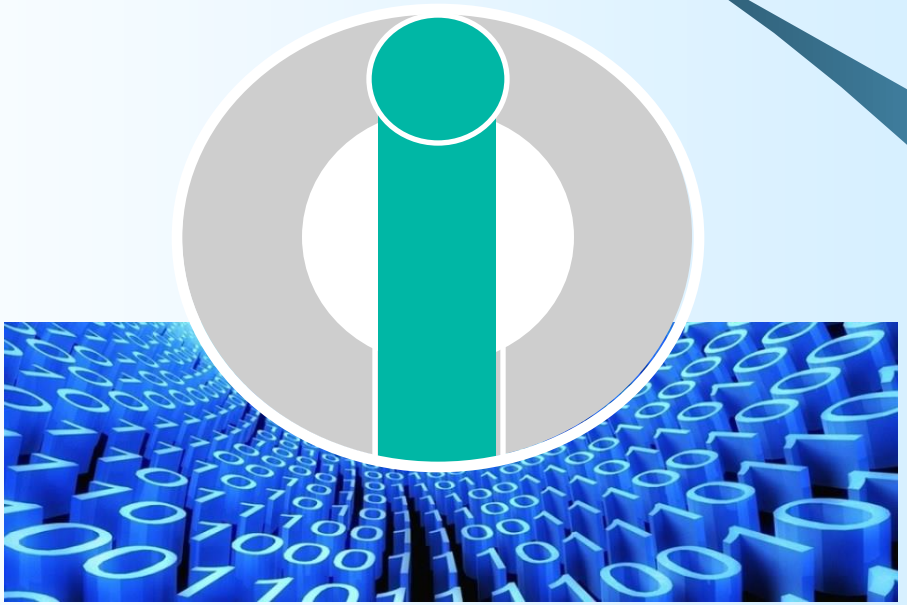
Upravljanje bezbednošću informacija



dr Miodrag Vuković
Senior konsultant, Lead Auditor ISO 27001
m.vukovic@conseko.rs

Informacije o izbornom predmetu

Jednosemestralni predmet koji daje osnove za zaštitu informacija u organizacijama i informacionim sistemaima

- Pristustvo predavanjima je obavezno
- Uslov za izlazak na kolokvijum: najviše 3 izostanka

Uslovu za položen ispit:

- Položen kolokvijum
- Predat seminarski rad
- Usmeno odbranjen seminarski rad

Način formiranja konačne ocene

Kriterijumi za konačnu ocenu:

- Položen kolokvijum -40%
- Predat seminarski rad - 40%
- Usmeno odbranjen seminarski rad -20%

Literatura

- Gojko Grubor, Projektovanje menadžment sistema zaštite informacija, Univerzitet Singindunum 2012
- Gojko Grubor, Milan Milosavljević, Osnove zaštite informacija, Univerzitet Singidunum, 2010 (dostupna online)
- ISO 27002 Bezbednost informacija, sajber bezbednost i zaštita privatnosti — Kontrole bezbednosti informacija
- Dragan Pleskonjić, Nemanja Maček, Borislav Đorđević, Marko Carić, Sigurnost računarskih mreža, Viša elektrotehnička škola u Beogradu 2006 (dostupna online)

