Univerzitet u Novom Sadu
Fakultet Tehničkih Nauka

Informaciona bezbednost

Predavanja:
prof. dr Goran Sladić
sladicg@uns.ac.rs
NTP-405
Vežbe:
Nikola Milosavljević
milosavljevic.ra5.2018@uns.ac.rs
NTP-322

Konsultacije

- Za konsultacije kod nastavnika nema predefinisanih termina, već se dogovorimo putem email-a
  - Pošaljete email
  - **Obavezno navesti tačan naziv predmeta, broj indeksa, ime i prezime i temu/problem**
- Za konsultacije kod asistenata ćete dobiti informaciju od asistenata o terminima
- Ako želite da vam se mail pročita i dobijete odgovor morate poslati sa **@uns.ac.rs** domena

Ocenjivanje

- Raspon poena i ocene na FTN-u
  - za poene od 0 do 50 ocena 5
  - za poene od 51 do 60 ocena 6
  - za poene od 61 do 70 ocena 7
  - za poene od 71 do 80 ocena 8
  - za poene od 81 do 90 ocena 9
  - za poene od 91 do 100 ocena 10

Ocenjivanje

- Predispitne obaveze: max 50 bodova
- Završni ispit: max 50 bodova

- **Da bi ste položili ispit morate položiti i predispitne obaveze i ispitne obaveze**
  - Predispitne: min 50% poena
  - Ispitne: min 50% poena

- Predispitne + ispitne: min 51 bod

Ocenjivanje

- Predispitne obaveze - projekat
  - 50 poena
  - Minimum 25
  - Kontrolne tačke
- Usmeni ispit
  - 50 poena
  - Minimum 25
- Da bi izašli na usmeni ispit morate imati odbranjen projekat

Upis ocene

- Da bi se ocena evidentirala u studentskoj službi morate prijaviti ispit u nekom od zvaničnih rokova
- Tek kad prijavite ispit nastavnik može ocenu proslediti studentskoj službi
- Treba da prođe neko vreme od datuma ispita do trenutka da vam ocena postane vidljiva preko studentskog servisa

Zašto samo odluči(la/o) da slušam ovaj predmet?

- Predmet je obavezan
- Nešto moram da slušam, a ...
- Rekli su mi da lako položi
- Možda će mi koristiti u budućnosti
- Zanimljiva mi je ova oblast zanimljiva
- …

Zašto bi trebalo slušam ovaj predmet?

- Sajber bezbednost (cyber security) postaje sve važnija i važnije
  - Veliki gubici zbog nebezbednih sistema
    - Finansijski
    - Reputacijski
    - …
  - Sve više i više se zahteva da imamo bezbedne sajber sisteme
    - Softver
    - Hardver
    - Celokupno rešenje

Neki cyber napadi –2022

- Medibank Data Breach
  - one of the largest health insurance providers in Australia, confirmed that data belonging to 9.7 million past and present customers, including 1.8 million international customers, had been accessed by an unauthorized party
- LAUSD Data Breach
  - Russian-speaking hacking group Vice Society leaked 500GB of information from The Los Angeles Unified School District (LAUSD)
- Optus Data Breach
  - Australian telecommunications company Optus, which has 9.7 million subscribers, suffered a massive data breach that exposed names, dates of birth, phone numbers and email addresses.
- DoorDash Data Breach
  - Food delivery giant DoorDash confirmed a data breach 4.9 million customers, workers and merchants that exposed personal information.

Neki cyber napadi –2022

- Uber Data Breach
  - While the data breach occurred in 2016 and was revealed in 2017, Uber admitted it covered up a data breach that affected 57 million users. The rideshare company paid $100,000 to the threat actors to ensure the information wasn't made public.
- Twitter Data Breach
  - Twitter suffered a data breach that affected 5.4 million accounts, including phone numbers and email addresses. The data was collected in December 2021 using a Twitter API vulnerability disclosed in a bug bounty program that allowed people to submit phone numbers and email addresses into the API to retrieve the associated Twitter ID. Using this ID, the threat actors could then retrieve public information about the account to create a user record containing both private and public information.
- Costa Rica Government Data Breach
  - In a high-profile cyberattack, the Conti ransomware gang breached the Costa Rican government. The threat group accessed the government's systems, stole highly valuable data and demanded $20 million, forcing the Central American government to declare a state of emergency. A total of 670GB of data — or 90% of data accessed — was posted to a leak site weeks after.

Neki cyber napadi –2022

- SuperVPN, GeckoVPN and ChatVPN Data Breach
  - A breach involving several widely used Android VPN services — SuperVPN, GeckVPN and ChatVPN — led to 21 million users having their information leaked. Full names, usernames, country names, billing details, email addresses and randomly generated password strings were among the information available.
- Google Blocks “Largest Ever” DDoS Attack
  - Google successfully thwarted what has been deemed the largest distributed denial of service (DDoS) attack ever recorded. The attack, which targeted a Google Cloud Armor user with HTTPS, reached a peak of 46 million requests per second and lasted for 69 minutes. It was carried out from a staggering 5,256 source IPs located in 132 countries and was 76% larger than the previous record-holding attack.
- Dropbox Experiences Data Breach Following Phishing Attack
  - Dropbox suffered a data breach after a phishing attack targeted the company’s employees. The attack saw a malicious actor pose as code integration and delivery platform CircleCI in order to obtain login credentials and authentication codes from employees. As a result of the attack, 130 of Dropbox’s source code repositories were affected, and the hacker was able to access some of the code stored on the platform, including API keys used by developers.

