FAKULTA ELEKTROTECHNIKY A INFORMATIKY

Computer CNL Networks Laboratory

Začíname...

Bezpečnostný manažment

Miroslav Michalko

Laboratórium počítačových sietí

Organizácia predmetu

- prednášky prezenčne – streda 15:10-16:40
- cvičenia v spolupráci so Siemens Healthineers

- Zápočet: záverečný test
- Skúška: ústna z prednášok a odporúčanej literatúry

Odporúčané zdroje:

1. **Ivan Makatura. Základy bezpečnostných opatrení - Príručka manažéra kybernetickej bezpečnosti**
2. Dušan Levický. Bezpečnosť digitálnych informácií. 2022. ISBN: 978-80-553-4122-4
3. Chlipala-Makatura-Pilár. Zákon o kybernetickej bezpečnosti. Komentár. 2019. ISBN: 978-80-8155-086-7

Čo je bezpečnostný manažment

Bezpečnostný manažment (Security Management) je špecifická zmysluplná činnosť, zameraná na odvrátenie alebo minimalizáciu bezpečnostných rizík, resp. bezpečnostných ohrození rôznej povahy a príčiny voči životu a majetku občanov, obcí a spoločnosti, obsahujúca v sebe prvky rizikového, krízového, havarijného a hodnotového manažmentu.

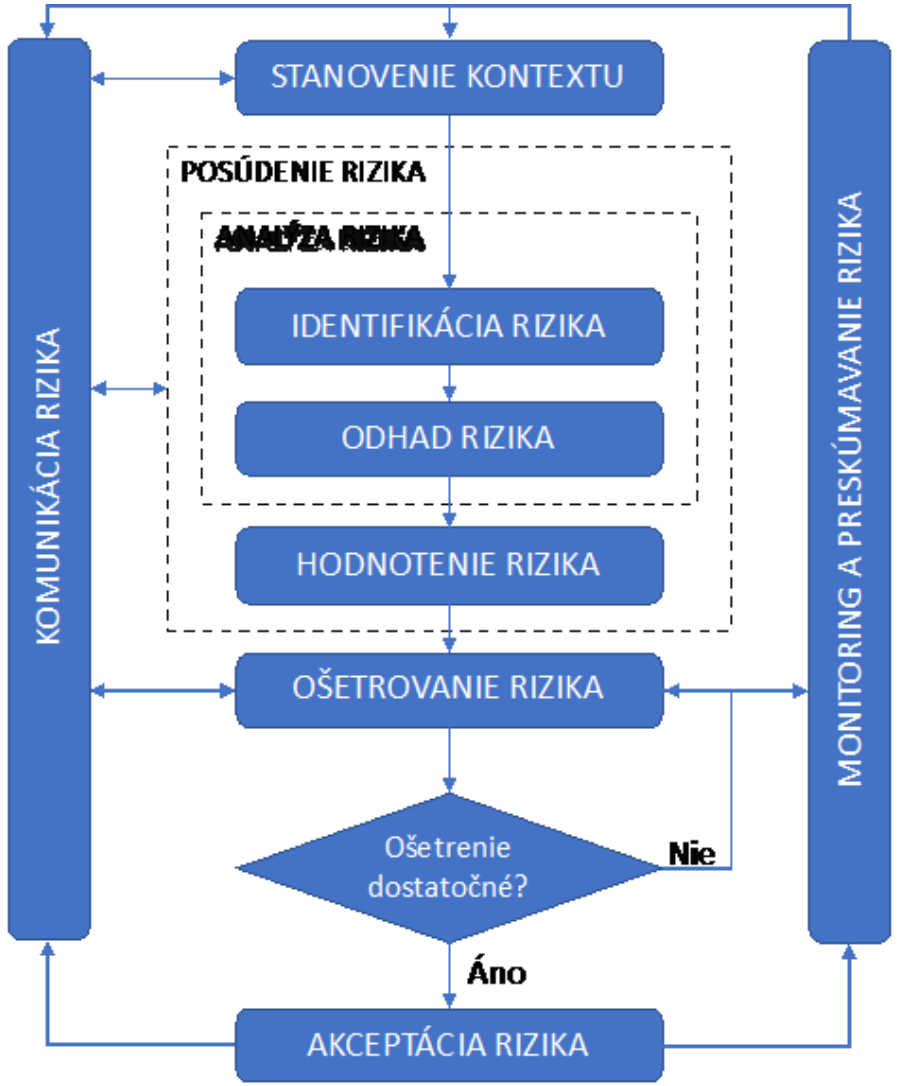
(terminologický slovník bezpečnostného manažmentu)

zjednodušene: cieľom BM je zabrániť škodám na životoch, majetku a životnom prostredí

Čo BM zahŕňa

Medzi špecifické aktivity bezpečnostného manažmentu patrí najmä riešenie nasledovných druhov bezpečnosti:

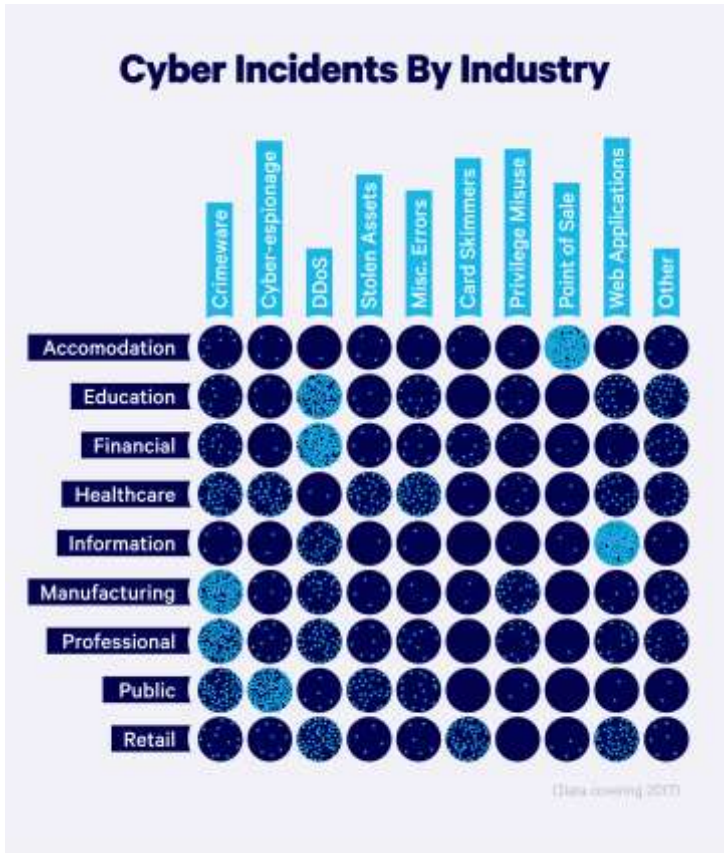
- bezpečnosť osôb,
- bezpečnosť objektov a chránených priestorov s utajovanými skutočnosťami,
- bezpečnosť objektov s inými aktívami,
- bezpečnosť práce a ochranu zdravia,
- bezpečnosť prevádzkových činností – technicko-prevádzkovú bezpečnosť, bezpečnosť technických zariadení, bezpečnosť kontinuity činností (BCM), predchádzanie závažným priemyselným haváriám,
- protipožiarna bezpečnosť,
- počítačová bezpečnosť a informačná bezpečnosť – bezpečnosť informačných systémov, bezpečnosť dôležitých informácií, ochrana utajovaných skutočností, ochrana osobných údajov,
- bezpečnosť pred podvodmi a zneužitím,
- bezpečnosť vnútorného poriadku a riešenie incidentov,
- bezpečnosť vnútorného i vonkajšieho životného prostredia,
- ďalšie oblasti bezpečnosti.



