SIA STALLION

Kaspars Fišers
Ivans Aļošins

kaspars.fisers@stallion.lv
ivan.alyoshin@stallion.lv

2016

www.stallion.lv

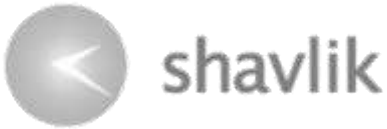
Par uzņēmumu

- Stallion - informācijas un komunikāciju sistēmu drošības risinājumu veidošana, piegāde un apkalpošana
- Stallion birojs darbojas Tallinā kopš 1997. gada un Rīgā kopš 2008. gada

Risinājumi ko mēs piedāvājam

- Tīkla Drošības risinājumi (Ugunsmūri , VPN , ielaušanās novēršanas sistēmas, Web Aplikāciju Ugunsmūri, Drošības Web vārtejas , Antispam risinājumi);
  Palo Alto Networks, Sophos, IMPERVA, CISCO, Blue Coat
- Darbstaciju un serveru drošības risinājumi (Antiviruss , ierīču kontrole, aplikāciju kontrole , disku šifrēšana , datu noplūdes novēršana);
  Sophos, Kasperky LAB
- Ievainojamības un ielāpu vadības risinājumi;
  Qualys, HEAT Software
- Log vadības un SIEM risinājumi;
  Splunk, IBM Qradar
- Aplikāciju piegāde kontrolieru un DDoS aizsardzības risinājumi;
  A10, F5 Networks
- Mobilo iekārtu drošības risinājumi;
  Sophos, Kaspersky LAB
- Divu faktoru autentifikācijas (2FA) risinājumi;
  RSA, VASCO
- Priviliģētās identitātes pārvaldība (PIM);
  CyberArk
- Konsultāciju un integrācijas pakalpojumi

Mūsu partneri



Mūsu klienti

RĪGAS DOME

JELGAVAS DOME

LATVIJAS BANKA

DNB

Jānis Roze

aizdevums.lv
IESPĒJA PĀRMAIŅĀM

SMARTLYNX

RĪGAS SATIKSME

LIAA

TSI
TRANSPORTA UN SAKARU INSTITŪTS

Informācijas tehnoloģiju drošības likums

- **Likuma mērķis** ir uzlabot informācijas tehnoloģiju drošību, nosakot svarīgākās prasības, lai garantētu tādu būtisku pakalpojumu saņemšanu, kuru sniegšanai tiek izmantotas šīs tehnoloģijas.

Informācijas tehnoloģiju drošības likums

- **6.pants. Rīcība informācijas tehnoloģiju drošības incidenta gadījumā**
- (2) Valsts vai pašvaldības institūcija, informācijas tehnoloģiju kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs drošības incidenta gadījumā nekavējoties veic visas tā novēršanai nepieciešamās darbības (it īpaši izpilda Drošības incidentu novēršanas institūcijas rekomendācijas par vēlamo sākotnējo rīcību drošības incidenta gadījumā), kā arī tūlīt informē par notikušo Drošības incidentu novēršanas institūciju. Drošības incidentu novēršanas institūcija vienojas ar drošības incidenta pieteicēju par atbalsta sniegšanu drošības incidenta novēršanā.
- **6.[1] pants. Rīcība informācijas tehnoloģiju drošības nepilnības konstatēšanas gadījumā**
- (1) Informācijas tehnoloģiju drošības nepilnība (turpmāk — drošības nepilnība) ir būtiska informācijas sistēmas vai elektronisko sakaru tīkla izveides, uzturēšanas vai pārveidošanas gaitā tīši vai nejauši radīta sistēmiska vājība, kuras rezultātā var tikt apdraudēta informācijas tehnoloģiju integritāte, pieejamība vai konfidencialitāte.
- (2) Valsts vai pašvaldības institūcija, informācijas tehnoloģiju kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs, konstatējis drošības nepilnību, 90 dienu laikā veic visas tās novēršanai nepieciešamās darbības, kā arī par konstatēto tūlīt informē Drošības incidentu novēršanas institūciju.
- (3) Drošības incidentu novēršanas institūcija, konstatējusi drošības nepilnību, par šo faktu tūlīt informē informācijas sistēmas vai elektronisko sakaru tīkla īpašnieku vai tiesisko valdītāju. Valsts vai pašvaldības institūcija, informācijas tehnoloģiju kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs Drošības incidentu novēršanas institūcijas noteiktajā termiņā, bet ne vēlāk kā 90 dienu laikā kopš informēšanas brīža veic visas drošības nepilnības novēršanai nepieciešamās darbības.,

SIA STALLION piedāvātie risinājumi lai nodrošinātu informācijas un tehnoloģiju sistēmu atbilstību minimālajām drošības prasībām

