UNIVERZITA
PAVLA JOZEFA ŠAFÁRIKA
V KOŠICIACH

Financované
Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Úvod do kybernetickej a informačnej bezpečnosti

(Vzdelávanie pre zamestnancov verejnej správy v kategórií používateľov „laik“, „odborný zamestnanec“ a „manažér“ – modul č. 1)

Meno Priezvisko

XX.XX.XXXX

KC KB UPJŠ (I.)

- UPJŠ – všetky fakulty / CSIRT-UPJS / CCVaPP
- cieľ: zvýšenie bezpečnostného povedomia relevantných subjektov | operatívnej bezpečnosti | výskum v KB

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KC KB UPJŠ (II.)

A1 - Zariadenie a vybavenie KC

A4 - Výskumná činnosť

A7 – Zvyšovanie odbornosti

A2 - Tvorba materiálov, predmetov

A5 - Expertná činnosť

A8 - Spolupráca

A3 - Tvorba metodík, vzdelávacích materiálov

A6 - Celoživotné vzdelávanie

A9 - Odborné poradenstvo

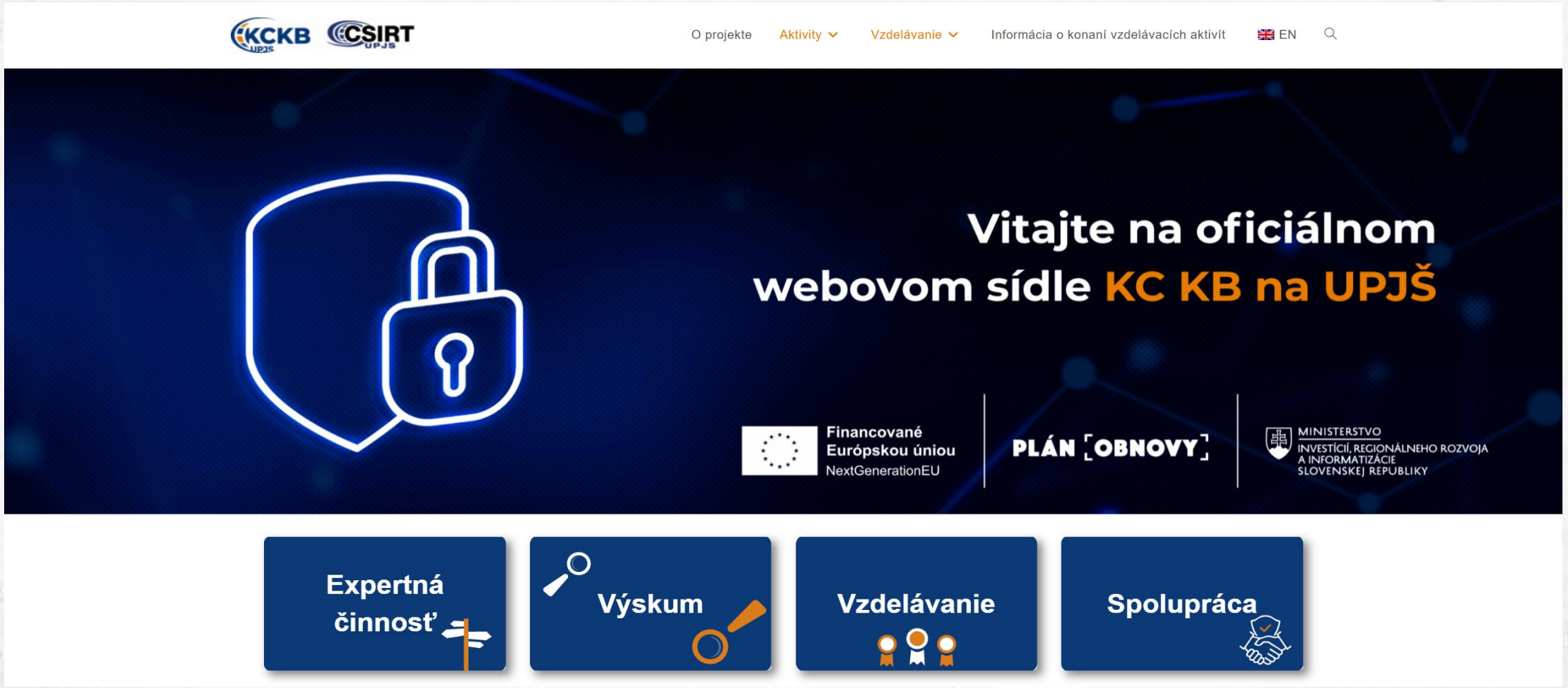
Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KC KB UPJŠ (III.)

https://**cyberawareness.sk/**



Vzdelávacia aktivita (I.)

- Vyhláška č. 492/2022 Z. z. ktorou sa ustanovujú znalostné štandardy v oblasti kybernetickej bezpečnosti
  - kategória používateľov **„IT manažér“, „informatik“, „zamestnanec v kybernetickej bezpečnosti"**
  - kategória používateľov **„laik“, „odborný zamestnanec“ a „manažér“**

Odborný zamestnanec

Rola:	**Odborný zamestnanec**	
Vedomosti:	1) vybrané základné pojmy v kybernetickej bezpečnosti	BL2
	2) význam osobných údajov a citlivých informačných aktív	BL2
	3) zdroje typických hrozieb a kategórie hrozieb (úmyselné hrozby, náhodné hrozby, hrozby prostredia)	BL2
	4) aktuálne typy hrozieb (napr. škodlivý kód, phishing, spam, útok na internetové služby alebo stránky (Denial of Service (DoS)/znemožnenie prístupu k požadovanej službe (Distributed denial of service (DDoS), botnety, krádež identity a ďalšie)	BL2
	5) identifikácia, autentizácia, autorizácia	BL2
	6) spôsoby overenia digitálnej totožnosti význam viacfaktorovej autentizácie a typy autentizačných faktorov	BL2
	7) základné princípy bezpečného používania hesiel	BL2
	8) význam škodlivého kódu (malvér) a spôsoby útokov škodlivým kódom	BL2
	9) riziká používania zariadení IKT	BL2
	10) základné zraniteľnosti smartfónov	BL2
	11) základné princípy vzdialeného prístupu a bezpečnostné zásady pri práci na diaľku	BL2
	12) obsah pojmu digitálne súkromie	BL2
	13) význam pojmov digitálny popis, elektronický podpis, kvalifikovaný elektronický podpis, časová pečiatka	BL2
	14) základné zásady bezpečnosti, ochrany osobných údajov a etikety pri telekonferenciách a online rokovaniach, stretnutiach	BL2
	15) bezpečnostné riziká a riziká ochrany súkromia pri používaní sociálnych sietí pokiaľ sú v organizácii povolené	BL2
	16) podstata útokov formou sociálneho inžinierstva (phising, vishing, smishing, Business Email Compromise)	BL2
	17) základné poznatky na úseku trestného práva	BL2

Vzdelávacia aktivita (II.)

