Loeng 2
Sissejuhatus, mõisted, definitsioonid, probleemid,

Erika Matsak, PhD

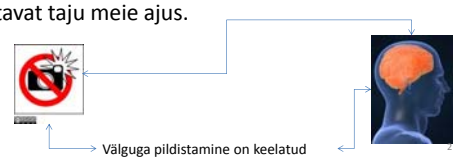
1

Teadmised, andmed, informatsioon

Semiootikud:

Antud teooria raames teadmiste all vaadeldakse kolmikuid, mis koosnevad

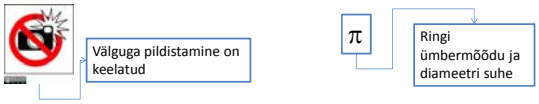
- kujutisest (näiteks pilt, ikoon jne),
- selle tähendusest (näiteks tekstina),
- vastavat taju meie ajus.



2

Teadmised, andmed, informatsioon

- P. Lorents (NATO Cooperative Cyber Defence Centre of Excellence): "*Teadmiseks nimetame iga niisugust järjestatud paari, mille esimese elemendi tähenduseks on teine element, teise elemendi tähenduseks on esimene element*".



Definitsioon (vt Lorents 2008). X on andmed, kui on mingis teadmises tähiseks või tähenduseks.
Definitsioon (vt Lorents, Ottis, Rikk 2009). M on informatsioon, kui M on kas teadmine või andmed.

3

Turvaprobleemide näited

- Firmal on mitu kontorit, mis paiknevad üksteisest kaugel. Konfidentsiaalse info edastamisel interneti kaudu peab olema kindel, et mitte keegi ei saa infot ei näha ega muuta.
- Võrgu administraator juhib serveri tööd olles väljastpoolt kontorit. Vastane napsab juhtkäsu, muudab seda ja saadab serverisse
- Kasutaja saab liigipääsu arvutisse mitteseaduslikult, või omades üht ligipääsu ühtede õigustega, saab liigipääsu veel mujale või suuremate õigustega.
- Firma avab interneti poe, mis võtab vastu makseid elektroonselt. Müüa peab olema kindel, et kaup, mille ta annab üle on ka tegelikult makstud. Ostja aga peab olema kindel, et saab selle kauba kätte ja seejuures mitte keegi ei saaks teada tema krediitkaardi andmeid.
- Firma avab internetis oma saidi. Mingil momendil asendatakse saidi sisu teise sisuga või tekib selline päringute koormus, et server ei tule sellega toime ning jookseb kinni.

4

Mõned terminid

- **Andmete käideldavus** (availability) on teabe õigeaegne ning mugav kättesaadavus ning kasutatavus selleks volitatud isikutele ning subjektidele
- (Lorents 2010) ***Info käideldavus*** seisneb olukorras, mille raames peab saama vastava teadmise või eelmainitud teadmise moodustamist võimaldava tähise või tähenduse (ehk *andmete*) kasutamine ettenähtud viisil
- **Andmete terviklus** (integrity) on andmete pärinemine autentsest allikast ning veendumine, et need pole hiljem muutunud ja/või neid pole hiljem volitamatult muudetud
- (Lorents 2010) ***Info terviklus*** seisneb olukorras, mille raames on vastaval teadmisel või eelmainitud teadmise moodustamist võimaldaval tähisel või tähendusel (ehk *andmetel*) või nendevahelisel seosel olemas kõik ettenähtud komponendid ning ettenähtud ülesehitus
- **Andmete konfidentsiaalsus** (confidentiality) ehk salastus on andmete kättesaadavus ainult selleks volitatud isikutele (ning kättesaamatus kõikidele ülejäänutele)
- (Lorents 2010) ***Info konfidentsiaalsus*** seisneb ühe süsteemi (edaspidi salastaja) loodud olukorras, mille sihiks on muuta teiste süsteemide jaoks võimatuks vastava teadmise (ehk *salastatud teadmise*) omandamine või muuta teiste süsteemide jaoks võimatuks eelmainitud teadmise moodustamist võimaldava tähise või tähenduse (ehk *salastatud andmete*) või nendevahelise seose omandamine