- **Sistēmas drošībai īsteno pasākumu kopumu, lai:**
- 5.3. nodrošinātu informācijas konfidencialitāti (informācijas nodošanu tikai tām personām, kuras ir pilnvarotas to saņemt un lietot); Sophos E-pastu šifrēšana
- 5.5. aizsargātu sistēmas tehniskos resursus (datorus, programmatūru, datu nesējus, datortīkla iekārtas un citas tehniskās iekārtas, kuras nodrošina sistēmas darbību); Sophos
- 5.6. noteiktu sistēmas drošības apdraudējumu (ar nodomu (tīši) vai aiz neuzmanības izdarītu darbību vai notikumu, kas var izraisīt sistēmas informācijas vai tehnisko resursu izmaiņas, bojājumu, iznīcināšanu vai nonākšanu tādu personu rīcībā, kuras nav tam pilnvarotas, vai kura dēļ piekļūšana sistēmas informācijas resursiem var būt traucēta vai neiespējama); Sophos
- 5.7. novērtētu sistēmas drošības risku; Qualys
- 5.8. atklātu sistēmas drošības incidentu; Splunk

SIA STALLION piedāvātie risinājumi lai nodrošinātu informācijas un tehnoloģiju sistēmu atbilstību minimālajām drošības prasībām

- **Izstrādājot sistēmas drošības politiku, paredz, ka:**
- 15.2. katrs lietotāja konts ir saistīts ar konkrētu fizisko personu. Ja sistēmā tiek izmantoti konti, kas nav piesaistāmi konkrētai fiziskai personai (turpmāk – sistēmkonti), tad sistēmā jābūt iestrādātiem tehniskiem līdzekļiem, kas novērš iespēju lietotājiem izmantot sistēmkontus; CyberArk
- 15.3. ja sistēmā netiek izmantota daudzfaktoru autentifikācija, tas ir, viens atribūts, kam nav statiska daba (piemēram, kodu kalkulators, vienreiz lietojams īsziņas kods), un vismaz viens cits atribūts, tad sistēmas lietotājiem obligāti jālieto paroles; 2FA – RSA, VASCO
- 15.4. sistēmas lietotāja paroles garums nav mazāks par deviņiem simboliem un satur vismaz vienu lielo latīņu alfabēta burtu, mazo latīņu alfabēta burtu, ciparu un speciālu simbolu; Qualys, Cyberark DNA
- 15.5. sistēmas lietotāja paroles aizliegts elektroniski glabāt un transportēt nešifrētā veidā, arī lietotāja autentifikācijas procesa ietvaros, izņemot šo noteikumu 15.7. apakšpunktā minēto gadījumu; Sophos E-pastu šifrēšana
- 15.7. sistēmas lietotāja parole, kas nosūtīta publiskā datu pārraides tīklā nešifrētā veidā, ir lietojama vienu reizi un derīga ne ilgāk kā 72 stundas pēc tās nosūtīšanas; Sophos E-pastu šifrēšana
- 15.11. jebkura piekļuve sistēmai ir izsekojama līdz konkrētam sistēmas lietotāja kontam vai interneta protokola (IP) adresei; Sophos ugunsmūris
- 15.12. sistēmai jābūt uzliktiem visiem pieejamiem programmatūras atjauninājumiem, iepriekš izvērtējot to nepieciešamību; Qualys ievainojamības kontroles sistēma
- 15.13. visās institūcijas valdījumā esošajās galalietotāju iekārtās, kas ikdienā tiek izmantotas, lai pieslēgtos sistēmai, jābūt iekļautai pretvīrusu funkcionalitātei; Sophos antivīruss
- 18. Institūcija nodrošina, ka pirms jaunas sistēmas pieņemšanas ekspluatācijā tai ir veikti ielaušanās testi. Ielaušanās testus veic juridiska persona vai institūcijas darbinieki, kuri nav piedalījušies sistēmas izstrādē. Qulays WEB aplikāciju skanēšana

SIA STALLION piedāvātie risinājumi lai nodrošinātu informācijas un tehnoloģiju sistēmu atbilstību minimālajām drošības prasībām

- **Prasības paaugstinātas drošības sistēmām**
- 24.4. ar sistēmas administratora kontu piekļūt sistēmai, izmantojot iekārtas, kas atrodas ārpus iestādes telpām, kā arī iekārtas, kas neatrodas iestādes valdījumā, iespējams, tikai izmantojot daudzfaktoru autentifikāciju; 2FA – RSA, VASCO
- 24.6. tiek nodrošināta sistēmas pierakstu veidošana un uzglabāšana vismaz 18 mēnešus pēc ieraksta izdarīšanas, uzglabājot sistēmas pierakstus vai to kopijas atsevišķi no sistēmas; Splunk Enterprise
- 24.8. tiek nodrošināta sistēmas pierakstu satura plānveida uzraudzība un analīze, lai konstatētu incidentus; Splunk Enterprise
- 24.10. plūsma starp sistēmu un tās lietotājiem, kā arī starp sistēmu un citām sistēmām tiek kontrolēta, piemēram, izmantojot ugunsmūri; Sophos ugunsmūris

Informācijas resursi:

Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām, **Ministru kabineta noteikumi Nr. 442** , http://likumi.lv/ta/id/275671-kartiba-kada-tiek-nodrosinata-informacijas-un-komunikacijas-tehnologiju-sistemu-atbilstiba-minimalajam-drosibas-prasibam

Informācijas tehnoloģiju drošības likums, http://likumi.lv/doc.php?id=220962

CERT.LV - Pašvaldību un valsts iestāžu IT drošības noteikumu vadlīnijas, https://www.cert.lv/uploads/Iest%C4%81d%C4%93m/noteikumi20111011web.pdf