2015. gada 11. oktobra *versija 0.81*

Atbildīgas ievainojamību atklāšanas politika (RDP)

materiāls mērķa grupu sākotnējai iesaistei

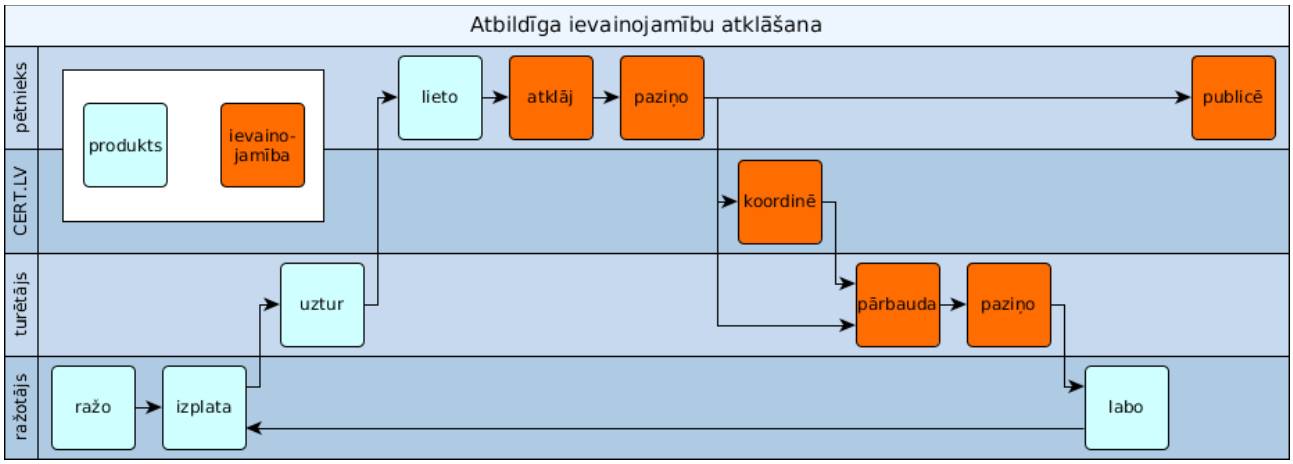
Mg. sc. comp. Kirils Solovjovs,
IT drošības eksperts

Pieaugot informācijas tehnoloģiju un sistēmu lietojumam un to nozīmei sabiedrības ikdienā, kiberdrošības jautājumi iegūst arvien lielāku aktualitāti. Būtiska kiberdrošības apdraudējuma daļa izriet no informācijas tehnoloģiju drošības nepilnībām jeb ievainojamībām. To pastiprina arī tas, ka Informācijas tehnoloģiju drošības likums 2015. gada sākumā ir ticis papildināts[1] ar prasībām, kas nosaka rīcību informācijas tehnoloģiju drošības nepilnības konstatēšanas gadījumā.

Sistemātiska ievainojamību atklāšana ir ļoti dārgs process, jo prasa liela skaita augsti kvalificētu speciālistu laika ieguldījumu. Ņemot vērā Latvijas cilvēkresursu situāciju un fiskālo telpu, sistemātiska ievainojamību atklāšana valsts līmenī šobrīd nav iespējama, tāpēc ir jāizmanto citi risinājumi mērķa sasniegšanai.

Arī oportūnistiska ievainojamību atklāšana spēj dot redzamu ieguldījumu drošības situācijas uzlabošanā. Informācijas tehnoloģiju drošības entuziasti visā pasaulē, tajā skaitā Latvijā, dažādu mērķu vadīti meklē un atrod ievainojamības publiski pieejamās informācijas sistēmās. Viņu motivācija ir ļoti plaša – sākot no iespējas gūt atzinību vai atlīdzību līdz pat vēlmei uzlabot kopējo drošību Interneta vidē un pienākuma apziņai pārliecināties, ka informācijas sistēma, kas glabā viņu datus, ir pietiekami droša.

