Organizacije, standardi, preporuke

Sigurnost i bezbednost

Fakultet tehničkih Nauka, Univerzitet u Novom Sadu

Imre Lendak, 2019

Sadržaj današnjeg predavanja

- Kompanije
- Državne institucije
- Standardizaciona tela
- Nezavisne organizacije
- Preporuke

Organizacije, standardi, preporuke

KOMPANIJE

Kaspersky

- **DEF:** Kaspersky Lab je međunarodna grupa za računarsku bezbednost
  - Centrala: Moskva (Rusija)
  - Osnovan: Kaspersky Anti-Virus je objavljen 1997. godine
  - Broj zaposlenih: ~2800
  - Broj korisnika: 300 miliona
  - Portfolio: anti-malware za pojedince i kompanije, istraživanje (eksperti za lov na malware), SecureList.com stranica za edukaciju
- **Detekcije:** BlackEnergy (2010), Flame (2012), Equation Group (2015)
- **Trivia:** 2015. su optuženi za saradnju sa Ruskom vojskom i tajnim službama

Symantec

- **DEF:** Symantec Corporation je tehnološka kompanija:
  - Centrala: Mountain View, California, USA
  - Osnovan: 1982, sa National Science Foundation (NSF) podrškom
  - Broj zaposlenih: 11,000
  - Portfolio: softver za sigurnost, skladištenje, bekap, istraživanje
- **Detekcije:** DDoS napadi preko IoT uređaja
- **Trivia #1:** 2012. godine su hakeri ukrali izvorni kod starijih Symantec proizvoda nakon upada na server državne uprave u Indiji
- **Trivia #2:** Vlasnik Norton brenda

ESET

- **DEF:** ESET je kompanija čija je primarna delatnost IT sigurnost
  - Centrala: Bratislava, Slovačka
  - Osnovan: 1992 – najuspešnija slovačka kompanija 2008, 2009 i 2010
  - Portfolio: anti-malware, firewall
  - Istraživački centri u Slovačkoj, SAD, Kanadi, Poljskoj
- **Trivia:** Isis (ili Eset) je egipćanska boginja zdravlja, braka i ljubavi

Avast

- **DEF:** Avast je češka kompanija fokusirana na razvoj softvera sigurnost i bezbednost
  - Osnovan: 1988, privatna kompanija od 2010. godine
  - Centrala: Prag (Češka)
  - Korisnika: 400 miliona
  - Zaposlenih: 650 (u Češkoj)
  - Portfolio: anti-malware (nema IPS)
- **Nagrade:** 2016 PCMag.com Editor's Choice za besplatan anti-malware
- **Trivia:** 2016. su kupili AVG Technologies

Hewlett Packard Enterprise (HPE)

- **DEF:** Hewlett Packard (HP) je globolna tehnološka kompanija
  - Osnovan: 1939 – za HP, HPE je nastao razdvajanjem 2015. godine
  - Centrala: Palo Alto, California, USA
  - Korisnika: 10,000 kompanija
  - Zaposlenih: 3000 istraživača (samo sigurnost i bezbednost)
  - Portfolio: bezbedan kod (Fortify), SIEM (ArcSight), IPS, rešenja za enkripciju, istraživanje, Security Operations Center, reakcija na incidente na zahtev
  - U poslu informacione bezbednosti od kraja 1960ih godina
- **Trivia #1:** Saradnja sa velikim kompanijama, npr. 67 SOC-ova za Fortune 500
- **Trivia #2:** Jaki istraživački timovi i (veoma skupa) usluga reakcije na incidente

International Business Machines (IBM)

- **DEF:** International Business Machines (IBM) je globolna tehnološka kompanija
  - Osnovan: 1911, pod imenom IBM od 1924. godine
  - Centrala: Armonk, USA
  - Korisnika: ?
  - Zaposlenih: ~380,000 (ukupno)
  - Portfolio: bezbedan kod (Security AppScan), SIEM (QRadar), IPS, istraživanje i forenzička analiza, SOC
- **Trivia:** IBM se potpuno preorijentisao na IT **usluge**, npr. prodaja PC ogranka Lenovu (2004)

Organizacije, standardi, preporuke

STANDARDIZACIONA TELA

International Organization for Standardization (ISO)

