VARAM pieredze centralizētas IS drošības pārvaldības organizēšanā

Arnis Vārslavs,
Valsts reģionālās attīstības aģentūras Informācijas sistēmu drošības pārvaldības nodaļas vadītājs

Drošības pārvaldība

Valsts vai pašvaldību institūcija

- **Iestādes vadītājs**
  - Valsts un pašvaldību institūciju informācijas tehnoloģiju drošības pārvaldību nodrošina katras attiecīgās institūcijas vadītājs

Atbildīgā persona

Valsts vai pašvaldības institūcijas vadītājs nosaka atbildīgo personu, kura īsteno informācijas tehnoloģiju drošības pārvaldību attiecīgajā institūcijā

profesijas standarts, kods 1330 09

Normatīvo aktu noteiktais modelis

Drošības pārvaldība

Valsts vai pašvaldību institūcija

- Iestādes vadītājs

Nespēj

Atbildīgā persona

Nav pieejami

profesijas standarts, kods 1330 09

Realitātes problēma – cilvēkresursu ar specifiskām kompetencēm un pieredzi trūkums !
Ko darīt šādā situācijā ? – mēģinām problēmu sadalīt apgabalos, kurus varam pārvaldīt

Drošības pārvaldība

Atbildīgā persona

Nav pieejami

profesijas standarts, kods 1330 09

Lomas «Atbildīgā persona» pienākumu kopas sadalīšana:

- konkrētās iestādes/institūcijas praktiskā pārstāvniecība
  - atrodam iestādē komunikatīvi sasniedzamu «pārmijnieka» lomas pildītāju (iestādes darbinieku)
    «sasniedzams» : ir sazvanāms incidentu gadījumos, spēj noteikt personu, kuras atbildībā «iekrīt» konkrētais incidents
- drošības pārvaldība (stratēģija, politika, noteikumi) – centralizēta pārvaldības struktūra resorā
  - Veidojam 1-2 līmeņu pārvaldības struktūru, kura spēj pieņemt finansiālus lēmumus, izprot iestādes iekšējos darbības procesus, spēj attiecināt drošības pārvaldības jautājumus uz konkrētās iestādes iespējām un vajadzībām
- drošības uzraudzība (kontroles funkcija)
  - Resora ietvaros atrodam CISA kompetenci un deleģējam auditora pienākumus
  - pārvaldība (praktiskā) – uz IT kompetences centru
- drošības realizācija (praktiskie izpildes jautājumi)
  - jāizveido spēcīgs kompetences centrs ar pietiekamu kapacitāti nosegt visas uzraugāmās resora struktūras gan no praktiskā konteksta, gan no metodoloģiskā konteksta (dokumentācija, noteikumi, apmācība, konsultācijas) + labi attīstīts intranets (visiem darbiniekiem pieejama informācija)

Drošības pārvaldības struktūra VARAM resorā

VARAM

rīkojums

Pilnvaro un deleģē

VARAM

- IT Padome — Saskaņo pārvaldības kārtības
- IT ekspertu darba grupa — Izstrādā normatīvo bāzi, ievērojot iestādes intereses
- Audita departaments — Informācijas drošības kontroles (uzraudzības) funkcija

VRAA

- IS drošības pārvaldības nodaļa (kā kompetences centrs) — Īsteno pārvaldību
- IS drošības pārvaldības nodaļas vadītājs — Veic metodiskā vadība , pārstāv kā resora «drošības pārvaldnieks»

Iestāde

- IT eksperts — Pārstāv iestādi IT ekspertu darba grupā
- kontakpersona — Pārstāv iestādi pret trešajām pusēm incidentu gadījumos

Kompetences centra loma

VARAM

IT ekspertu darba grupa

VRAA

IS drošības pārvaldības nodaļa

- Pārstāv iestādes biznesa struktūras intereses IT resursu izmantošanā
- Koriģē un saskaņo iekšējos normatīvos aktus

- Izstrādā metodoloģiju
- Izstrādā normatīvos aktus
- Nodrošina to ieviešanu
- Uzrauga un atbalsta izpildi

Šis modelis ir veiksmīgs, ja:

- Ir visu resora iestāžu vadības atbalsts
- Ir koncentrēta kvalitatīva , pieredzējusi un darbspējīga kompetence
- Ir koncentrēti (unificēti) IT izpildes dienesti
- resorā ir izveidoti strādājoši tiešās komunikācijas un informācijas apmaiņas kanāli un pieejams intranets