Neki cyber napadi –2022

- Meta Fires Employees for Allegedly Hacking into User Accounts
  - Meta has reportedly fired or disciplined a dozen of its employees for allegedly hacking into user accounts and violating Facebook's terms of service. According to reports, some of the employees, who were being contracted to work as security guards at Meta, used a heavily regulated internal access tool called "OOps" to reset access to Facebook accounts.
- Binance Cryptocurrency Exchange Suffers Data Breach
  - Hackers accessed the personal data of some customers of the cryptocurrency exchange, Binance. The hackers obtained a large amount of user data, including names, email addresses, and hashed passwords, but no financial data was compromised.
- Cash App Data
  - The mobile payment service Cash App experienced a serious data breach that affected over 8.2 million current and previous users.

Neki cyber napadi –2022

- Twitter Confirms Data Breach Affecting 5.4 Million Accounts
  - A hacker going by the alias “devil” claiming to be selling the personal details of 5.4 million Twitter accounts. The hacker stated that they had accessed this information through a previously reported vulnerability on the social media platform.
- Hackers Steal $32 Million in Cryptocurrency from Bitfinex Exchange
  - Hackers successfully stole $32 million worth of cryptocurrency from the popular exchange, Bitfinex. The hack was executed through a phishing attack that targeted the exchange’s employees, tricking them into giving the hackers access to the company’s systems and the cryptocurrency.

Najveći poznati cyber napadi u poslednjih 10ak godina

- 2011 Sony PlayStation Network
  - 77M podataka o korisnicima
- 2013 Edward Snowden
  - NSA dokumenta
- 2013 i 2014 Yahoo
  - 500M podataka o korisnicima

Najveći poznati cyber napadi u poslednjih 10ak godina

- 2015 US Office of Personnel Mgmt
  - 21.5M SSN (”JMBG”) i 5.6M otisaka prsta
- 2017 Equifax kreditni biro
  - 157M podatka o korisnicima
- 2017 Ransomworm WannaCry
  - 230K računara, 150 država
  - Iskoristio je ranjivost EternalBlue koju je napravila/otkrila NSA - MS ranjivost u SMB protokolu

Najveći poznati cyber napadi u poslednjih 10ak godina

- 2017 Uber
  - 57M podatka o klijentima i vozačima
- 2018 Marriott Hoteli
  - Podaci o 500M gostiju
- 2018 British Arways
  - 500K podatka uključujući platne kartice
- 2020/2021 SolarWind
  - Cybersecurity company
  - 18000 klijenata
  - *“When we analyzed everything that we saw at Microsoft, we asked ourselves how many engineers have probably worked on these attacks. And the answer we came to was, well, certainly more than 1,000”*

Najveći poznati cyber napadi u poslednjih 10ak godina

- **2022**
  - **Co**lonial Pipeline: The fuel pipeline operator was struck by ransomware, courtesy of DarkSide, leading to fuel delivery disruption and panic buying across the United States. The company paid a ransom, but the damage was already done.

I mnogo drugih – feb 2021

Google Roulette

Developer console trick can trigger XSS in Chromium browsers

17 November 2022

Zimbra RCE vulnerability actively exploited in the wild

10 October 2022

Critical flaw in open source WebPageTest remains unpatched

07 October 2022

Car companies massively exposed to web vulnerabilities

04 January 2023

Zero-day bug in healthcare devices could allow attackers full control

13 December 2021

ProxyNotShell

Microsoft confirms 'limited' abuse of Exchange Server zero-days

03 October 2022

Deserialized roundup

KeePass dismisses 'vulnerability' report, OpenSSL gets patched, and Reddit admits phishing hack

10 February 2023

Serious security hole plugged in infosec tool binwalk

03 February 2023

Researcher drops Lexmark RCE zero-day rather than sell 'for peanuts'

01 February 2023

Unpatched plugins threaten millions of WordPress websites

16 March 2022

Git security audit reveals critical overflow bugs

20 January 2023

All Day DevOps

Third of Log4j downloads still pull vulnerable version despite growing awareness of supply chain attacks

14 November 2022

Supply chain attack surge

Researchers find 633% rise in assaults on open source repositories

18 October 2022

Novi Sad – 02.03.2020

Blokirani serveri novosadskih službi, hakeri traže bitkoine da bi otključali vredne baze podataka

Serveri gradskih uprava, ali i nekolicine drugih javnih službi koji su u JKP "Informatika" hakovani su tokom vikenda i hakeri traže bitkoine da bi otključali sisteme, saznaje 021.

