Svarūs informacijos saugumo aspektai ir praktika organizacijoje

Tomas Pivoras
www.tuvuolektis.lt

ISVS – kas svarbu?

- **ISVS nėra atskira sistema,**
- **ISVS nėra mūsų tiesioginis darbas,**
- **ISVS efektyvumas pasimato įvykus incidentui,**
- **ISVS greitai gali tapti vieno žmogaus darbu,**
- **ISVS gali tapti formalia.**

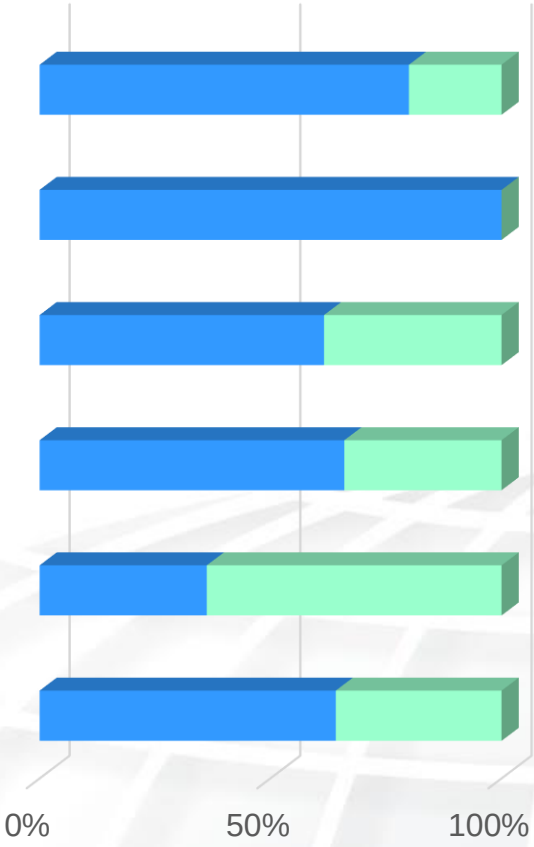
Subalansuotas požiūris į ISVS

- **Sistema patikima tiek kiek patikimos visos jos dalys.**

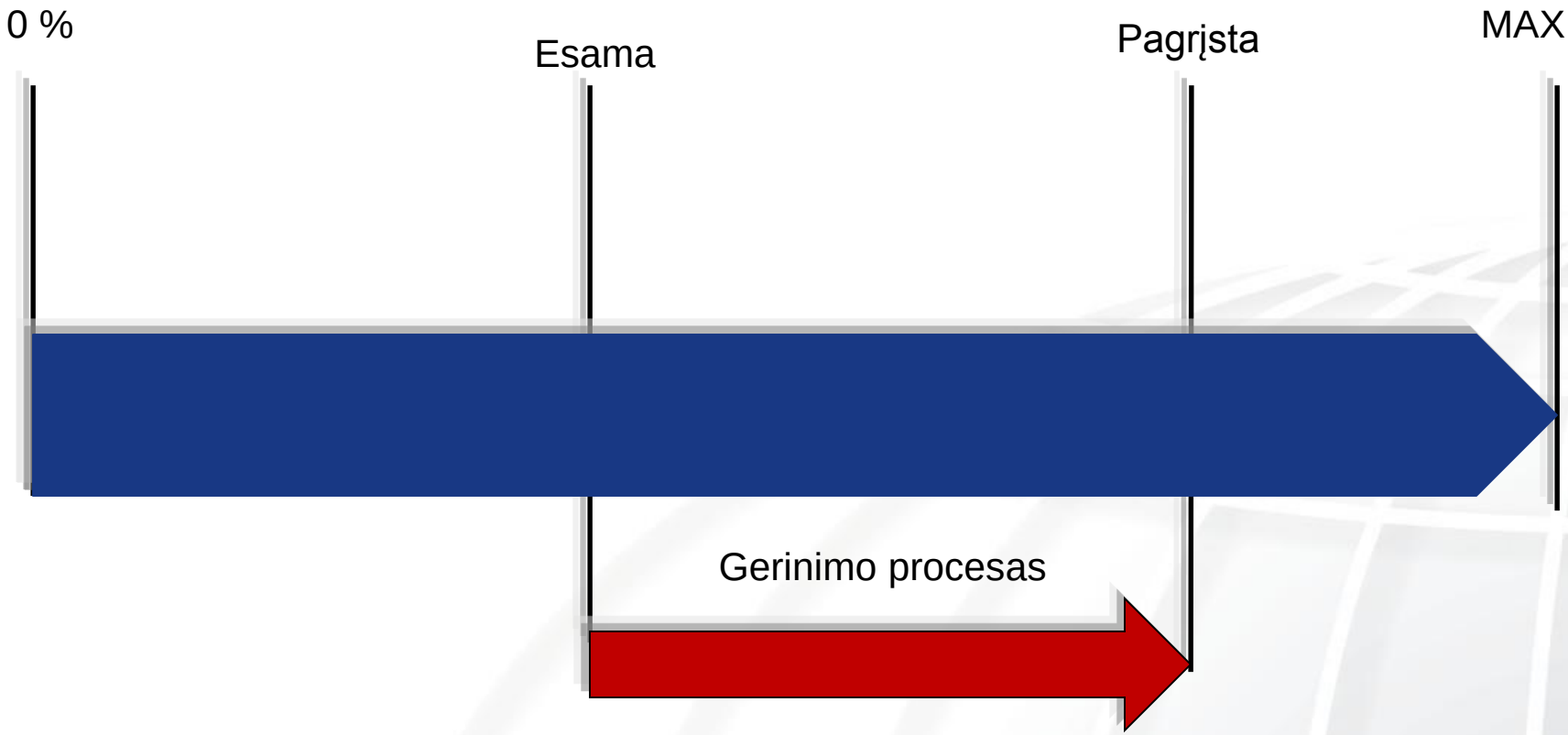
TÜV THÜRINGEN

Subalansuotas požiūris į ISVS 2

- Žmonės;
- Patalpos infrastruktūra;
- Pastatai;
- Įranga;
- Informacinės sistemos;
- Komunikacija;
- ...



IS tai procesas



Rizikos vertinimas

- Suvokiamas;
- Leisti aiškiai suvokti situaciją;
- Leisti priimti sprendimus;
- Pagrįstas faktais ir tendencijomis;
- Parodyti realias situacijas.

Mitai apie kiber atakas

- **1. Tai izoliuota problema.**

  2. Ugniasienė pakankamas sprendimas.

  3. Kompiuterio rakinimas pakankamas sprendimas.

  4. Atsisiuntimai – pagrindinis šaltinis.

  5. Problema ateina iš į išorę.

  6. Niekas nenori šnipinėjimo programų.

  - **Harnish Patel - SurfControl**

Realūs faktai

- **1. Dauguma šnipinėjimo atvejų sąlygota vartotojo.**
- **2. T.b. saugoma ir ugniasienės – ir darbo vietoje.**
- **3. Kompiuterio rakinimas (locking) neapsaugo.**
- **4. Parsisiuntimai net neturėtų įvykti.**
- **5. Šnipinėjimo programos patenka vidun nes kažkas palieka atviras duris...**
- **6. Blogi dalykai patenka su gerais dalykais.**
  - **Harnish Patel - SurfControl**