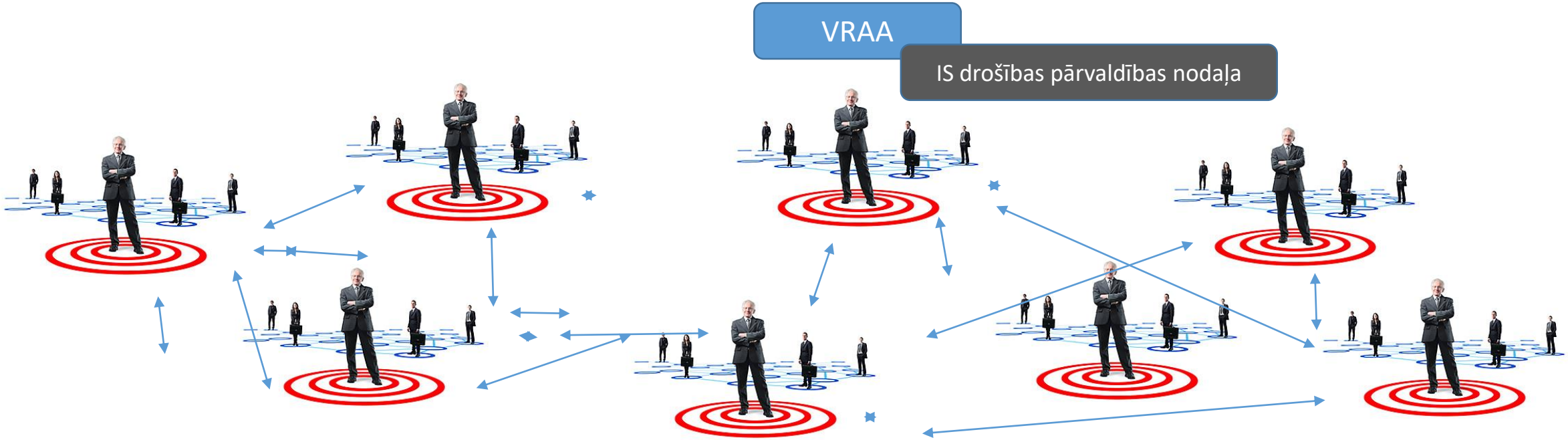
Tiešās komunikācijas kanāls

Nepareizi izprasts pārvaldības modelis ir iemels, kāpēc drošības pārvaldība NESTRĀDĀ:

Bieži pielietotais modelis : iestādes struktūras un drošības pārvaldība ir katra pati par sevi, katra veic savas funkcijas, neveicot horizontālo sadarbību :

drošības darbinieki ir tāpēc , ka tādu pieprasa regulējošie likumi un noteikumi
drošības nodaļa lai raksta iekšējos noteikumus
drošības nodaļa atbild par notikumu, ja tāds radīsies, tā ir viņu atbildība

Tiešās komunikācijas kanāls



Modelis: drošības pārvaldnieks atbalsta darbinieka vadītāju , kurš dod tiešos uzdevumus savam darbiniekam, kurš savukārt šos uzdevumus realizē

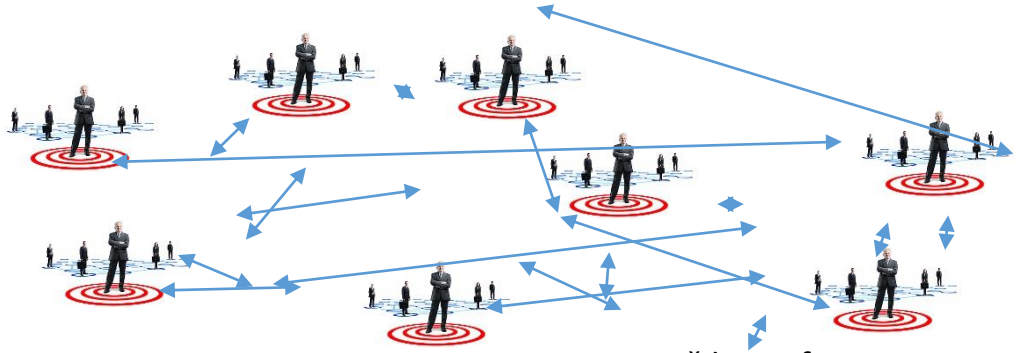
Drošības informācija ir apritināma starp:

- Drošības pārvaldība <> darbinieka vadītāji (metodika, noteikumi, kārtības, atbalsts)
- Drošības pārvaldība <> darbinieki (konsultatīvais atbalsts)
- darbinieka vadītāji <> darbinieki (procedūras, darba uzdevumi, operatīvā kontrole)

Tiešās komunikācijas kanāls

VRAA

IS drošības pārvaldības nodaļa



Drošības informācija ir apritināma starp:

- Drošības pārvaldība <> darbinieka vadītāji (metodika, noteikumi, kārtības, atbalsts)
- Drošības pārvaldība <> darbinieki (konsultatīvais atbalsts)
- darbinieka vadītāji <> darbinieki (procedūras, darba uzdevumi, operatīvā kontrole)

KATRS DARBINIEKS atbild par drošību lielākā vai mazākā mērā

KATRAM IR JĀZINA savi atbildības apmēri

Nepieciešams ērts, viegli izprotams, VISIEM viegli pieejams, viegli izmantojams, spējīgs saturēt VISU nepieciešamo informāciju komunikatīvs informācijas izplatīšanas iekštīkls (Intranets)

Tiešās komunikācijas kanāls Intranets Confluence

Pages

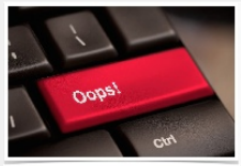
Edit Save for later Watching

VRAA_Informācijas_drošība Home

Created by Unknown User (arnis.varslavs@vraa.gov.lv), last modified by Arnis Vārslavs on Mar 14, 2018

Uzmanību visiem IT produktu turētājiem - lūdzu izvērtēt savas saimniecības, vai kaut kur netiek izmantoti risinājumi, kas balstās uz MD5 vai SHA1 jaucējummu algoritmiem - atkārtoti brīdinām, ka tie ir uzlauzti un ir jāveic to aizstāšana ar SHA256 , SHA2 vai SHA3 risinājumiem

Informācijas apmaiņa



Jaunumi Informācijas drošības laukā ...

Standarti un regulējumi

Starptautiskā pieredze	**ISACA euroCACS 2017 konference**
Normatīvie akti , rekomendācijas , standarti	

Pārvaldības apgabali

- Resursu reģistrs
- Paaugtinātas drošības sistēmas
- Drošības auditi
  - **Iepriekšējā līguma ietvaros veiktie auditi (arhīvs)**
  - **Drošības auditu kalendārais plāns līdz 2020 gadam**
  - **Vienotā līguma (2015) ietvaros veiktie auditi**
  - **Aktuālā**
- Risku analīze
- Darbības atjaur
- SSL: sertifikāti
- Interneta piekļu

Tehniskie apgabali

Komunikācija (e-pasta adreses, telefoni)

Confluence

Vienotā terminoloģija (IT pārvaldībā lietoto ter

Servisu pārvaldība

Darba plā

- Kalen
- Darba
- Darba
- Aktivi

Personas

- Sistē
- ārpak

VRAA_IT_Home

Created by Unknown User (arnis.varslavs@vraa.gov.lv), last modified by Arnis Vārslavs on Jan 05, 2018

Jaunumi un informācijas apmaiņa

Uzmanību visiem IT produktu turētājiem - lūdzu izvērtēt savas saimniecības, vai kaut kur netiek izmantoti risinājumi, kas balstās uz MD5 vai SHA1 jaucējummu algoritmiem - atkārtoti brīdinām, ka tie ir uzlauzti un ir jāveic to aizstāšana ar SHA256 , SHA2 vai SHA3 risinājumiem

Uzmanību !! INTEL procesoriem atrastas kritiskas

Risku pārvaldība	Reģistrs	plānotās aktivitātes	Protokols	Saistītai normatīv akts
Operacionālie	risku registrs	risku plans	risku protokols	Risku vadības procedū
Projektu pārvaldība	risku reģistrs	2017.01.25	ikgadējais 2017	
IS resursu				
IS Projektu				

Pages / Valsts reģionālās attīstības aģentūras darbinieku iekštīkls / Darbinieku centrs

Darbinieka pirmās dienas mape "Tas ir jāzina !"

