

Paraliza države u nekoliko koraka

Dejan Levaja

Network Security Solutions d.o.o.

<http://www.netsec.rs>



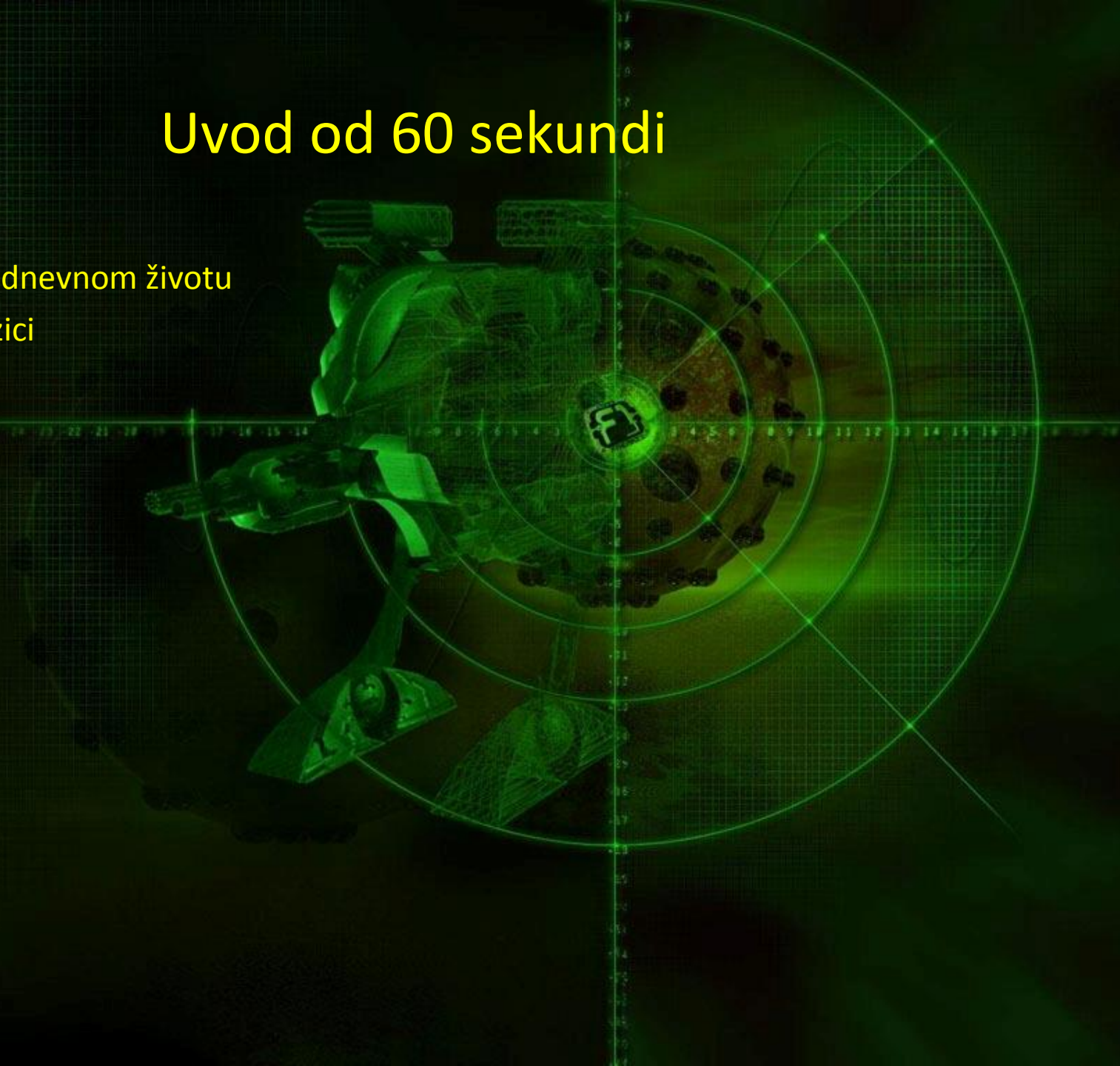
Network Security Solutions d.o.o.

- Network Security Solutions
 - bavimo se isključivo bezbednošću informacionih sistema
 - projektovanje
 - implementacije
 - održavanje
 - Ethical Hacking (testiranje bezbednosti)



Uvod od 60 sekundi

- ICT u svakodnevnom životu
- Pretnje i rizici
- Posledice



Scenario

- Direktan cilj: Napad na infrastrukturu države u cilju paralize sistema
- Indirektan cilj: finansijski gubici, širenje panike, gubitak poverenja u državu...
- Kritična infrastruktura:
 - Elektroprivreda
 - Vodoprivreda
 - Elektronske komunikacije
 - Proizvodnja
 - eUprava
 - <...dodajte svoj cilj...>

Profil ciljeva

- Zajedničke osobine velikih sistema:
 - Veliki broj potencijalnih vektora napada
 - Heterogenost – mnogo gvožđa i softvera
 - Ažuriranje (patching)?
 - Disciplina?
 - IT budžet?
 - Zaposleni
 - socijalni inženjering (zadovoljni i nezadovoljni radnici)
 - obuka (IT bezbednosna kultura?)
 - premalo ljudi u IT (ažuriranje i održavanje trpe posledice)
 - surevnjivosti između timova

Profil napadača

- Zajedničke osobine napadača
 - Neograničeno vreme
 - Nadprosečno znanje
 - profesionalci
 - amateri
 - Planiranje i organizacija
 - Timski rad
 - programiranje
 - operativni sistemi
 - networking
 - kriptografija
 - web aplikacije
 - baze podataka



Cilj: Elektro i vodoprivreda

- Struja
 - Februar 2003. -> Nuklearna elektrana Davis-Besse, Ohajo, SAD
 - Slammer
 - Avgust 2003. -> Mičigen, Ohajo, Njujork i delovi Kanade -> 55 miliona ljudi bez struje
 - software bug (*race condition*) u Unix baziranom sistemu
 - 256 elektrana offline
 - 2008. – 2009. -> Kinezi i Rusi instaliraju hiljade trojanskih konja u elektromrežu SAD
 - “Zero day exploits”, Microsoft Windows i Office
 - Maj 2009. -> bivši radnik onesposobio nuklearnu elektranu iz svoje dnevne sobe
- Voda
 - Januar 2000. -> Maroochy Water Services, Australia
 - nezadovoljni radnik == kanalizacija u vodovodu
 - Oktobar 2006. -> Waterplant Harrisburg, SAD
 - zaražen laptop == zaražena cela mreža



SCADA

(supervisory control and data acquisition)

- Protokoli
 - DDE
 - DeviceNet
 - DF1 - serial communications
 - DH - Data Highway
 - DH+ - Data Highway Plus
 - K-Sequence
 - Modbus
 - OPC - Object Linked and Embedded for Process Control
 - RIO - Remote I/O
 - RS232
 - RS485
 - SuiteLink
 - TCP/IP - Ethernet
 - Tiway

Cilj: Elektronske komunikacije

- Internet pristup
 - linkovi
 - DNS
 - Telefonija
 - IP svuda!
 - VoIP
 - SMS worms
 - GPS zabava
 - “jamming”
 - “RDS-TMC injection”
 - Andrea Barisani & Daniele Bianco “Injecting RDS-TMC Traffic Information Signals”, CanSec West 2007.
- 

DEMO

- Administratorske privilegije u 2 koraka



HVALA!

dejan.levaja@netsec.rs
<http://www.netsec.rs>