- Registrácia – portál CCVaPP – https://portal.ccvapp.upjs.sk/

- Vzdelávanie prebieha online / prezenčne
  - Online – MS Teams platforma
  - pred každým stretnutím - odkaz

- 7 modulov – po ukončení všetkých – osvedčenie o absolvovaní
- Krátky test/zhrnutie
- Diskusia – priebežne aj na záver
- Spätná väzba

Vzdelávacia aktivita (III.)

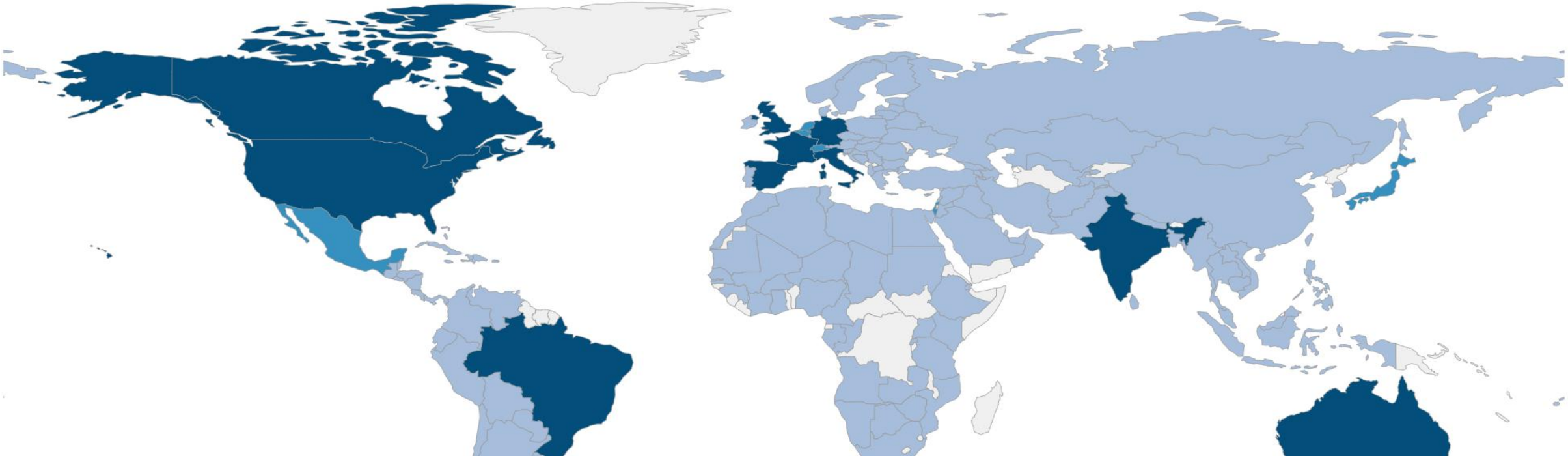
- Časový harmonogram
  - 08:30 – 10:00 – 1. blok
  - 10:00 – 11:30 – 2. blok
  - 11:30 – 12:30 – prestávka
  - 12:30 – 14:00 – 3. blok

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Vzdelávacia aktivita (IV.)

Číslo modulu	Názov modulu	Časová dotácia (45 min.)	Forma stretnutia
Modul č. 1	Úvod do kybernetickej a informačnej bezpečnosti (KIB)	6	Online / Prezenčne
Modul č. 2	Kritické myslenie a dezinformácie	8	Online / Prezenčne
Modul č. 3	Sociálne inžinierstvo	8	Online / Prezenčne
Modul č. 4	Bezpečnosť prevádzky a riešenie kybernetických incidentov	8	Online / Prezenčne
Modul č. 5	Digitálna identita a súkromie v online prostredí	6	Online / Prezenčne
Modul č. 6	Základy práva informačných a komunikačných technológií pre KIB I.	8	Online / Prezenčne
Modul č. 7	Základy práva informačných a komunikačných technológií pre KIB II.	8	Online / Prezenčne

Svet okolo nás (I.)



Groups	Victims	This year	This month
268	20 315	3 829	291

Zdroj: https://www.ransomware.live/

Svet okolo nás (II.)

2012

Hackeri napadli sociálnu sieť LinkedIn. Ukradli 6,5 milióna hesiel

06.06.2012 / Noviny.sk / Veda a technika

LUCIA HUSÁROVÁ

Zdroj: https://www.noviny.sk/veda-a-technika/104055-hackeri-napadli-socialnu-siet-linkedin-ukradli-6-5-miliona-hesiel

Od: Jhrasko <....@yahoo.jp>
Odoslané: sobota, 8. septembra 2018 3:36
Komu: xxx.xxx@upjs.sk <xxx.xxx@upjs.sk>
Predmet: Your password is vJanka

I am aware vJanka is your passphrase. Lets get right to purpose. You may not know me and you are most likely thinking why you are getting this e mail? None has compensated me to investigate about you.

...

You get just two solutions. Why dont we look at these types of options in particulars:

1st solution is to skip this e mail. In this situation, I most certainly will send your very own recorded material to almost all of your contacts and then just think regarding the humiliation you feel. Furthermore if you happen to be in a romantic relationship, exactly how it would affect?

Number 2 alternative would be to give me $4000. Let us describe it as a donation. Subsequently, I will asap eliminate your video. You could go on with your daily ro utine like this never happened and you will not hear back again from me.

Svet okolo nás (II.)

2020

Nemocnicu v Česku ochromil ransomvér, naplánované operácie sa rušia

Redakcia CyberSec.sk / 12.12.2019

Ransomware attack: Maastricht University pays out $220,000 to cybercrooks

Adam Bannister 07 February 2020 at 16:05 UTC
Updated: 11 May 2020 at 08:17 UTC

Ransomware | Netherlands | Cybercrime

Dutch institution regrets striking 'devil's bargain' but said it had to put staff and students first

Zdroje: https://mobil.sk/clanok/3517-hackeri-sa-naburali-do-kamier-android-smartfonov-keby-sa-nepriznali-nikto-by-to-ani-nevedel, https://portswigger.net/daily-swig/ransomware-attack-maastricht-university-pays-out-220-000-to-cybercrooks

Svet okolo nás (III.)

