Informacijska sigurnost – koristi ispod horizonta

Zlatko Švigir, direktor

ALTIN USLUGE d.o.o.

Informacijska sigurnost

Što je informacija?

Informacija je rezultat obrade, manipulacije i organiziranja podataka na način koji dodaje znanje primatelju. Drugim riječima, to je kontekst u kojem su podaci uzeti.

'Informacija' kao koncept ima mnoštvo značenja, od svakodnevnih pa do tehničkih uporaba. Općenito govoreći, koncept informacije je usko povezan s notacijama ograničenja, komunikacije, upravljanja, podataka, oblika, instrukcija, znanja, značenja, mentalnog podražaja, uzroka, opažanja i predstavljanja.

http://hr.wikipedia.org/wiki/Informacija

Informacijska sigurnost

Što je informacija?

Informacija je imovina, koja i poput druge važne imovine za organizaciju i njeno djelovanje, ima vrijednost i stoga mora biti adekvatno zaštićena.

Informacija se javlja u različitim oblicima:

- Ispisana na papiru
- Pohranjena u digitalnom obliku
- Poslana klasičnom ili e-poštom
- Izgovorena tijekom konverzacije
- .....

Informacijska sigurnost

Što moramo osigurati informaciji?

Povjerljivost (Confidentiality)

Osigurati da je informacija dostupna samo onima s ovlastima pristupa.

Princip „need to know”.

Integritet (Integrity)

Čuvanje točnosti i potpunosti informacije i metoda obrade.

Dostupnost (Availability)

Osigurati da ovlašteni korisnici imaju pristup informacijama kada je potrebno.

Informacijska sigurnost

Današnja situacija i trendovi

- Sve je veći značaj informacija za svaki poslovni sustav (informacija je kritična komponenta poslovnog sustava)
- Sve je veća ovisnost o informacijsko-komunikacijskim tehnologijama
- Sve je veća mogućnost napada na informacije
- Sve su teže posljedice uslijed gubitka ili kompromitiranja informacija

Što je sve predmet zaštite

Iz prethodne definicije informacije proizlazi da je informacija zapravo imovina.

(Imovina je sve ono što ima vrijednost za organizaciju.)

Imovina (sve što je uvezi s informacijama a ima vrijednost):

- Baze podataka
- Oprema
- Softver
- Dokumenti na papiru
- Digitalni sadržaji
- Ljudi
- Reputacija

Što je sve predmet zaštite

Ta imovina se može prepoznati kao:

- **Intelektualno vlasništvo**
  - **Autorsko pravo (vaš proizvod ali i kupljeni softver)**
  - **Žigovi, patenti i licence**
  - **Patenti**
- **Znanje o proizvodima i tehnologijama (istraživanje i razvoj)**
- Znanje o tržištu (kupci, konkurencija)
- Poslovna tajna
  - Komercijalni ugovori (kupci, dobavljači, posrednici, lobisti)
  - Ugovori o radu, menadžerski ugovori
  - Financijski podaci
- Osobni podaci
- Svi oblici javne prisutnosti organizacije

Izvori prijetnji

Broj napada na informacijske sustave organizacija koji su registrirani u proteklih desetak godina povećao se 20-50 puta (ovisno o izvorima!).

Prema istraživanjima:

- Više od 90% organizacija doživjelo je napad
- Više od 80% napadnutih organizacija potvrdilo je financijske gubitke
- Najmanje 70% organizacija imalo je incidente
- Oko 40% napada došlo je izvana (znači, više je napada iznutra!)
- Oko 66% organizacija doživjelo je probleme zbog malicioznog koda

Podaci o štetama uglavnom nisu dostupni ali procjene spominju >2 milijarde USD godišnje (vrijednost imovine u kontekstu informacije teško je procijeniti u novčanom ekvivalentu).

Najčešće posljedice

- Nedostupnost servisa
- **Otkrivanje informacija (namjerno ili nehotično)**
- **Krađa informacija (upad izvana ili kompromitacija iznutra)**
- **Izmjena ili uništavanje informacija (izvana ili iznutra)**
- Gubitak reputacije

Sve spomenuto podrazumijeva štetu u konkretnim gubicima kroz gubitak prihoda, gubitak kupaca, gubitak tržišnog udjela, pad vrijednosti dionica, gubitak reputacije, zaostajanje u plasmanu inovativnih proizvoda, ...