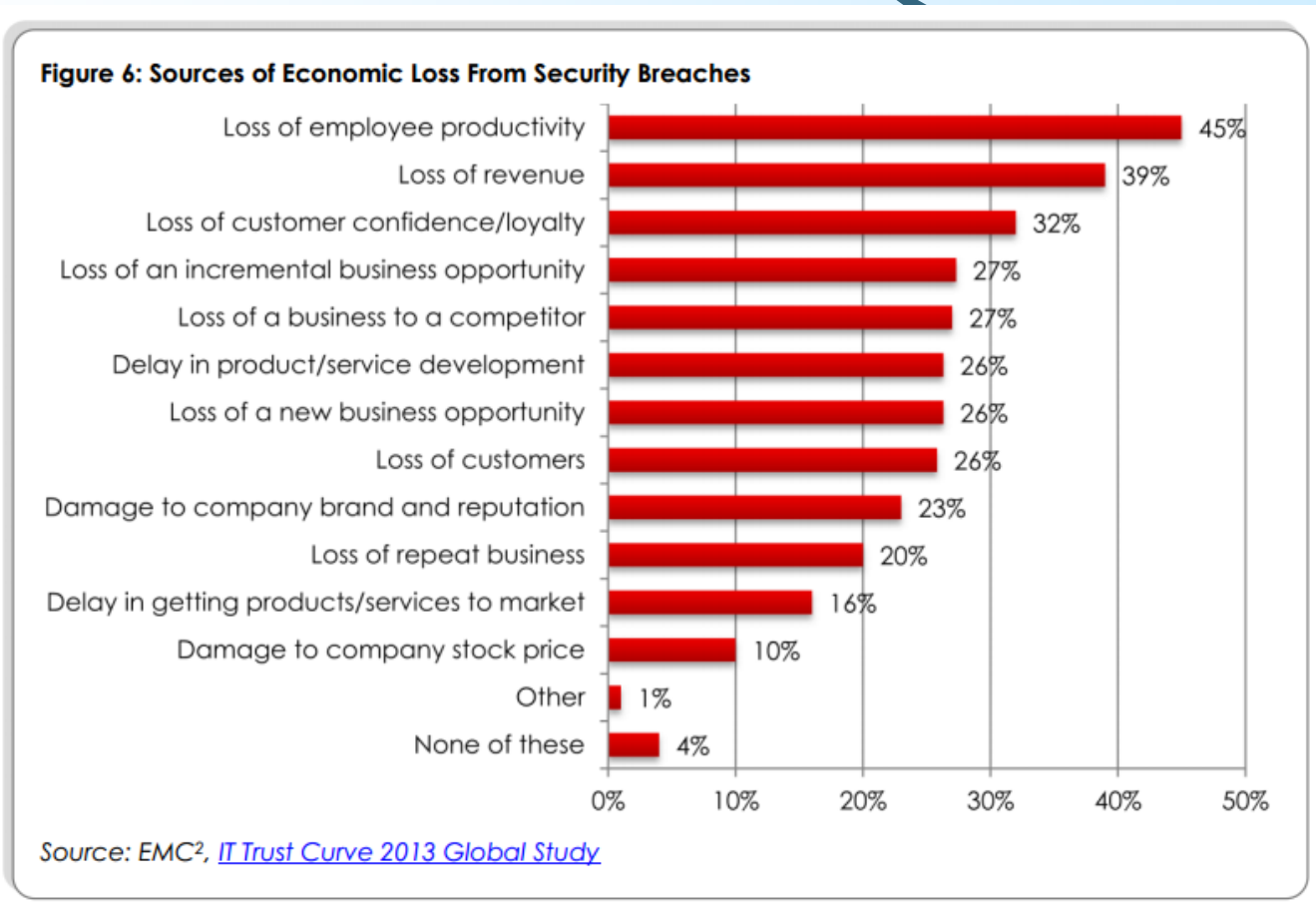
Sadržaj predmeta

- Povodi za zaštitu informacija
- Međunarodni standardi za bezbednost informacija
- Spoljašnje i unutrašnje pretnje bezbednosti informacija
- Zaštita računara
- Zaštita pristup aplikacijama i informacijama
- Osnove kriptografije
- Standard ISO 27001 Sistem menadžmenta bezbednosti informacija
- Politike bezbednosti informacija
- Metode zaštite informacija
- Konsultacije kod odabira teme za seminarski rad i izradu rada

Potrebe za bezbednošću informacija

- Informacije u današnjem poslovanju spadaju u najviše vrednosti resursa u organizacijama
- Sve više klijenata se interesuje za bezbednost informacija
- Potreba za zaštićenim podacima u poslovanju
- Potreba i zakonska osnovai za zaštitom privatnosti
- Novi rizici za bezbednost sa većim korišćenjem tehnologija
- Zahtevi nekoliko vrsta sertifikacija
  (ISO 27001, ISO 22301, PCI DSS ...)
- Zakonski zahtevi (Zakon o zaštiti podataka o ličnosti, Zaštita poslovne tajne, Zakon o tajnosti podataka, Zakon o informacionoj bezbednosti i dr.)

Ekonomske štete od povreda nad podacima



Ko biva najviše napadnut?