2021

Hackers Breached Colonial Pipeline Using Compromised Password

- Investigators suspect hackers got password from dark web leak
- Colonial CEO hopes U.S. goes after criminal hackers abroad

LIVE ON BLOOMBERG
Watch Live TV >
Listen to Live Radio >

Photographer: Samuel Corum/Bloomberg

By William Turton and Kartikay Mehrotra
June 4, 2021, 3:58 PM EDT

CYBER SECURITY NEWS · 4 MIN READ

IKEA Suffers Ongoing Phishing Attacks From Compromised Internal and Vendor Accounts

SCOTT IKEDA · DECEMBER 2, 2021

Internal emails published by Bleeping Computer reveal that leading furniture retailer IKEA is battling an ongoing campaign of phishing attacks, fueled by internal and vendor accounts that have already been compromised.

Zdroje: https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password,
https://www.cpomagazine.com/cyber-security/ikea-suffers-ongoing-phishing-attacks-from-compromised-internal-and-vendor-accounts/

Svet okolo nás (IV.)

2022

6. septembra 2022 17:37 Firmy Lesy SR

Štátne lesy zostali po hekerskom útoku bez systémov. Nemôžu predávať palivové drevo a padol im aj portál na kontrolu ťažby

IVAN HALUZA + Zapnúť články e-mailom

Ťažba dreva v lesoch. Ilustračné foto – TASR

28.6.2022 06:55 | Telekom

AKTUALIZOVANÉ Telekom zasiahol ransomvérový útok. Funguje aktivácia balíčkov aj e-shop

Zdroj: iStock a úprava Živé.sk

Zdroj: https://zive.aktuality.sk/clanok/j42eNLl/telekom-zasiahol-ransomverovy-utok-funguje-aktivacia-balickov-aj-e-shop/, https://e.dennikn.sk/2999023/statne-lesy-zostali-po-hekerskom-utoku-bez-systemov-nevedia-predavat-drevo-a-padol-im-aj-portal-na-kontrolu-tazby/

Svet okolo nás (V.)

2023

11.7.2023 15:14 | Bezpečnosť

TOP Hackeri zverejnili dáta ukradnuté Univerzite Mateja Bela, začínajú sa šíriť internetom

Zdroj: Ján Koliba

8.9.2023 13:59 | Bezpečnosť

Košická župa čelila kybernetickému útoku, elektronické služby úradu sú dočasne nefunkčné

Zdroj: Pixabay

Podobne ako v minulosti, aj tentoraz malo ísť o ransomvér.

Zdroj: https://zive.aktuality.sk/clanok/8rvLPeR/kosicka-zupa-celila-kybernetickemu-utoku-elektronicke-sluzby-uradu-su-docasne-nefunkcne/
https://zive.aktuality.sk/clanok/cfRr3Xq/hackeri-zverejnili-data-ukradnute-univerzite-mateja-bela-zacinaju-sa-sirit-internetom/

Svet okolo nás (VI.)

2024

22.3.2024 15:46 | Bezpečnosť

Hackeri udreli na Slovenskú národnú knižnicu. Nejdú prístupy k zdrojom ani kontakty

Zdroj: reprofoto Snk.sk, iStock a úprava redakcia

Rumunské nemocnice napadnuté ransomvérom

Vypublikované 13. 02. 2024

ransomware-nemocnice-860x360

Najmenej 25 rumunských nemocníc bolo odrezaných od online služieb po tom, čo útok ransomvéru znefunkčnil ich systém na správu zdravotnej starostlivosti. Cieľom útoku bol HIS, ktorý sa používa v nemocniciach na správu lekárskej činnosti a údajov o pacientoch. Útok, ktorý sa odohral počas noci z 11. na 12. februára 2024, zasiahol produkčné servery HIS a v dôsledku toho s**ystém prestal fungovať**, súbory a databázy boli zašifrované. **Rumunské ministerstvo zdravotníctva** uviedlo, že incident je predmetom vyšetrovania IT špecialistami, vrátane odborníkov na kybernetickú bezpečnosť z Národného riaditeľstva pre kybernetickú bezpečnosť (DNSC), a posudzujú sa možnosti obnovy. Zoznam zasiahnutých nemocníc bol aktualizovaný po zverejnení aktualizácie DNSC a zahŕňa nemocnice v rôznych regiónoch Rumunska vrátane centier pre regionálnu a onkologickú liečbu.

Zdroj: https://www.nbu.gov.sk/rumunske-nemocnice-napadnute-ransomverom/, https://zive.aktuality.sk/clanok/1CGRx85/hackeri-udreli-na-slovensku-narodnu-kniznicu-nejdu-pristupy-k-zdrojom-ani-kontakty/

Svet okolo nás (VII.)

2025

TREND Predplatiť

Hekeri po útoku na kataster žiadajú vysoké výkupné, štát nemusí disponovať zálohami dát

Daniel Ivančák
online editor

9.1. 7:35 | **Ak sa hekerský útok v takomto rozsahu potvrdí, na Slovensku môže nastať chaos**

ŽIVE Predplatné

TOP Kataster po mesiaci: Štát prelomil mlčanie. Čo radí a sľubuje ľuďom

Zdroj: iStock, reprofoto Zbgis.skgeodesy.sk, úprava redakcia

Lukáš Kosno

Filip Hanker

Zhrnuli sme novinky okolo katastra presne mesiac po útoku. Máme oficiálne vyjadrenia úradu.

Zdroj: https://www.trend.sk/spravy/hekeri-utoku-kataster-ziadaju-vysoke-vykupne-stat-nemusi-disponovat-zalohami-dat
https://zive.aktuality.sk/clanok/MkBBFdI/kataster-po-mesiaci-stat-prelomil-mlcanie-co-radi-a-slubuje-ludom/

Zdroj: https://www.timeout.com/chicago/tv/under-the-dome-tv-review

Zdroj: http://hellinahandbasket.net/?attachment_id=788

Čo je informačná bezpečnosť? (I.)

Všetky vaše medicínske záznamy sme omylom zaslali úplne cudziemu človeku

Odkazuje, že ani on bohužiaľ nevie čo s vami vlastne je...

Čo je informačná bezpečnosť? (II.)

Vaše medicínske záznamy nám bohužiaľ stále nezaslali naspäť

Nepamätáte si náhodou Vašu celú medicínsku históriu?