Situacija je vjerojatno još puno teža jer se objavi samo 15-20% slučajeva.

(Teorija sante leda.)

Oblici prijetnji – ljudski faktor

- Nepažnja
- Nedisciplina
- Nemar
- Neznanje
- Neodgovarajući oprema (hardver i/ili softver)
- Neodgovarajuća organizacija (odgovornosti)
- Namjera
- Posljedica izvanrednog događaja
- Primjena softvera iz nepouzdanih izvora

Vrijednost organizacije

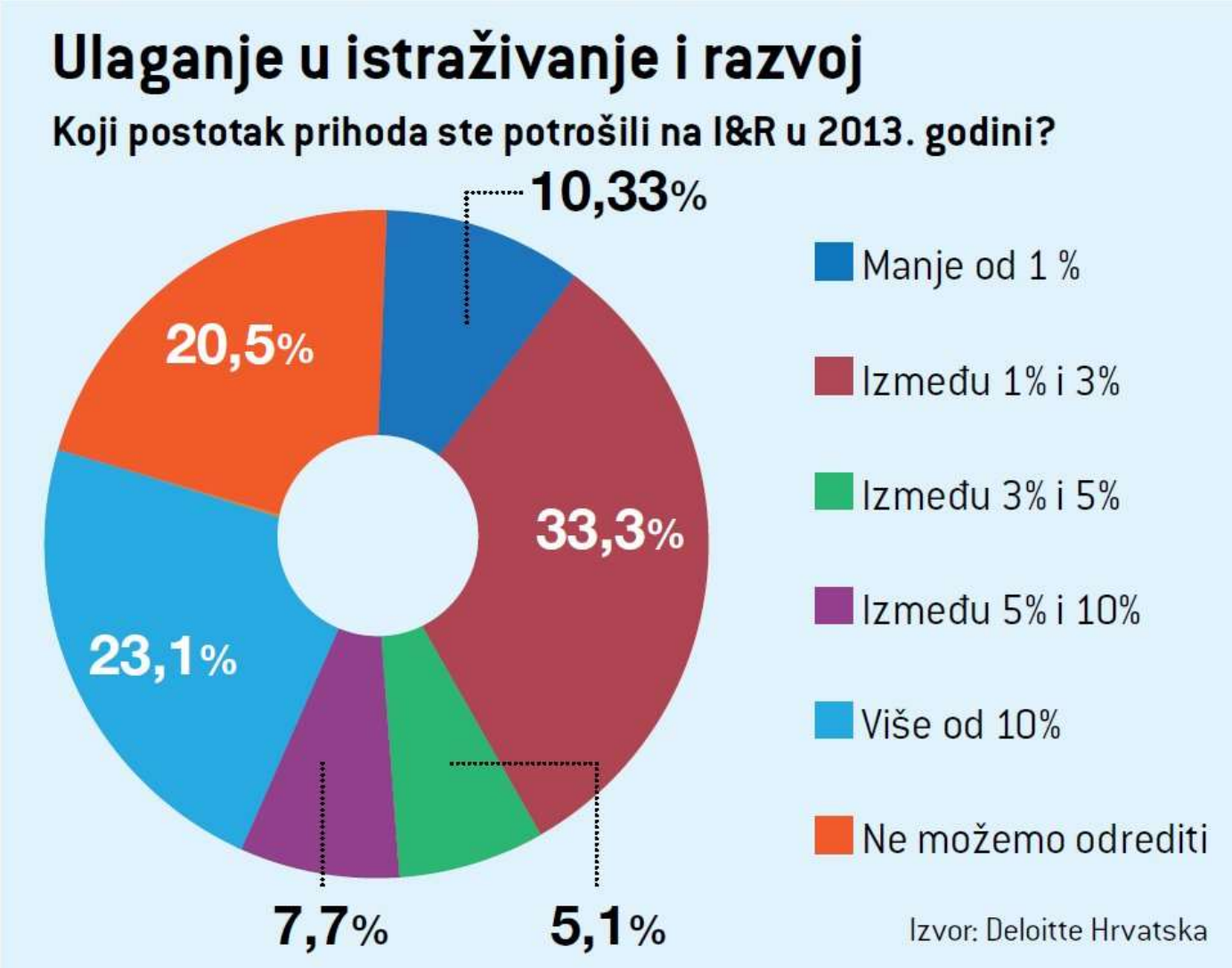
Vrijednost moderne organizacije (tržišna vrijednost):

