Latvijas Universitātes
Matemātikas un informātikas institūts

CERT.LV
Informācijas tehnoloģiju
drošības incidentu
novēršanas institūcija

LATVIJAS REPUBLIKAS
AIZSARDZĪBAS MINISTRIJA

Informācijas tehnoloģiju drošības rekomendācijas valsts un pašvaldību iestādēm

2014

CERT.LV šīs rekomendācijas ir izstrādājis, apvienojot SANS institūta (www.sans.org) izstrādātās Kritiskās drošības kontroles (licencētas saskaņā ar Creative Commons Attribution-NoDerivs 3.0 Unported License) un CERT.LV darbinieku pieredzi, strādājot ar Latvijas Republikas valsts un pašvaldību iestādēm.

Valsts un pašvaldību iestādēm ir atšķirīgs informācijas drošības līmenis, tādēļ katrai kontrolei aprakstīti sākotnējie ieviešanas soļi, ko ieteicams izdarīt, gatavojoties Latvijas republikas prezidentūrai Eiropas Savienībā. Ja tie ieviesti, iesakām apmeklēt http://www.sans.org/critical-security-controls , lai turpinātu uzlabot iestādes drošību.

Iestāde aktīvi pārvalda visas iekārtas tīklā, atļaujot piekļuvi tikai autorizētām iekārtām

- Regulāri veic iestādes (IT) iekārtu inventarizāciju (piemēram, izmantojot iekārtu monitoringa programmatūru). Ieteicams izmantot gan aktīvus rīkus (programmatūru), kas skenē tīkla adrešu diapazonu, gan pasīvus rīkus, kas identificē iekārtas, analizējot to datu plūsmu.
- Nodrošina procesu, kura rezultātā tīklam var pieslēgt tikai tās no jauna iegādātās ierīces, kuras tiek apstiprinātas.
- Ja tiek izmantots DHCP (Dynamic Host Configuration Protocol), ievieš DHCP servera auditācijas pierakstu procesu, tajā skaitā, izmantojot DHCP informāciju iekārtu inventarizācijas informācijas aktualizēšanai.
- Ievieš standarta nosaukumu veidošanu iestādes gala iekārtām.

Noderīgas saites:

http://nmap.org/book/man-host-discovery.html
http://www.sans.org/critical-security-controls/control/1

Iestāde aktīvi pārvalda visu programmatūru tīklā, pieļaujot tikai autorizētu programmu uzstādīšanu un darbināšanu

- Nosaka iestādē atļautās programmatūras sarakstu (piemēram, izmantojot programmatūras inventarizācijas risinājumus un grupas politikas nosacījumus programmatūras un izpildāmo failu baltajiem sarakstiem). Saraksts jāveido pietiekami plašs, lai ļautu lietotājiem veikt darba pienākumus. Iestāde nodrošina arī atļautās programmatūras saraksta uzturēšanu un atjaunināšanu.
- Atļautās programmatūras (un to atļautās versijas) sarakstu uztur katram iekārtu tipam (darbstacijām, serveriem) un nodrošina šī saraksta integritāti.
- Veic regulāru iekārtu skenēšanu ar mērķi atklāt neatļautas programmatūras izmantošanu.
- Ievieš un ievēro striktu programmatūras izmaiņu ieviešanas procesu.

Noderīgas saites:

http://whitelist.kaspersky.com/
https://browsercheck.qualys.com/
http://www.splunk.com/
http://www.sans.org/critical-security-controls/control/2

Iestāde nosaka un aktīvi pārvalda portatīvo datoru, serveru, maršrutētāju, galiekārtu un citu izmantoto iekārtu drošu konfigurāciju

