Risku apzināšana un novērtēšana, ierobežošanas pasākumu izvēle

Metodika

- Risk Management Guide for Information Technology Systems
- http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf (izmantots slaidos)

Riska pārvaldības process

- Lomas
- Riska novērtēšana
  - Sistēmas raksturošana
  - Apdraudējumu identificēšana
  - Ievainojamību identificēšana
  - Vadīklu (*controls*) analīze
  - Iespējamību noteikšana
  - Ietekmju analīze
  - Risku noteikšana
  - Vadīklu (*controls*) ieteikšana
  - Rezultātu dokumentēšana
- Riska ierobežošana

Mērķis

- to enable the organization to accomplish its mission(s)
- (1) by better securing the IT systems that store, process, or transmit organizational information
- (2) by enabling management to make well-informed risk management decisions to justify the expenditures that are part of an IT budget
- (3) by assisting management in authorizing (or accrediting) the IT systems on the basis of the supporting documentation resulting from the performance of risk management

Lomas

- Senior Management
- Chief Information Officer (CIO)
- System and Information Owners
- Business and Functional Managers
- ISSO
- IT Security Practitioners
- Security Awareness Trainers

Sistēmas raksturošana

- Aparatūra, programmatūra, dati, uzturēšanas process, sistēmas misija, kritiskums, CIA prasības
- Funkcionālās prasības, lietotāji, drošības arhitektūra, tīkla shēma, informācijas plūsmas, pārvaldības procedūras, fiziskā aizsardzība
- Informācijas iegūšanas tehnikas
  - Aptaujas anketas
  - Intervijas
  - Dokumentu analīze
  - Automātiski rīki
- Rezultāts: IT sistēmas raksturojums, laba izpratne par vidi un sistēmas robežām

Apdraudējumu identificēšana

- Apdraudējumu avoti
  - Daba (plūdi, zemestrīce)
  - Cilvēki (nejaušas kļūdas, ļaunprātīga rīcība, iekšēji/ārēji uzbrukumi)
  - Vide (elektrības piegādes traucējumi, uguns, tehnikas problēmas)
- Ļaunprātības motivācija: hakeri, noziedznieki, spiegi, neapmierināti darbinieki
- Rezultāts: avotu saraksts, kas varētu izmantot sistēmas ievainojamības

Ievainojamību identificēšana

- Ievainojamību un apdraudējumu avotu pāri
- Ievainojamību datu avoti
  - Iepriekšējas risku analīzes
  - Audita ziņojumi
  - Dati no pētījumiem/ražotājiem
  - U.c.
- Sistēmas testi
- Drošības prasību kontrollapa
- Rezultāts: Sistēmas ievainojamību saraksts

Vadīklu (*controls*) analīze

- Tehniskas: programmatūra, aparatūra, šifrēšana, autentifikācija
- Netehniskas: noteikumi, procedūras, personāls, fiziskā aizsardzība
- Preventīvas un detektīvas
- Rezultāts: Esošu un plānotu vadīklu saraksts, kas paredzētas ievainojamības izmantošanas iespējamības vai ietekmes mazināšanai

Iespējamību noteikšana

- Augsta – apdraudējuma avots ir augsti motivēts, ar pietiekamiem resursiem, vadīklas neefektīvas
- Vidēja – apdraudējuma avots ir motivēts, ar resursiem, vadīklas ir, bet daļējas
- Zema – apdraudējuma avotam trūkst motivācijas un/vai resursu, vadīklas ir labas
- Rezultāts: Iespējamības novērtējums (HML)

Ietekmju analīze

- Jāatkārto sistēmas misija, kritiskums, utml.
- Integritātes, pieejamības, konfidencialitātes zudums
- Augsta – lielas izmaksas, būtiski ietekmē organizācijas misiju vai reputāciju, cilvēku dzīvības apdraudējums
- Vidēja – nozīmīgas izmaksas, ietekmē organizācijas misiju vai reputāciju, cilvēku veselības apdraudējums
- Zema – nelielas izmaksas, nedaudz ietekmē organizācijas misiju vai reputāciju
- Rezultāts: ietekmes lielums (HML)

Risku noteikšana

Table 3-6. Risk-Level Matrix

Threat Likelihood	Impact		
	Low (10)	*Medium* (50)	*High* (100)
High (1.0)	Low 10 X 1.0 = 10	Medium 50 X 1.0 = 50	High 100 X 1.0 = 100
Medium (0.5)	Low 10 X 0.5 = 5	Medium 50 X 0.5 = 25	Medium 100 X 0.5 = 50
Low (0.1)	Low 10 X 0.1 = 1	Low 50 X 0.1 = 5	Low 100 X 0.1 = 10

Risk Scale: High (>50 to 100); Medium (>10 to 50); Low (1 to 10)[8]

- Augsts – steidzami jāveido un jāīsteno riska ierobežošanas plāns
- Vidējs – papildus riska ierobežošanu veic saprātīgā termiņā
- Zems – visbiežāk risks ir pieņemamā līmenī
- Rezultāts: riska līmenis (HML)