Препоручите 19 | Подели | Tweet | KOMENTARI 0

NOVI SAD 02.03.2020. | 13:12 > 13:32

Srbija – 17.06.2022

Хакерски напад на катастар

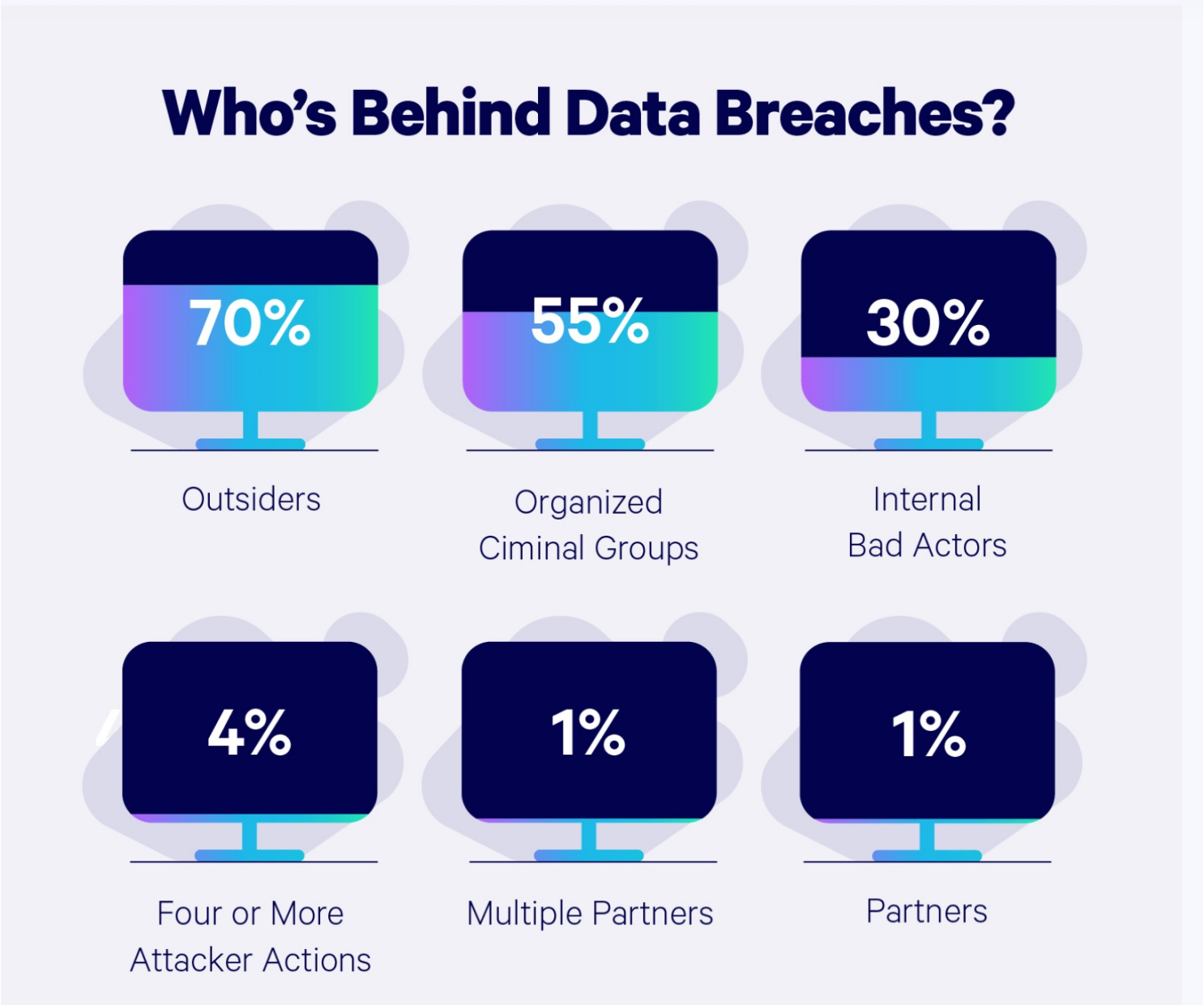
Сви термини које су грађани заказали код нотара у протекла три дана су пропали, а заказивање нових биће могуће кад систем поново проради

(Фото rgz.gov.rs)

