Niekoľko slov o kybernetickej bezpečnosti

17. Medzinárodná konferencia železničnej, oznamovacej a zabezpečovacej techniky

Peter Holečko

Katedra riadiacich a informačných systémov

24. 4. 2023

ŽILINSKÁ UNIVERZITA V ŽILINE
Fakulta elektrotechniky
a informačných technológií

Agenda

- CIA triáda
- Kybernetické útoky - príklady
- Ransomware
- Obrana
- Diskusia

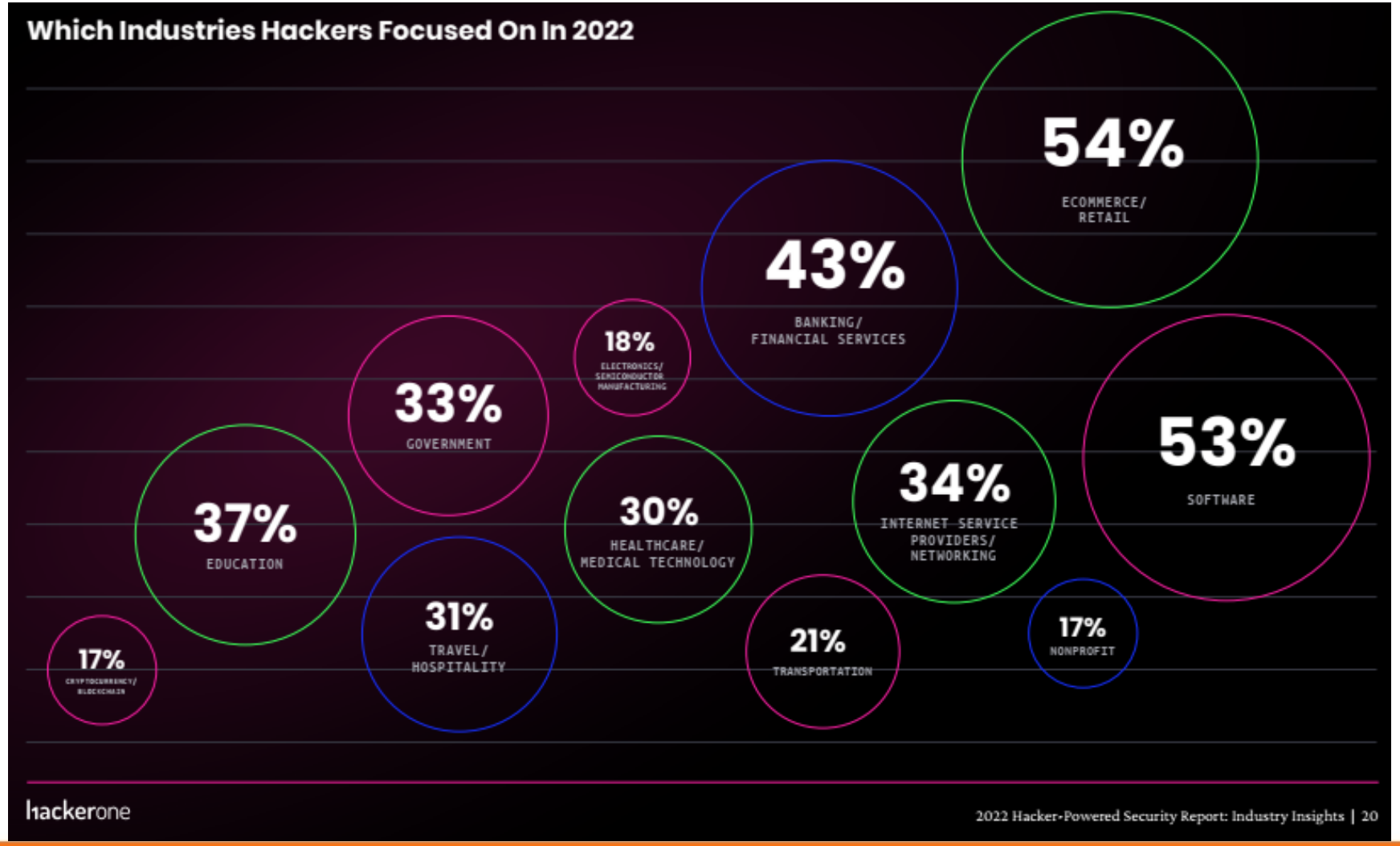
CIA triáda

Confidentiality - dôvernosť

Integrity - celistvosť

Availability - dostupnosť

Kybernetické útoky globálne



Kybernetické útoky na železničné spoločnosti

NotPetya (2017)

