ZAŠČITA PODATKOV V ELEKTONSKI OBLIKI

mag. Janko Uratnik, dipl.ing.el.
PRIS, CISA, CISM, CGEIT
Sodni izvedenec in sodni cenilec za računalništvo in informatiko

SICOS, Ljubljana, 10.11.2012

PODATKI

- Sodoben posameznik ali podjetje zelo težko živi in posluje brez informatike in brez podatkov v elektronski obliki.
  - Komunikacijski sistemi
  - Informacijski sistemi v organizacijah,
  - Industrijski krmilni, merilni in nadzorni sistemi .....
- Veliko vsakodnevnih aktivnosti je vezanih na informatiko
  - Telefoniranje
  - Elektronsko bančništvo
  - Nakupovanje
  - Rezervacije, ...

PODATKI

- Na podatke prežijo mnoge grožnje
- Grožnje in tveganja so zelo raznolike in kompleksne
- Tveganja je zato potrebno prepoznavati in obvladovati
- To je stalen proces, saj se okolje stalno spreminja (proces P-D-C-A)

PODATKI

Podatki so največja lastnina posameznika
ali podjetja (ang. Asset), zato jih je potrebno varovati in zagotavljati:

Zaupnost – Confidentiality C

Celovitost – Integrity I

Dostopnost – Availability A

RANLJIVOSTI SISTEMA

- Informacijski sistem s katerim obdelujemo podatke nikoli ni popolnoma idealno varen,
- Informacijski sistem ima pomanjkljivosti in napake, kar povzroča njegovo ranljivost,
- Strojna oprema se lahko pokvari
- Programska oprema ima lahko napake
- Uporabniki se tudi motijo, slučajno ali pa namenoma

GROŽNJE

- Na informacijski sistem in na podatke v njem preži veliko groženj iz okolja:
  - Premalo ali nedoločeni postopki uporabe,
  - Človeške nenamerne napake ali namerna zlonamerna dejanja (Gartner: 80 % storilcev je notranjih),
  - Kriminalne dejavnosti,
  - Napake v opremi,
  - Zunanji človeški ali naravni vzroki.

VIRI GROŽENJ

TVEGANJE

- Tveganje je verjetnost, da se bo z napadom na določeno slabost sistema uresničila določena grožnja, kar bo imelo neželene posledice. (COBIT)
  - grožnja
  - slabost (ranljivost)
  - posledice

OBVLADOVANJE TVEGANJ

TVEGANJA

Vse navedeno so operativna tveganja za informacijski sistem in za podatke, na katera se je potrebno pripraviti.

- Za banke velja Baselski dogovor o upravljanju operativnih tveganj
- Za zavarovalnice velja Solventnost II

V obeh primerih je potrebno zagotavljati minimalni razpoložljivi kapital.

TVEGANJA

- Nepooblaščeno razkritje podatkov lahko povzroči poslovno ali osebno škodo,
- Pomanjkljivi ali pokvarjeni podatki povzročajo napake in onemogočajo normalno poslovanje,
- Izguba ali nedostopnost podatkov lahko za podjetje pomeni veliko poslovno škodo ali celo neizbežen konec poslovanja (ZBan)

TVEGANJE OSEBNIH IN POSLOVNIH PODATKOV

Nepooblaščeno razkritje osebnih podatkov, občutljivih osebnih podatkov in zaupnih poslovnih podatkov (ZVOP-1, KZ):

- neposredna škoda v obliki kazni urada informacijskega pooblaščenca zaradi neskladnosti z ZVOP-1,
- neposredna škoda v obliki odškodninskih tožb oškodovanih posameznikov,
- neposredna finančna škoda,
- posredno gospodarsko škodo in
- posredno škodo v obliki izgube zaupanja in ugleda družbe.

TVEGANJE OSEBNIH IN POSLOVNIH PODATKOV

Ukrepi za zmanjšanje tveganja:

- Zagotavljanje informacijske varnosti
  - Sistem ISMS (SVVI, SUVI)
- Zagotavljanje revizijske sledi (Audit Trail)
  - Kdo, kdaj, kaj, vsebina

TVEGANJE NEPREKINJENOSTI POSLOVANJA

Izguba celovitosti podatkov in izguba dostopnosti podatkov:

- Nepopolni podatki, dodatno ročno delo,
- Moteno poslovanje, potrebno je ročno delo,
- Ogroženo je poslovanje in obstoj organizacije.