src: https://www.nbu.gov.sk/kyberneticka-bezpecnost/riadenie-rizik/index.html
Belan. Bezpečnostný manažment. UNIZA. 2015

Výzvy súčasnosti z pohľadu rizík KB

- Každých 11 sekúnd dochádza k hackerskému útoku *(štúdia Cybersecurity Ventures)*.
- Počítačová kriminalita bude stáť spoločnosti na celom svete do roku 2025 odhadom 10,5 bilióna dolárov ročne, čo je nárast z 3 biliónov dolárov v roku 2015.



src: https://www.embroker.com/blog/cyber-attack-statistics/

Trendy 2024

1. Continuous threat exposure management (CTEM) programs
2. Extending identity and access management’s (IAM) cybersecurity value
3. Third-party cybersecurity risk management
4. Privacy-driven application and data decoupling
5. Generative AI
6. Security behavior and culture programs
7. Cybersecurity outcome-driven metrics
8. Evolving cybersecurity operating models
9. Cybersecurity reskilling

src: https://www.gartner.com/en/cybersecurity/topics/cybersecurity-trends

Štatistiky a fakty

- 95% narušení kybernetickej bezpečnosti je spôsobených ľudskou chybou (World Economic Forum),
- Predpokladá sa, že celosvetový trh informačnej bezpečnosti dosiahne v roku 2028 hodnotu 366,1 miliardy USD (Fortune Business Insights),
- USA boli v roku 2020 cieľom 46 percent kybernetických útokov, čo je viac ako dvojnásobok v porovnaní s ostatnými krajinami (Microsoft),
- Priemerne je správne zabezpečených iba päť percent spoločností (Varonis),
- 54% spoločností tvrdí, že ich IT oddelenia nie sú dostatočne kvalifikované na to, aby zvládli pokročilé kybernetické útoky (Sophos),