- Knjigovodstvena vrijednost (financijski kapital) =>10-30%
- Intelektualni kapital (informacije) =>70-90%

Primjer svjetski poznatih brendova

- Kapitalizacija na burzi višestruko premašuje knjigovodstvenu vrijednost

Neovisno istraživanje (1)



Neovisno istraživanje (2)

Neovisno istraživanje (3)

- U istraživanje i razvoj ulažu se relativno velika sredstva.
- Za IT industriju to znači i puno veći postotak jer se dobar dio aktivnosti upravo bazira na razvoju novih ili usavršavanju postojećih proizvoda.
- Patentna zaštita je skupa, a kod softvera i teško primjenjiva
- Zaštita autorskog prava je diskutabilna
- Organizacijama preostaju sustavne mjere zaštite intelektualnog kapitala:
  - Pravne (ugovori, primjena odredbi o poslovnoj tajni, pravni mehanizmi)
  - Organizacijske mjere (odgovornost, nadležnost, svijest zaposlenika)
  - Tehnološke mjere (upravljanje pristupom informacijama, kriptiranje, i druge raspoložive mjere)

Zaštita intelektualnog kapitala

Primjena najbolje prakse koje nudi rješenja za primjenu spomenutih mjera:

- ISO 27001 Informacijska sigurnost
- ISO 31000 Upravljanje operativnim rizicima
- ISO 9001 Upravljanje kvalitetom proizvoda/usluge (poslovanja)

Model informacijske sigurnosti ISO 27001

A5. Politika informacijske sigurnosti
A6. Organizacija informacijske sigurnosti
A7. Sigurnost vezana uz osoblje
A8. Upravljanje (informacijskom) imovinom
A9. Kontrola pristupa
A10. Kriptografija
A11. Fizička sigurnost i sigurnost okruženja
A12. Sigurnost operativnih postupaka
A13. Sigurnost komunikacija
A14. Nabava, razvoj i održavanje informacijskih sustava
A15. Odnosi s dobavljačima
A16. Incidenti informacijske sigurnosti
A17. Informacijska sigurnost u upravljanju kontinuitetom poslovanja
A18. Sukladnost sustava sa zahtjevima

Prevencija po pitanju zakonskih zahtjeva

Zaštita osobnih podataka
Informacijska sigurnost (kazneno zakonodavstvo)
Poslovna tajna
Osiguranje kontinuiteta poslovanja
Upravljanje softverskom imovinom (autorsko pravo)
Zaštita intelektualnog kapitala
Odgovornost i nadležnost (radno zakonodavstvo)

Čuvanje informacija i arhivsko gradivo
- Records Management

Plan kontinuiteta poslovanja (uspostava i redovita provjera)

Plan reakcije za moguće incidente

To uključuje osiguranje potrebnih resursa (materijalnih, organizacijskih, ...) i dokumentirane procedure npr. za:

- Interna komunikacija, eskalacija
- Eksterna komunikacija (posao za PR stručnjake)
- Dislokacija poslovanja ili dijela poslovanja
- Pokretanje pravne zaštite
- Prijava nadležnim tijelima