- Ievieš un izmanto iestādes standarta operētājsistēmu drošās konfigurācijas (piemēram, izmantojot pieejamās attiecīgo ražotāju rekomendācijas). Veido standarta diska attēlus ar nodrošinātām sistēmām un izmantotām aplikācijām (t.sk. nevajadzīgo kontu noņemšana, nevajadzīgo pakalpojumu noņemšana, atjauninājumu uzlikšana, nelietoto tīkla portu slēgšana).
- Ievieš automātiskus atjauninājumu uzlikšanas rīkus un procesus gan aplikācijām, gan operētājsistēmām. Dzēš nevajadzīgu un novecojušu programmatūru no sistēmām.
- Ierobežo administratora tiesības minimāli nepieciešamajam cilvēku skaitam.
- Ievieš un ievēro stingru konfigurēšanas pārvaldību, izveidojot drošu attēlu, ko izmanto visām jaunām sistēmām. Jebkuru kompromitētu sistēmu atjauno no drošā attēla.
- Drošos attēlus uzglabā drošā vietā, nodrošinot regulāru integritātes pārbaudi (piemēram, glabā tos tīklam nepieslēgtās iekārtās, nepieciešamības gadījumā kopējot).

Noderīgas saites:

http://www.cisecurity.org/
http://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/
http://www.microsoft.com/en-us/download/details.aspx?id=7558
http://www.sans.org/critical-security-controls/control/3
http://www.sans.org/critical-security-controls/control/10

Iestāde seko līdzi informācijai par ievainojamībām un pēc iespējas ātrāk tās novērš

- Regulāri sistēmām izmanto automātiskos ievainojamību skenēšanas rīkus, kritiskāko ievainojamību informāciju nododot atbildīgajam sistēmas administratoram.
- Pārskata žurnālfailu ierakstus, korelējot tos ar ievainojamību skenēšanas rezultātiem, lai pārliecinātos, vai tajos uzrādās skenēšanas aktivitātes, kā arī uzbrukuma gadījumā būtu iespējams noskaidrot, vai izmantota zināma ievainojamība.
- Pierakstās uz ievainojamību izpētes un apziņošanas resursiem.

Noderīgas saites:

https://nvd.nist.gov/SCAP-Validated-Tools/
https://cert.lv/rss/viruses.xml
https://cert.lv/rss/attacks.xml
http://www.sans.org/critical-security-controls/control/4

Iestāde nodrošina aizsardzību pret ļaunatūru (malware)

- Izveido un attīstīta antivīrusa, anti-spiegošanas programmatūru, ugunsmūrus, IPS rīkus, kas nepārtraukti uzrauga darbstacijas, serverus, mobilās iekārtas.
- Konfigurē darbstacijas un serverus, lai tie automātiski nepalaiž saturu no pārvietojamiem datu nesējiem.
- Konfigurē sistēmas, lai anti-ļaunatūras skenēšana notiktu automātiski pārvietojama datu nesēja pievienošanas gadījumā.
- Skenē un nepieciešamības gadījumā bloķē e-pastu pielikumus, ja tie neatbilst iestādes drošības prasībām.
- Ierobežo un uzrauga ārējo iekārtu (t.i. tādas iekārtas, kas nav iestādes īpašumā vai lietošanā) lietošanu vai lietošanas mēģinājumus.

Noderīgas saites:

http://www.microsoft.com/security/pc-security/malware-removal.aspx
http://www.sans.org/critical-security-controls/control/5

Iestāde nodrošina izstrādātās vai pielāgotās lietojumprogrammatūras drošības pārvaldību

- Iestrādā labākās prakses drošības prasības jau programmatūras projektējuma dokumentācijā. Pārbauda, vai visas izmantotās lietojumprogrammas to izstrādātājs joprojām uztur. Lietojumprogrammām uztur jaunāko versiju un uzstāda izstrādātāja ieteiktos drošības atjauninājumus.
- Ievieš tīkla aplikāciju ugunsmūrus (WAF).

Noderīgas saites:

https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
http://samurai.inguardians.com/
http://www.sans.org/critical-security-controls/control/6

Iestāde uzrauga un kontrolē tās izmantotos bezvadu tīkla risinājumus

- Pārliecinās, vai katra pieslēgtā bezvadu tīkla ierīce atbilst apstiprinātajai konfigurācijai ar dokumentētu īpašnieku un darba nepieciešamību. Ierīcēm, kas neatbilst iepriekšminētām prasībām, jāliedz piekļuve tīklam.
- Veic regulāru bezvadu piekļuves punktu inventarizāciju, nepieļaujot neapstiprinātu piekļuves punktu darbību tīklā (piemēram, izmantojot tīkla skenēšanas risinājumus).
- Ievieš un uztur bezvadu ielaušanās atklāšanas sistēmas (WIDS), lai identificētu nevēlamās iekārtas un uzbrukuma mēģinājumus.