5

Küberründed ning informatsiooni konfidentsiaalsus, terviklus ja käideldavus

- (Lorents, Ottis 2010) ***Konfidentsiaalsuse vastu suunatud küberrünne*** on säärane küberrünne, mille soovitud tagajärjeks on salastatuse kadu ehk olukord, kus mingi süsteem (nt konkureeriv firma) võib omandada teadmise, mida ei soovi selle teadmise salastaja
- (Lorents, Ottis 2010) ***Tervikluse vastu suunatud küberrünne*** on säärane küberrünne, mille soovitud tagajärjeks on teadmise või selles sisalduvate asjade (nt tähiste, tähenduste, nendevahelise seose vms) ettenähtud struktuuri (ehk kindlaksmääratud ülesehituse) rikkumine (näiteks "kustutakse" sihtmärgi koordinaatides mõned arvud, "lõigatakse" ettekandest välja teatavad tekstiosad)
- (Lorents, Ottis 2010) ***Käideldavuse vastu suunatud küberrünne*** on säärane küberrünne, mille soovitud tagajärjeks on teadmise või selles sisalduvate asjade (nt tähiste, tähenduste, nendevahelise seose vms) ettenähtud kasutamise võimatuks muutmine (näiteks sel teel, et "ummistatakse" infoedastuskanalid)

6

Mõned terminid

- Nõrkused – süsteemi nõrgad kohad, turvaaugud, vms, mida kasutatakse rünneteks
- Risk – võimaliku kahju suuruse ning selle kahju tekke tõenäosuse korrutis (nt kui teostatakse konkreetne rünne konkreetsete turvaaukude kaudu). Iga organisatsioon peab enda jaoks selgitama välja "lubatavad" riskid.
- Turvameetmed on organisatsioonilised toimingud ja vahendid, tehnilised protsessid ja tehniliste vahendite rakendamine andmete ja infosüsteemide andmete turvalisuse saavutamiseks ja säilitamiseks
- Turvapoliitika on organisatsiooni infoturbetegevuse alusdokument.
- Rünne – iga tegevus, mille sihiks on kahjustada infosüsteemi turvalisust

7

Turvateenused

- **Turvateenused** takistavad ohtude realiseerumist ja/või aitavad vähendada ohtude realiseerumisel saadavat kahju.
- Konfidentsiaalsuse tagamine
- Käideldavuse tagamine
- Autentimine – kinnitus sellele, et info on saadud seaduslikest allikatest ning saaja on just see isik kellena ta end esitab.
- Terviklus – kinnitus sellele, et info ei ole säilitamisel või edastamisel muudetud.

8

Turvateenused

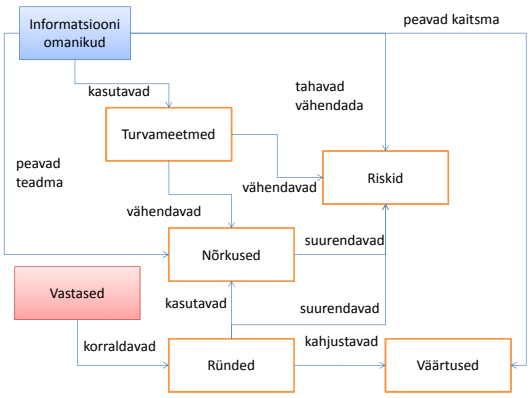
- Salgamise vääramine – Saaja ning vastuvõtja ei saa keelduda info edastamisest. Kui info on saadetud, siis vastuvõtja saab võimaluse kindlaks teha (tõestuse) kas info on saadetud ja kas saatja oli legaalne. Samuti, kui info on vastuvõetud, siis saatja saab võimaluse kindlaks teha (tõestuse), et see on võetud vastu ning legaalse vastuvõtjaga.
- Pääsu reguleerimine (*access control*) – võimalus piirata ja kontrollida juurdepääsu süsteemidesse kommunikatsiooni liinide kaudu
- Juurdepääsevus – rünnete tagajärjeks võib olla süsteemi või teenuse juurdepääsu häire. Antud teenus vähendab teenuse tõkestamise DoS-ründeid

9

Turvamehhanismid

- Sümmeetriline šifreerimine – algoritmid kasutavad ühte ja sama võtit nii šifreerimiseks kui ka dešifreerimiseks, või siis dešifreerimise võtit on võimalik saada šifreerimise võtmest.
- Asümmeetriline šifreerimine – algoritmides kasutatakse kaht erinevat võtit šifreerimiseks ja dešifreerimiseks, kusjuures teades üht ei ole ise-enesest veel võimalik saada teist.
- Räsifunktsioonid (Hash functions) – funktsioonid, mille sisendiks on suvalise pikkusega sõnum ning väljundiks on **kindla** pikkusega krüptograafiline lühend.
- Taastemehhanismid – varundamine, infosüsteemi kriitiliste sõlmede dubleerimine, operatsioonide päeviku pidamine