src: https://www.varonis.com/blog/cybersecurity-statistics

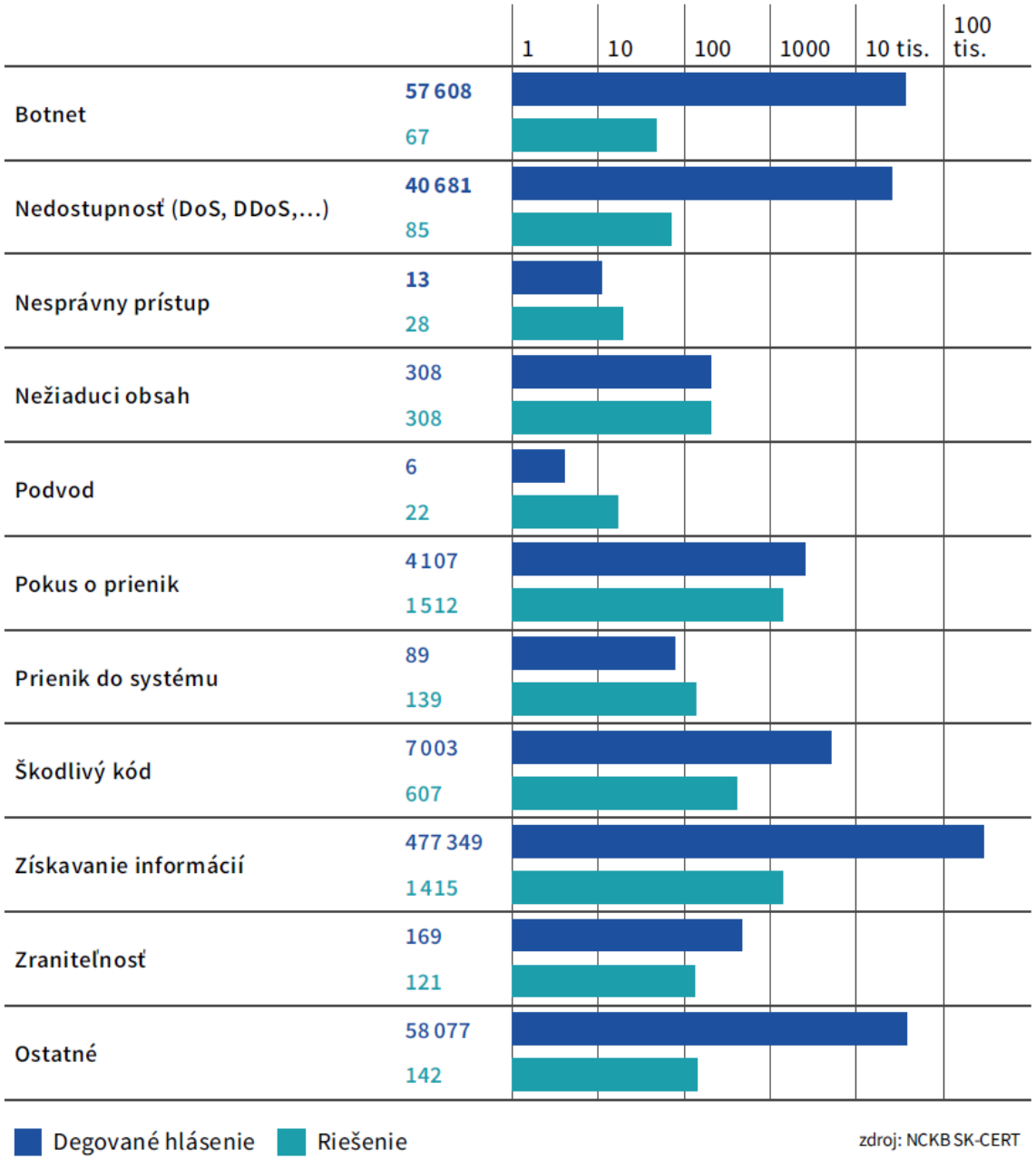
Štatistiky a fakty

- 43% všetkých incidentov sú vnútorné hrozby, či už úmyselné alebo neúmyselné (Check Point),
- približne 70 percent porušení v roku 2021 bolo finančne motivovaných, zatiaľ čo menej ako päť percent bolo motivovaných špionážou (Verizon),
- v roku 2021 sa takmer 40 percent porušení týkalo phishingu, asi 11 percent malvéru a asi 22 percent hackingu (Verizon),
- najnebezpečnejšie typy príloh e-mailov sú .doc a .dot, ktoré tvoria 37 percent; ďalšia najvyššia je .exe s 19,5 percentami (Symantec),
- približne 40 percent svetovej populácie je offline, čo z nich robí zraniteľné ciele pre kybernetické útoky, ak a keď sa spoja (Data Reportal).