Piebilde: Kārtības, kas nosaka Informācijas drošības un personas datu pārvaldību, ir atrodamas un izlasāmas šo

Darba kārtības noteikumi			Izmaiņas A Ētikas kode
PDF	PDF	Docum...	
Ugunsdrošības instrukcija A10 (2017)	Ievadapmācība nr 1 (2017)	Darba aizsardzības instrukcija darbam birojā (2017)	Elektrodroš

Pages / Valsts reģionālās attīstības aģentūras darbinieku iekštīkls

Edit Save for later Watching Share

Normatīvie akti un rekomendācijas

Eiropas savienība | Eiropas savienība - 29WP | Latvija | VARAM, CERT | VRAA | Rekomendācijas un labā prakse | Standarti (ISO) | IS ESVIS

Vispārējās normas

Likums	Ministru kabineta noteikumi	Spēkā no	Komentāri
Informācijas tehnoloģiju drošības likums		01.02.2011	
	442 "Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām"	04.08.2015	aizstāj spēku zaudējušos MK noteikumus 765
	100 "Informācijas tehnoloģiju kritiskās infrastruktūras drošības pasākumu plānošanas un īstenošanas kārtība "	16.02.2011	
	496 ." Kritiskās infrastruktūras, tajā skaitā Eiropas kritiskās infrastruktūras, apzināšanas un drošības pasākumu plānošanas un īstenošanas kārtība"	19.06.2010.	
Valsts informācijas sistēmu likums		05.06.2002	
	Nr. 764 "Valsts informācijas sistēmu vispārējās tehniskās prasības"	15.10.2005	
	Nr. 421 "Valsts informācijas sistēmu savietotāju un integrēto valsts informācijas sistēmu aizsardzības prasības"	27.06.2012	pēdējās izmaiņas 07.03.2014
	Nr. 374. "Valsts informācijas sistēmu savietotāja noteikumi"	17.06.2016	
	Nr. 572 "Valsts informācijas sistēmu reģistrācijas noteikumi"	05.08.2005	
	Nr. 71 "Valsts informācijas sistēmu attīstības projektu uzraudzības kārtība"	28.01.2006	

Tiešās komunikācijas kanāls Intranets Confluence

VARAM resora IKT pārvaldība

Created by Unknown User (sandris.laukazile@vraa.gov.lv), last modified by Arnis Vārslavs on Mar 16, 2018

- **Padomes locekļi,eksperti un kontaktpersonas**
- **IKT pārvaldības procesi (centralizācijas procesi)**
- Normatīvā bāze
- Pārvaldības audita ieteikumu izpilde
- **IT pakalpojumu katalogs**

IT drošības pārvaldība

	VARAM	VPVB	VVD	VRAA	DAP	LDM	LVAFA	NBD
Normatīvie dokumenti	VARAM	VPVB	VVD	VRAA	DAP	LDM	LVAFA	NBD
Resursu reģistrs	VARAM	VPVB	VVD	VRAA	DAP	LDM	LVAFA	NBD
Resursu valdītāji	VARAM	VPVB	VVD		P	LDM	LVAFA	NBD
Paaugstinātas drošības sistēmu skaits	0	0	0	20		0	0	0
Risku analīze		Feb_2018	Q1_2018	VRAA	Q			
Drošības auditi				VRAA				
Darbības atjaunošana	?	n/a	n/a	VRAA	Q1_201 DAP			
Incidentu reģistrs								
Veicamo aktivitāšu plāni								

Resursu pārvaldība

- Lietotāju pārvaldība AD

Pages / VRAA_Informācijas_drošība Home

Informācijas resursu reģistrs

Created by Unknown User (arnis.varslavs@vraa.gov.lv), last modified by Arnis Vārslavs on Mar 07, 2018

IS resursu reģistrs
Reģistrā tiek apkopots VRAA pārziņā un turējumā esošu produkcijā izmantotu IS saraksts. Sarakstā netiek iekļauti infrastruktūras resursi .

Rīkojumi	Datums	Komentāri	References
Rīkojums par atbildīgām personām	19.09.2017.	skaidrojums par personu lomām	**Struktūrvienību vadītāji**
Rīkojums par informācijas reģistru	23.05.2017.	apstiprināta klasifikācija	
	2018.g. maijs	Nākošā plānotā regulārā caurskate un apstiprināšana	

Reģistra pārvaldība, tajā uzskaitīto resursu valdītāji, aizbildņi

Npk	IS nosaukums	IS / apakšsistēmas nosaukums	Klasifikācijas datums	VIS statuss	Konfidencialitāte (slepenība) (K1, K2)	Vērtība (V1, V2, V3)	Pamata (PM) / paaugstinātas drošības (PA)	Maks. pieļaujamā dīkstāve (P1, P2, P3)	Pie P%
1.	Informācijas sistēma	Valsts informācijas sistēmu savietotājs (VISS), kuru veido:	20.10.2015.	savietotājs	K1	V1	PA	P1	
1.1	Koplietošanas komponente	Maksājumu modulis (MM)	13.10.2015.		K1	V1	PA	P1	
1.2	Koplietošanas komponente	Vienotās pieteikšanās modulis (VPM)	13.10.2015.		K1	V1	PA	P1	