Noderīgas saites:

http://www.wireshark.org/
https://www.kismetwireless.net/
http://www.stumbler.net/
http://www.sans.org/critical-security-controls/control/7

Iestāde izmanto un regulāri pārbauda piemērotus rezerves kopēšanas risinājumus būtiskai informācijai

- Nodrošina katrai sistēmai automātisku un regulāru (vismaz reizi nedēļā) rezerves kopiju veidošanu. Rezerves kopēšana svarīgajām sistēmām jāveic gan operētājsistēmai, gan lietojumprogrammām un lokālajiem datiem.
- Saglabā vairākas dažādu laiku rezerves kopijas, lai nodrošinātu iespēju atjaunot sistēmu infekcijas gadījumā.
- Veic regulāru rezerves kopiju testēšanu.

Noderīgas saites:

http://www.sans.org/critical-security-controls/control/8

Iestāde novērtē informācijas drošības pārvaldībā iesaistīto darbinieku zināšanas un prasmes un pastāvīgi tās pilnveido un uzlabo

- Izvērtē atbildīgo darbinieku zināšanas un prasmes un izveido attiecīgu mācību programmu.
- Izmanto iestādes iekšējos resursus, lai veiktu darbinieku apmācību.
- Ievieš vispārējo informācijas drošības programmu lietotājiem un nodrošina visu darbinieku apmācību vismaz reizi gadā.

Noderīgas saites:

http://www.cert.lv/section/show/85
https://www.enisa.europa.eu/media/multimedia/material
http://www.sans.org/critical-security-controls/control/9

Iestāde ierobežo un kontrolē tās tīkla iekārtu portus, protokolus un pakalpojumus

- Nodrošina, lai sistēmā darbojas tikai tie porti, protokoli un pakalpojumi, kas nepieciešami iestādes darba vajadzībām.
- Pielieto „*default deny*" likumu gala sistēmām, kas atļauj tikai to datu plūsmu, kas īpaši atļauta (izmantojot, piemēram, galiekārtu ugunsmūrus vai portu filtrāciju).
- Veic regulāru automātisku protu skenēšanu svarīgākajiem serveriem.
- Uztur aktuālus pakalpojumus un noņemt nevajadzīgās sistēmas komponentes.

Noderīgas saites:

http://nmap.org/
http://www.sans.org/critical-security-controls/control/11

Iestāde kontrolē administratora tiesību izmantošanu visās iekārtās un sistēmās

- Minimizē administratīvās tiesības un izmanto tās tikai tad, kad nepieciešams.
- Auditē visas administratīvās darbības.
- Nodrošina, ka administratoru paroles atbilst drošības prasībām (piemēram, pietiekams garums, simboli, burti un cipari, regulāra maiņa).
- Ieviešot jaunas sistēmas, nomaina noklusētās (ražotāja) paroles.
- Paroles glabā ar jaucējfunkciju vai šifrētas.

Noderīgas saites:

http://csrc.nist.gov/publications/nistpubs/800-132/nist-sp800-132.pdf
http://www.sans.org/critical-security-controls/control/12

Iestāde aizsargā savu ārējo IT robežu

- Bloķē piekļuvi ļaundabīgām internet adresēm (*blacklist*) vai atļauj piekļuvi tikai noteiktām adresēm (*whitelist*). Ieteicams izmantot *Whitelist* principu.
- Ievieš tīkla DMZ uzraudzību (piemēram, IDS sensori).