Globálny kybernetický útok zameraný na niekoľko spoločností po celom svete. Útočníci použili variant ransomvéru Petya na infikovanie firemných systémov a po sieti sa šírili pomocou exploitu EternalBlue. Útok spôsobil značné narušenie vlakových poriadkov a iných železničných operácií a mal za následok finančné straty spoločnosti.

https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Kybernetické útoky na železničné spoločnosti

USA (2018)

Kybernetický útok zameraný na železničný priemysel v USA. Útočníci použili phishingový e-mail na doručenie škodlivého softvéru, ktorý im umožnil získať neoprávnený prístup k systémom železničnej spoločnosti a ukradnúť prihlasovacie údaje zamestnancov. Útočníci potom použili tieto prihlasovacie údaje na prístup k iným železničným systémom vrátane cestovných poriadkov vlakov a údajov o zákazníkoch. Využili softvér typu trójsky kôň so vzdialeným prístupom (Remote Access Trojan, RAT) na udržanie trvalého prístupu k infikovaným systémom a zostali neodhalení bezpečnostným softvérom.

https://railsecurity.org/wp-content/uploads/2019/08/US-Freight-Rail-and-Transit-Cyber-Vulnerabilities-Updated-July-16-2019.pdf

Kybernetické útoky na železničné spoločnosti

Švajčiarsko (2020)

Stadler, výrobca vlakov so sídlom vo Švajčiarsku, sa stal obeťou kybernetického útoku, ktorý vyústil do krádeže firemných údajov. Útočníci využili zraniteľnosť vo virtuálnej privátnej sieti (VPN), aby získali neoprávnený prístup k podnikovým systémom a ukradli citlivé údaje vrátane technických výkresov a údajov o zamestnancoch. Útočníci požadovali výkupné, aby zabránili zverejneniu ukradnutých údajov

https://www.bleepingcomputer.com/news/security/rail-vehicle-manufacturer-stadler-hit-by-cyberattack-blackmailed/

Kybernetické útoky na železničné spoločnosti

Taliansko (2022)

IT systémy patriace talianskym štátnym železniciam (FS) a ich dcérskym spoločnostiam Trenitalia a Italian Rail Network (RFI) zasiahol v marci rozsiahli kybernetický útok ransomwarom, ktorý narušil predaj lístkov na staniciach, obrazovky s informáciami pre cestujúcich a tablety používané železničným personálom.

https://www.railjournal.com/infrastructure/italian-railway-it-system-suffers-major-cyber-attack/

Kybernetické útoky na železničné spoločnosti

Dánsko (2022)

Rozsiahly ransomware útok na subdodávateľa IT pre dánske železnice (DSB) ho prinútil vypnúť svoje servery, čo následne znefunkčnilo aplikácie využívané rušňovodičmi prístup k dôležitým prevádzkovým informáciám, ako sú rýchlostné limity a informácie o práci na železnici.