Vadīklu (*controls*) ieteikšana

- Jānovērtē
  - Efektivitāte
  - Ierastā prakse
  - Uzticamība, u.c.
- Rezultāts: Ieteicamās vadīklas vai citi pasākumi

Rezultātu dokumentēšana 1/3

- I. Vispārīga informācija
  - Mērķis
  - Riska novērtējuma tvērums
- II. Riska novērtējuma pieeja
  - Dalībnieki
  - Informācijas iegūšanas tehnikas
  - Riska skalas apraksts

Rezultātu dokumentēšana 2/3

- III. Sistēmas raksturojums
  - Aparatūra, programmatūra, saskarnes, dati un lietotāji
  - Sistēmas ieeju un izeju plūsmkarte, lai attēlotu risku novērtējuma tvērumu
- IV. Apdraudējumu pārskats
  - Potenciālo apdraudējumu avotu un apdraudējumu uzskaitījums

Rezultātu dokumentēšana 3/3

- V. Riska novērtējuma rezultāti
  - Novērojumu saraksts (ievainojamību/apdraudējumu pāri)
    - Novērojuma numurs un īss apraksts
    - Esošo drošības vadīklu uzskaitījums
    - Iespējamības apraksts un novērtējums (HML)
    - Ietekmes analīze un novērtējums (HML)
    - Riska vērtējums, kas balstīts riska līmeņu matricā
    - Ieteicamās vadīklas vai citi ieteikumu riska samazināšanai
- VI. Kopsavilkums
  - Novērojumu skaits un kopsavilkums, iekļaujot riska līmeņus, ieteikumus un komentārus. Tabulas formā, lai atvieglotu ieteikto vadīklu ieviešanas un risku ierobežošanas procesu

Riska ierobežošanas stratēģijas

- Riska pieļaušana (To accept the potential risk and continue operating the IT system or to implement controls to lower the risk to an acceptable level)
- Izvairīšanās no riska (To avoid the risk by eliminating the risk cause and/or consequence (e.g., forgo certain functions of the system or shut down the system when risks are identified)
- Riska samazināšana (To limit the risk by implementing controls that minimize the adverse impact of a threat's exercising a vulnerability (e.g., use of supporting, preventive, detective controls)
- Riska plānošana (To manage risk by developing a risk mitigation plan that prioritizes, implements, and maintains controls)
- Riska nodošana (To transfer the risk by using other options to compensate for the loss, such as purchasing insurance)

Jautājumu paraugi

- What is the purpose of the system in relation to the mission of organization?
- What information is generated by, consumed by, processed on, stored in, and retrieved by the system?
- How important is the information to the user organization's mission?
- What are the paths of information flow?
- What is the sensitivity (or classification) level of the information?
- Where specifically is the information processed and stored?
- What is the potential impact on the organization if the information is disclosed to unauthorized personnel?
- What are the requirements for information availability and integrity?
- How much system downtime can the organization tolerate?
- Could a system or security malfunction or unavailability result in injury or death?

Personas dati un to aizsardzība

- Jebkāda informācija, kas attiecas uz identificētu vai identificējamu fizisko personu (FPDAL)
  - Personas dati var būt jebkur un gandrīz jebkas
  - Sensitīvi personas dati
- **Jāizmanto atbilstoši mērķim**
  - Personas datu apstrāde ir atļauta tikai tad, ja likumā nav noteikts citādi un ja ir vismaz viens no šādiem nosacījumiem:
    - ir datu subjekta piekrišana
    - datu apstrāde nepieciešama pārzinim likumā noteikto pienākumu veikšanai
  - Var būt pretruna starp organizācijas interesēm un datu subjekta interesēm, bet jāsargā jebkurā gadījumā
- Personas datu apstrādes reģistrācija (speciālists)
- Personas datu aizsardzības obligātās tehniskās un organizatoriskās prasības (MK 40. noteikumi)

Valsts informācijas sistēmu drošības pārvaldība

- Valsts informācijas sistēmas pārzinis drošības prasību izpildes organizēšanai un vadīšanai ieceļ valsts informācijas sistēmas drošības pārvaldnieku
- Valsts informācijas sistēmu vispārējās drošības prasības (765)
  - Sistēmas pārzinis nodrošina
    - sistēmas drošības politikas izstrādi un īstenošanu
    - iekšējo sistēmas drošības noteikumu izstrādi un ievērošanu
    - sistēmas lietošanas noteikumu izstrādi un ievērošanu
    - sistēmas drošības riska pārvaldības plāna izstrādi un izpildi
    - sistēmas atjaunošanas plāna izstrādi un izpildi
    - apmācību sistēmas drošības jautājumos
- Valsts informācijas sistēmu vispārējās tehniskās prasības (764)

Jautājumi?

Ilze Murāne

Latvijas Bankas informācijas sistēmu drošības vadītāja

Ilze_at_latnet.lv