noņemt kaitīgo saturu, liegt piekļuvi kaitīgajam resursam.
      5.2.4. Pārbaudīt žurnālfailus un sadarbībā ar klientu savākt un sniegt CERT.LV informāciju par šo kaitīgo failu izvietotājiem (IP adreses, žurnālfailu kopijas utt.)
      5.2.5. Informēt tiesībsargājošās iestādes (iespējams, ka to jau ir izdarījis CERT.LV).
      5.2.6. Informēt klientu, ja tiesībsargājošās iestādes nedod citus norādījumus.
      5.2.7. Informēt avotu, kas ziņoja par incidentu (CERT.LV, NetSafe Latvia) par veiktajām darbībām un problēmas risinājumu.
      5.2.8. Reģistrēt veiktās darbības *ticketing* sistēmā

6. Rīcības plāns citu incidentu gadījumos

6.1 XYZ999 dežurējošais administrators informē CERT.LV par uzbrukumiem XYZ999 tīklam, zvanot uz +371 67085858, rakstot cert@cert.lv jebkurā diennakts laikā un rīkojas atbilstoši iekšējām instrukcijām.

6.2 XYZ999 dežurējošais administrators saņem informāciju par incidentu no kāda avota:
   6.1.1. *Dežurējošā administratora rīcība:*
   6.1.2. Reģistrēt, klasificēt incidentu un rīkoties atbilstoši iekšējai instrukcijai (iepriekš aprakstītie piemēri)
   6.1.3. Sazināties ar klientu un informēt par problēmu, dot norādījumus par problēmas novēršanu.
   6.1.4. Ja klients nav sasniedzams un incidents var nodarīt būtisku kaitējumu XYZ999 tīklam, vienas stundas laikā atslēgt klienta piekļuvi XYZ99 tīklam, uz laiku līdz 24 stundām[6].
   6.1.5. Informēt CERT.LV par veiktajām darbībām un sekot turpmākiem CERT.LV norādījumiem.
   6.1.6. Reģistrēt incidentu un veiktās darbības *ticketing* sistēmā.

6.3 XYZ999 ir parakstījis sadarbības memorandu par drošas interneta vides veidošanu un cīņu ar kriminalizēto pornogrāfiju saturošu materiālu apriti internetā.

[6] MK noteikumi Nr. 327, III nodaļa

Katru dienu dežurējošais administrators no CERT.LV saņem e-pastu par inficētajām IP adresēm un darba dienas laikā nosūta gala lietotājam informāciju uz lietotāja e-pastu, kas satur:

6.3.1 Inficētā IP adrese un/vai incidenta identifikators, TCP/IP ports, uz kuru norādītajā laikā IP adrese pieslēdzas sensoram;

6.3.2 Datorvīrusa nosaukums, ieteikumi, kā problēmu risināt;

6.3.3 Norāde, ka informācija saņemta no CERT.LV.

Informācija vienam lietotājam jāizsūta ne biežāk kā reizi 10 dienās.
Ja gala lietotājs nereaģē, IP adrese turpina parādīties inficēto IP adrešu sarakstā, dežūrējošais administrators sazinās ar gala lietotāju telefoniski un paskaidro, kā situāciju risināt un sniedz CERT.LV kontaktus, ja tas nepieciešams.

Komentāri:
-CERT.LV incidentu kategorijas, prioritātes un reaģēšanas laiks pieejams CERT.LV tīmekļa vietnē (http://www.cert.lv/section/show/90)
-Aprakstot reaģēšanas kārtību uz IT incidentiem, jāapraksta sadarbība starp dažādām uzņēmuma struktūrvienībām vai darbiniekiem, ja tāda nepieciešama.

6. Elektroniskā sakaru tīkla darbības atjaunošanas plāns[7]

6.1. Centrālo punktu bojājumu novēršanas laiks 4 stundas, aktīvās aparatūras atbalsta pakalpojums paredz bojātās aparatūras nomaiņu 4 stundu laikā.

6.2. Mezglu punktu bojājumu novēršanas laiks 8 stundas, aktīvās aparatūras rezerves tiek uzglabātas noliktavā.

6.3. Līgumos ar klientiem atrunāts pakalpojumu pieejamības līmenis (SLA).

6.4. *Dežurējošā administratora rīcība, lai atjaunotu piekļuvi XYZ999 tīklam pēc IT drošības incidenta:*

6.4.1. Sazināties ar klientu un saņemt apstiprinājumu, ka problēma novērsta. noskaidrot kādas darbības tika veiktas problēmas novēršanai.

6.4.2. Pieslēgt piekļuvi XYZ999 tīklam pēc laika posma, kāds norādīts CERT.LV pieprasījumā (ja tāds bijis norādīts), bet ne vēlāk kā 24 stundas kopš atslēgšanas.

6.4.3. Informēt CERT.LV par veiktajām darbībām.

6.4.4. Ja klients vēlas uzzināt papildinformāciju par iespējām uzlabot sava datora drošību, sniegt CERT.LV kontaktinformāciju.

6.5. Par citiem apstākļiem, kas izraisījuši elektronisko sakaru tīkla pārtraukumu izstrādātas iekšējās instrukcijas:

- 6.1.1 Darbinieku rīcība ugunsgrēka gadījumā Centrālajos punktus, Mezglu Punktos;
- 6.1.2 Darbinieku rīcība applūšanas gadījumā Centrālajos punktus, Mezglu Punktos;
- 6.1.3 Darbinieku rīcība, lai novērstu aktīvās aparatūras bojājumu (fiziskos un programmatūras) Centrālajos punktus, Mezglu Punktos;
- 6.1.4 Darbinieku rīcība, lai novērstu Pasīvās infrastruktūras bojājumu XYZ999 tīklā, Centrālajos punktos, Mezglu Punktos;

6. Nobeigums

Vienu reizi gadā Rīcības Plāns tiek pārskatīts un aktualizēts. Izmaiņas tiek noformētas un nosūtītas CERT.LV 1 mēneša laikā.

[7] MK Noteikumi Nr. 327 punkts 2.6