Zdroj: https://www.newyorker.com/magazine/2018/11/12/why-doctors-hate-their-computers

Čo je informačná bezpečnosť? (III.)

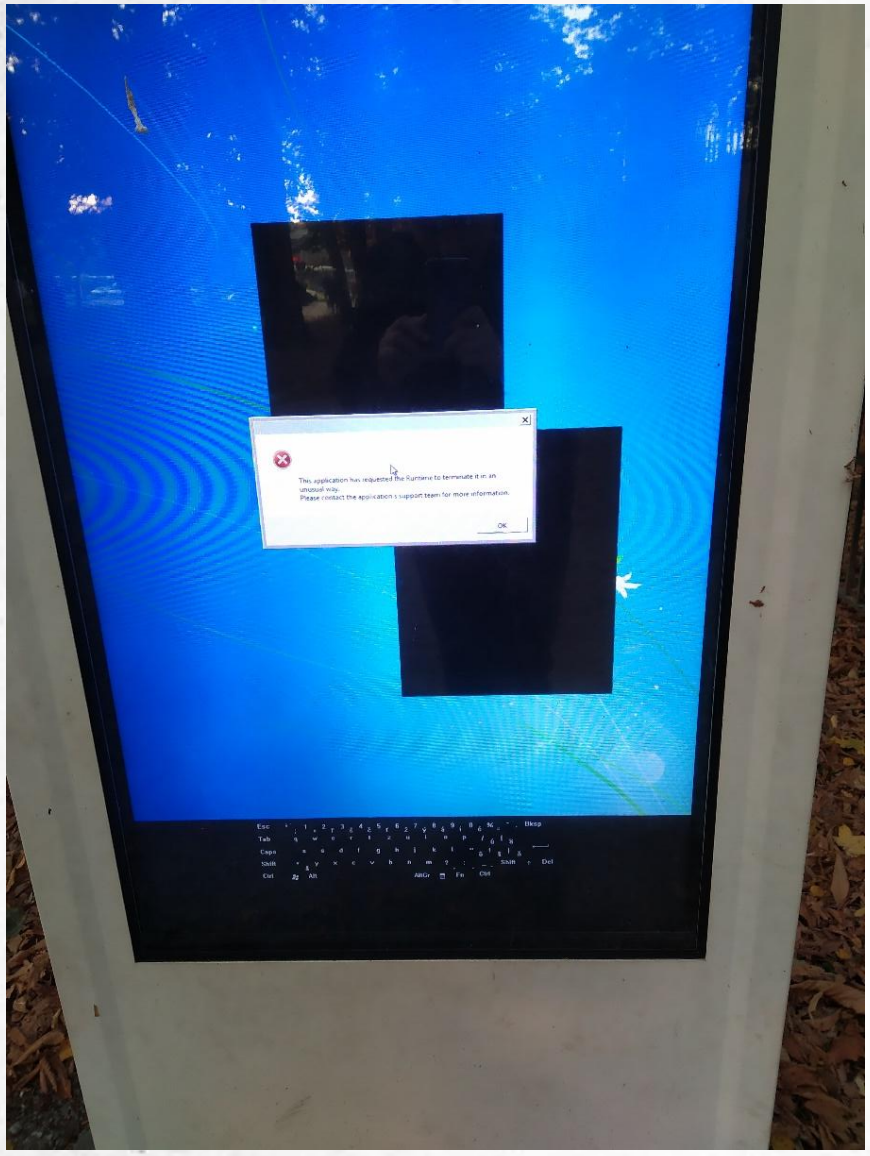
Vážený pane, vaše medicínske záznamy nám konečne zaslali späť a konečne poznáme príčinu vašich problémov

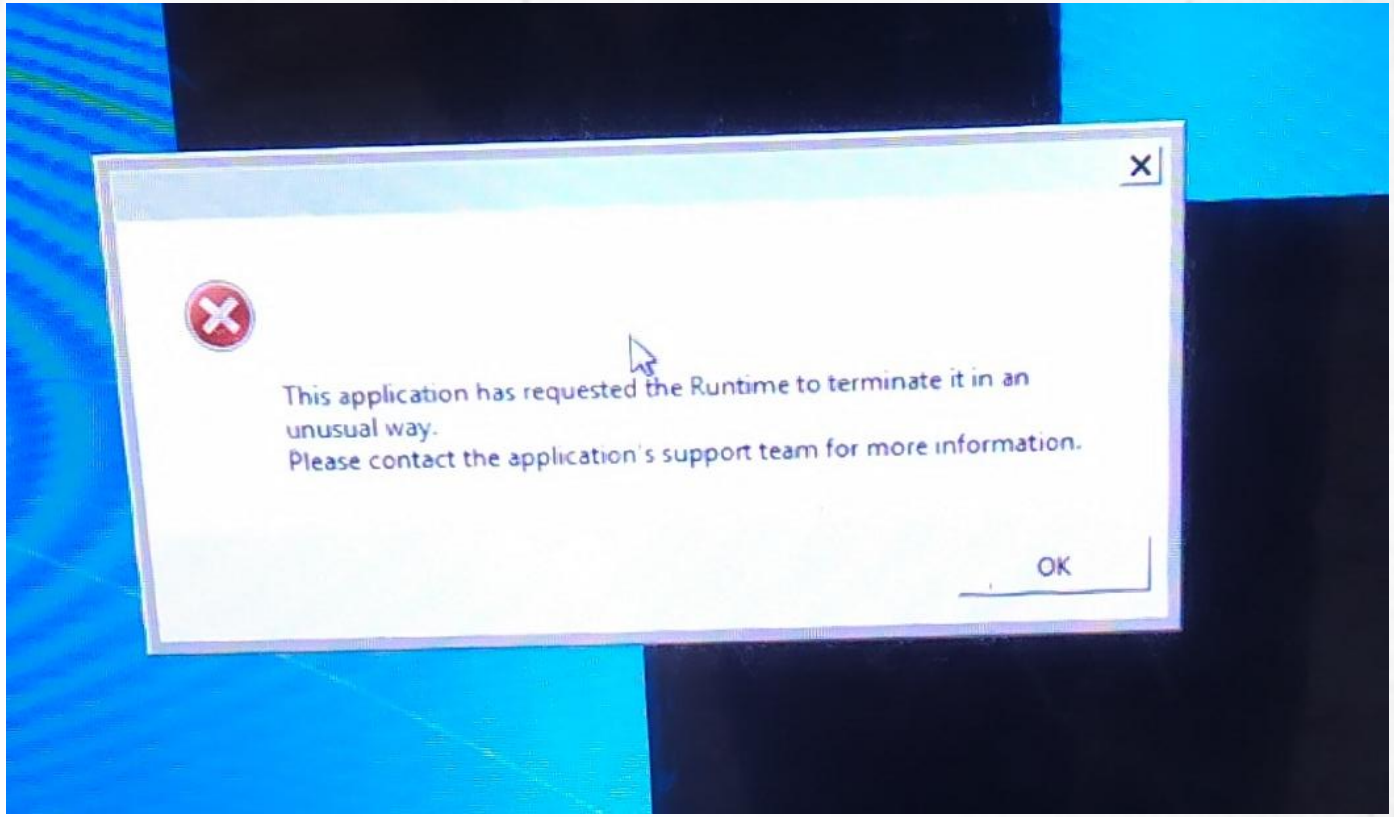
Ste tehotný!

