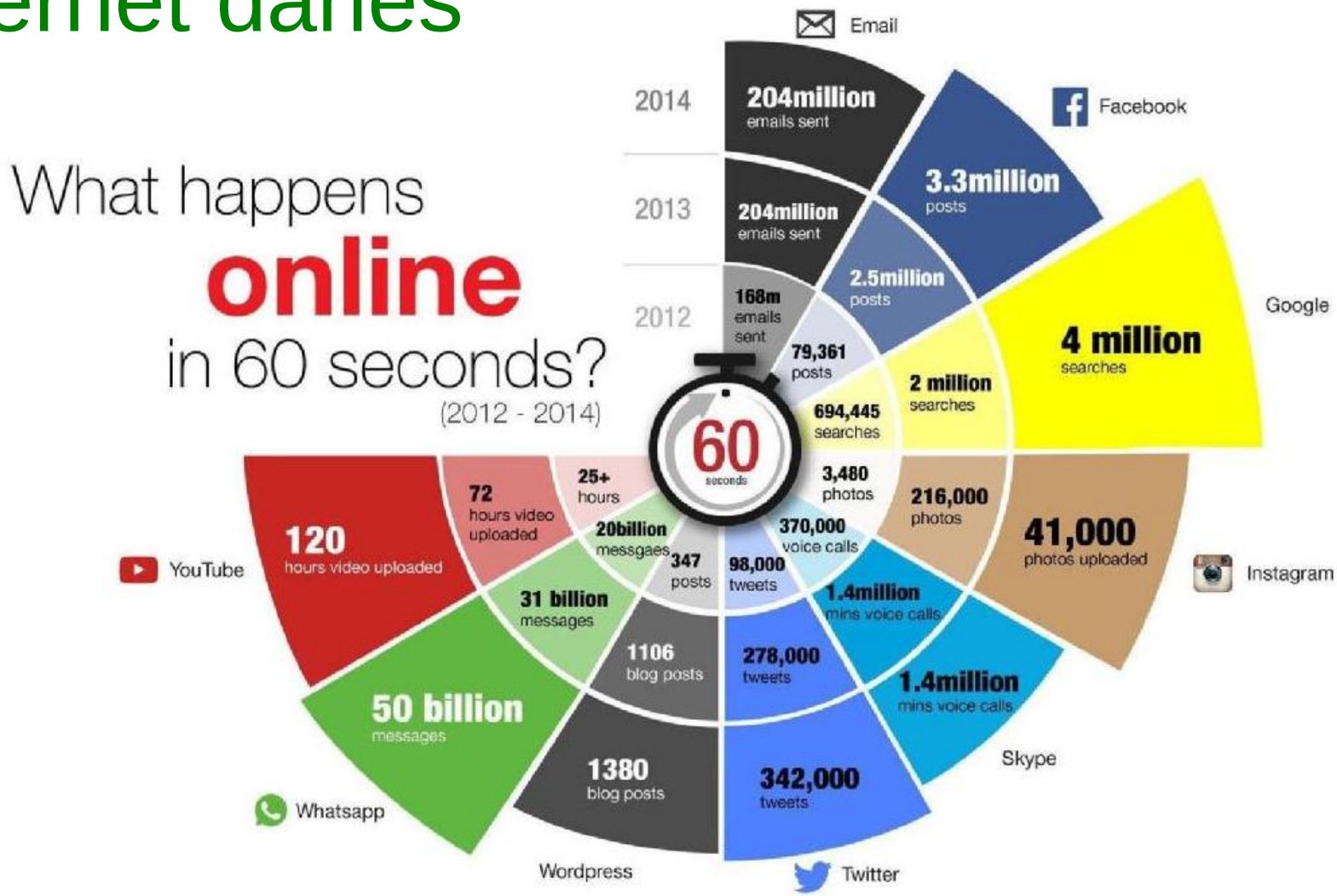
INTERNETNA VARNOST

Davor Katanovič, mag. družb. inf.