- Internacionalna organizacije za standardizaciju u oblastima tehnologije i proizvodnje
  - ISO je osnovan 1947. godine
  - Centrala se nalazi u Ženevi u Švajcarskoj
  - Objavio preko 21,000 standarda
- **Trivia:** Skraćenica ISO potiče od grčke reči „isos“ što znači jednako – na svakom jeziku se piše isto
- ISO 27000 grupa standarda je fokusirana na sigurnost i bezbednost
  - Prvenstveni fokus je uređivanje neophodnih procesa na nivou cele kompanije

National Institute of Standards and Technology (NIST)

- Nacionalna organizacija SAD za standardizaciju na polju tehnologije
  - Osnovan 1901. godine, trenutno je deo Ministarstva trgovine SAD (engl. Department of Commerce)
- NIST 800 grupa standarda je za sigurnost i bezbednost
  - NIST 800-53 definiše zaštitne mere za federalne agencije – izuzetno detaljan opis zaštitnih mera grupisanih u 18 familija
  - NIST 800-37 upravljanje rizicima, itd.
- 2014. godine je NIST objavio okvir *Framework for Improving Critical Infrastructure Cybersecurity*
  - Grupiše zaštitne mere: identify, protect, detect, respond, recover
  - Sadrži mapiranje između mera definisanih u raznim standardima i preporukama (ISO, NIST, CCS, COBIT, ISA – nema NERC CIP)

NIST 800-53 Security Control Families

- Access Control (AC)
- Awareness & Training (AT)
- Audit & Accountability (AU)
- Security Assessment & Authorization (CA)
- Configuration Management (CM)
- Contingency Planning (CP)
- Identification and Authentication (IA)
- Incident Response (IR)
- Maintenance (MA)
- Media Protection (MP)
- Physical and Environmental Protection (PE)
- Planning (PL)
- Personnel Security (PS)
- Risk Assessment (RA)
- System and Services Acquisition (SA)
- System and Communications Protection (SC)
- System and Information Integrity (SI)
- Program Management Controls (PM)

NERC Critical Infrastructure Protection (CIP)

- North American Electric Reliability Corporation (**NERC**) je međunarodno regulatorno telo za unapređivanje pouzdanosti elektroenergetskog sistema (EES)
  - Formiran 2006. godine kao neprofitna korporacija
  - Nastavlja tradiciju NERC (C = Council) koji je osnovan 1968. god.
  - Fokus na SAD i Kanadu – u SAD je obavezno poštovanje CIP mera
- NERC Critical Infrastructure Protection (**CIP**) standard definiše minimalan skup zaštitnih mera za kompanije u EES
  - Sastoji se od skupa dokumenata sa oznakama CIP002 – CIP014
  - Verzija 6 (u odnosu na v5) uvodi minimalne mere za kompanije niskog značaja (Low Impact) – ranije one nisu imale nikakve (CIP) obaveze
  - Za neadekvatnu primenu CIP mera su zaprećene visoke kazne

NERC CIP – Dokumenta

- CIP002-5.1: Critical Cyber Asset Identification
- CIP003-6: Security Management Controls
- CIP004-6: Personnel & Training
- CIP005-5: Electronic Security Perimeter(s)
- CIP006-6: Physical Security of Critical Cyber Assets
- CIP007-6: Systems Security Management
- CIP008-5: Incident Reporting and Response Planning
- CIP009-6: Recovery Plans for Critical Cyber Assets
- CIP010-2: Configuration Change Management and Vulnerability Assessments
- CIP011-2: Information Protection
- CIP014-2: Physical Security

Organizacije, standardi, preporuke

DRŽAVNE AGENCIJE

National Security Agency (NSA)

- National Security Agency (NSA) – zaštita državne bezbednosti unutar SAD bez ovlašćenja za izvršavanje kiber-napada
  - NSA ima departman za razvoj kiber-oružja
- US Cyber Command (USCC) – ogranak vojske, ima ovlašćenje za izvršavanje kiber-napada
  - Funkcioniše u sklopu NSA, ali postoje planovi da se izdvoji i sa tim stekne šire operativne mogućnosti
- NATO je u junu 2016. godine klasifikovao sajber prostor (eng. *cyberspace*) kao operativni domen pored kopna, mora, vazduha i svemira

Department of Homeland Security (DHS)

- **DEF:** Department of Homeland Security je novo ministarstvo SAD formirano nakon 9/11 napada
- Cilj: Koordiniše rad agencija u domenu sigurnosti i bezbednosti zarad zaštite unutar granica SAD
- Zaposleni: 240,000
- Top prioriteti:
  - Zaštita SAD u civilnoj sferi unutar, na i van granica
  - Odgovara na domaća hitna stanja, npr. terorističke napade, prirodne katastrofe (uragan, poplava, tornado)