Zdroj: https://dribbble.com/shots/6278477-Composition-with-little-doctors

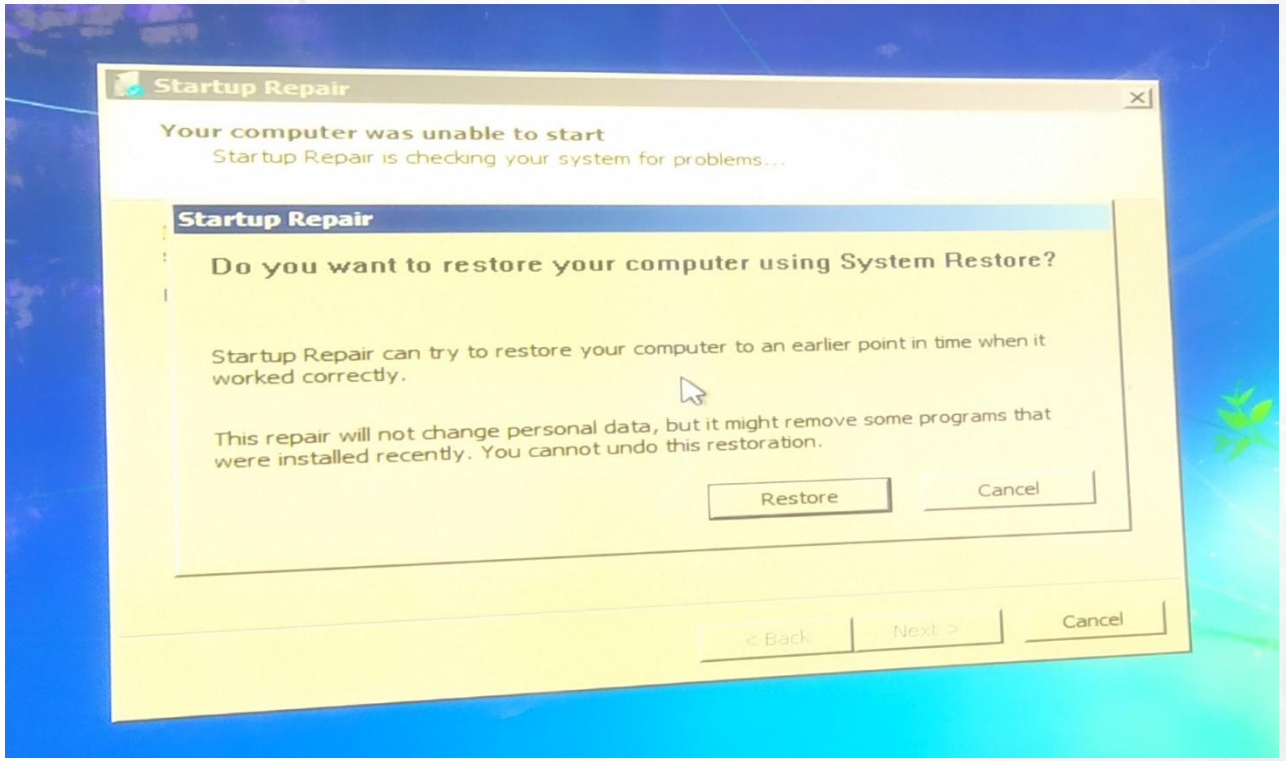

Search Google Maps
Stanične námestie
Košice, Košice Region
Google Street View
Apr 2024
See more dates
Košice
Stredná
škola že
Google
Image capture: Apr 2024
© 2024 Google
Slovakia
Terms
Privacy
Report a problem


Bez internetu



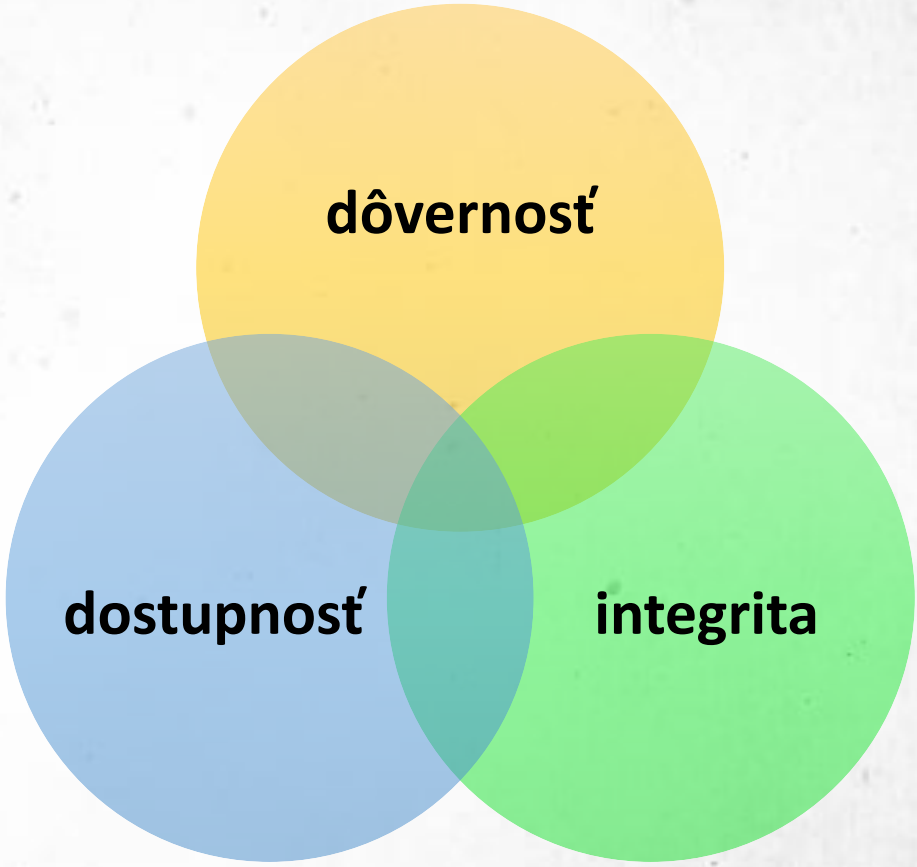

This application has requested the Runtime to terminate it in an unusual way.
Please contact the application's support team for more information.
OK