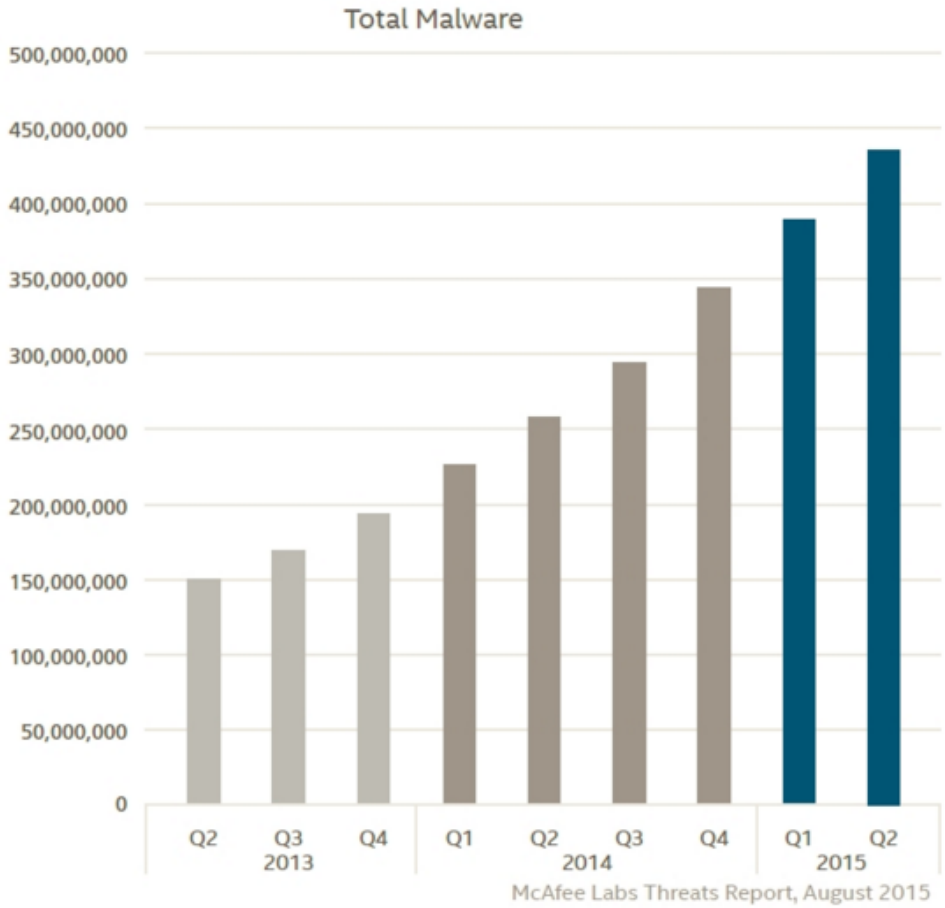
CISSP, Security+

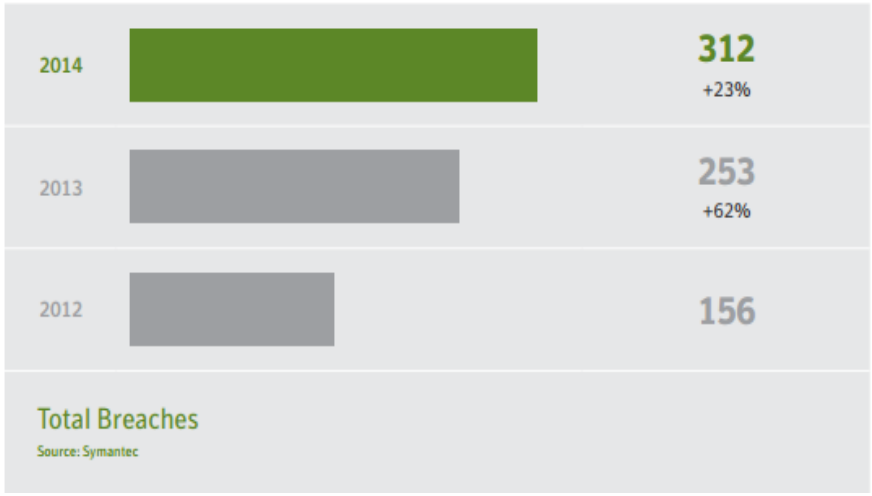
Internet danes

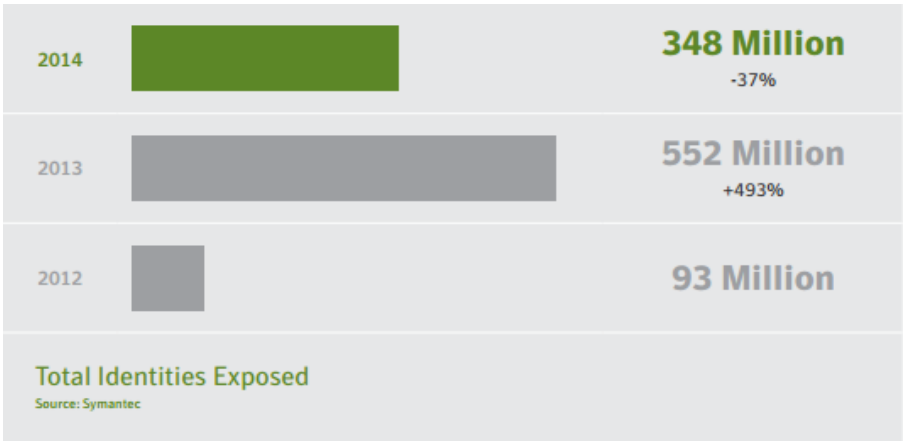


Vir: https://afrikanet.wordpress.com/2015/05/22/the-importance-of-internet-today/

Internet – temna stran







Vir: http://www.symantec.com/security_response/publications/threatreport.jsp

Inf. varnost v podjetju -> SVVI