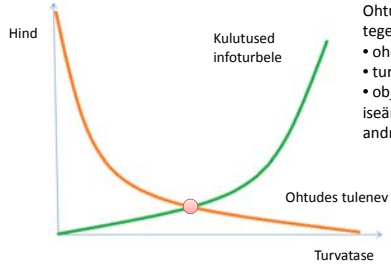
10



11

Turvarisk

varade väärtus × ohtude realiseerumise tõenäosus



Ohtude realiseerumise tegelik sagedus sõltub:
• ohu tüübist,
• turvaaugu "suurusest"
• objekti ja ta varade iseärasustest, näiteks andmete tundlikkusest.

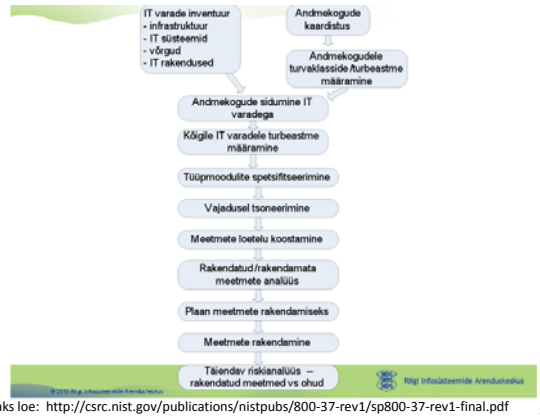
12

Turvarisk

“ *Turvariskide hindamise tarkvara (McAfee Vulnerability Manager) abil on võimalik kas ühekordselt või regulaarselt hinnata ettevõtte infrastruktuuri ohustavaid turvariske, nii sise- kui välisvõrgust tulevate rünnete puhul. Turvariskide põhjalikuks hindamiseks kontrollitakse kõikide võrgus olevate seadmete haavatavust; isegi IP aadressi omava printeri või kohvimasina kaudu võib tekkida reaalne oht ettevõtte võrgule. Vulnerability Manager'i võib võtta kui organisatsiooni IT audiitorit.*”

http://www.secsoft.ee/et/10/turvariskid/
http://www.mcafee.com/us/products/vulnerability-manager.aspx

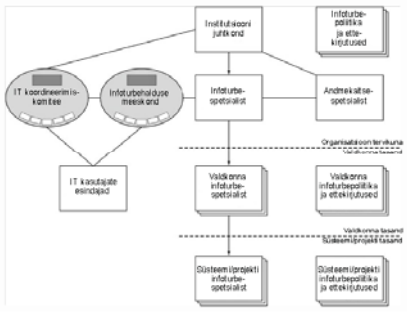
13



Lisaks loe: http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf

14

Rollide jaotus



Joonis 3.1. Suure organisatsiooni infoturbehalduse töökorraldus

https://www.ria.ee/public/ISKE/Standard_BSI_100-2.pdf

15

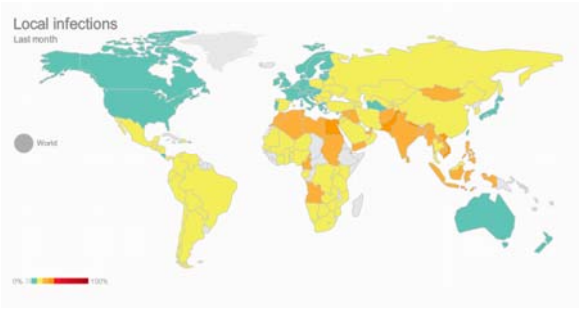
http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

SC information system = {(confidentiality, *impact), (integrity, impact), (availability, impact)}, where the acceptable values for potential impact are LOW, MODERATE, or HIGH.

