IT DROŠĪBAS RISKU APZINĀŠANA UN NOVĒRTĒŠANA

V.Minkevičs, CISA

2012

Risku analīzes veidi

- Kvalitatīva (augsts vidējs zems)
  - Viegli saprotama un sasniedz mērķi norādot uz potenciāli bīstamiem apdraudējumiem, kas iestājoties, var ietekmēt resursu.
- Kvantitatīva (cik maksā?)
  - To labprāt akceptē biznesa cilvēki (organizāciju vadītāji) jo tā ļauj novērtēt cik biznesa cilvēkam maksās kontroļu ieviešana un cik maksās riska iestāšanās.

Sekas

- īslaicīgs vai ilgstošs pārtraukums biznesa darbībā
- klientu neuzticēšanās sistēmai
- savlaicīgi neatklātas krāpnieciskas darbības
- darbinieku neapmierinātība ar sistēmu un neefektīva izmantošana
- augsts kļūdu procents datos
- imidža zaudēšana
- tirgus daļas zaudēšana
- tiesvedība

IS DROŠĪBAS RISKU VĒRTĒŠANA

- RV – resursa vērtība
- IE – iestāšanās biežums laika periodā
- IF – ietekmes koeficents, jeb kaitējums (cik stipri tiek ietekmēts resurss)
- Risks = (RV * IF) * IE
  ietekme iespējamība
- Svarīgi ir pareizi izvēlēties laika periodu, kurā riski tiek vērtēti

Ietekmes vērtēšana izmantojot skalu (kaitējums)

1 Neievērojama ietekme

2 Zema ietekme

3 Vidēja ietekme

4 Ievērojama ietekme

5 Katastrofāla ietekme

Iespējamības vērtēšana laika periodā

1 Visticamāk, ka neiestāsies ne reizi

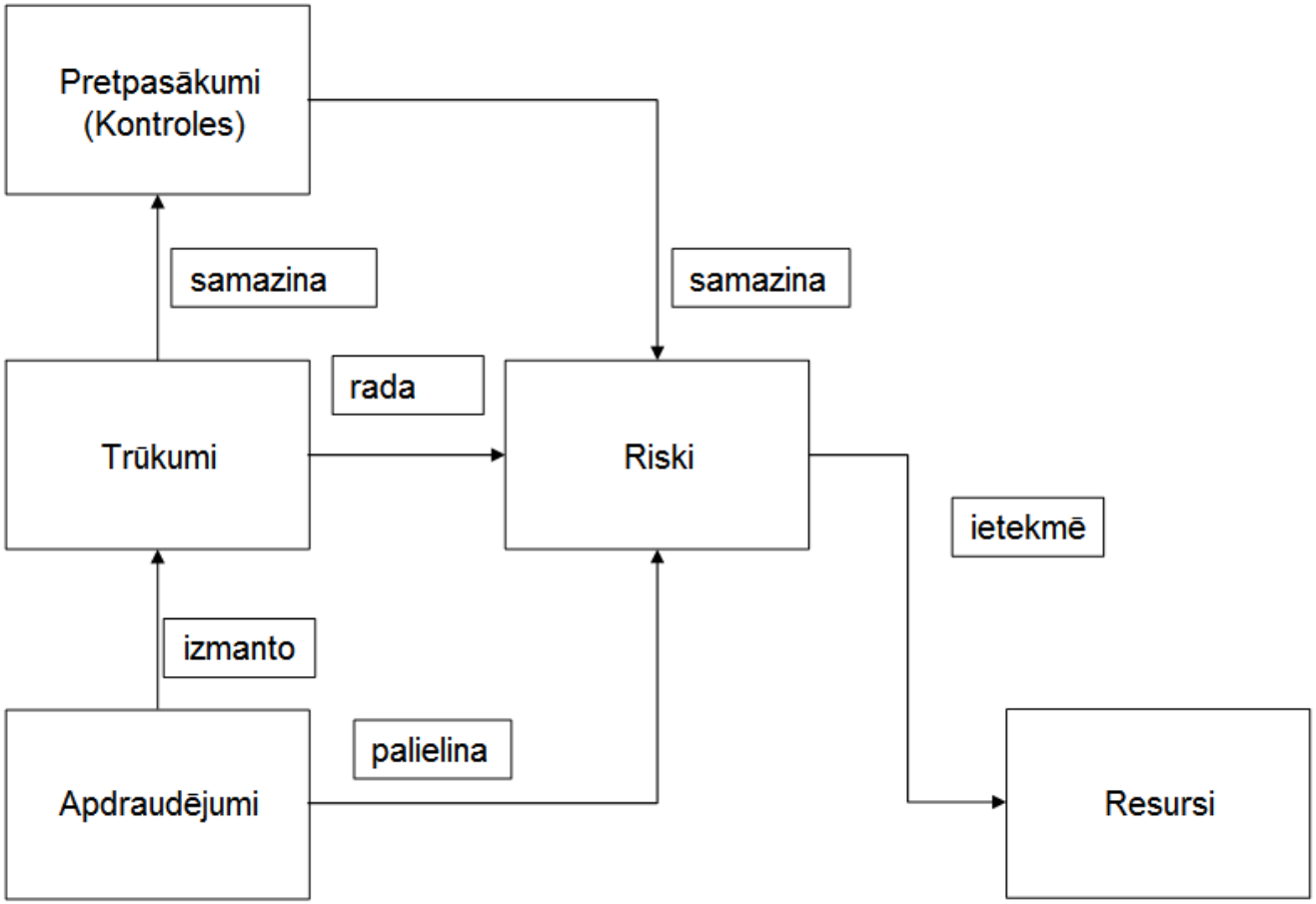
2 Visticamāk ka neiestāsies biežāk kā 1 reizi