Cilj **Sistema vodenja varovanja informacij** je varovati podatke:

- RAZPOLOŽLJIVOST
- ZAUPNOST
- CELOVITOST

- Identifikacija ključnih podatkov: Kaj je najbolj dragoceno in kje se to nahaja?
- Ocena tveganj:
  - GROŽNJE
  - RANLJIVOSTI
  - TVEGANJA
  - UKREPI ZA ZMANJŠANJE TVEGANJ (tehnični in organizacijski)

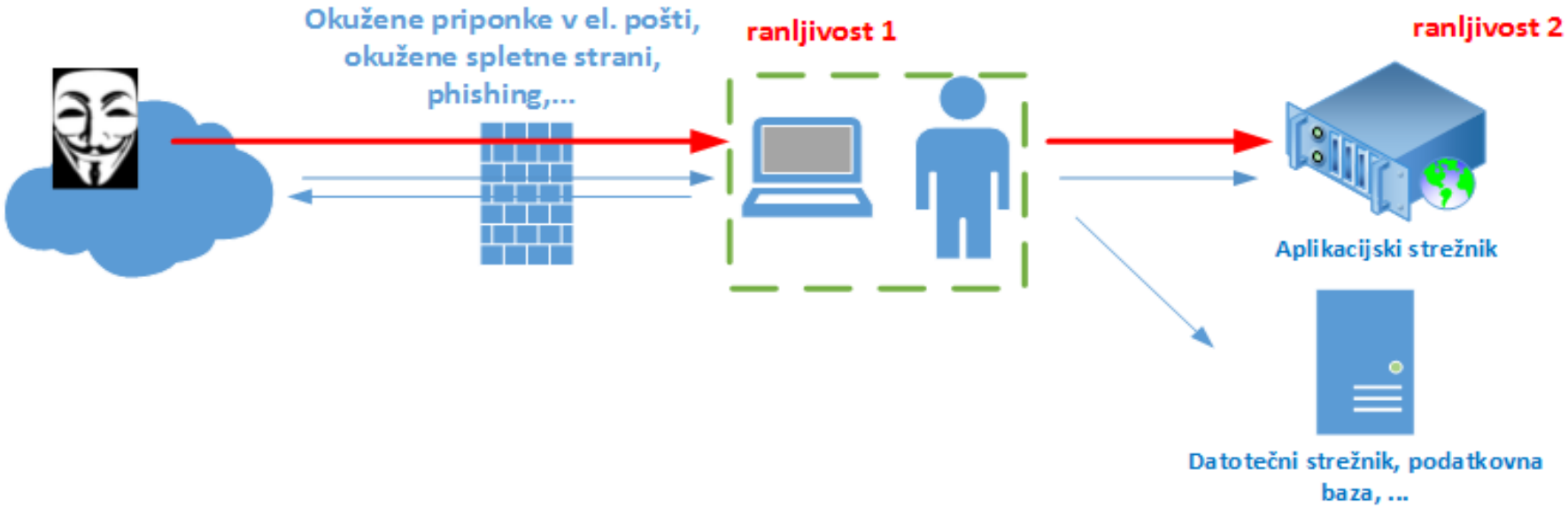
Ključni IS, podatki, dragocenosti?

