Atbildīga ievainojamību atklāšana: ziņot vai neziņot?

Agris Krusts, SIA IT Centrs
13.12.2016

Daži vārdi ievadam

Procesa ieviešana ir apsveicama, bet …..

Kas ir atbildīga ievainojamību atklāšana?

Aizsardzības ministrija

Kas ir atbildīga ievainojamību atklāšana?

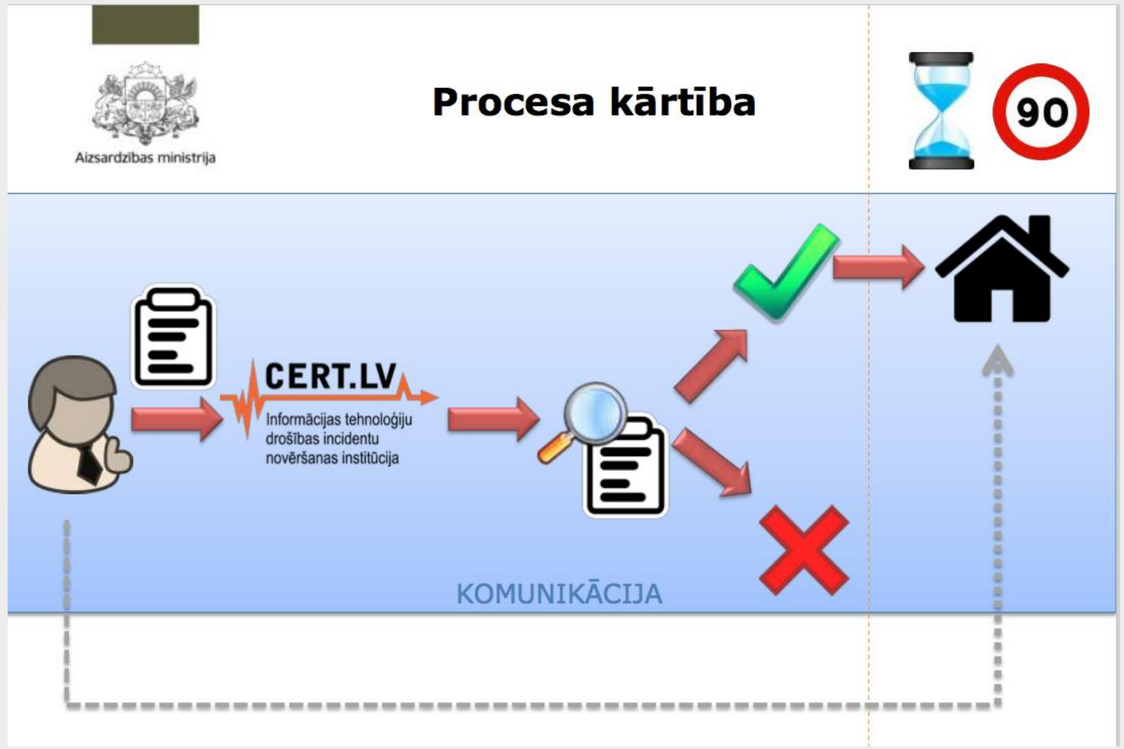
Iesaistītās puses

1)Resursu turētāji

2) Pētnieki, ētiskie hakeri, lietotāji

Procesa elementi

1) Ziņošana
2) Koordinācija
3) Novēršana
4) Publiskošana



No Ievas Ilvesas prezentācijas CERT.LV IT drošības seminārā «Esi drošs», 2016.gada 26.aprīlī

Problēmas procesā – aizmirstie likumi

Krimināllikumā šobrīd nav izmaiņu:

241.pants. Patvaļīga piekļūšana automatizētai datu apstrādes sistēmai

244’ pants. Datu, programmatūras un iekārtu iegūšana, izgatavošana, izmainīšana, glabāšana un izplatīšana nelikumīgām darbībām ar elektronisko sakaru tīklu galiekārtām

200.pants. Neizpaužamu ziņu, kas nav valsts noslēpums, izpaušana, komercnoslēpumu saturošu ziņu neatļauta iegūšana un izpaušana un finanšu tirgus iekšējās informācijas nelikumīga izpaušana

Varbūt vēl kāds?