TÜV THÜRINGEN

Duomenys

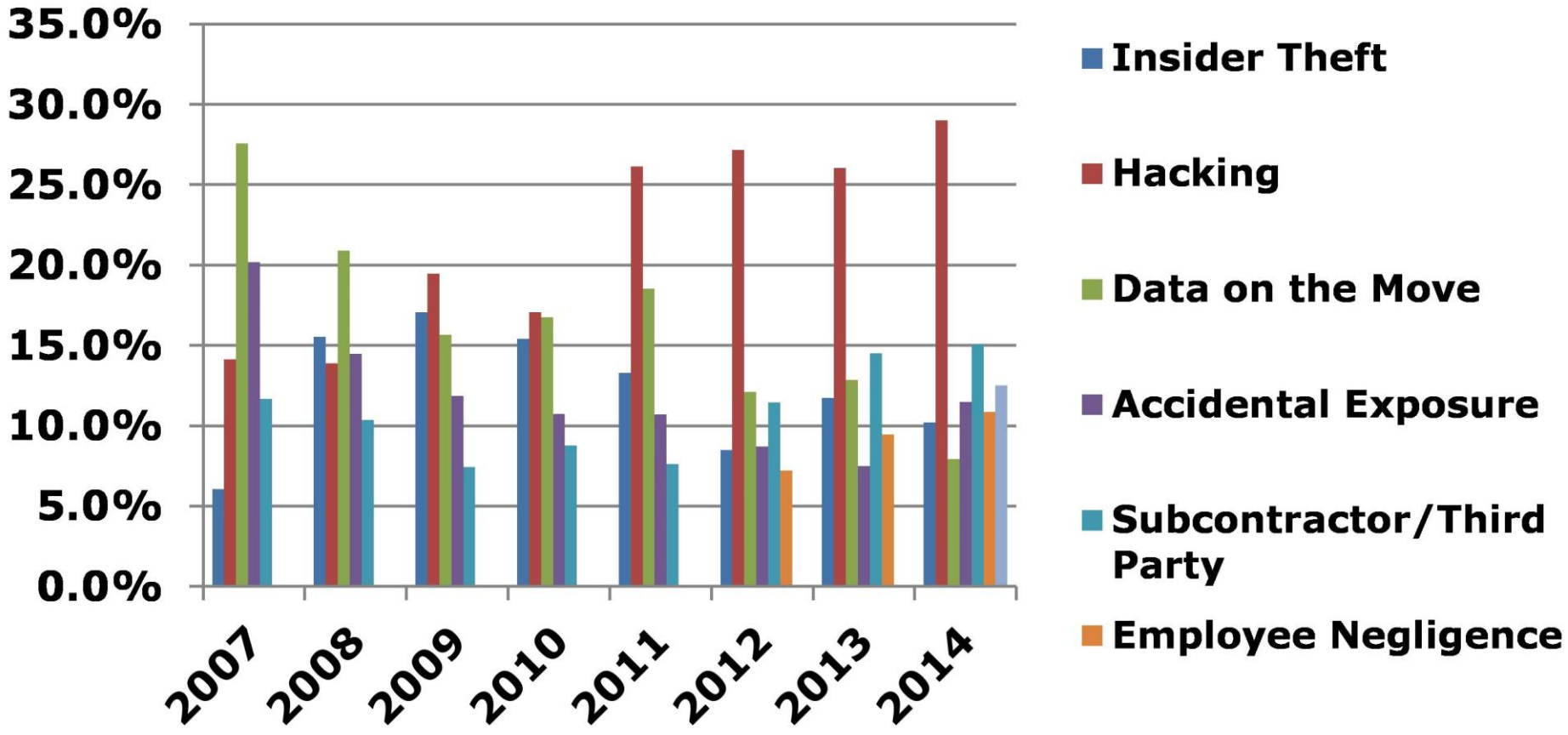
- The Open Security Foundation DataLossDB (JAV):
- 1611 informacijos praradimų atvejų (2012):
  - verslas 58%
  - mokslas 12%
  - Valstybinės institucijos15%
- 43% priežasčių organizacijos viduje;

Duomenys 2

- 2014 duomenų paradimų atvejų sk. išaugo 27.5 %
- Verslo sektoriuje 33.0 %,
- Valstybiniam/ kariniam 11.7 %,
- Mokslo įstaigose 7.3 %,
- Finansų 5.5 %.

- JAV, ITRC.

Priežastys


35.0%
30.0%
25.0%
20.0%
15.0%
10.0%
5.0%
0.0%
2007
2008
2009
2010
2011
2012
2013
2014
Insider Theft
Hacking
Data on the Move
Accidental Exposure
Subcontractor/Third Party
Employee Negligence

Duomenų vagysčių atvejai

- Darbuotojai sekti iš išorės(22%)
- Vogti iš vidaus(16%)
- malware (16%)
- phishing (14%)

- www.bakerlaw.com.

10 duomenų praradimų sričių (Verizon)

- Web aplikacijų atakos
- Įvairios klaidos
- Kiber špionažas
- Įsibrovimas į pardavimų sistemas
- ATM
- Fizinės vagystės ar praradimai
- Pasinaudojimas privilegijomis viduje
- Kenkėjiškos priemonės (Toolkits)
- Denial-Of-Service atakos
- Visa kita

Viską sprendžia kadrai! (J.V.S)

Bendras suvokimo lygis

- **Bendrieji mokymai;**
- **Žinių atnaujinimas;**
- **Specialieji mokymai;**
- **Aktualios informacijos gavimas;**
- **Geroji praktika;**
- **Informuotumas apie esamą situaciją.**

Veiklos tęstinumas

- Turi būti dalis bendros sistemos;
- Organizaciniai <-> detalūs;
- Detalumas priklauso nuo situacijos;
- Turi atitikti tikslus;
- Turi būti įmanoma pamatuoti;
- Turi būti testuojami!

IS tiekimo grandinėje

IS tiekimo grandinėje

- IS reikalavimai sistemoms;
- Komunikavimo reikalavimai;
- Reikalavimai duomenų saugojimui;
- Konfidencialumo įsipareigojimai;
- Reikalavimai duomenų valdymui;
- Reikalavimai procesams?????!

Tiekėjo procesai

- ISVS
- Veiklos tęstinumas
- IT paslaugų valdymas (ISO 20000-1)

- Ačiū už dėmesį