So tisti podatki, ali IS katerih **ne-razpoložljivost**, **nepooblaščeno spreminjanje** ali **nepooblaščeno razkritje** tretjim osebam podjetju povzroči veliko škodo (materialno, ugled, …):

- ključni IS sistemi,
- elektronsko bančništvo (podatki za prijave),
- zaupni podatki (prodajni načrti, razvoj, ipd.),
- osebni podatki (zakonodaja),
- itd..

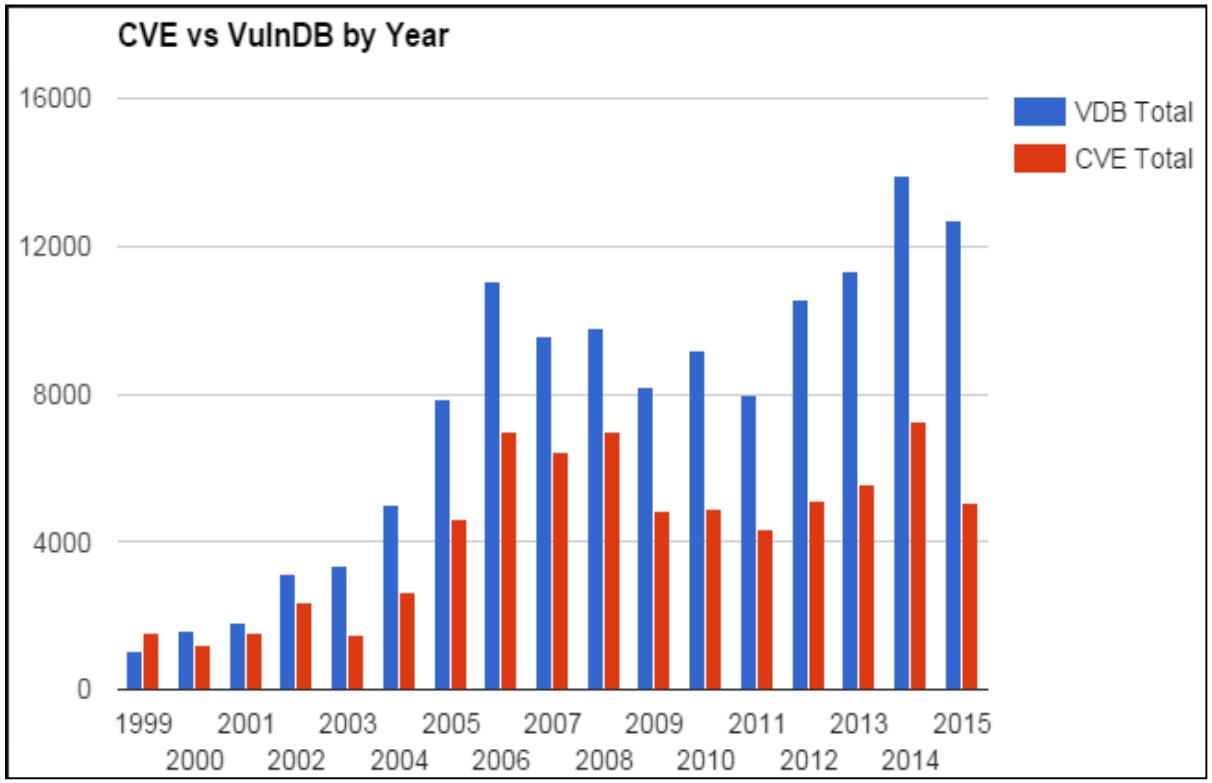
Grožnje (notranje in zunanje):

- **RAZPOLOŽLJIVOST**: okoljske grožnje, fizične grožnje (požar, voda), fizičen dostop, DoS – napad s ciljem onemogočanja storitve, itd..
- **ZAUPNOST IN CELOVITOST**: spletne zlorabe, škodljiva koda, kraja računalniške opreme, socialni inženiring itd.