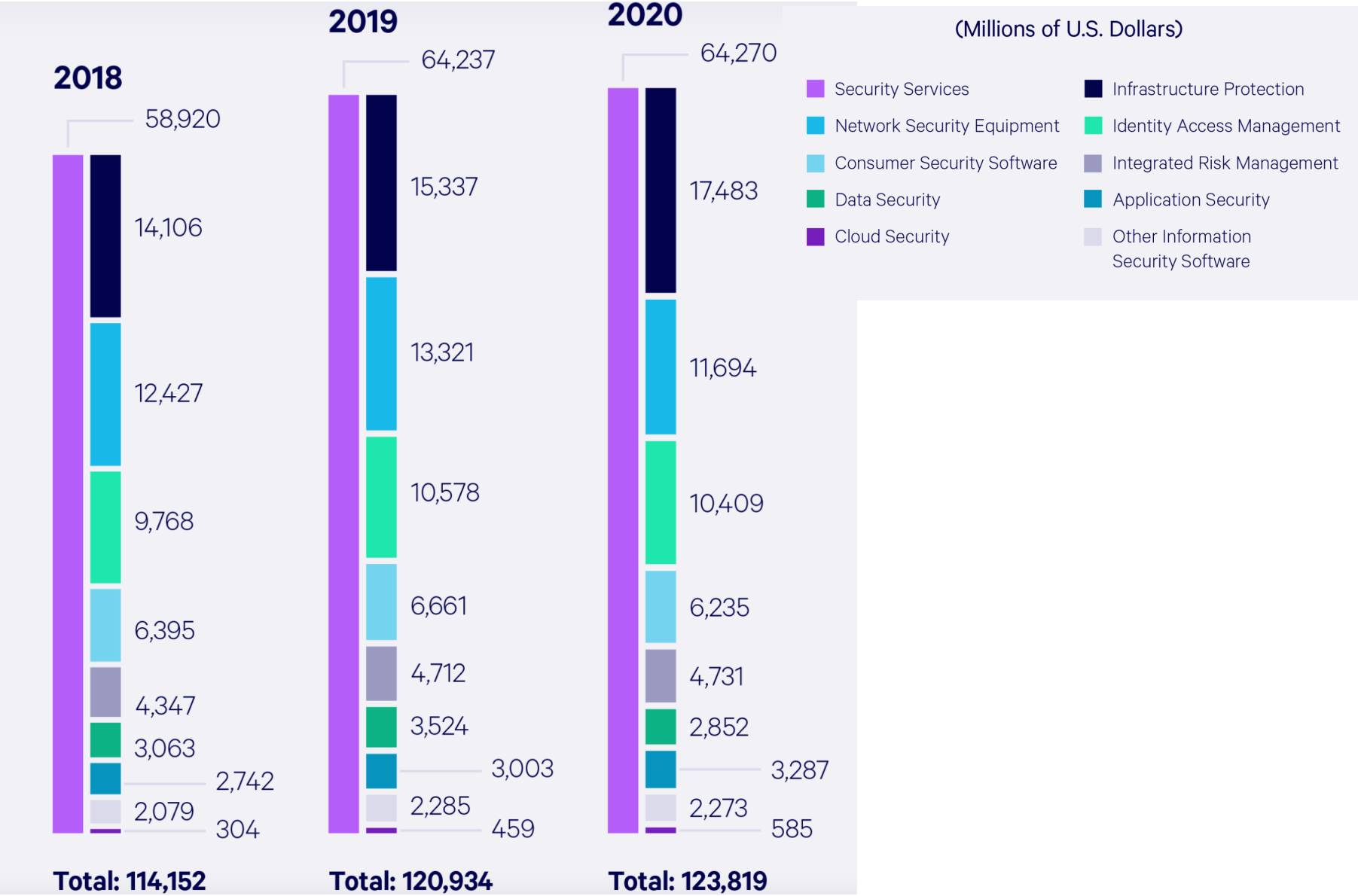
Cifre

- Procenjeni godišnji troškovi za sajber kriminal$10.5*10^{12}$ $ do 2025
  - rast od 15% godišnje
- Ukupni troškovi za sajber criminal 1% svetskog GDP-a
- Procena da će cybersecurity budžet rasti 71% za naredne tri godine
- 43% napda je na SME kompanije
  - samo 14% kompanija ima kapitete za odbranu
- 66% kompanija i organizacija je biloizloženo napadu u poslednjih 12 meseci
- Vrste napada
  - Phishing/socijalni inzenjering 57%
  - krađa/kompromitovanje uređaja 33%
  - krađa kredencijala 30%
- Ramsomware napad na svakih 11 sec
- 197 dana da se detektuje upad i 69 da se reši
- 92% malware-a se isporuči email-om
- 98% napada se oslanja na socijalni inženjering
- Prosečni trošak kompanija od malware napad je 2.4M$