Atbildīgas ievainojamību atklāšanas (*responsible disclosure*) politika ir ietvars, kas apraksta kārtību, kādā sabiedrības locekļi var ziņot par informācijas sistēmās atrastajām ievainojamībām, nosaka tiesības un pienākumus iesaistītajām pusēm, nodrošina pušu tiesisko aizsardzību, kā arī veicina arvien plašāku atbildīgas ievainojamību atklāšanas procesa pielietošanu. RDP veicina to, ka jebkurš drošības pētnieks vai lietotājs var ziņot par atrastajām ievainojamībām informācijas sistēmās, produktos vai pakalpojumos, aicinot informācijas sistēmas turētāju novērst identificētās nepilnības. Parasti uzņēmums vai valsts iestāde paziņo par savu vēlmi piedalīties atbildīgas ievainojamību atklāšanas procesā, publicējot RDP savā mājaslapā.



1 http://likumi.lv/ta/id/272268

RDP šobrīd īsteno galvenokārt globālās korporācijas, taču ir vairākas valstis, piemēram, Nīderlande, kur šāda politika tiek izmantota arī valsts un pašvaldību iestāžu līmenī. Tas neprasa papildus resursus no valsts puses, ļaujot izmantot sabiedrībā apslēptās prasmes un talantus, kā arī veicina sabiedrības iesaisti drošākas virtuālās telpas veidošanā.

Lai nodrošinātu RDP izstrādi un ieviešanu Latvijā, ir nepieciešama priekšizpēte, veicot informācijas apmaiņu ar vairākām mērķa grupām, kuru darbu vai ikdienu tieši ietekmēs RDP ieviešana. Šīs mērķa grupas ir: potenciāli ievainojamo informācijas sistēmu turētāji (gan valsts iestādes, gan privātas juridiskas personas), VP GKrPP ENAP 4.N[2], prokuratūra, Tieslietu ministrija un drošības ievainojamību pētnieki.

Zemāk ir aprakstītas tēzes, ko nepieciešams skaidrot katrai no mērķa grupām, lai nodrošinātu veiksmīgu RDP ieviešanu, kā arī darbības un informācija, kas tiek sagaidīta no katras mērķa grupas.

Tēzes katrai mērķa grupai:

- Informācijas sistēmu turētāji
  - Ļaundabīgie uzbrucēji meklēs un izmantos vai pārdos ievainojamības informācijas sistēmās neatkarīgi no tā, vai turētājs ieviesis RDP; viņi neziņos turētājam par ievainojamībām.
  - Pat, ja turētājs nebūs ieviesis RDP, starptautiskajai interneta kultūrai attīstoties, pētnieki meklēs ievainojamības un ziņos turētajam par tām arvien biežāk.
  - Pirms RDP publicēšanas, nepieciešams izstrādāt reaģēšanas plānu, jābūt gatavam labot ievainojamības; turētājam jāsagatavojas spēt atsijāt īstos ziņojumus no neīstajiem, steidzamos no mazāk svarīgiem.
  - Pēc RDP publicēšanas uz relatīvi īsu brīdi strauji pieaugs saņemto ziņojumu skaits.
  - Organizācijas iesaiste atbildīgas ievainojamību atklāšanas procesā ļauj tai vieglāk plānot savus cilvēkresursus, jo vairs nav jāveido “krīzes komandas”, lai risinātu pēkšņi atklātu kritisku ievainojamību.
  - Pētniekiem ir būtiski saņemt atgriezenisko saiti, turētajam ir nepieciešams nekavējoties reaģēt uz iesūtīto ievainojamības pieteikumu, uzturēt regulāru komunikāciju, informēt par plānotajiem termiņiem un paziņot, kad ievainojamība novērsta vai arī pieņemts lēmumus to nelabot.
  - Bieži vien pēc tam, kad ievainojamība būs novērsta (arī gadījumos, kad saņemts atteikums novērst ievainojamību vai sistēmas turētājs neizrāda patiesu vēlmi novērst ievainojamību), pētnieks izvēlēsies darīt ievainojamības aprakstu zināmu plašākai sabiedrībai.

- VP GKrPP ENAP 4.N, prokuratūra un Tieslietu ministrija
  - Cilvēkiem, kas pēta drošības ievainojamības ne vienmēr ir noziedzīgs motīvs.
  - RDP ir veiksmīgi ieviests citās valstīs, kur tas ir populārs gan valsts iestāžu starpā, gan privātajā sektorā. Valsts sektorā vislielāko progresu uzrāda Nīderlande, bet privātajā sektorā – ASV.
  - Skaidra valsts nostāja pret RDP vairo uzticību valstij un veicina hakeru iznākšanu no pelēkās zonas un viņu kļūšanu par atbildīgiem drošības pētniekiem, turklāt RDP rezultātā samazinās kopējais ievainojamību skaits, tādējādi mazinot kibernoziedzību.
  - RDP ieviešana palielina risku, ka kāds, izmantojot “balto piesegu” (izliekoties par ētisku pētnieku), var veikt kibernoziegumus.