Ranljivosti IT sistemov/storitev:

- ranljivosti prog. opreme,
- napake v nastavitvah (konfiguracijah) IT sistemov,
- človeški faktor.



…in posledično **tveganja**:

- tveganje ne-razpoložljivosti IT sistemov/storitev (ali podatkov),
- nepooblaščen dostop do poslovnih podatkov (kraja intelektualne lastnine),
- zlorabe v zvezi spletnim bančništvom, „online“ plačevanjem (kraja denarja).

Cilj SVVI je **zmanjšanje tveganj**. Na grožnje nimamo vpliva, torej lahko z ukrepi zmanjšujemo le **ranljivosti**.

Zmanjševanje/odprava ranljivosti – razpoložljivost, celovitost

- varnostno kopiranje podatkov,
- visoka redundanca in podvojenost IS sistemov (sistemskih prostorov),
- ustrezna fizična zaščita (dostop do IS),
- ustrezen sistemski prostor (senzorji za dim, podvojene klime, dvignjena tla, aktivno gašenje, neprekinjeno napajanje – UPS, itn.),
- varnostno posodobljeni IS (odprava DoS ranljivosti.).

Zmanjševanje/odprava ranljivosti – zaupnost (1)

Varnostne kontrole na **mrežnem nivoju** za **preprečevanje** in **detekcijo** zlorab:

- požarne pregrade (požarne pregrade nove generacije),
- ločen segment omrežja za storitve objavljene v splet (DMZ),
- naprave za varen prehod v internet (proxy strežnik),
- varnostni mehanizmi sistema el. pošte (preprečevanje neželene pošte SPAM, phishing, protivirusna zaščita),
- sistemi za detekcijo in preprečevanje neželenega prometa (IDS/IPS sistemi),
- sistemi za varen oddaljen dostop do omrežja,

Zmanjševanje/odprava ranljivosti – zaupnost (2)

- kontroliran dostop do internega omrežje (802.1x) in ustrezne kontrole za preprečevanje MiM napadov v internem omrežju
- varno brezžično omrežje z varno prijavo v omrežje in ustreznim šifriranjem prometa,
- upravljanje z ranljivostmi (zaznavanje in čimprejšnja odprava),
- tehnologije nove generacije (t.i. ATP – Advanced Threat Protection sistemi),
- periodični zunanji varnostni pregledi stanja varnosti (t.i. penetracijski testi).

Zmanjševanje/odprava ranljivosti – zaupnost (3)

Varnostne kontrole na **nivoju strežnikov in računalnikov:**

- upravljanje z ranljivostmi (zaznavanje in čimprejšnja odprava slednjih),
- utrjevanje (ang. hardering) IS,
- preprečevanje zaganjanja škodljive kode:
  - protivirusna zaščita (strežniki, računalniki, mobilne naprave Android, …),
  - tehnologije za varovanje aplikacij (npr. Microsoft EMET),
  - tehnologije za preprečevanje zagona „neodobrene“ programske opreme (t.i. whitelisting),

Zmanjševanje/odprava ranljivosti – zaupnost (4)

- ustrezne politike gesel (uporabniška, skrbniška, …) ,
- šifriranje podatkov na prenosnih poteh v in izven domačega omrežja,
- dodatne varnostne kontrole na napravah, ki zapustijo „domače“ omrežje (zaščita dostopa, šifriranje podatkov, …),
- omejevanje dostopa do interneta (okužene spletne strani),
- dodatne varnostne kontrole na kritičnih računalnikih (domenski administratorji, administratorji, računalniki za spletno plačevanje, ipd.).

Zmanjševanje/odprava ranljivosti – zaupnost (5)

Človeški faktor:

- ustrezne varnostne politike in seznanjenost zaposlenih,
- izobraževanja in povečevanje osveščenosti zaposlenih,
- t.i. „need to know“ pristop pri dodeljevanju pravic,
- ustrezne politike gesel (privat in službena gesla različna, čista miza in zaslon, nedeljene prijav med zaposlenimi ipd.),
- „nezadovoljen“ zaposleni?

Vprašanja

?