Cifre - vrste napadača



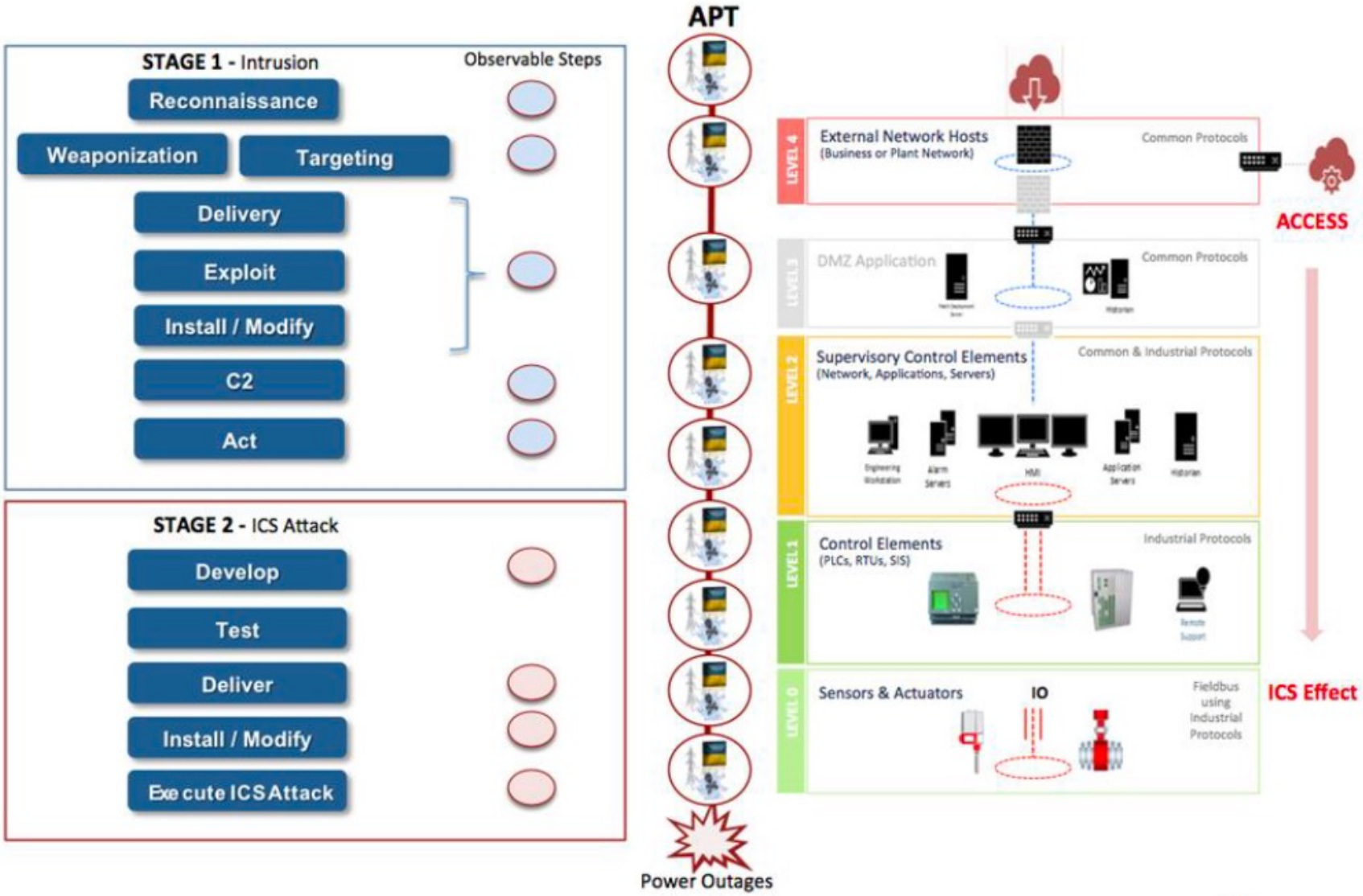
Investicije po oblastima 2018-2020



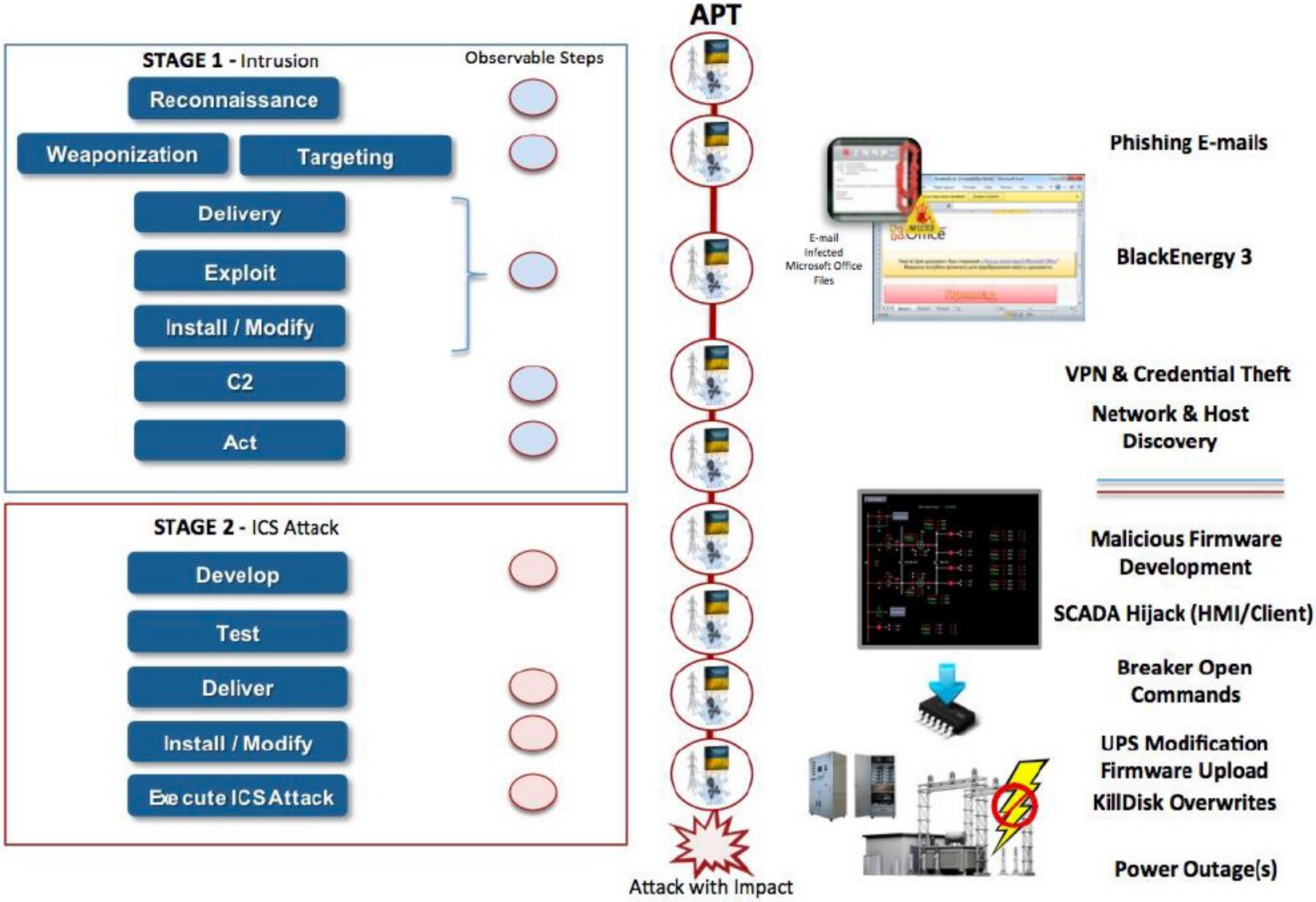
When Lights Went Out

- Dva napada na Ukrajinsku elektrodistribuciju 2015 i 2017
  - Delovi Ukrajine ostali bez struje
  - Moguće je bilo proizvesti mnogo veću šetu