Pokretači za ISO 27001

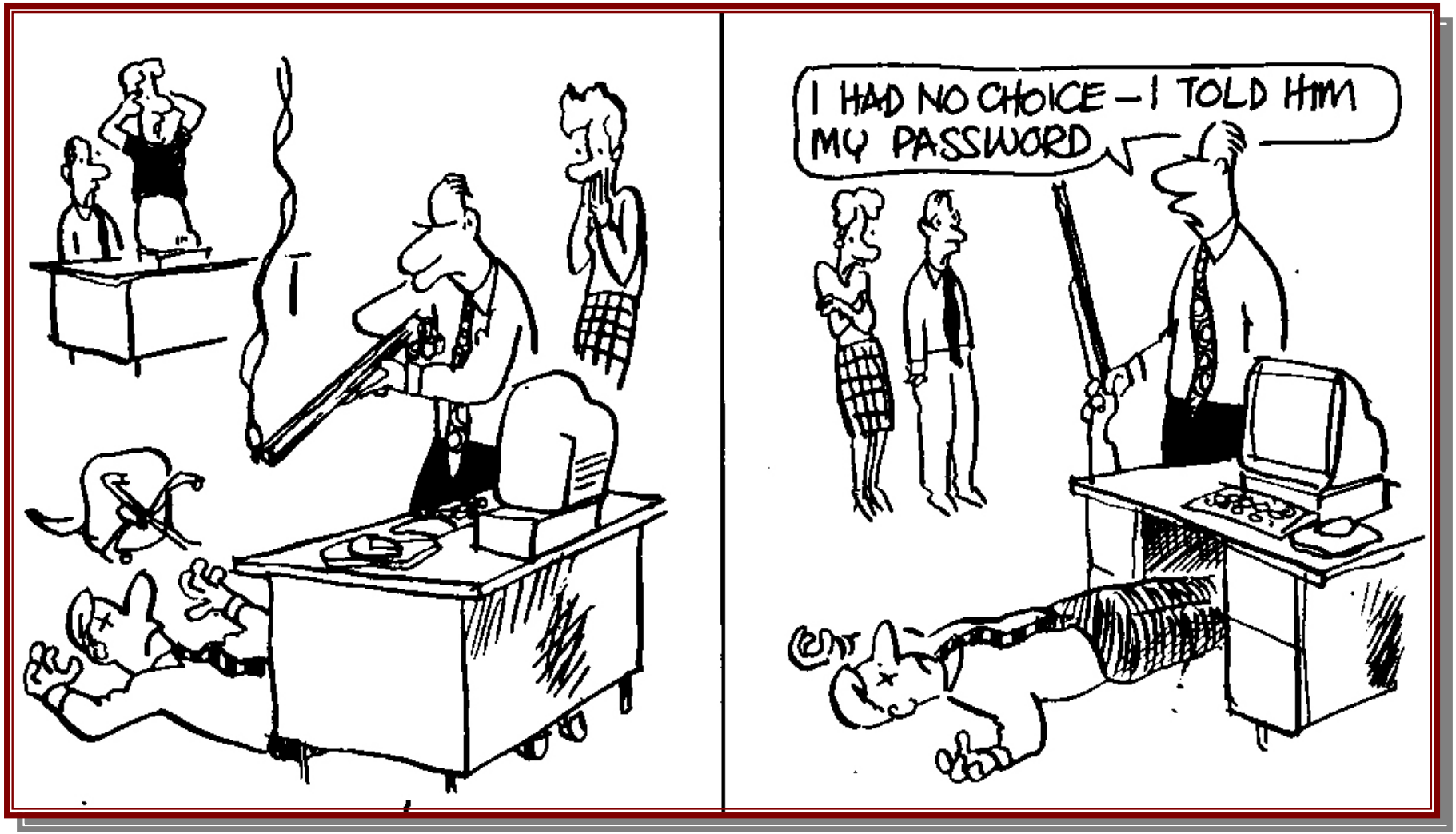
- Jedinstveno korporativno upravljanje
- Povećanje svijesti o izloženosti rizicima
- Povećanje konkurentnosti
- Očekivanja kupaca
- Očekivanja tržišta
- Povećanje ugleda u javnosti
- Zakonski i regulatorni zahtjevi

Sustav upravljanja informacijskom sigurnošću

Dobrobiti od zadovoljenja zahtjeva prema ISO 27001

- Djelotvorna kontrola informacijske sigurnosti
- Diferencijacija od konkurencije
- Zaštita tajnosti kupaca, dobavljača i ostalih uključenih strana
- Jedina globalno prihvaćene i prepoznatljiva norma
- Sukladan sa zakonskom regulativom

Svijest o značaju informacijske sigurnosti



Pitanja i diskusija

ALTIN USLUGE d.o.o., Zagreb

www.altin-usluge.hr

info@altin-usluge.hr

+385 (0)1 3655 040

www.dnvgl.com

SAFER, SMARTER, GREENER