Noderīgas saites:

http://www.snort.org/
http://communities.alienvault.com/community
http://www.sans.org/critical-security-controls/control/13

Iestāde uztur un regulāri pārskata žurnālfailu ierakstus

- Ietver vismaz divus sinhronizētus laika avotus (piemēram, NTP) no kuriem visi serveri un tīkla aparatūra saņem laika informāciju, lai laika zīmogs visiem žurnālfailu ierakstiem būtu vienāds (+ UTC).
- Pārbaudīt, vai visiem žurnālfailiem ir pieejams datums, laika zīmogs, avota adrese, mērķa adrese. Vēlams žurnālfailus uzkrāt standarta formātā.
- Nodrošināt pietiekamu uzglabāšanas vietu žurnālfailu datiem, kā arī nodrošināt to arhivēšanu.
- Regulāri pārskata žurnālfailus, lai atklātu anomālijas vai aizdomīgas darbības.

Noderīgas saites:

http://www.ossec.net/
http://www.sans.org/critical-security-controls/control/14

Iestāde nodrošina, ka tās kritiskajiem resursiem piekļūst tikai noteikts darbinieku skaits, kam tas tiešām nepieciešams darba pienākumu veikšanai

- Iestādei jānosaka tās kritiskie un aizsargājamie resursi (piemēram, ierobežotas pieejas informācija, serveru telpa) un jānodrošina tiem atbilstoša uzglabāšana vai aizsardzība.
- Ierobežotas pieejamības informāciju publiskajos tīklos pēc iespējas pārsūta šifrētā veidā.

Noderīgas saites:

http://www.sans.org/critical-security-controls/control/15
http://en.wikipedia.org/wiki/Pretty_Good_Privacy

Iestāde pārvalda sistēmu un programmatūras lietotāju kontus

- Regulāri veic sistēmas lietotāju kontu inventarizāciju un izdzēš tos, kas nav nepieciešami iestādes darbībai.
- Nodrošina, ka visiem kontiem ir noteikti derīguma termiņi.
- Nodrošina, ka visas sistēmas automātiski uzskaita informāciju par kontiem (piemēram, atslēgtie konti, konti kam nav mainītas paroles).
- Uzraudzīt lietotāja kontu darbību, atslēdzot lietotājus pēc standarta bez aktivitātes perioda.

Noderīgas saites:

http://www.sans.org/critical-security-controls/control/16

Iestāde aizsargā tās rīcībā esošos sensitīvos datus

- Nepieciešamības gadījumā ieviest cietā diska šifrēšanu mobilām ierīcēm un sistēmām, kas satur sensitīvus datus.
- Pārskata ārpakalpojumu datu uzglabāšanas drošības nosacījumus.

Noderīgas saites:

https://www.enisa.europa.eu/media/news-items/cloud-computing-speech
http://www.sans.org/critical-security-controls/control/17

Iestāde nosaka un īsteno drošības incidentu pārvaldības procesu

- Nodrošina, ka iestādē ir noteikta rakstiska incidentu apstrādes procedūra, ieskaitot personāla atbildību incidentu risināšanā.
- Sakārto un uztur aktuālu nepieciešamo kontaktinformāciju (trešās puses, interneta pakalpojumu sniedzējs, mājas lapas uzturētājs, citas valsts iestādes), kas nepieciešama incidentu risināšanā.
- Informē lietotājus/personālu par nepieciešamām darbībām IT anomāliju vai incidenta paziņošanai.
- Apstrādā CERT.LV brīdinājumus par incidentiem un ziņo par darbībām incidentu novēršanai un risku mazināšanai.

Noderīgas saites:

http://www.sans.org/critical-security-controls/control/18

Iestāde izveido drošu tīkla arhitektūru

- Sadala tīklu drošības zonās, piemēram, izveidojot DMZ, proxy un privātā tīkla zonu.
- Uztur aktuālu tīkla diagrammu.
- Nodrošina, ka sistēmas ar sensitīviem datiem atrodas privātā tīkla zonā.

Noderīgas saites:

http://www.nagios.org/
http://www.sans.org/critical-security-controls/control/19

Iestāde pārbauda savu aizsardzības līmeni (IT, procesi, cilvēki)

- Veic regulārus ielaušanās testus (gan iekšējos, gan ārējos).
- Uzrauga kontus, kas tiek izmantoti testiem, un reģistrē visas veiktās darbības žurnālfailos.

Noderīgas saites:

http://www.sans.org/critical-security-controls/control/20