imotion

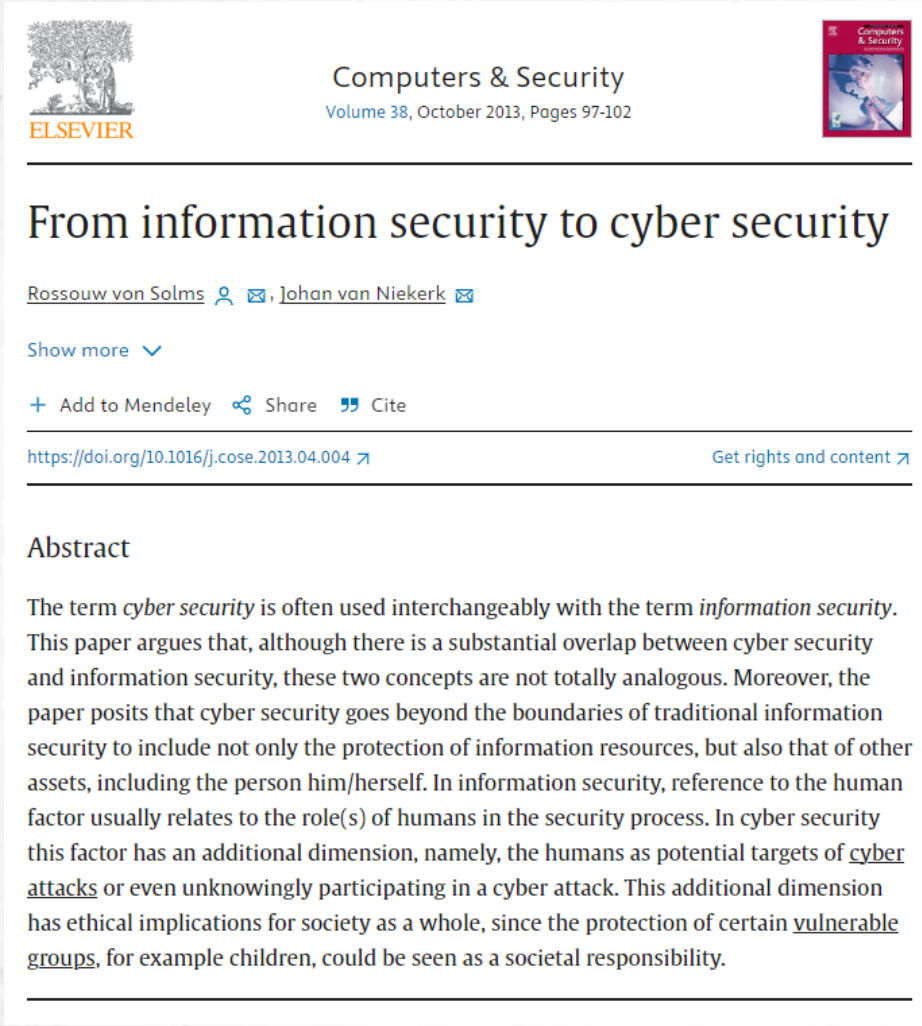

Startup Repair
Your computer was unable to start
Startup Repair is checking your system for problems...
Startup Repair
Do you want to restore your computer using System Restore?
Startup Repair can try to restore your computer to an earlier point in time when it worked correctly.
This repair will not change personal data, but it might remove some programs that were installed recently. You cannot undo this restoration.
Restore
Cancel
< Back
Next >
Cancel

Informačná bezpečnosť (I.)

- **dôvernosť**
  - informácie prístupné len osobám, ktoré určíme
- **integrita**
  - informácie sú úplné a neboli nevedomky upravované
- **dostupnosť**
  - informácie prístupné na požiadanie týchto osôb v tom čase



Informačná a kybernetická bezpečnosť (I.)