https://www.securityweek.com/cyberattack-causes-trains-stop-denmark/

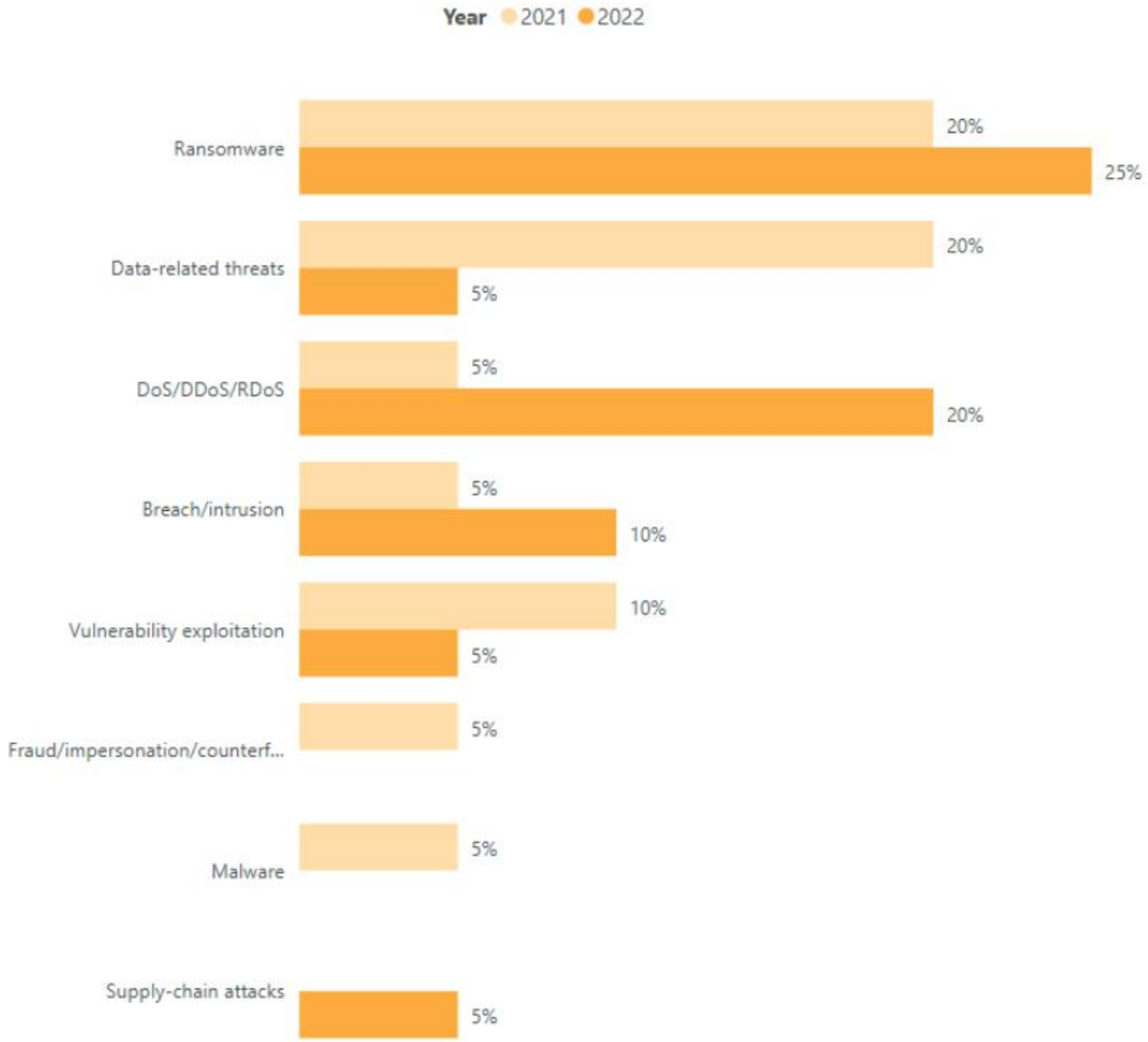
Kybernetické útoky na železničné spoločnosti

Holandsko (2023)

Útok na agentúru pre prieskum trhu, s ktorou železnice spolupracujú, spôsobil únik osobných údajov 780 000 zákazníkov.

https://nieuws.ns.nl/ns-informeert-klanten-uit-voorzorg-over-datalek-bij-leverancier/

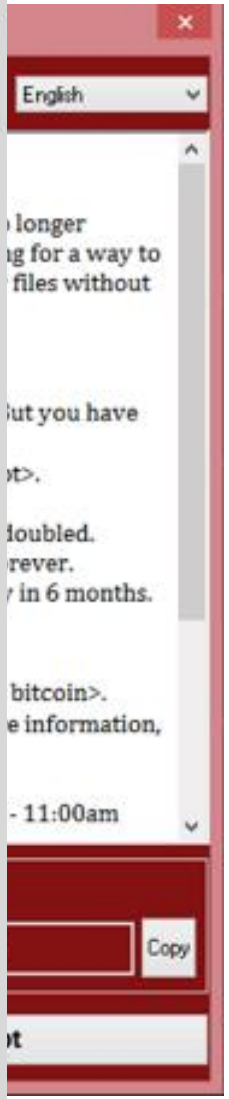
Kybernetické útoky na železničné spoločnosti



Zdroj: ENISA (European Union Agency for Cybersecurity)