src: https://www.varonis.com/blog/cybersecurity-statistics

Ako sme na tom na Slovensku

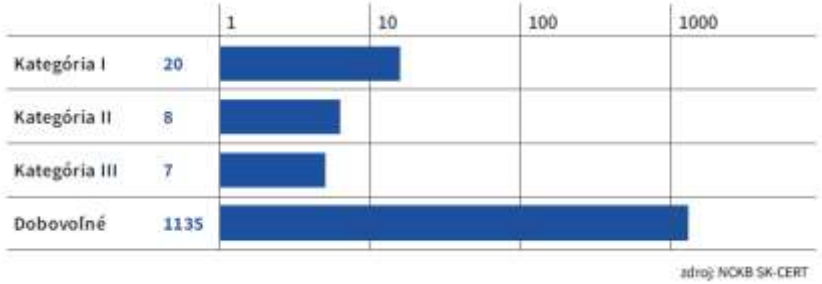
Správa NBÚ za rok 2022



Ako sme na tom na Slovensku

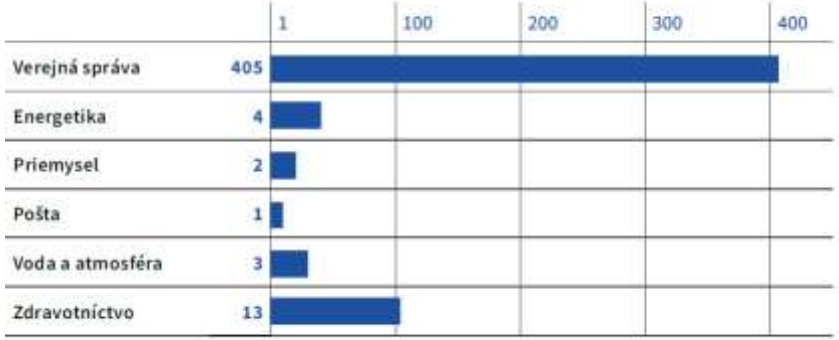
Správa NBÚ za rok 2021

Počet hlásených kybernetických bezpečnostných incidentov podľa zákona – rok 2022



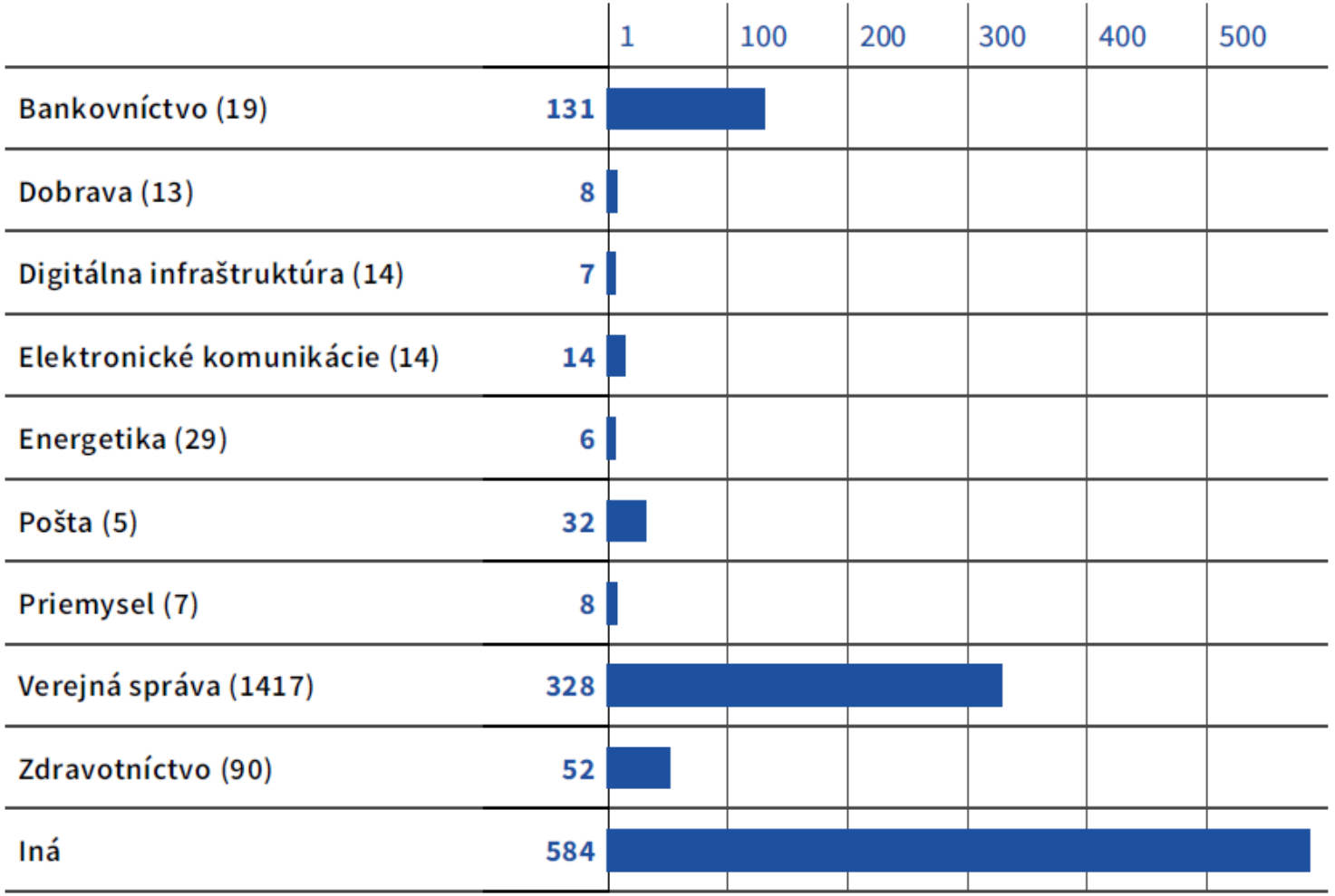
zdroj: NCKB SK-CERT

Počet hlásených kybernetických bezpečnostných incidentov podľa zákona – rok 2022



zdroj: Doručené samohodnotenia 2022, NBÚ

Hlásenia kybernetických bezpečnostných incidentov v sektoroch – rok 2022



zdroj: NCKB SK-CERT

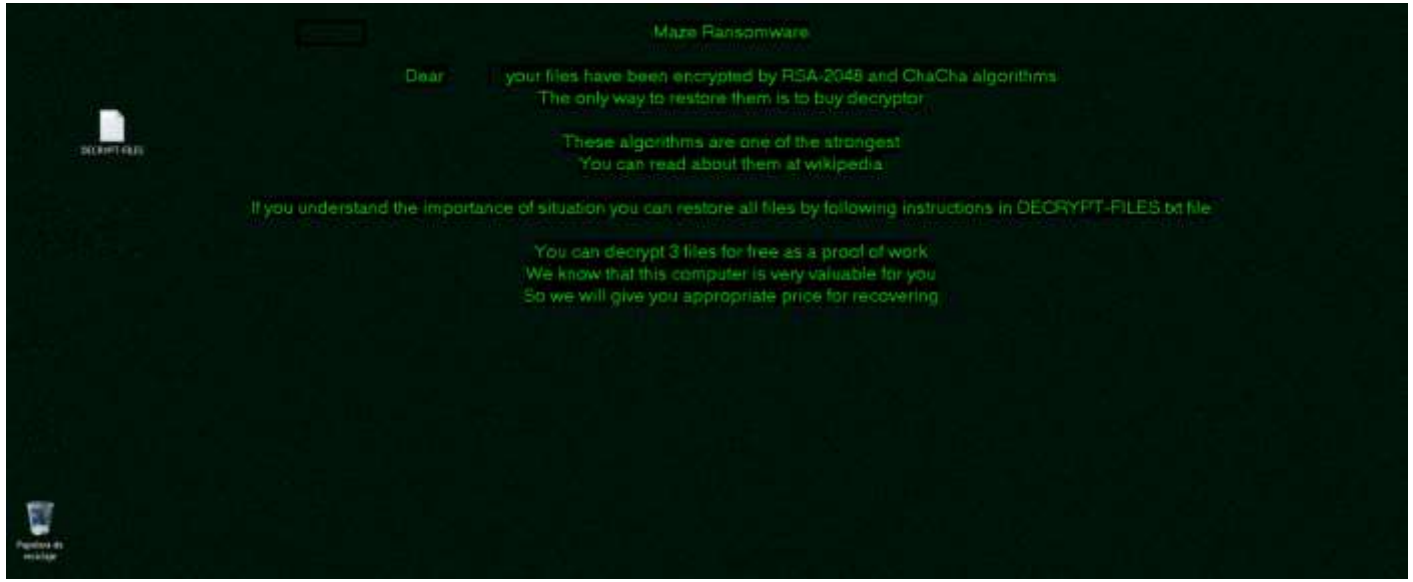
FAKULTA ELEKTROTECHNIKY A INFORMATIKY

Computer CNL Networks Laboratory

Kto útočí najčastejšie

U nás

- **FancyBear** (iné mená: APT28, Pawn Storm, Sofacy Group, Sednit, Tsar Team, Strontium) – podľa niektorých zdrojov na 90% GRU.
- **APT29** (Cozy Bear) – FSB.
- **APT41 + APT10** - Čína
- **MAZE** – koniec 2020,
- **FIN8** – globálna skupina,
- **GandCrab** – Rusi



Globálne

- **Bureau 121** + **Lazarus** – Severná Kórea
- **DarkSide** (Colonial Pipeline ☺)- ?
- **Unit 8200** – Rusi, **PLA Unit 61398** – Čína