- Finansijske institucije i banke
- Internet servis provajderi
- Farmaceutske kompanije
- Vlada i agencije za odbranu
- Ugovarači vladinih agencija
- Multinacionalne korporacije
- Bilo ko, da se nalazi na mreži

Ove organizacije treba da zaštite svoju ranjivost

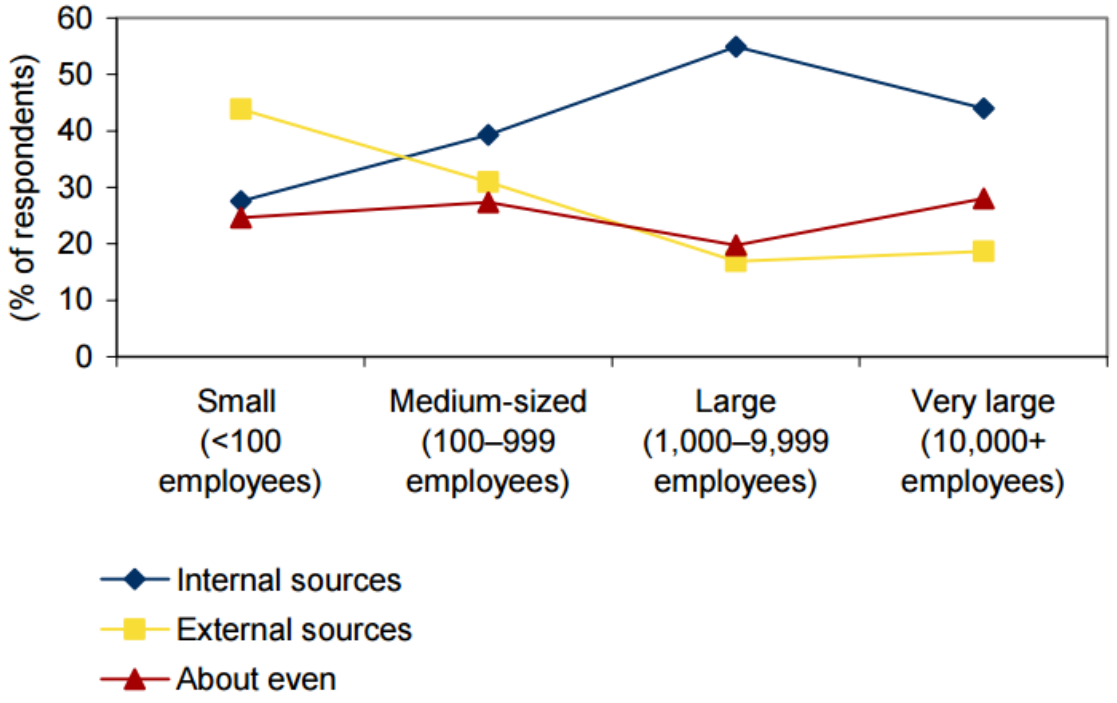
Poverljive informacije za privredne subjekte

- tehnološke i komercijalne informacije koje se odnose na organizaciju ili njene poslovne partnere,
- odnose se na njihovo poslovanje, objekte, proizvode, tehnička rešenja i procese

Organizacije su obavezne da štite poverljive informacije

Pretnje spolja i iznutra

Origin of Most Serious Threats: Internal Sources or External Sources?