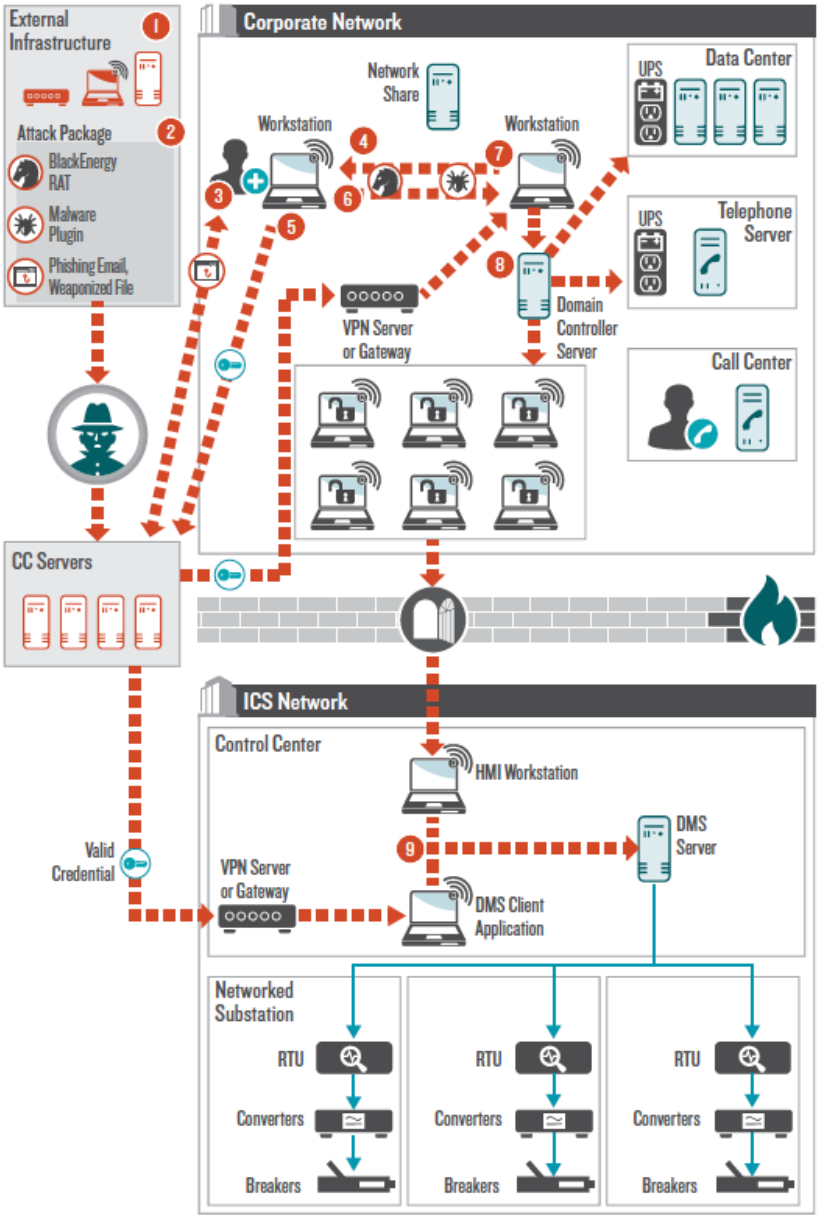
Napad 2015


STAGE 1 - Intrusion
Observable Steps
Reconnaissance
Weaponization
Targeting
Delivery
Exploit
Install / Modify
C2
Act
STAGE 2 - ICS Attack
Develop
Test
Deliver
Install / Modify
Execute ICS Attack
APT
Power Outages
LEVEL 4
External Network Hosts
(Business or Plant Network)
Common Protocols
ACCESS
LEVEL 3
DMZ Application
Common Protocols
LEVEL 2
Supervisory Control Elements
(Network, Applications, Servers)
Common & Industrial Protocols
LEVEL 1
Control Elements
(PLCs, RTUs, SIS)
Industrial Protocols
LEVEL 0
Sensors & Actuators
IO
Fieldbus using Industrial Protocols
ICS Effect