16

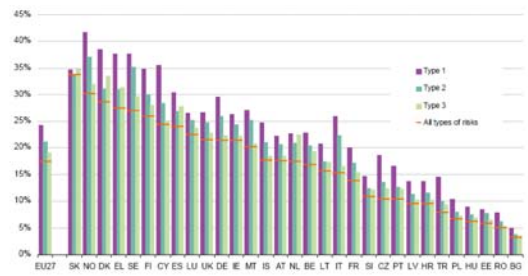
Interneti ohtude statistika



http://www.securelist.com/en/statistics

17

Enterprises having a formally defined ICT security policy with a plan for regular review which addresses specific security risks, by country and type of risk, January 2010, (% of enterprises)



http://epp.eurostat.ec.europa.eu/statistics_explained/index.php/ICT_security_in_enterprises#Types_of_risks

18

Infosüsteemide turvameetmete süsteemi kehtestamine

- Vastu võetud 20.12.2007 nr 252, jõustumine 01.01.2008

https://www.riigiteataja.ee/akt/13125331?leiaKehtiv

(1) Määrusega kehtestatakse riigi ja kohaliku omavalitsuse andmekogude pidamisel kasutatavate infosüsteemide ning nendega seotud infovarade turvameetmete süsteem.

(2) Turvameetmete süsteem koosneb turvanõuete spetsifitseerimise korrast ning andmete organisatsiooniliste, füüsiliste ja infotehniliste turvameetmete kirjeldustest.

(3) Määrust ei kohaldata riigisaladust töötlevate infosüsteemide turbeks.

19

Turvaklassid

- **Mis on andmete turvaanalüüs?**
- Andmete turvaanalüüs on turvaklassi määramiseks sooritatav andmete tähtsuse hindamine ning andmete turvalisuse puudumisest tulenev kahjude hindamine.
- **Mis on turvaklass?**
- Turvaklass on andmete tähtsusest tulenev andmete nõutav turvalisuse tase, väljendatuna neljaastmelisel skaalal ning kolmekomponendilisena, st kolme turvaosaklassi ühendina.
- **Mis on turvaosaklass?**
- Turvaosaklass on andmete tähtsusest tulenev infoturbe eesmärgi saavutamise nõutav tase väljendatuna neljaastmelisel skaalal (0–3).

https://www.ria.ee/iske-kkk/#turvaanaluus

20

Infosüsteemide turvameetmete süsteemi kehtestamine

Vastu võetud 12.08.2004 nr 273

§1. Reguleerimisala
§2. Turvameetmete süsteemi rakendamine
§3. Mõisted
§4. Turvanõuete spetsifitseerimine
§5. Turvaklassi määramine
§6. Turvatasemed
§7. Turvaosaklassid
§8. Turvaklasside moodustamine
§9. Turvaklassidele vastavate turvameetmete valimine

§ 9¹. Turvameetmete süsteemi rakendamise auditeerimine riigi infosüsteemi kuuluvate riigi andmekogude pidamisel
§ 9². Turvameetmete süsteemi rakendamise auditeerimine kohaliku omavalitsuse riigi infosüsteemi kuuluvate andmekogude pidamisel

§10. Määruse jõustumine

§ 11. Turvameetmete süsteemi rakendamise auditeerimise tähtajad riigi infosüsteemi kuuluvate riigi andmekogude pidamisel

21

Näide — konfidentsiaalsus

- S3 – ülisalajane info: info kasutamine on lubatud ainult teatud kindlatele kasutajatele, juurdepääs teabele on lubatav juurdepääsu taotleva isiku õigustatud huvi korral.

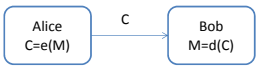
22

Krüptosüsteemi baas-stsenaarium

- Alice ja Bob tahavad suhelda salaja.
- Alice saadab teade Bobile

  Formaalselt on Alice teade avatekst (plaintext) *M*. See krüpteeritakse funktsiooniga *e().* Tulemuseks on krüptogramm *C=e(M).*

  Bob võtab krüptogrammi vastu ning dekrüpteerib selle kasutades funktsiooni *d()*. Sellisel juhul d(C)=d(e(M))=M.



23

Saladused

- Määratlus (P. Lorents, 2006). *H jaoks on saladuseks selline teadmine, mida H ei tohi omada. Saladust eristab mitteteadmisest asjaolu, et "ei tohi omada", mis pole sugugi samaväärne asjaoluga "ei oma"*.
- **Näide:** Inimese palk kui saladus. Kui on kirjutatud inimese nimi, siis ei tohi kõrval olla kirjutatud palga numbrit.
- **Salastatud andmed:** Meenutame, et andmeteks on teadmise "pooled" (kus esimene on tähise, teine aga tähenduse jaoks). Andmete salastamiseks tuleb vähemalt üks "pooltest" ära varjata. Seega tähis saadaksegi kätte, siis tähendust ei tohiks kätte saada. Ning vastupidi, kui on tähendus on kätte saadud, siis tähis peaks jääma kättesaamatuks.
- **Näide:** krüptogramm – tähis, mille tähendus ei tohi sattuda sattuda võõra kätte.