-= PACKAGES COMPARISON =-

	Package #3	Package #2	Package #1	Package #ELITE
Subscription	1 Month	6 Months	12 Months	12 Months
Darknet C&C Dashboard	Yes	Yes	Yes	Yes
Features: Delayed Start, Delayed Encryption, Mutex, Task Manager/Registry Editor Disabler, UAC Bypass, Desktop Wallpaper Changer	Yes	Yes	Yes	Yes
Offline Encryption	No	Yes	Yes	Yes
Support	No	Yes	Yes	Yes
Real-Time Client Manager	No	Yes	Yes	Yes
Dropper	No	Buy	Yes	Yes
Clone	No	Buy	Buy	Yes
FUD+Obfuscator	Buy	Buy	Buy	Yes
Unkillable Process	No	Buy	Buy	Yes
FUD Stub #	1	1	2	**12**
Price	120 USD	490 USD	900 USD	1900 USD



Obrana

Modelovanie hrozieb (Threat Modelling)

Na vytvorenie efektívnej stratégie kybernetickej bezpečnosti je nevyhnutné poznať potenciálne hrozby a zraniteľné miesta.

Modelovanie hrozieb pomáha identifikovať potenciálne vektory útokov a priorizovať bezpečnostné kontroly.

Zabezpečenie sietí (Network Security)

Železničné siete sú komplexné a vzájomne prepojené, vďaka čomu sú potenciálne zraniteľné voči kybernetickým útokom.

Implementácia firewallov, systémov detekcie a prevencie prienikov (IDPS) a riadenia prístupu môže pomôcť zabezpečiť siete a zabrániť neoprávnenému prístupu.

Obrana

Ochrana prevádzkových technológií (OT Protection)

Prevádzkové technológie (Operational Technology, OT), ako sú signalizačné systémy a riadiace systémy, sú kritickými komponentmi železníc. Tieto systémy musia byť chránené pred kybernetickými útokmi, aby sa zabránilo narušeniu cestovných poriadkov vlakov a zaistila sa bezpečnosť cestujúcich.

Niektoré osvedčené postupy na ochranu OT zahŕňajú:

- Implementácia segmentácie siete na izoláciu kritických systémov od menej bezpečných systémov
- Používanie priemyselných riešení kybernetickej bezpečnosti, ako sú systémy prevencie a detekcie narušenia, na detekciu a prevenciu útokov
- Vykonávanie pravidelných hodnotení zraniteľností a penetračných testov na identifikáciu a riešenie zraniteľností v systémoch OT
- Okamžité aplikovanie bezpečnostných opráv a aktualizácií na zmiernenie známych zraniteľností

Obrana

Ochrana koncových bodov (Endpoint Protection)

Koncové body, ako sú pracovné stanice a mobilné zariadenia, sú bežnými vstupnými bodmi pre kybernetické útoky. Implementácia ochrany koncových bodov, ako je antivírusový softvér a hostiteľské systémy detekcie a prevencie narušenia, môže pomôcť odhaliť a zabrániť útokom na koncové body.

Reakcia na incidenty (Incident Response)

V prípade kybernetického útoku je dôležité mať pripravený plán reakcie na incidenty. Ten by mal zahŕňať postupy na odhaľovanie kybernetických útokov a reakciu na ne, ako aj na komunikáciu so zainteresovanými stranami, ako sú cestujúci, zamestnanci a regulačné orgány.

Plán obnovy (Disaster Recovery)

Zostavenie procedúr na obnovenie prevádzky systému a dostupnosti dát. Implementácia metód redundancie a zálohovania.

Referencie

- VACCA, J.: **Computer and Information Security Handbook** 3rd Edition. Morgan Kaufmann, 2017, ISBN 978-0128038437
- WHITMAN, M.E., Mattord, H.J.: **Principles of Information Security**. 5th Edition. Cengage Learning, 2016, ISBN 78-1-285-44836-7
- KIM, P..: **The Hacker Playbook: Practical Guide To Penetration Testing**. Secure Planet LLC, 2015, ISBN 978-1512214567
- https://www.cve.org
- https://www.cvedetails.com
- https://www.zerodayinitiative.com
- https://konbriefing.com/en-topics/cyber-attacks.html
- https://www.hackerone.com/reports/6th-annual-hacker-powered-security-report
- https://aag-it.com/the-latest-ransomware-statistics/

Ďakujem za pozornosť