Napad 2015 - BlackEnergy

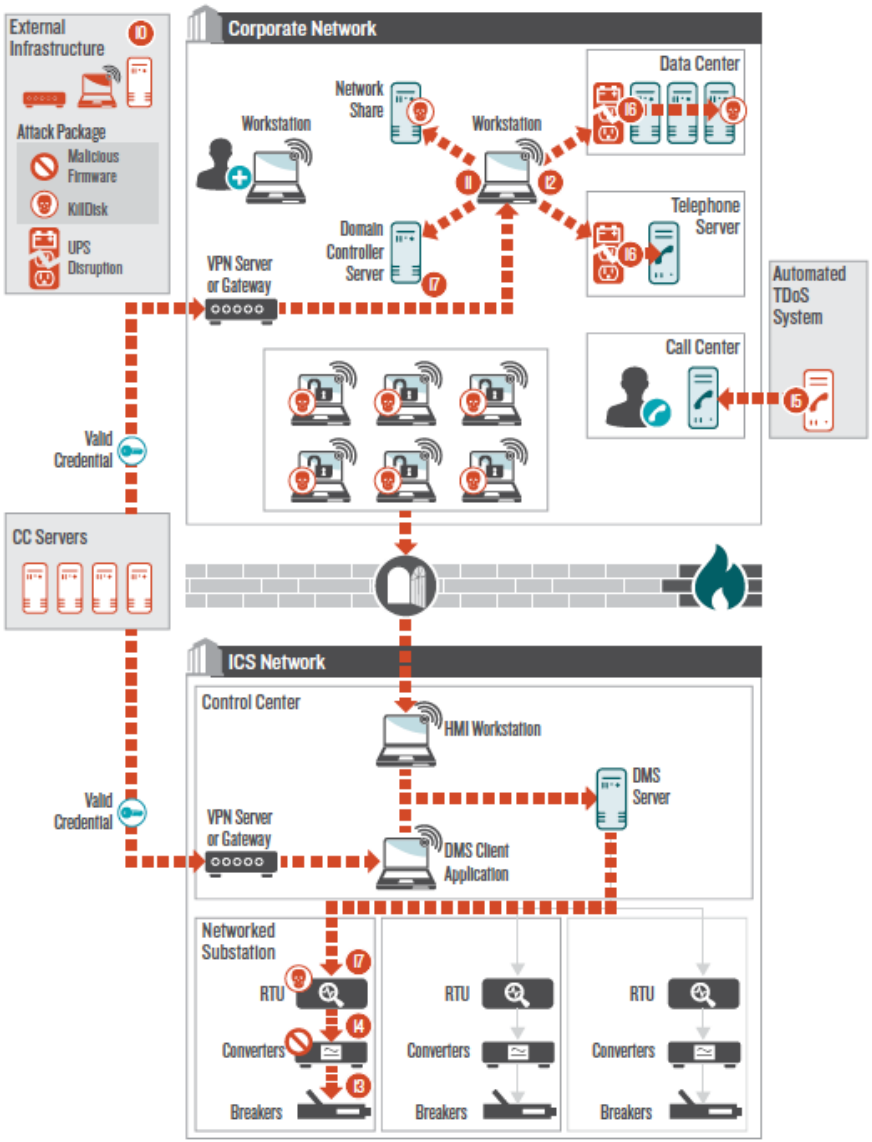


Napad 2015 - BlackEnergy



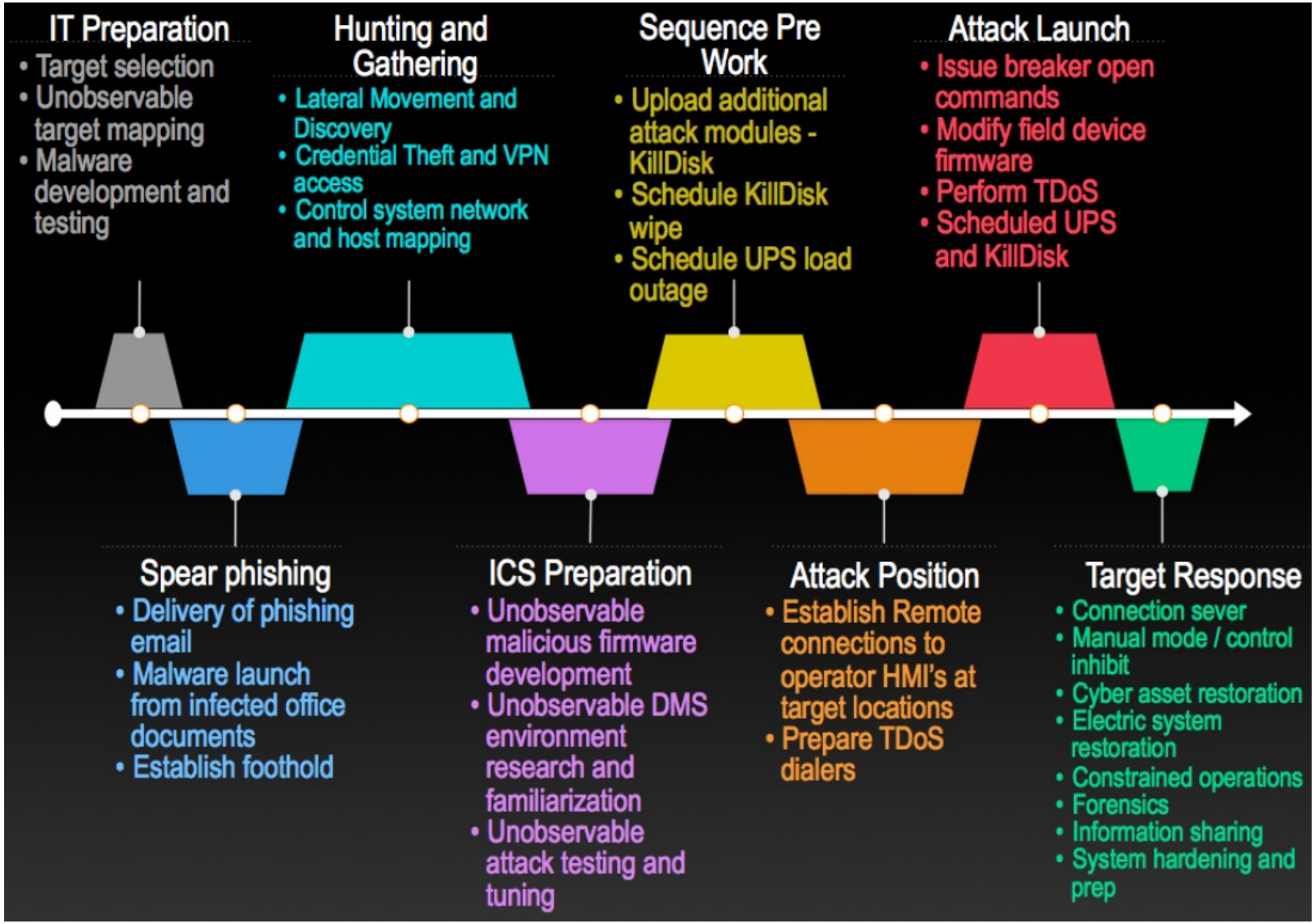
1. Reconnaissance and Intelligence Gathering
2. Malware Development and Weaponization
3. Deliver Remote Access Trojan (RAT).
4. Install RAT
5. Establish Command-and-Control (CC) Connection
6. Deliver Malware Plugins
7. Harvest Credentials
8. Lateral Movement and Target Identification on Corporate Network
9. Lateral Movement and Target Identification on ICS network