Ransomware by FIN8 – White Rabbit

```
|----------------------------------------------------------------------

                        HELLO

If you are reading this message, means that:
      - your network infrastructures have been compromised,
      - critical data has leaked,
      - files are encrypted

            â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"
            â"ƒ          Welcome to the Ransom House              â"ƒ
            â"ƒ                 You are locked by                 â"ƒ
            â"ƒ              W H I T E    R A B B I T             â"ƒ
            â"ƒ       Knock, Knock. Follow the White Rabbit...    â"ƒ
            â"ƒ                                                   â"ƒ
            â"ƒ                    (\(\                           â"ƒ
            â"ƒ                    (-.-)                          â"ƒ
            â"ƒ                    (")(")                         â"ƒ
            â"ƒ                                                   â"ƒ
            â"—â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"â"›

            The best and only thing you can do is to contact us
              to settle the matter before any losses occurs.

----------------------------------------------------------------------

                                  1. THE FOLLOWING IS STRICTLY FORBIDDEN

1.1 DELETION THIS NOTE.
                            Each note carries the encryption key
                            needed to decrypt the data,
                            don't lose it

1.2 EDITING FILES OR HDD.
                            Renaming, copying or moving any files
                            could DAMAGE the cypher and
                            decryption will be impossible.

1.3 USING THIRD-PARTY SOFTWARE.
                            Trying to recover with any software
                            can also break the cipher and
                            file recovery will become a problem.

1.4 SHUTDOWN OR RESTART THE PC.
                            Boot and recovery errors can also damage the cipher.
                            Sorry about that, but doing so is entirely at your own risk.

1.5 HIRING THE FBI AND OTHERS
                            Cooperating with the FBI|CIA and so on
                            and involving their officers in negotiations
                            will end our communication with you
                            and we will share all the leaked data for free.

-----------------------------------------------------------------------------------------------

                                  2. EXPLANATION OF THE SITUATION
2.1 HOW DID THIS HAPPEN

The security of your IT perimeter has been compromised (it's not perfect at all).
We encrypted your workstations and servers to make the fact of the intrusion visible and to prevent you from hiding critical
data leaks.
We spent a lot of time for researching and finding out the most important directories of your business, your weak points.
We have already downloaded a huge amount of critical data and analyzed it. Now it's fate is up to you, it will either be deleted
or sold, or shared with the media.

2.2 VALUABLE DATA WE USUALLY STEAL:
                            - Databases, legal documents, billings, clients personal information, SSN...
                            - Audit reports
                            - Any financial documents (Statements, invoices, accounting, transfers etc.)
                            - work files and corporate correspondence
                            - Any backups

2.3 TO DO LIST (best practice)
```

FAKULTA ELEKTROTECHNIKY A INFORMATIKY

WannaCry (*2017)

Ciele predmetu

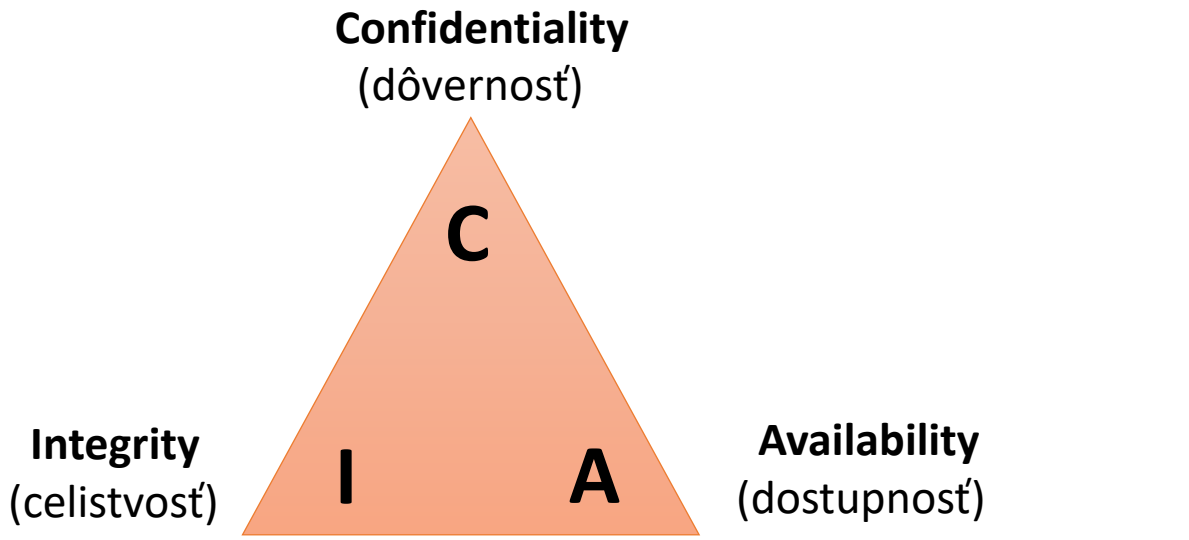
- Získať nové znalosti v oblasti kybernetickej bezpečnosti
- Porozumieť aké sú požiadavky na bezpečnosť IKT
- Spoznať existenciu štandardov pre procesy v informačnej a kybernetickej bezpečnosti
- Predstaviť slovenskú legislatívu, kde sme dnes a kam sa chceme dostať
- Porozumieť problematike reálneho sveta informačnej a kybernetickej bezpečnosti, výzvam pre firmy a najmä pochopiť súvislosti

Informačná vs. kybernetická bezpečnosť

Informačná bezpečnosť – je zachovanie dôvernosti, integrity a dostupnosti informácií

Kybernetická bezpečnosť - je zachovanie dôvernosti, integrity a dostupnosti informácií v kybernetickom priestore

Kybernetická bezpečnosť je podmnožinou informačnej bezpečnosti.



src: ISO/IEC 27032

Kybernetický priestor

Zákon 69 / 2018 Z.z., **§ 3**, písm. b:

kybernetickým priestorom globálny dynamický otvorený systém sietí a informačných systémov, ktorý tvoria aktivované prvky kybernetického priestoru, osoby vykonávajúce aktivity v tomto systéme a vzťahy a interakcie medzi nimi.

- „je ohraničený používaním eln. zariadení a eln. spektra na vytvorenie, uloženie, modifikovanie, výmenu a využívanie dát prostredníctvom vzájomne závislých a prepojených sietí“
  (s. 35, Zákon o kybernetickej bezpečnosti. Komentár, 2019. Chlipala – Makatura - Pilár)

Pravidlá hry

EÚ

Smernica EÚ č. 2016/1148	Nariadenie EÚ č. 2019/881	Nariadenie EÚ č. 2016/679
o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii	o agentúre ENISA a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií	o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe takýchto údajov (všeobecné nariadenie o ochrane údajov)
NIS	**Cyber Act**	**GDPR**

SK

Zákon č. 69/2019 Z.z.	Vyhláška 362/2018 NBÚ	Zákon č. 18/2018 Z.z.
o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov	ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení	ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení

Rozšírenie pojmového aparátu – základné pojmy

Podľa kľúčového zákona 69 / 2018 Z.z., **§ 3** sa rozumie:

- **sieťou** elektronická komunikačná sieť podľa osobitného predpisu (*zákon 351/2011 o eln. komunikáciach*)
- **informačným systémom** funkčný celok, ktorý zabezpečuje získavanie, zhromažďovanie, automatické spracúvanie, udržiavanie, sprístupňovanie, poskytovanie, prenos, ukladanie, archiváciu, likvidáciu a ochranu údajov prostredníctvom technických prostriedkov alebo programových prostriedkov,
- **kontinuitou** strategická a taktická schopnosť organizácie plánovať a reagovať na udalosti a incidenty s cieľom pokračovať vo výkone činností na prijateľnej, vopred stanovenej úrovni,
- **dôvernosťou** záruka, že údaj alebo informácia nie je prezradená neoprávneným subjektom alebo procesom,
- **dostupnosťou** záruka, že údaj alebo informácia je pre používateľa, informačný systém, sieť alebo zariadenie prístupné vo chvíli, keď je údaj a informácia potrebná a požadovaná,
- **integritou** záruka, že bezchybnosť, úplnosť alebo správnosť informácie neboli narušené,

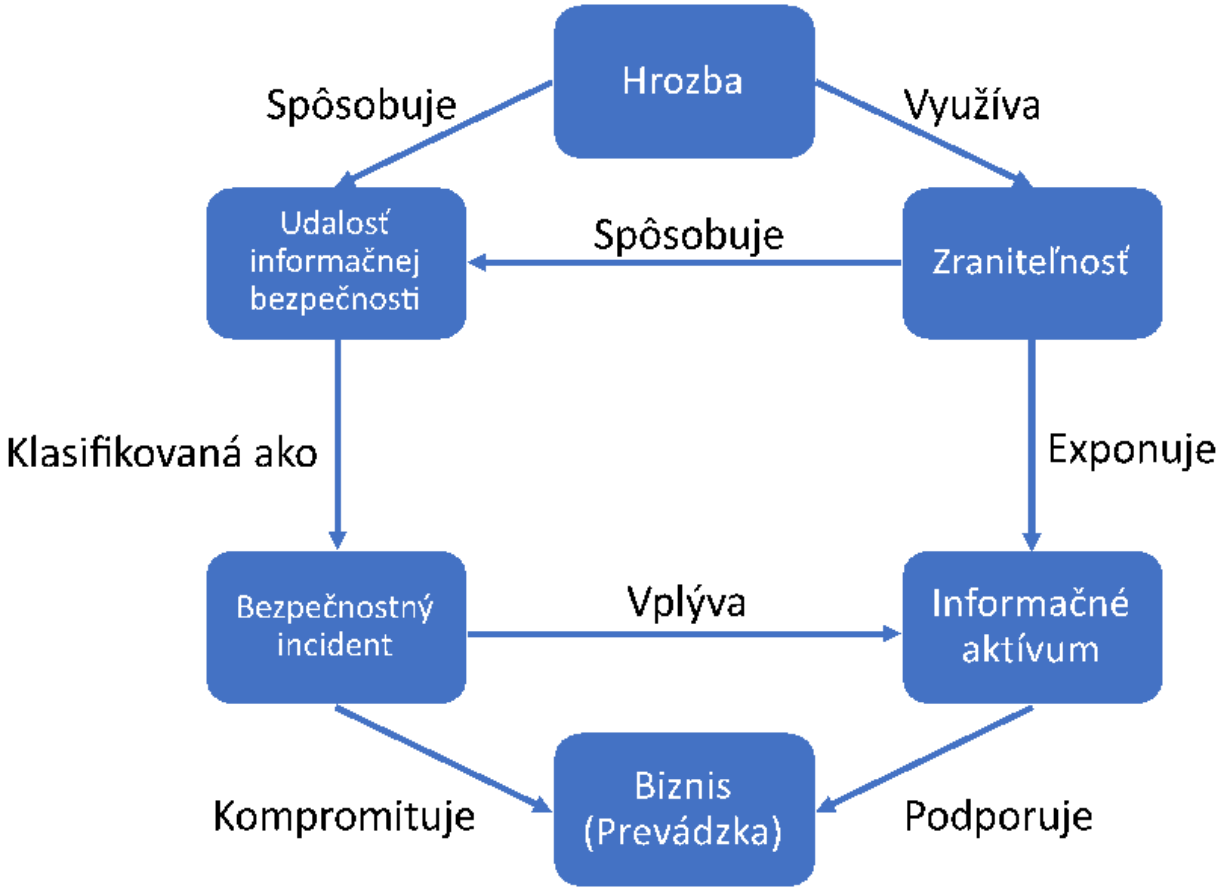
Rozšírenie pojmového aparátu – základné pojmy

Podľa kľúčového zákona 69 / 2018 Z.z., **§ 3** sa rozumie:

- **kybernetickou bezpečnosťou stav, v ktorom sú siete a informačné systémy schopné odolávať na určitom stupni spoľahlivosti akémukoľvek konaniu, ktoré ohrozuje dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo súvisiacich služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov,**
- **rizikom** miera kybernetického ohrozenia vyjadrená pravdepodobnosťou vzniku nežiaduceho javu a jeho dôsledkami,
- **hrozbou** každá primerane rozpoznateľná okolnosť alebo udalosť proti sieťam a informačným systémom, ktorá môže mať nepriaznivý vplyv na kybernetickú bezpečnosť,
- **kybernetickým bezpečnostným incidentom** akákoľvek udalosť, ktorá má z dôvodu narušenia bezpečnosti siete a informačného systému, alebo porušenia bezpečnostnej politiky alebo záväznej metodiky negatívny vplyv na kybernetickú bezpečnosť alebo ktorej následkom je
  - strata dôvernosti údajov, zničenie údajov alebo narušenie integrity systému,
  - obmedzenie alebo odmietnutie dostupnosti základnej služby alebo digitálnej služby,
  - vysoká pravdepodobnosť kompromitácie činností základnej služby alebo digitálnej služby alebo
  - ohrozenie bezpečnosti informácií.