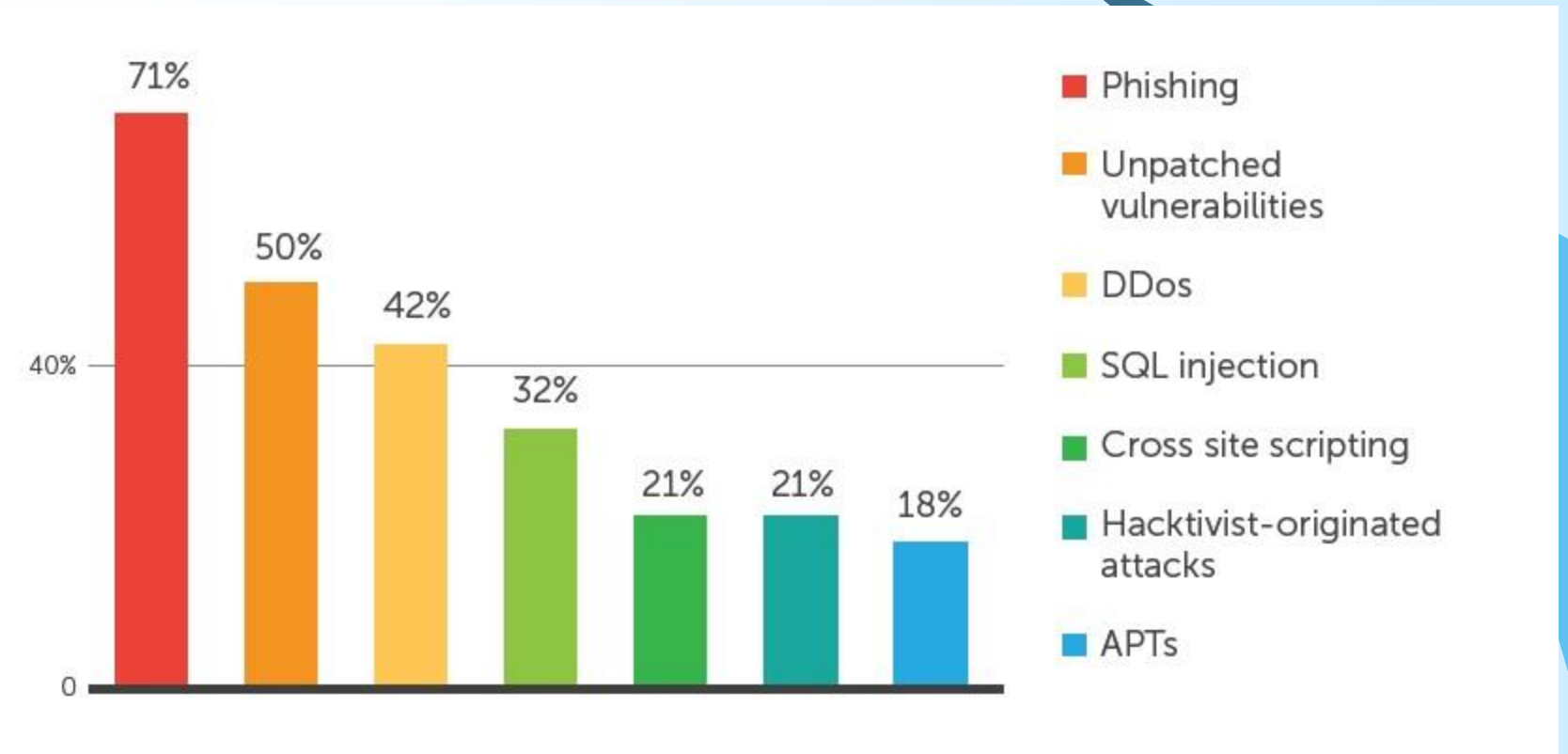
Source: IDC's 2007 *Enterprise Security Survey*

U velikim organizacijama povrede su češće unutar organizacije

Najčešćih 20 lozinki na svetu

1. 123456
2. 123456789
3. Qwerty
4. Password
5. 12345
6. 12345678
7. 111111
8. 1234567
9. 123123
10. Qwerty123
11. 1q2w3e
12. 1234567890
13. DEFAULT
14. 0
15. Abc123
16. 654321
17. 123321
18. Qwertyuiop
19. Iloveyou
20. 666666

Najčešći vektori sajber napada



Razlozi uspostavljanja ISO 27001
Sistem menadžmenta bezbednošću informacija

Sistem omogućava organizaciji da:

- zadovolji zahteve bezbednosti informacija organizacije, kupaca i drugih zainteresovanih strana;
- ostvaruje svoje planove i aktivnosti;
- ispuni ciljeve bezbednosti informacija;
- bude u skladu sa propisima, zakonima, ugovornim obavezama i očekivanjima zainteresovanih strana; i
- upravlja informacionom imovinom na organizovan način

13

Principi uspostavljanja bezbednosti informacija prema ISO 27001

- Razdvajanje zaduženja
- Pristup dokumentima i podacima na „need to know“ osnovi
- Razmena informacija u skladu sa procenom rizika
- Obezbeđenje redundantosti da bi se izbegao „single point of failure“
- Monitoring aktivnosti, uključujući privilegovane korisnike
- Kontrola spoljnjeg pristupa mrežama i razdvajanje mreža
- Testiranja aplikacija (sa anonimizovanim podacima)
- Enkriptovanje osetljivih podataka u bazama i podataka u saobraćaju
- Učenje iz incidenata

Hvala na pažnji!