Napad 2015 - BlackEnergy



10. Develop Malicious Firmware
11. Deliver Data Destruction Malware
12. Schedule Uninterruptable Power Supply (UPS) Disruption
13. Trip Breakers
14. Sever Connection to Field Devices
15. Telephony Denial-of-Service Attack
16. Disable Critical Systems via UPS Outage
17. Destroy Critical System Data.

Prilike za sprečavanja napad



Napad 2017 – Petya malware

- Ramsonware napad ne samo na elektro distribuciju, već i na adruge komapnije (banke, državna uprava, mediji, …)
- Napad započet korz update regularnog softvera za poreze MeDoc
  - 90% firmi u Ukrajini je koristilo ovaj softver
  - Uhakovan update server i promenjena instalacija update-a
- Napad je iskoristio EternalBlue ranjivost

Na šta napadi utiču?

- CIA triada
  - Confidentiality (C)
  - Integrity (I)
  - Availability (A)

Šta je uzrok svih ovih napada?

- Ranjivosti u sistemu
- Kako ranjivosti nastaju
  - Greške tokom razvoja softvera i hardvera
  - Greške tokom isporuke softvera i hardvera
  - Greške prilikom instalacije i konfiguracije softvera i hardvera
  - Greške prilikom ažuriranja softvera

Ranjivosti u softveru i hardveru

- Javljaju se na svim nivoima
  - Mikroarhitektura hardvera
  - Firmware
  - OS
  - DB
  - Aplikativni server
  - Aplikacija

- Softverske kompanije regularno publikuju security update-ove

- Neke hardverske ranjivosti se ne mogu efikasno otkloniti

OWASP Top 10

- OWASP – online zajednica koja se bavi bezbednošću web aplikacija
- Definišu 10 najvećih rizika po bezbednost aplikacija
  1. Injection
  2. Broken Authentication.
  3. Sensitive Data Exposure
  4. XML External Entities (XXE)
  5. Broken Access Control
  6. Security Misconfiguration
  7. Cross-Site Scripting XSS
  8. Insecure Deserialization
  9. Using Components with Known Vulnerabilities
  10. Insufficient Logging & Monitoring

Kritičnost ranjivosti

- Sve ranjivosti nisu jednako kritične
- Common Vulnerability Scoring System (CVSS) – standard za ocenu kritičnosti računarskih ranjivosti
- CVV vrednost se računa na osnovu
  - Metrika iskoristivosti - Exploitability Metrics
    - Vektor napada - Attack Vector (AV)
    - Složenost napada - Attack Complexity (AC)
    - Potrebne privilegija - Privileges Required (PR)
    - Korisničke interakcije - User Interaction (UI)
    - Opseg - Scope (S)
  - CIA metrika
    - Confidentiality Impact (C)
    - Integrity Impact (I)
    - Availability Impact (A)

Standardi za ranjivosti

- Common Weakness Enumeration (CWE) - standardno označavanje ranjivosti
- Common Vulnerabilities and Exposures (CVEs) - repozitorijum za prijavu i kategorizaciju softverskih ranjivosti
- National Vulnerability Database - proširenje CVE sa CVSS

- Primer log4j CVE-2021-44228

Severity CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** 10.0 CRITICAL **Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.

Cyber Security

- Bezbednost računarski sistema se prožima kroz 3 komponente
  - Procesi
  - Tehnologije
  - Ljudi

Cyber Security

- Procesi
  - Dokumentacija koja definiše na različite načine i na različitim nivoima apstrakcije kao se štite računarski resursi
  - Politike
  - Procedure
  - Uputstva
  - Poslovni procesi koji se odnose na bezbednost
  - Modeli pretnji
  - …

Cyber Security

- Tehnologije
  - Tehnički mehanizmi kako se štiti računarski sistem
  - Autentifikacija
  - Kriptografija
  - Firewall
  - Antivirusi
  - …
- *Primarni fokus na IB*

Cyber Security

- Ljudi
  - Obučiti ljude da da budu svesni računarske bezbednosti
  - Security awareness training
  - Specijalizovane obuke