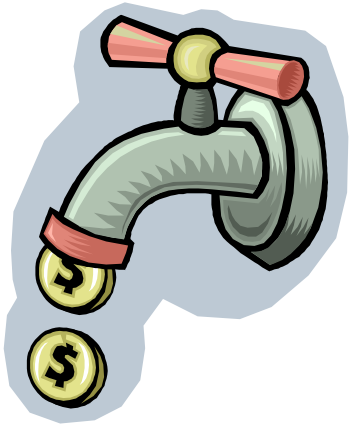
3 Visticamāk ka iestāsies vismaz vienreiz

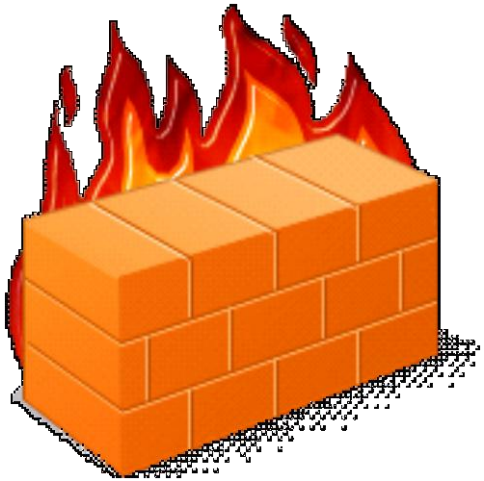
4 Notiks biežāk kā vienreiz

5 Notiks regulāri

Jēdzienu mijiedarbība







Piemērs

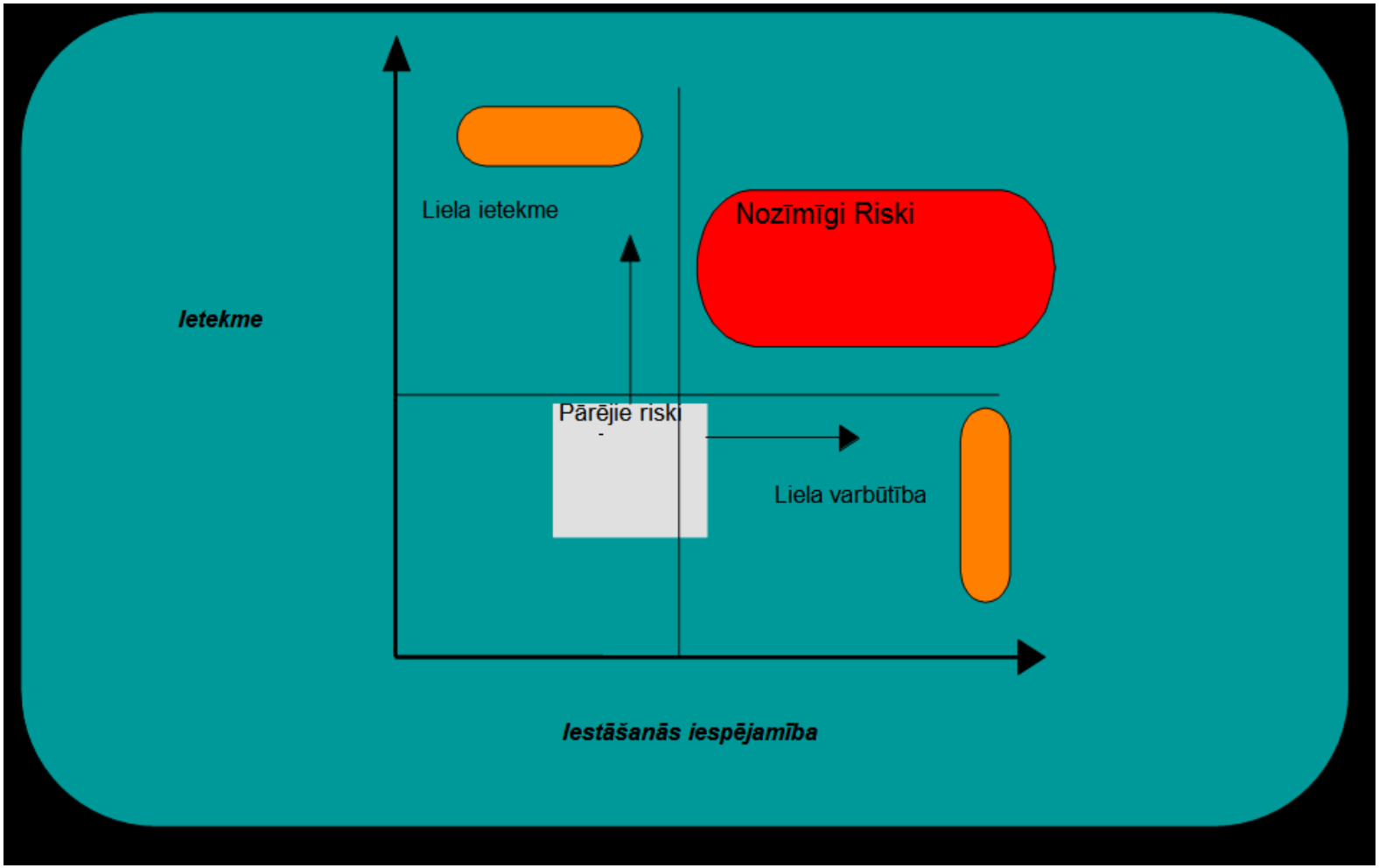
- Novērtējot vīrusa aktivizācijas iespējamības risku uz konkrētas informācijas sistēmas, pieņemsim tika iegūta varbūtība 0,3 jeb 30%. Lai aprēķinātu drauda ietekmi, tā ir jānovērtē jebkādā izteiksmē – to var novērtēt naudā. Pieņemsim, ka vīrusa aktivizācijas gadījumā organizācijas zaudējumi sastādīs $2000. Aprēķins ir šāds: 30% no $2000 un sastāda $600. Tas nozīmē, ka lai mazinātu risku, maksimālā risku mazinošo pasākumu, tādu kā ugunsmūra ierīkošana un antivīrusu uzstādīšanas maksa, nedrīkst pārsniegt $600.

Risku novērtēšana

K – konfidencialitāte; P – pieejamība; I – integritāte.