24

Konfidentsiaalsuse tagamine krüpteerimise abil

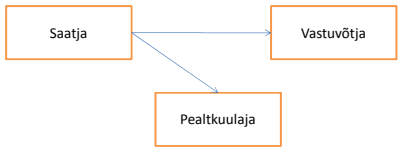
- SSL/TLS
- SSH
- IPSec
- PGP
- jne

Šifreerimine (erijuhul krüpteerimine) on niisugune kodeerimine, mille korral kodeeritavad tekstid, kõnede või piltide salvestused jms jäävad teise (mittelubatud) isiku jaoks saladusse.

25

Rünnete klassifikatsioon

I. **Passiivne**. Rünne, kus vastane kuulab pealt, aga ei saa andmeid muuta, kustutada või lisada midagi omapoolset.



Andmete korjamine, analüüs

26

Rünnete klassifikatsioon

II **Aktiivne rünne-** rünne, kus vastane saab edastavat informatsiooni muuta (sh täiendada)

1. teenuse tõkestamine ehk **DoS rünnakud (Denial of Service)**- tekitatakse tõrge normaalses funktsioneerimises. Tõrge võib olla nii tarkvara kui riistvara tasemel (nt. elektromagnetilised rünnakud).

Näited:

- **BGP rünnak (*Border Gateway Protocol*):**
  - Mustade aukude tekitamine (*blackholing*)
  - Ümbersuunamine (*redirection*)
  - Alamversiooni tekitamine (*subversion*)
  - Võrguliikluse mittestabiilsus (*instability*)
- **PDoS (Permanent Denial-of-Service):** ruuteri või mõne muu võrguseadme vastu suunatud rünnakud. Mõjutavad seadme tarkvara või teevad tarkvara uuendusi (firmware flashing)

27

Näide: Denial of Service

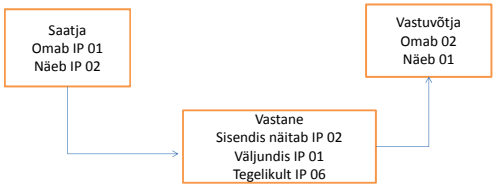
- Ülekoormus
- Ressursside ammendamine
  - Kettaruum
  - Mälu, protsessitabel
  - Protsessoriaeg (näiteks tehakse "tühja" krüpteerimist)
  - Võrguriba (ujutatakse pakettidega üle)
- Vead süsteemi ja protokollide disainis ja realisatsioonis

Meelis Roos, Tartu Ülikool, http://math.ut.ee/~mroos/turve/vork.pdf

28

Rünnete klassifikatsioon

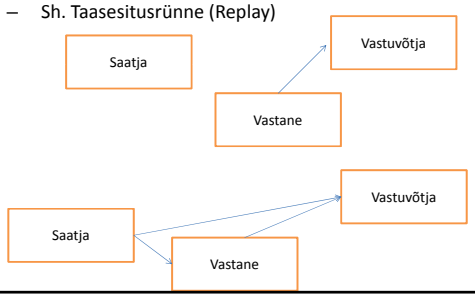
2. Vahemehe rünnak (Main in the middle): muudab kas saadetud info või info pakettide järjekorda. Saatja ja vastuvõtja seadmetele valetatakse oma tõelist identiteeti ning nad ei tea, et "räägivad" läbi kolmanda isiku.



29

Rünnete klassifikatsioon

3. Võltsimine, falsifitserimine – vastane näitab end teise isikuna (autentimisjada kasutamine teeskluseks)
   - Sh. Taasesitusrünne (Replay)



30

Näited: Kuidas võltsida…

- IP aadressi vahetus
- MAC aadressi vahetus
- IP aadressi võltsimine (*IP spoofing)*
- MAC aadressi võltsimine
- ARP võltsimine
- DNS kirjete võltsimine, valed pöördteisendused
- Source ruuting
- Marsruutimisinfo võltsimine
- Ühenduste kaaperdamine (*hijacking)*