TVEGANJE NEPREKINJENOSTI POSLOVANJA

Ukrepi za zmanjšanje tveganja:

Zagotavljanje informacijske varnosti (ISMS)

Uvedba sistema neprekinjenosti poslovanja:

- Upravljanje z neprekinjenostjo poslovanja (BCM): analiza poslovanja - BIA, strategija, politika, krizna skupina,
- Načrti neprekinjenega poslovanja za poslovna področja (BCP),
- Načrti za povrnitev poslovanja po krizi

VARNOST IS

- Postavitev sistema informacijske varnosti (ang. ISMS, slov. SVVI ali SUVI)
- Zagotavljanje skladnosti s standardom ISO/IEC 27001, ISO/IEC 27002

VARNOST IS

Koliko varnosti

Princip čebule

Najšibkejši člen

STANDARD ISO/IEC 27001

- Varnostne politike (zagotoviti usmeritve in podporo vodstva skladno s poslovnimi zahtevami)
- Organizacija varovanja podatkov (znotraj in proti zunanjosti)
- Upravljanje sredstev (evidenca in lastništvo sredstev, klasifikacija informacij)
- Varovanje človeških virov

STANDARD ISO/IEC 27001

- Fizična zaščita in zaščita okolja (nepooblaščeni dostopi, varovanje opreme)
- Upravljanje s komunikacijami in s produkcijo (pravilno in varno delovanje, storitve zunanjih izvajalcev, prevzem sistema, zlonamerna koda, varnostno kopiranje, upravljanje omrežja, nosilci podatkov)

STANDARD ISO/IEC 27001

- Nadzor dostopa (pooblaščeni dostopi do IS)
- Nakup, razvoj in vzdrževanje IS (varnostne zahteve, obdelave, kriptiranje)
- Upravljanje incidentov pri varovanju podatkov (poročanje, analiziranje)
- Upravljanje neprekinjenega poslovanja
- Združljivost (zakonodaja, standardi, varnostne politike, presoje)

KAJ VSE TO POMENI V VSAKODNEVNEM ŽIVLJENJU

?

ZLORABE NA BANKOMATIH

Prestrezanje magnetnega zapisa na kartici in video zapis vnosa kode (Skimming):

- Prepis magnetnega zapisa
- Razkritje osebne kode PIN
- Izdelava ponarejenih bančnih kartic
- Oškodovanje imetnikov kartic

Card Skimming Devices

Camera Skimming device

Camera Skimming device

Additional Costs

ZLORABE NA BANKOMATIH

Vdor v sistem procesorja kartic ali banke in izdelava ponarejenih kartic (10 do 15 USD za podatke ene kartice):

- Uvedba „čip“ kartic
- Uvedba sistema PCI DSS
- Uvedba večje informacijske in fizične varnosti

ZLORABE NA BANKOMATIH

- S pomočjo „vilic“ na vratih za bankovce s fizično silo odvzet denar, kar avtomat zabeleži kot napako na mehanizmu za izplačilo bankovcev in zavede stornacijo dviga.

ZLORABA TERMINALOV POS

- Namestitev predelanega terminala POS
  - Vgrajeno drugo ali dodatno vezje za prestrezanje podatkov
  - Vgrajena komunikacija drugam
  - Vgrajena brezžična komunikacija
- Prestrezanje podatkov s kartic
- Izdelava ponarejenih bančnih kartic
- Oškodovanje imetnikov kartic

INTERNET

Kaj se dogaja:

- Spamware, spyware, malware, ...
- Phishing, spam,
- Virusi, črvi, trojanski konji, ...
- Groba sila, ...
- Napadi, pridobivanje zbirk podatkov,
- Socialni inženiring, ...

INTERNET

- Nepooblaščen dostop, vdor, kraja podatkov,
- Kraja identitete,
- Kraja intelektualne lastnine,
- Kršenje zasebnosti,
- Preprečevanje dostopa do storitev (DOS),
- Računalniške prevare,
- Širjenje dezinformacij, ...

INTERNET

- Izdelava spletne strani, ki je zelo podobna neki resnični spletni strani, npr. bančni
- Bančni komitent na takšno stran vtipka svoje bančno uporabniško ime in geslo
- Storilec tako dobi podatke o bančnem računu in ga čim prej izprazne

INTERNET

- Namestitev zlonamerne programske kode s pomočjo e-sporočila,
- nepooblaščen prevzem elementov identitete (geslo, digitalno potrdilo),
- Izvajanje nepooblaščenih transakcij – dvigov,
- Nakazovanje denarja na račune posrednikov – mul.

INTERNET

Vzroki za navedene grožnje:

- Nezadovoljni notranji uslužbenci (sabotaža),
- Radovednost,
- Objestnost, dokazovanje, tekmovanje,
- Nezakonito pridobitništvo,
- Zbiranje informacij – varnostne službe,
- Elektronsko vojskovanje, ...

BREZŽIČNO KOMUNICIRANJE

- Uporaba brezžične komunikacije brez ustreznih varnostnih nastavitev (kako imate doma nastavljen vaš ruter),
- Možnost vdora v naš sistem in izraba zaupnosti podatkov,
- Možnost predstavljanja z lažnim imenom

POZORNOST

- Pri uporabi informacijskega sistema je vedno potrebno predvideti tudi neljube dogodke,
- Potrebna je stalna pazljivost.
- Vprašanja, komentarji ?

Hvala za pozornost

j.uratnik@siol.net