Federal Bureau of Investigation (FBI)

- Primarno telo za federalno sprovođenje zakona u SAD
  - Rešavanje problema koji prevazilaze granice pojedinih država SAD
- Osnovan: 1908 – pod imenom FBI od 1935. godine
- Centrala: J. Edgar Hoover Building, Washington, USA
- Zaposlenih: ~35,000
- Top prioriteti:
  - Zaštita SAD od terorističkih napada
  - Zaštita SAD od delovanja stranih obaveštajnih službi
  - Zaštita SAD od napada iz kiber prostora i visoko-tehnološkog kriminala
  - Borba protiv korupcije
  - …

Agencije, univerziteti, kompanije u Srbiji

Visoko školstvo

- Fakultet bezbednosti, Beograd
  - Bezbednost u geo-političkom i fizičkom domenu
- Kriminalističko-policijski univerziteta (KPU)
  - Ranije akademija i skraćenica KPA
  - Školuje kadar za MUP
- Univerzitet odbrane
  - Školuje kadar za Vojsku Srbije
- Akademija za nacionalnu bezbednost
  - Visoka strukovna škola – školuje kadar za BIA-u

Agencije, kompanije

- Bezbednosno Informativna Agencija (BIA)
  - Formirana 2002. godine (ranije Državna Bezbednost – DB)
- Advanced Security Technologies (AST), Niš
  - Razvija SIEM
  - Međunarodno poznati
- NetSet Global Solutions
  - Centrala: Beograd
  - Fokus: integrisani mehanizmi zaštite podataka, tj. kriptografija

Organizacije, standardi, preporuke

NEZAVISNE ORGANIZACIJE

SANS Institute

- **DEF:** SANS Institute je privatna kompanija koja pruža usluge na polju istraživanja i treninga na polju sigurnosti informacionih sistema
- Osnovan: 1989
- Centrala: Boston (USA), u Evropi Swansea (UK)
- Portfolio: trening, sertifikacija, izveštaji istraživanja, Internet Storm Center
- Sertifikati: -

- **Trivia:** SANS je skraćeno od SysAdmin, Audit, Network, Security

Center for Internet Security (CIS)

- **DEF:** Center for Internet Security (CIS) je neprofitna organizacija za jačanje bezbednosti informacija na Internetu
- Osnovan: 2000
- Centrala: East Greensbush, SAD
- Zaposlenih: 180 članova širom sveta
- Portfolio: The CIS Critical Security Controls for Effective Cyber Defense (CSC) – 20 zaštitnih mera

International Information System Security Certification Consortium (ISC)2

- **DEF:** ISC2 je međunarodna, neprofitna organizacija sa ciljem razvoja sigurnog i bezbednog kiber prostora
- Osnovan: 1988
- Centrala: Palm Harbor (Florida, USA)
- Članstvo: 115,000
- Portfolio: trening, sertifikacija
- Najtraženiji sertifikati (brojevi iz maja 2019. godine):
  - Certified Information Systems Security Professional (CISSP) – menadžer
    - Srbija – 33, Hrvatska - 69, Mađarska – 179, Češka – 167
  - Security Certified Practitioner (SSCP) – IB tehničari
    - **Srbija – 1**, Hrvatska - 3, Mađarska – 7, Češka – 16
  - Certified Cloud Security Professional (CCSP) – Računarstvo u oblaku
    - **Srbija – 0**, Hrvatska - 3, Mađarska – 8, Češka – 4

Organizacije, standardi, preporuke

HAKERSKE ORGANIZACIJE

Equation Group

- **DEF:** Equation Group je hakerska grupa koja (najverovatnije) radi za SAD
  - Detektovan od strane: Kaspersky Labs
  - Osnovan: 2001 (po pretpostavkama predstavnika Kaspersky)
- Aktivnosti:
  - 500 identifikovanih malware zaraza u 2015. godini
  - Većina meta u: Iran, Rusija, Pakistan, Afganistan, Indija, itd.
- Potencijalna podrška: National Security Agency (NSA) – SAD
- Trivia: u avgustu 2016. godine je hakerska grupa “The Shadow Brokers” navodno ukrala izvorni kod za malware „proizvode“ od Equation

