Koliko varnosti pravzaprav potrebujemo?

Dr. Dušan Caf

3. posvet dolenjskih in belokranjskih informatikov

Otočec, 25. 3. 2010

Kaj pomeni “biti varen”?

- Kako varovati dragocena sredstva?
  - Napredni sistemi za varovanje
- Tudi informacije so organizacijsko sredstvo
  - Varovanje informacij pomembno za poslovanje
  - Še zmeraj obdobje “divjega zahoda” – kraja informacij je donosen posel

Kako razmišljajo vsiljivci?

- Uporabijo vsa možna sredstva in poti
- Poti in sredstev, ki smo jih predvideli, ne uporabijo
- Vedno so poti in sredstva, ki jih nismo predvideli

Varovanje informacij

- Različne vrste informacij:
  - Elektronske, zapisane na papirju, druge oblike
- Cilj varovanja informacij:
  - **Zaupnost:** zaščita informacij pred nepooblaščenim dostopom in/ali razkritjem
  - **Neokrnjenost:** varovanje točnosti in popolnosti informacij
  - **Razpoložljivost:** dostopnost informacij uporabnikom, ko jih potrebujejo

Vloga in obseg varovanja

- Varovanje informacij je **upravljavski** in ne **tehnološki** proces
- Varovanje informacij **ni omejeno** na informacijski sistem
- Različni deležniki imajo **različna pričakovanja** glede varnosti

Primer: varnostni pogledi deležnikov v telekomunikacijah

Stranke / naročniki	• Zaupanje v omrežje in storitve • Razpoložljivost storitev, zlasti v primeru naravnih nesreč
Državni organi	• Varnostne zahteve, izhajajoče iz direktiv in uredb EU ter nacionalne zakonodaje, glede zagotavljanja razpoložljivosti storitev, poštene konkurence in varovanja zasebnosti
Operaterji	• Zagotoviti nemoteno obratovanje omrežja in storitev • Zaščititi lastne poslovne interese • Izpolniti obveznosti do naročnikov in javnosti • Izpolniti obveznosti do državnih organov

Primer: varnostni incidenti pri telekomunikacijskih operaterjih

Varnostni incident	Vpliv
• Okvara omrežnih elementov	• Hitro se lahko razširi prek omrežja na druge objekte in opremo
• Napaka v protokolih in topologijah	• Nedelovanje storitev • Težaven razvoj interoperabilnih protokolov, zlasti pri povezovanju fiksnih in mobilnih omrežij v NGN
• Izpad omrežja in storitev	• Zelo dragi z vidika odnosov s kupci, izgube prihodkov in stroškov ponovne vzpostavitve delovanja
• Vdor hekerjev	• Kraja storitev prek proženja različnih diagnostičnih funkcij, spreminjanja obračunskih podatkov, podatkov v bazi priključitev, prisluškovanje naročniškim klicem
• Notranji incidenti	• Namerne ali nenamerne spremembe podatkov o uporabnikih, upravljanju omrežja, konfiguracijah

Vir: ISO/IEC, ITU-T 2008

Primer: katera sredstva varujemo?

Vrsta sredstva	Primeri
• Informacije	• Podatki o komunikacijah, prometu, naročnikih, neplačnikih (črna lista), registriranih storitvah, delovanju omrežja, napakah, konfiguracijah, uporabnikih, obračunu, klicanih, uporabniških geografskih lokacijah, prometnih statistikah • Pogodbe in dogovori, sistemska dokumentacija, razvojne in raziskovalne informacije, uporabniški priročniki, gradivo za usposabljanje, obratovalni in podporni postopki, načrt za neprekinjeno poslovanje, revizorska poročila, arhivirane informacije
• Programska sredstva	• Programska oprema za nadzor komunikacij, upravljanje omrežja, upravljanje informacij o naročnikih, zajem merilnih podatkov, zaračunavanje storitev; aplikativna in sistemska programska oprema, razvojna orodja in sistemska orodja

Vir: ISO/IEC, ITU-T 2008

Primer: katera sredstva varujemo?

Vrsta sredstva	Primeri
• Strojna oprema	• Stikala, kabli, terminali, računalniška oprema (strežniki, osebni računalniki in delovne postaje), prenosni mediji in druga oprema
• Storitve	• Fiksna telefonija, mobilna telefonija, širokopasovni dostop (xDSL/optika), zakup kapacitet, dostop do interneta, podatkovni centri, (CA)TV, vsebine, upravljane storitve (xSP), naročniške storitve (zaračunavanje storitev, klicni center)
• Objekti in podporni infrastrukturni sistemi	• Zgradbe, ogrevalni sistemi, električne napeljave in oprema, prezračevalni in klimatski sistemi, protipožarni sistemi

Vir: ISO/IEC, ITU-T 2008

Primer: katera sredstva varujemo?

Vrsta sredstva	Primeri
• Človeški viri	• Zaposleni v podpori uporabnikom, telekomunikacijski inženirji, informatiki za podporo obratovanju / poslovanju, zaposleni za odnose z dobavitelji
• Neopredmetena sredstva	• Sistem organizacijskega nadzora, znanje in izkušnje, ugled in javna podoba organizacije

Vir: ISO/IEC, ITU-T 2008

Motivi za upravljanje varnosti

- Zmanjšanje varnostnih tveganj
- Izpolnjevanje zahtev deležnikov (dobaviteljev, strank, regulatorjev)
- Boljše upravljanje partnerstev
- Upravljanje informacijske varnosti
- Doseganje konkurenčne prednosti
- Ohranjanje / povečanje vrednosti podjetja

Izzivi za direktorje IT

- Varnost sodi med 10 glavnih IT tem
  - Kako jo primerno umestiti?
- Gospodarska kriza je oklestila IT proračune
  - Kako se boriti proti zmanjšanju proračunov?
  - Kako z manj doseči več?
  - Ceneje se je varnostnim incidentom izogniti!
- Varnostna ogroženost je v recesiji še večja
  - Vrstijo se napadi na največje ponudnike storitev
  - Pojavljajo se nove grožnje

Pragmatični pristop

- Spremeniti varnostne procese
- Varnost umestiti na korporativno raven
- Uvesti sistem vodenja (ISO 27000)
- Nižji izdatki ne pomenijo nujno nižje varnosti
- Nad zmanjšanje proračunov z večjo učinkovitostjo in uspešnostjo na operativni ravni

Vloga FIŠ

- Skrbi za celostno izobraževanje študentov s področja informacijske varnosti
- Povezuje strokovnjake različnih profilov
- Organizira izobraževanje za podjetja
- Izvaja svetovalne projekte