Meelis Roos, Tartu Ülikool,
http://math.ut.ee/~mroos/turve/vork.pdf

31

Rünnete mehhanismid

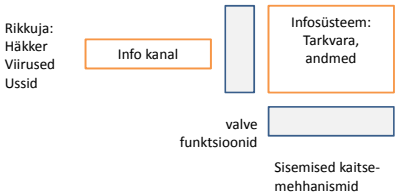
1000 - Mechanism of Attack

- Data Leakage Attacks - *(118)*
- Resource Depletion - *(119)*
- Injection (Injecting Control Plane content through the Data Plane) - *(152)*
- Spoofing - *(156)*
- Time and State Attacks - *(172)*
- Abuse of Functionality - *(210)*
- Probabilistic Techniques - *(223)*
- Exploitation of Authentication - *(225)*
- Exploitation of Privilege/Trust - *(232)*
- Data Structure Attacks - *(255)*
- Resource Manipulation - *(262)*
- Physical Security Attacks - *(436)*
- Network Reconnaissance - *(286)*
- Social Engineering Attacks - *(403)*
- Supply Chain Attacks - *(437)*

http://capec.mitre.org/data/graphs/1000.html

32

Infosüsteemi turvamudel



-rünne eesmärgiga saada või muuta süsteemis paiknevad andmed
-rünne teenuste vastu, et häirida turvateenuste tööd

Turvateenused:
Valvefunktsioonid: Antud mehhanismid sisaldavad näiteks autentimist, tulemüüre.
Sisemised kaitse- mehhanismid: sise-monitooring, mis kontrollib, et kes on ühenduses ja mis on tema tegevus.

33

IT-relvad ja küberrelvad

- (Lorents, Ottis 2010) ***Infotehnoloogiliseks relvaks*** nimetame sellist IT-lahendustele rajatud süsteemi, mis on loodud just selleks, et lõhkuda teiste süsteemide ülesehitust või muuta võimatuks nende (ettenähtud viisil) toimimine

  Näide. "Targad piloodita lahingulennukid", mis suudavad iseseisvalt, vajadusel marsruuti valides ja korrigeerides hävitatava sihtmärgini jõuda, on IT-relvad. 11. septembril New Yorgi kaksiktorne tabanud ja väga palju protsessoreid ja tarkvara kasutavad "Boengid" pole IT-relvad

- (Lorents, Ottis 2010) ***Küberrelvaks*** nimetame sellist IT-süsteemi, mis on loodud just selleks, et lõhkuda teiste IT-süsteemide ülesehitust või muuta võimatuks nende (ettenähtud viisil) toimimine

  Näide. Arvutiviirused on küberrelvad. Nn fondi- või foonivärvijad pole relvad, kuigi nende abil võib kirjutatu mittenähtavaks muuta (nt punane kiri punasel taustal)

34

Küberintsidendid ja küberründed

- (Lorents, Ottis 2010) ***Küberintsident*** on sündmus (*event*), mis põhjustab või võimalik, et põhjustab mittelubatavaid muutusi IT-süsteemi ülesehituses või toimimises ettenähtud viisil

  Näited. Välgulöök, viirusest nakatumine.
- (Lorents, Ottis 2010) ***Küberrünne*** on küberrelva või küberrelvana kasutatava süsteemi ettekavatsetud kasutamine küberintsidendi esilekutsumiseks või selleks, et lõhkuda teiste IT-süsteemide ülesehitust või muuta võimatuks nende (ettenähtud viisil) toimimine

35

Küberspionaaž ja küberkonflikt

- (Lorents, Ottis 2010) ***Küberspionaaž*** on küberrünnete selline kasutamine, mille eesmärgiks on rikkuda rünnatavates süsteemides sisalduva info (st teadmiste või andmete) konfidentsiaalsust.
- (Lorents, Ottis 2010) ***Küberkonflikt*** on küberrünnete kasutamine (sh ründed info tervikluse ja kasutatavuse vastu) poliitiliste sihtide saavutamiseks

36

KÜBERSÕDA

(Lorents, Ottis 2010) Kübersõda on riikide vaheline küberkonflikt

37

Kokkuvõte

- Infosüsteemi turvalisus peab vastama organisatsiooni rollidele ja eesmärkidele
- Infoturbe osutamiseks on vaja terviklikku lähenemisviisi
- Infoturve peaks olema lahutamatu osa organisatsiooni haldamise korraldamises
- Infoturve peab olema majanduslikult põhjendatud
- Vastutus süsteemi turvalisuse eest peab olema selgelt määratletud
- Infosüsteemi ohutust tuleks perioodiliselt uuesti hinnata
- Suure tähtsusega infosüsteemide turvalisuse juures on olulised ka sotsiaalsed tegurid, samuti haldus-, organisatsiooniline- ja füüsiline turvalisus

38