Sandworm

- **DEF:** Sandworm je hakerska grupa koja (najverovatnije) radi za Rusiju
  - Ime su dobili na osnovu referenci na naučno-fantastički serijal „Dune“ u izvornom kodu njihovih malware „proizvoda“
  - Osnovani: 2010 (ili ranije)
- Aktivnosti:
  - Navodno su povezani sa napadom na elektroenergetski sistem u Ukrajini 23.12.2015. godine
  - Industrijska špijunaža i upadi u industrijske kontrolne sisteme na teritoriji SAD, prvenstveno uz pomoć BlackEnergy malware-a (trojanac)
- Potencijalna podrška: Rusija

Odred 61398

- **Def:** Odred 61398 je (navodno) deo armije Narodne Republike Kine
  - Specijalizovan za kiber-rat
  - Napadi na korporacije i državne institucije barem od 2006
- **Motiv:** krađa intelektualne svojine
- **Metod:** zero-day exploit, reverzni inžinjering pogađanje lozniki, trojanci
- **Mete:** Telvent, Lockheed Martin, Google (?)
  - Advanced Persistent Threat 1 (APT1)
- **Sinonimi (tj. drugi nazivi):** Elderwood Group, Comment Group

Mete odreda 61398

- Qinetiq – vojna industrija SAD
- Diablo Canyon nuklearna elektrana – Kalifornija, SAD – email trojanci i spyware
- Evropska Komisija i “spašavanje” Grčke
- Wiley Rein advokatska firma koja se bavi trgovinskim pravom
  - Npr. dumping cene kineskih solarnih panela

Lazarus Group

- **Def:** Lazarus Group je hakerska grupa (najverovatnije) finansirana od strane Severne Koreje
- **Motiv:** razni tipovi napada
- **Metod:** botnet, backdoor, zero-day exploit, pogađanje lozniki, trojanci
- **Mete:**
  - The WannaCry ransomware outbreak of 2017;
  - Attempts of hacking US defense contractor Lockheed Martin in 2016;
  - The 2016 Bangladesh Central Bank cyber-heist;
  - The breach at Sony Pictures Entertainment in 2014;
  - Breaches at US movie theatre chains AMC Theatres and Mammoth Screen in 2014;
  - A long string of hacks of South Korean news media organizations, banks, and military entities across several years, and;
  - Hacks of banks all over the world from 2015 through 2018
- **Sinonimi:** -

Organizacije, standardi, preporuke

PREPORUKE

CIS Top 20 Critical Security Controls (CSC) – 1/2

- CSC 1: Inventory of Authorized and Unauthorized Devices
- CSC 2: Inventory of Authorized and Unauthorized Software
- CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
- CSC 4: Continuous Vulnerability Assessment and Remediation
- CSC 5: Controlled Use of Administrative Privileges
- CSC 6: Maintenance, Monitoring, and Analysis of Audit Logs
- CSC 7: Email and Web Browser Protections
- CSC 8: Malware Defenses
- CSC 9: Limitation and Control of Network Ports, Protocols, and Services
- CSC 10: Data Recovery Capability

CIS Top 20 Critical Security Controls (CSC) – 2/2

- CSC 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
- CSC 12: Boundary Defense
- CSC 13: Data Protection
- CSC 14: Controlled Access Based on the Need to Know
- CSC 15: Wireless Access Control
- CSC 16: Account Monitoring and Control
- CSC 17: Security Skills Assessment and Appropriate Training to Fill Gaps
- CSC 18: Application Software Security
- CSC 19: Incident Response and Management
- CSC 20: Penetration Tests and Red Team Exercises

10 zapovesti – 1

- 10 zapovesti iz Little Black book of Computer Security

1) Biti svestan socijalnog inženjeringa i pripremiti zaposlene na odbranu
2) Razviti jasnu i dostupnu bezbednosnu politiku
3) Realizovati fizičku bezbednost
4) Pametno birati novo osoblje i ograničiti pristup licima van firme
5) Uvesti jasna i stroga prava pristupa
6) Lozinke da budu jake i da se čuvaju u tajnosti

10 zapovesti - 2

7) Ažuriranje softvera (update) i primena zakrpa (patch)
8) Obezbediti servere, unutrašnjost i granice sistema
9) Kontrolisati udaljeni pristup i bežične mreže
10) Redovno vršiti
    - bekap podataka i sistema
    - bezbednosne kontrole
    - probne upade u sopstveni sistem
    - analizirati programski kod
    - dokumentovati sve i pripremiti za inspekciju

Rezime

- Kompanije
- Standardizaciona tela
- Državne agencije
- Nezavisne organizacije
- Preporuke

Hvala na pažnji!