2 Valsts policijas Galvenās kriminālpolicijas pārvaldes Ekonomisko noziegumu apkarošanas pārvaldes 4. nodaļa (Kibernoziegumu apkarošana un intelektuālā īpašuma tiesību aizsardzība)

- Drošības ievainojamību pētnieki
  - Sistēmas turētājam ir nepieciešams pietiekams laiks, lai novērstu ievainojamību; šis laiks var būt atkarīgs no problēmas tehniskās sarežģītības.
  - Ievainojamās sistēmas turētājs ne vienmēr būs tehniski kompetents novērst ievainojamību, tāpēc, jo smalkāk tiek aprakstīti rekomendējamie soļi ievainojamības novēršanai, jo labāk.

Jautājumi un uzdevumi katrai no mērķa grupām:

- Informācijas sistēmu turētāji
  - Kādi ir priekšnosacījumi, lai Jūs teiktu, ka Jūsu organizācijai ir vērtīgi ieviest RDP?
  - Kā (vai) Jūs būtu gatavi motivēt pētniekus pievērsties tieši Jūsu sistēmu izpētei? (atlīdzība, balvas, atzinība?)
  - Vai CERT.LV būtu obligāti jābūt iesaistītam kā starpniekam katrā atbildīgas ievainojamību atklāšanas procesā?

- VP GKrPP ENAP 4.N un prokuratūra
  - Kādu risku šobrīd uzņemas drošības pētnieki, iesaistoties atbildīgas ievainojamību atklāšanas procesā (ar sistēmas turētāja piekrišanu / bez sistēmas turētāja piekrišanas)? Ko pētnieks katrā individuālā gadījumā var darīt, lai šos riskus mazinātu?
  - Kādus grozījumus normatīvajos aktos būtu nepieciešams veikt, lai šīs darbības būtu legālas gadījumos, kad ir stingri sekots RDP?
  - Nepieciešama izpratne par ētiskiem drošības pētniekiem, viņu nodomiem un pozitīvo pienesumu sabiedrībai.
  - Nepieciešams izstrādāt kriminālo risku novērtējumu RDP ieviešanas gadījumā.

- Tieslietu ministrija
  - Kā mazināt risku, ka kibernoziedznieki varētu izlikties par pētniekiem un aizbildināties ar dalību atbildīgas ievainojamību atklāšanas procesā?
  - Nepieciešams veikt RDP projekta juridisko analīzi un risku izvērtējumu.
  - Nepieciešams sagatavot attiecīgus Krimināllikuma un Kriminālprocesa likuma grozījumus.

- Drošības ievainojamību pētnieki
  - Vai CERT.LV būtu obligāti jābūt iesaistītam kā starpniekam katrā atbildīgas ievainojamību atklāšanas procesā? Kāpēc?
  - Kas Jūs motivētu ziņot par ievainojamību? Kas Jūs demotivētu to darīt?
  - Pie kādiem apstākļiem Jūs būtu gatavs pārdot atrastās ievainojamības melnajā tirgū?
  - Nepieciešams laicīgi sadarboties ar citām mērķa grupām, skaidrojot tām savus mērķus.
  - Nepieciešams ar masu mediju palīdzību skaidrot sabiedrībai RDP un pētnieku lomu tajā.

Secība, kādā tiek uzrunātas mērķa grupas, nav būtiska. Kad komunikācija ar visām grupām ir noslēgusies, atbilstoši iegūtajai informācijai ir nepieciešams spert tālākos soļus RDP ieviešanai:

1. Saeima sagatavo un pieņem atbilstošus likumu grozījumus.
2. CERT.LV sagatavo RDP paraugus – mājaslapā publicējamo RDP tekstu, reaģēšanas vadlīnijas u.tml.
3. Valsts iestādes izziņo savu RDP un sāk pieņemt ziņojumus.
4. Privātie komersanti tiek aicināti ieviest un izziņot RDP.
5. Sabiedrība un starptautiskie partneri tiek informēti par RDP ieviešanu valsts līmenī.