Sola atbrīvot no KL tikai nesvarīgām sistēmām

Problēmas procesā – aizmirstie likumi likumi

Kā būs ar FPDAL un ES datu aizsardzības regulu 2016/679?

Vai paredzētas izmaiņas Stratēģiskas nozīmes preču aprites likumā?

Kā ir ar Elektronisko sakaru likumu?

Varbūt vēl kāds?

Par kādām problēmām vērts ziņot?

SSL konfigurācijas nepilnības

Bīstamu failu augšupielāde

“500 Internal server” kļūdas

Daži neuzstādīti sīkdatnes parametri vai galvenes (headers)

Pie “logout”:

Set-Cookie: _mb_session=6a28e12a69dd3ff1a11f8e8b94d4ee10; domain=.manabalss.lv; path=/; expires=Sun, 11 Dec 2016 18:37:40 -0000; HttpOnly

Pēc veiksmīgas autentifikācijas

Set-Cookie: _mb_session=6a28e12a69dd3ff1a11f8e8b94d4ee10; domain=.manabalss.lv; path=/; expires=Sun, 11 Dec 2016 18:38:30 -0000; HttpOnly

Ko jūs domājat par šāda veida autorizācijas mehānismu?

https://manidati.lv/dati/138aa010-2213-4cbf-9d49-aa29b327d52e

Izpratne par riskiem un drošību

Regulāras diskusijas ar valsts pārvaldes klientiem par ievainojamībām piešķirto risku līmeni

- Privātajā sektorā dažreiz klienti lūdz paaugstināt riska līmeni

Izstrādātāju izpratne par drošu lietojumu izstrādi

- Ik pa laikam atbildes: “Nepiekrītam” un līdzīgas
- Vai ”logout” neesamība ir drošības problēma
- Pēdējos gados nespēja novērst problēmu ar pirmos vai otro mēģinājumu

Novēršana 90 dienu laikā

Dažreiz novērš vienas dienas laikā brīvdienās

Kritiskas problēmas nevar novērst gadiem:

- SQL injekcijas
- OS komandu izpilde
- Autentifikācijas apiešana
- Informācijas noplūdes

Kas ir minimālie pierādījumi?

“Bling SQL” injekcijas

Starpvietņu skriptēšana starp sistēmām

Personu dati un komercnoslēpums un “minimālie pierādījumi”

Prasības pierādījumu glabāšanai?

Darbības traucējumi pierādījumu vākšanas laikā

Ko Windows programma “domās” par failu ar nosaukumu

Mans\kredīta\ieteikums.docx?

Ar pieredzi arī ir dažādi

Slikts piemērs

“atbildīgās ziņošanas”

reklāmai

Aizsardzības ministrija

Pieredze Latvijā

- Swedbank
- Vairāki atsevišķi gadījumi CERT.LV pieredzē:
  - Valmieras pašvaldības hakatons
  - Banku autentifikācija
  - Vairākas valsts un pašvaldību mājas lapas un informācijas sistēmas
  - Mobilās lietotnes
  - «Rīgas satiksmes» mobilā lietotne

No Ievas Ilvesas prezentācijas CERT.LV IT drošības seminārā «Esi drošs», 2016.gada 26.aprīlī

Tad ziņot vai neziņot?

Vai izstrādātāji ir ieinteresēti ievainojamību atklāšanā?

Ieteikumi procesa uzlabošanai

Visticamāk izmaiņas KL nebūs pietiekamas

Varbūt vajag sistēmu sarakstu kurās drīkst “atrast” problēmas?

Noderētu detalizētākas prasības par pierādījumu vākšanu un glabāšanu un atklājēja atbildību

Jāsaprot ko darīt, ja problēmu nevarēs novērst

Paldies par uzmanību!

Jautājumi un diskusija

Agris Krusts

E-pasts: Agris.Krusts@itcentrs.lv

Tālr. +371 29151412

Twitter: @agris_krusts