Darba plāni un kontroles

	Aktivitāšu plāns detalizēts (project)	Saskaņotās aktivitātes	Izpilde (Excel)

Pārvaldības kārtība

- **VARAM rīkojums par centralizāciju**
- **VARAM IKT pārvaldība**

Paveiktais 2018 gadā

- Sakārtots informācijas drošības pārvaldības process VARAM resorā:
  - Izveidota un darbu veic pārvaldības struktūra (IT padome, IT ekspertu darba grupa), noteikti uzraugošo, praktisko un metodoloģisko procesu vadītāji
  - VARAM ietvaros apstiprināta unificēta drošības pārvaldības dokumentu pakete
    - Informācijas un komunikācijas tehnoloģiju sistēmu drošības kārtība;
    - Informācijas sistēmu drošības noteikumi;
    - Informācijas sistēmu lietošanas noteikumi ;
    - Informācijas sistēmu klasifikācijas noteikumi;
    - Informācijas sistēmu drošības risku pārvaldības plāna izstrādes noteikumi;
    - IT pakalpojumu sniegšanas un lietošanas noteikumi;
    - Datoru un programmatūras iegādes un pārvaldības noteikumi
- veiktas ikdienas (regulārās) pārvaldības aktivitātes resora iestādēs (VRAA, VPVB, VVD, DAP, LDM, LVAFA un NBD)
- VRAA kā kompetences centrs ir ieguvis apliecinājumu (sertifikātu) par VRAA pārziņā un turējumā esošo IS izstrādes, ekspluatācijas un uzturēšanas procesu atbilstību ISO/IEC 27001:2013 drošības pārvaldības standarta prasībām
- organizēti un vadīti kopumā 8 ārējie ielaušanās /penetrācijas/ veiktspējas auditi
- Sakārtots personas datu apstrādes process VRAA atbilstoši VDAR prasībām
- Sakārtots un uzturēts VRAA Intranets uz Confluence bāzes, nodrošinot IT drošības un pārvaldības informācijas pieejamību VRAA , resora iestāžu un iesaistīto trešo pušu IT darbiniekiem)
- Uzsākta drošības pārvaldības kvalitātes un mērķu metriku KPI ieviešana (Key Performance Index)
- Uzsākta virkne drošības pārvaldības tehnoloģisko projektu

Izaicinājumi

Procesi:

- Drošība ir mērķu, risku , vēlmju un iespēju optimāla balansēšana, līdz ar to drošības pārvaldībai ir jābūt iesaistītai KATRĀ biznesa un IT risinājumā un projektā sākot no idejas izstrādes brīža, un beidzot ar procesa izņemšanu no veicamo darbu saraksta (kompetents drošības pārvaldnieks ir iesaistīts praktiski visu lēmumu /projektu apritē (dokumentu vīzēšanā) - Drošības pārvaldība ir ne tikai drošības noteikumu radīšana, bet katra ikdienas darba komponente

Attīstība un nepārtrauktība

- Katra diena pienes tehnoloģisko iespēju un apdraudējumu jaunumus. Drošības pārvaldība ir veiksmīga tikai tad, ja tā nepārtrauktiem šiem jaunumiem seko un attīstās (mainās) – nepieciešama atzīta profesionālā kompetence /kompetences centri (uz resoru vismaz viens CISA,CISM,CISSP etc)

Atbalsts un komunikācija

- Drošības izpratne ir jāveido katru dienu katrā darbiniekā un vadītājā (top vadības atbalsts !!)
- Drošība ir ne tikai tehnoloģiska «lieta», bet gan arī ikdienišķa saruna darbiniekam saprotamā terminoloģijā
- Lai darbinieks zinātu un ievērotu kaut ko ikdienā, šim «kaut kam» ir jābūt pieejamam, izlasāmam un saprotamam
- Katrs darbinieks cer, ka tehnoloģiskie risinājumi palīdzēs viņam cīņā pret kiberapdraudējiem. Drošības pārvaldniekam ir jāatbalsta šī «cerība», organizējot aizsardzības fronti.