ELSEVIER

Computers & Security

Volume 38, October 2013, Pages 97-102

From information security to cyber security

Rossouw von Solms, Johan van Niekerk

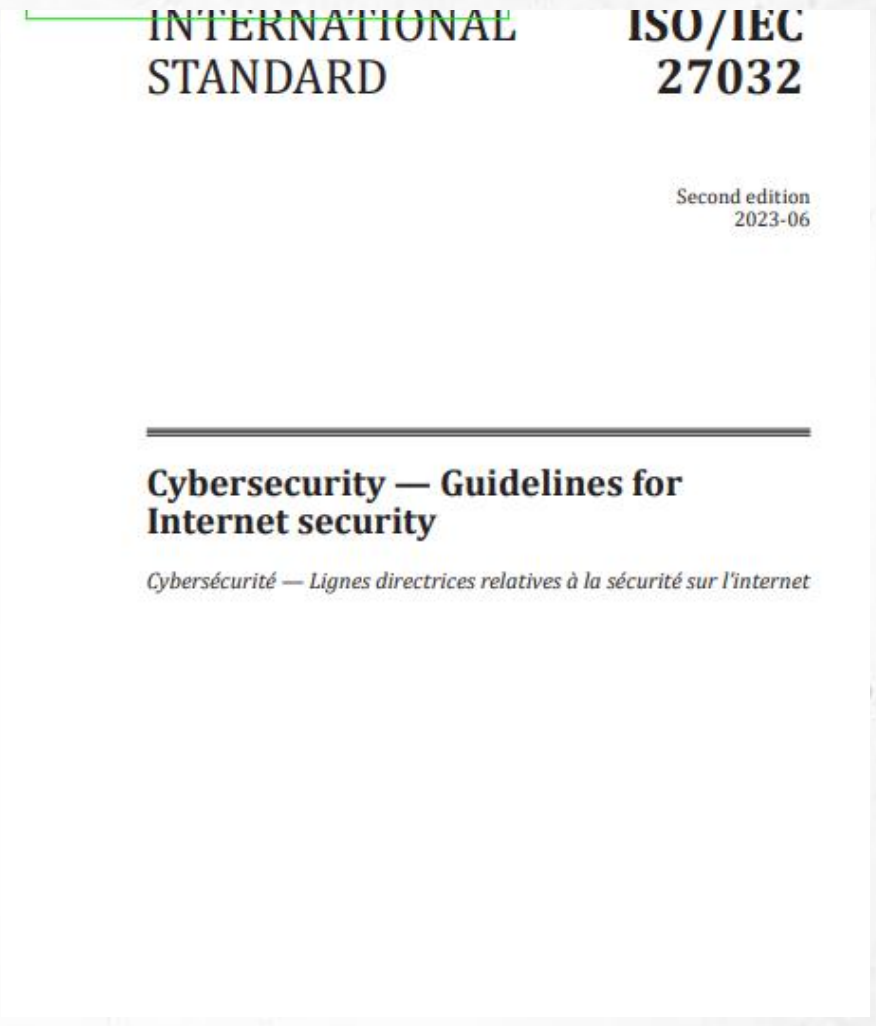
Show more

+ Add to Mendeley Share Cite

https://doi.org/10.1016/j.cose.2013.04.004 Get rights and content

Abstract

The term *cyber security* is often used interchangeably with the term *information security*. This paper argues that, although there is a substantial overlap between cyber security and information security, these two concepts are not totally analogous. Moreover, the paper posits that cyber security goes beyond the boundaries of traditional information security to include not only the protection of information resources, but also that of other assets, including the person him/herself. In information security, reference to the human factor usually relates to the role(s) of humans in the security process. In cyber security this factor has an additional dimension, namely, the humans as potential targets of cyber attacks or even unknowingly participating in a cyber attack. This additional dimension has ethical implications for society as a whole, since the protection of certain vulnerable groups, for example children, could be seen as a societal responsibility.