Nr. p.k.	Apdraudējums	Apraksts	Kaitējums			Varbūtība	Informācijas sistēmas risks
			K	P	I		
		Aparatūra					
1.	Ekspluatācijas kļūda	Kļūda aparatūras ekspluatācijā, piemēram, dators tiek novietots tuvu spēcīgam magnētiska lauka starotājam.	X	4	4	1	4
2.	Apkalpošanas kļūda	Kļūdas aparatūras apkopē, piemēram, detaļu nomaiņa netiek veikta ievērojot instrukciju (aparatūru atvienot no strāvas), kā rezultātā aparatūra tiek bojāta	X	4	4	1	4
3.	Aparatūras nepietiekama veiktspēja	Strauji pieaugot datu apjomam, tiek pārslogota aparatūra un sistēma vairs nespēj savlaicīgi apkalpot pieprasījumus	X	4	4	2	8
4.	Bezpārtraukuma barošanas iekārtu (UPS) darba traucējumi	Traucējumi sistēmā UPS bateriju nolietošanās dēļ	X	4	4	1	4
5.	Aparatūras darbības traucējumi	Kļūda aparatūras darbībā, tās iekšēja defekta vai fiziskā nolietojuma dēļ	X	4	4	1	4

Risku vērtēšanas rezultāti



Kontroļu izvēle

- Vadībai ir jāakceptē tie riski, kuriem netiek ieviestas papildu kontroles. Ieviešanas prioritātes ir jānosaka atbilstoši riskiem
- Ieviešanas izmaksām ir jābūt samērojamām ar riska sekām

No pieredzes

- Riski tiek vairumā saistīti tikai ar tehnoloģiskiem aspektiem
- Riska ietekme uz organizāciju ir diezgan grūti kvantificējama
- Risku identifikācijā nevēlas iesaistīties IT darbinieki
- Viedokļi par risku nozīmīgumu krasi atšķiras atkarībā no tā, kurš to vērtē.
- Jaunas tehnoloģijas attīstās ātri un rada jaunus riskus
- Bieži vien nav pieejami vēsturiskie dati, vai salīdzināmi dati

Risku analīzes metodoloģijas

- FMECA (Failure Modes, Effects and Criticality Analysis)
  - MIL-STD (Procedures for Performing a FMECA)
  - FMECA.COM
- FMEA (Failure Mode and Effect Analysis)
  - IEC 60812 (FMEA Analysis techniques for system reliability)
  - SAE ARP 5580 (FMEA Practices for Non-Automobile Applications)
  - SAE J1739 (Design FMEA, Process FMEA and Machinery FMEA)
- FTA (Fault Tree Analysis)
  - IEC 61025 (Fault Tree Analysis)
  - NUREG-0492 (Fault Tree Handbook)
  - NASA (Fault Tree Handbook - Aerospace Applications)
- HAZOP (HAzard and Operability Analysis)
  - IEC 61882 (HAZOP Application guide)
- CCA (Cause Consequence Analysis)
- MORT (Management Oversight Risk Tree)
- SMORT (Safety Management Organization Review Technique)
- Risk Analysis Bibliographies by Tan Hiap Keong
- Security/Survivability Systems Analysis (S/SSA)
- CEA - Cost-Effectiveness Analysis in Emergency Medicine, Computer, and more by Zui-Shen Yen , and Primer on Cost-Effectiveness Analysis: Effective Clinical Practice
- Cost Benefit Analysis

Risku analīzes rīki

- The Australian Standard 4360 Risk management portal
- List of Risk Analysis, Assessment and Management Tools
- @RiskAccelerator
- Risk Analysis and Management System (RAMS)
- Toolkit for RAMS from IsographDirect
- FIDUCIA - Modelling Risk in Interoperable Public Key Infrastructures
- CORA - Cost-of-Risk-Analysis System
- BayesEngineTM Technology
- Introduction to Security Risk Analysis and the COBRA Approach
- Reliability, Availability, Maintainability and Safety Solutions from Reliability Software
- eRisk Managemet Model from mi2g
- List of Risk Analysis Books from Palisade
- Risk Analysis, Monte Carlo Simulation, Forcasting, Optimization - from Crystal Ball
- Callio Technologies offers ISO 17799 BS7799 Security Policies Software Tools and Expertise
- Tufin SecureTrack - Firewall Policy Auditing, Tracking and Compliance
- Proteus Enterprise Integrated Compliance and Information Risk Management Software - From InfoGov
- ASSET (Automated Security Self-Evaluation Tool) from NIST
- OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) from SEI

Jautājumi...