dnevi slovenske informatike

USTVARJAMO PRIHODNOST PRILOŽNOSTI

Kongresni center Bernardin, Portorož
11. in 12. april 2017

Prizadevanja Slovenije za obvladovanje tveganj v kibernetskem prostoru

mag. Samo Maček - Generalni sekretariat Vlade RS
mag. Franc Močilar, mag. Franci Mulec - Ministrstvo za zunanje zadeve

12.4.2017

Prizadevanja Slovenije za obvladovanje tveganj v kibernetskem prostoru

Opredelili bomo:

- tveganja in primere kibernetskih napadov (mejniki)
- kako se problematike loteva EU in SLO
- konkretne rešitve in ukrepi (vlada, MZZ)

grožnje: terorizem, organizirani in kibernetski kriminal

spletni kriminal <> družbene ali politične spremembe

viri: hacktivizem, nac., org. kriminal

sistemi, ki so ključni za varnost in delovanje države, so možne tarče

Primeri kibernetskih napadov

1984 – Prihodnost bojevanja pripada kibernetskemu prostoru – William Gibson, **Nevromant**

1988 – Robert Morris, MIT Cambridge – črv – izmeriti **velikost interneta**

2007 – **Estonija –** 3t (bančni, vladni, ekon., elektro sektor)

2010 – **Stuxnet**

Kritična infrastruktura - energetika– Ukr., TR, ZDA, Jap.

Drugi sektorji / storitve (zdravstvo, **mediji**…)

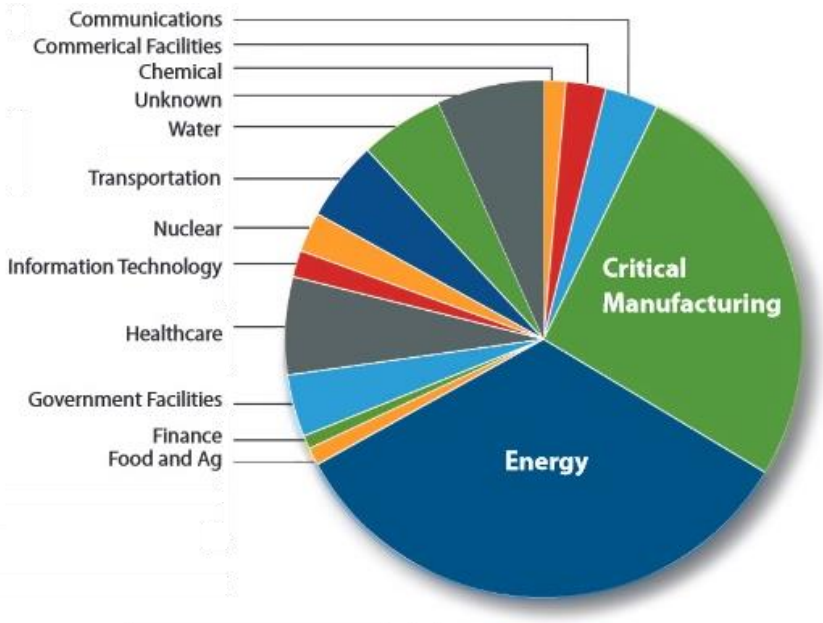
E-pošta – am. volitve

Vault 7 – CIA - varnostne pomanjkljivosti mobilnih telefonov, operacijskih sistemov, televizorjev - vohunjenje

Mirai – internet stvari – botnet – Amazon

Ukrajina – vojska – napadalec postane tarča

Severna Koreja – finančne zlorabe za polnjenje proračuna



Kibernetsko bojevanje

Naraščajoča tveganja - kib. kriminal in terorizem >>

Formiranje enot za kib. bojevanje - ZDA, Kit, Rus, Izr, VB
obramba in napad

EU je šibka pri razvoju
napadalnih zm.

najem kibernetske vojske
napad na Izrael

Regulativa EU (izbrani mejniki)

Konvencija o kibernetski kriminaliteti – 2001 (S)
- Podlaga za sodelovanje med državami in zasebnimi podjetji

Strategija kibernetske varnosti EU – 2013 (EK)

Evropska agendo za varnost - 2015 (EK)
- smernice za odzivanje EU na varnostne grožnje - 2015 do 2020
- Glavno odgovornost za varnost - države članice
- čezmejne grožnje (ter., org. in kib. kr.) – sodelovanje, skupno ukrepanje

Varšavska izjava 2016 (NATO)
- nadaljnja krepitev medsebojnega sodelovanja

Urejanje področja kib. varnosti v SLO

Nacionalna strategija kibernetske varnosti

Strategija kriptografske zaščite podatkov

Ustanovitev nacionalnega organa za kibernetsko varnost

Zakon o kritični infrastrukturi - v medresorskem usklajevanju

Začetek > sodelovanje gosp., akad. sfere in drž. organov

Ukrepi

Se izvajajo na več ravneh:

- uporaba pravnih okvirov – poslovna skrivnost, tajni podatki
- fizični ukrepi varovanja
- posebna pozornost zunanjim izvajalcem
- šifriranje
- akreditacija sistemov
- izbor in usposabljanje kadrov
- ločevanje sistemov glede na zaupnost (oziroma varnost)
- preprečevanje napadov preko stranskih kanalov (optični, akustični, TEMPEST)

Ukrepi za obvladovanje tveganj - stranski kanali

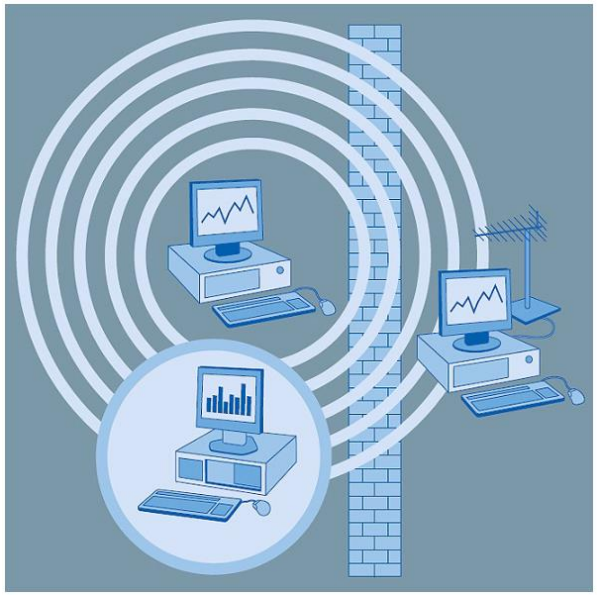
Uporaba IT > vplivi v okolico ~ podatki – rekonstr.

- optični – teleskopi – ekran
- akustični – tipk., laserski mikrofon, vf kamera
- TEMPEST – prestrezanje elektromagnetnega sevanja

  Uporaba IT > vplivi v okolico ~ podatki prestreže > rekonstruira vsebino

  - neposredno iz sevanja
  - preko prevodne infrastrukture

  MI5 – angleži so se bali, da bo De Gaulle blokiral VB pri vstopu v EU – stališče



namenska oprema, prostori, filtri

Ukrepi – človeški vidik

Najšibkejši člen je (še) vedno človek

- vzdušje na delovnem mestu oziroma v organizaciji
- tehnologija ni dovolj, če uporabniki niso ustrezno usposobljeni, se ne zavedajo groženj ali ne upoštevajo varnostnih ukrepov.
- ni vključevanja najboljših v projekte in v usposabljanje za prenos znanja na področju kibernetske varnosti (akademska sfera, gospodarstvo, javna uprava)

Ukrepi / šifriranje

- „Država, ki ne obvladuje šifrirnih rešitev v njihovem celotnem življenskem ciklu, ni država“
- Slovenija že ima organizacije, ki to zmorejo
  - številne rešitve slovenskih podjetij
  - sodelovanje državnih organov z akademsko sfero in gospodarstvom
- posebna funkcija je upravljanje s ključi „brezplačnih rešitev“

Ukrepi / ločevanje sistemov glede na zaupnost (oziroma varnost)

Ločevanje sistemov glede na varnostne zahteve npr.:

- nižje zahteve: običajna delovna mesta v gospodarstvu, javni upravi, domači računalniki, pametni telefoni, nekritična infrastruktura
- višje zahteve: zelo občutljive poslovne skrivnosti, državne skrivnosti, kritična infrastruktura
- povezovanje sistemov npr. koncept diode za prenos podatkov, podsistemi za povezovanje sistemov
- papir in osebni razgovor je še vedno najboljši za najobčutljivejše podatke

Ukrepi / obvladovanje podsistemov

Nekaterih tehnoloških podsistemov še ne obvladujemo v celoti

- večopravilne naprave (MFD)
- Windows 10
- Android
- storitve v oblaku
- telefonske centrale
- protivlomni sistemi
- .....

(Varnostna) kultura kot prednost in omejitev

HVALA ZA VAŠO POZORNOST!

VPRAŠANJA/PRIPOMBE/PREDLOGI

LITERATURA IN VIRI:

- Gradivo navedeno v članku na konferenci
- https://www.iot-now.com/wp-content/uploads/2015/03/Security.ICS-CERT_Monitor.crop_.jpg
- sika: http://www.kongregate.com/games/mike_id/doom-1
- Monitor, april 2017, Domen Savič, Digitalni tanki na naših mejnih prehodih
- https://www.rtvslo.si/znanost-in-tehnologija/kibernetsko-bojevanje-v-primeru-napada-na-slovenijo-konec-v-eni-uri/413340
- slika: http://w3.siemens.com/mcms/topics/en/tempest-products/maximum-protection/pages/default.aspx