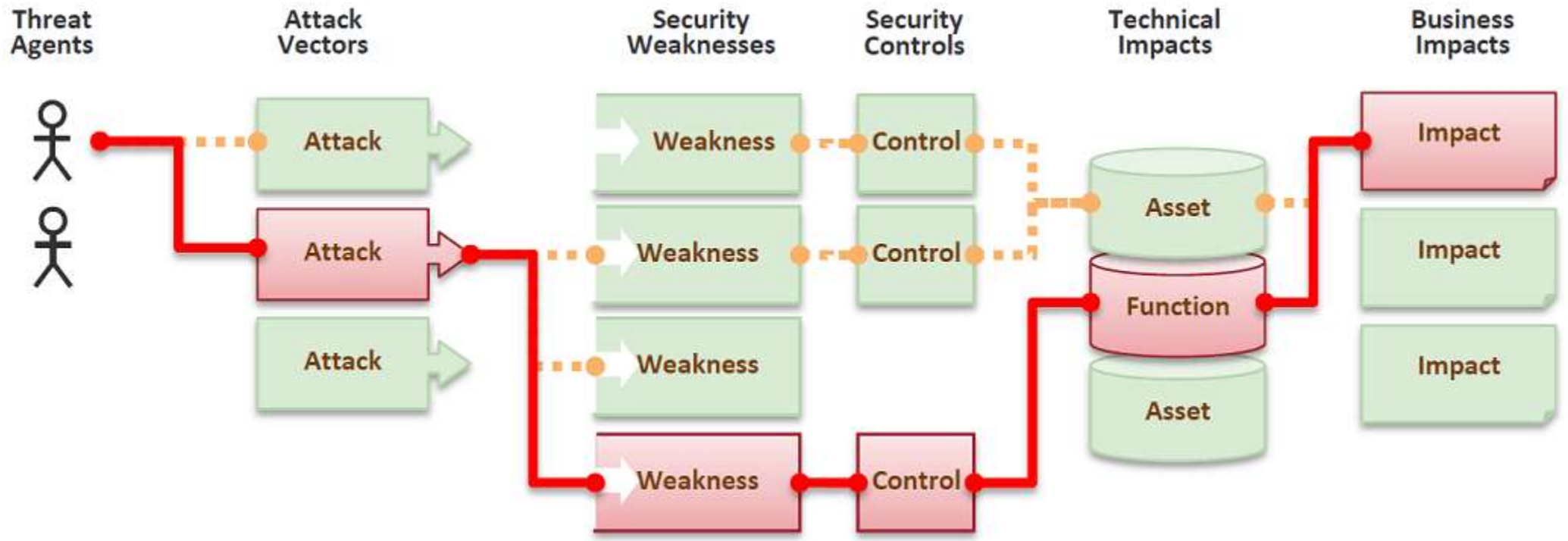
Princípy manažmentu incidentov

ISO/IEC 27035-1:2016

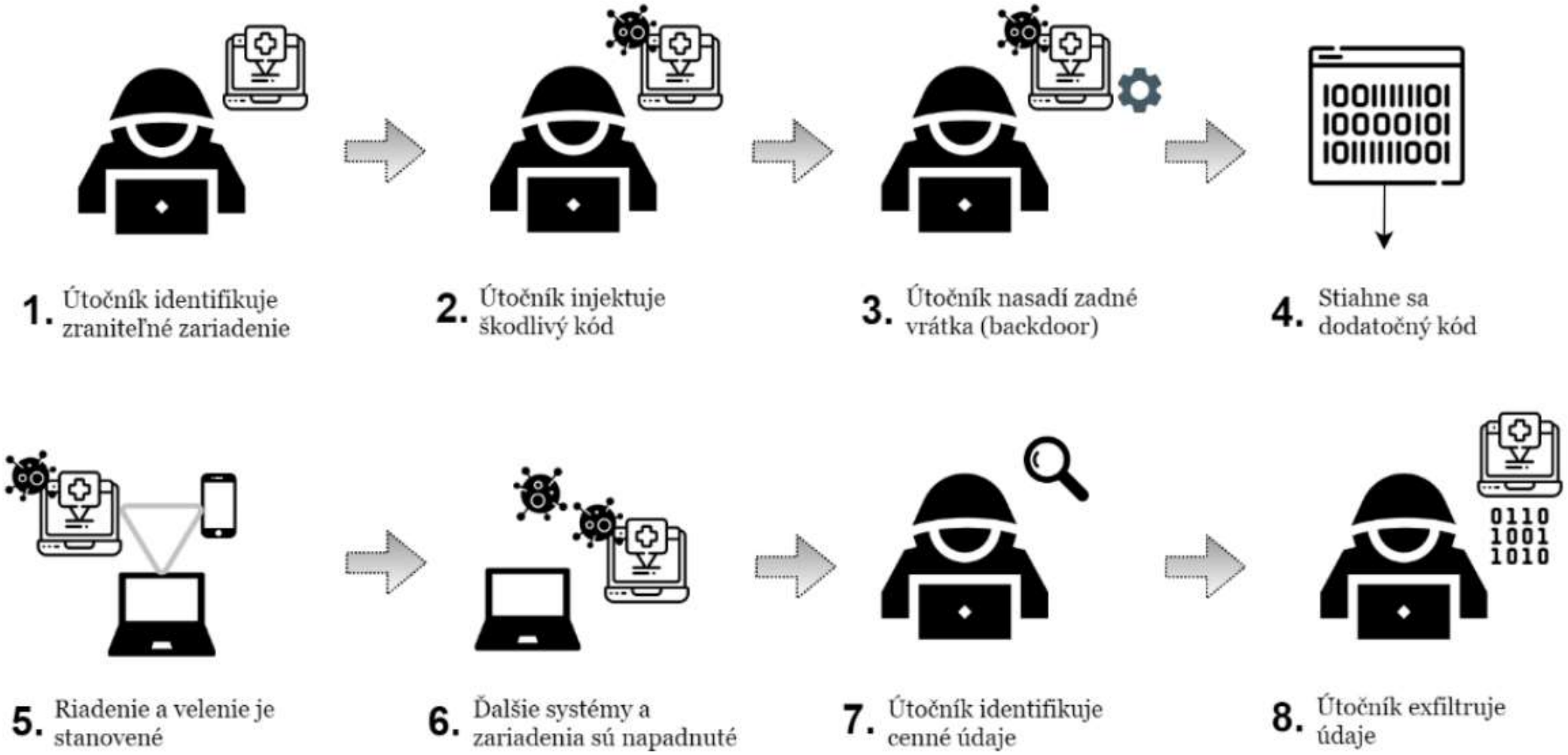


src: https://www.nbu.gov.sk/kyberneticka-bezpecnost/riadenie-rizik/index.html

Identifikácia vektoru útoku

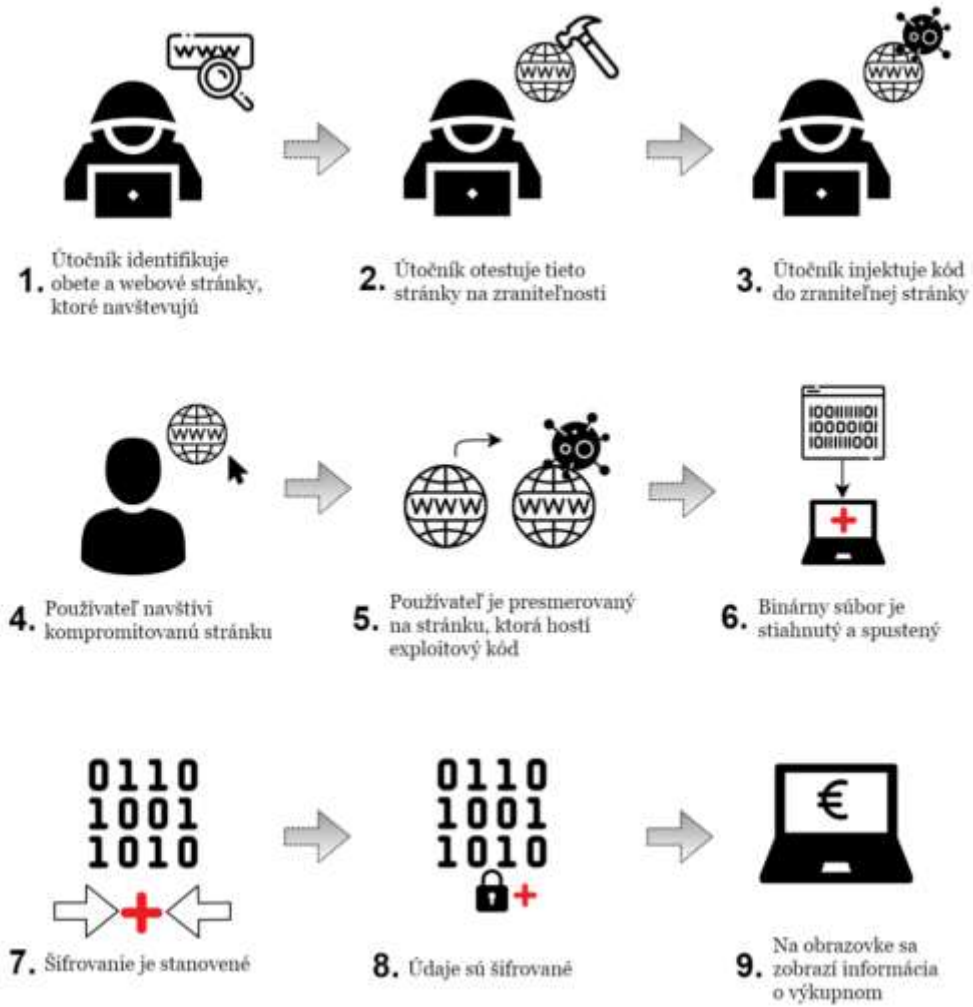


Scenár útoku s využitím malvéru



src: https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals

Scenár útoku s využitím ransomvéru



src: https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals

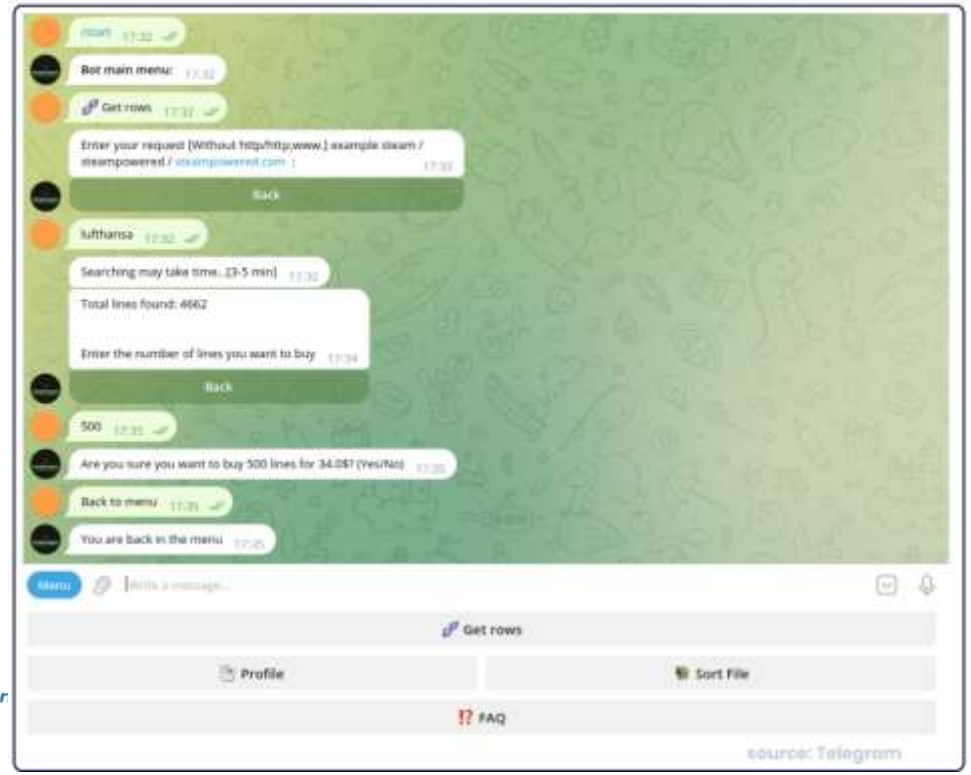
Najčastejšie vektory útoku

- zraniteľnosti softvéru,
- zneužitie prístupových údajov používateľov,
- jednoduché heslá a nedostatočná autentifikácia,
- nahnevaní zamestnanci,
- nedostatočné alebo chýbajúce šifrovanie,
- ransomvér,
- phishing,
- zlá konfigurácia zariadení,
- dodávateľský reťazec,
- DDoS útoky.

Ďalšie tooly

- **Infostealer**
  - Malvér na mobilných zariadeniach a PC
  - Vykrádanie obsahu, keyloggery
  - Existuje browser extension (kryptopeňaženky, sessions, cookies, cam/mic)
  - as-a-service
  - 1.000.000+ subscribers

sekoia | **Interactions with the Omega Request Telegram bot selling logs**



sekoia | **BSC cloud of logs advertised on Telegram**

Ďakujem za pozornosť

miroslav.michalko@cnl.sk

Laboratórium počítačových sietí

Katedra počítačov a informatiky, FEI TUKE