INTERNATIONAL STANDARD

ISO/IEC 27032

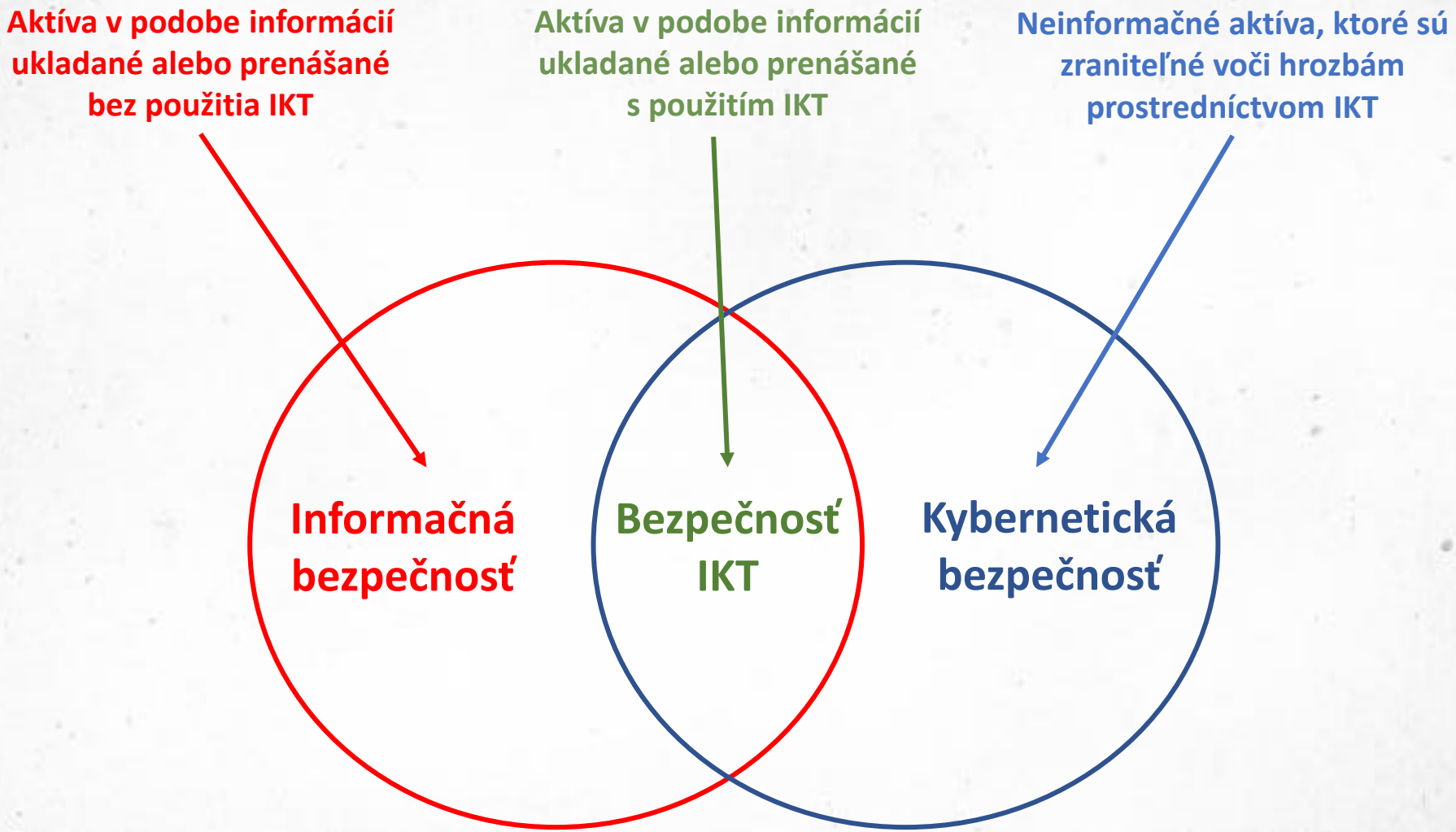
Second edition
2023-06

Cybersecurity — Guidelines for Internet security

Cybersécurité — Lignes directrices relatives à la sécurité sur l'internet

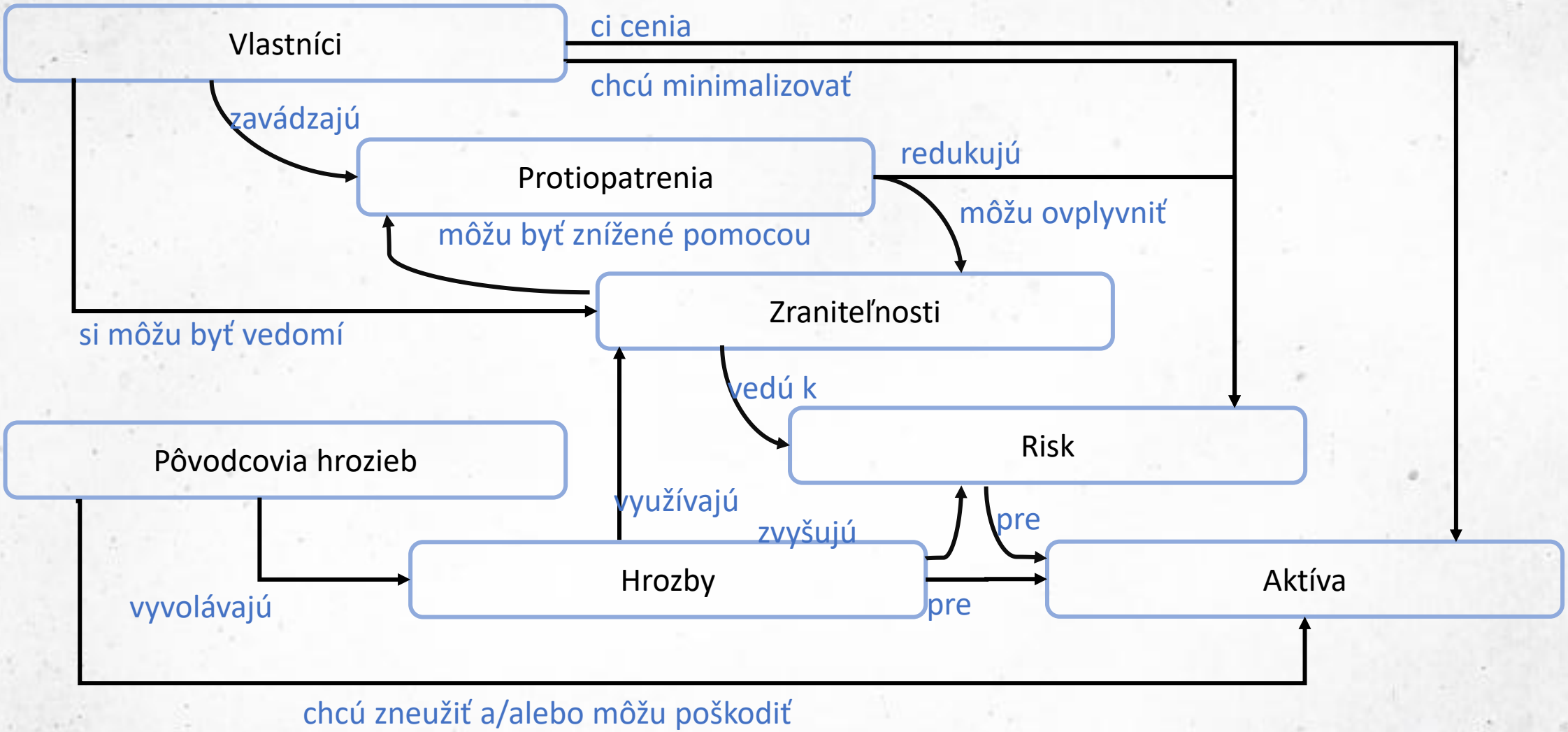
Zdroj: Von Solms, Rossouw, and Johan Van Niekerk. "From information security to cyber security." computers & security 38 (2013): 97-102.

Informačná a kybernetická bezpečnosť (II.)



Zdroj: Von Solms, Rossouw, and Johan Van Niekerk. "From information security to cyber security." computers & security 38 (2013): 97-102.

Model IB a KB


Vlastníci
ci cenia
chcú minimalizovať
zavádzajú
Protiopatrenia
redukujú
môžu ovplyvniť
môžu byť znížené pomocou
Zraniteľnosti
si môžu byť vedomí
vedú k
Risk
Pôvodcovia hrozieb
využívajú
zvyšujú
pre
Hrozby
Aktíva
vyvolávajú
pre
chcú zneužiť a/alebo môžu poškodiť

Aktívum (I.)

- **Aktívum (asset)** - všetky hmotné, ale aj nehmotné statky, všetko, čo má pre majiteľa systému určitú hodnotu.

  - **hardvér** – procesor, pamäť, terminály a pod.,
  - **softvér** – operačný systém, aplikačné programy a pod.,
  - **dáta** – dáta uložené v databázach, vstupné dáta, výstupné dáta a pod.
  - **ľudia** – užívatelia systému, administrátori, operátori a pod.

- **cena (hodnota)** aktíva
- najcennejšie aktíva - dáta a informácie, ktorých zneužitie, strata alebo modifikácia by organizácii alebo určitej osobe spôsobilo určitú škodu.

Aktívum (II.)

- **klasifikácia v súkromnej sfére (podľa dôvernosti):**
  - Verejné
  - Interné
  - Chránené
  - Prísne chránené

- **kritériá pre určenie celkovej hodnoty aktíva a následnej klasifikácie**
  - Hodnota
  - Vek
  - Náklady na výmenu
  - Úžitková životnosť

Bezpečnostné hrozby (I.)

- čokoľvek (napríklad objekt, materiál, človek) čo je schopné pôsobiť proti aktívu takým spôsobom, že ich môže poškodiť.
- potenciálna príčina nežiaduceho incidentu (ISO/IEC 13335).

- Zdroje:
  - **A (accidental)** - náhodný zdroj - činnosti, ktoré môžu náhodne poškodiť informačné aktíva
  - **D (deliberate)** - úmyselný zdroj - úmyselné akcie zamerané na aktíva
  - **E (environmental)** - environmentálny zdroj

Bezpečnostné hrozby (II.)

Typ	Hrozby	Zdroj
Fyzické poškodenie	Požiar	A,D,E
	Poškodenie vodou	A,D,E
	Znečistenie	A,D,E
	...	
Prírodná udalosť	Klimatický jav	E
	Povodeň	E
	...	
Strata základnej služby	Prerušenie dodávky elektriny	A,D,E
	...	
Ohrozenie informácií	Odposluch	D
	Krádež zariadenia	D
	...	
Neoprávnení činnosti	Neoprávnené použitie zariadenia	D
	Poškodenie dát	D
	...	
Ohrozenie funkčnosti	Chyba v používaní	A
	Nedostatok personálu	A,D,E
	...	

Bezpečnostné hrozby (III.)

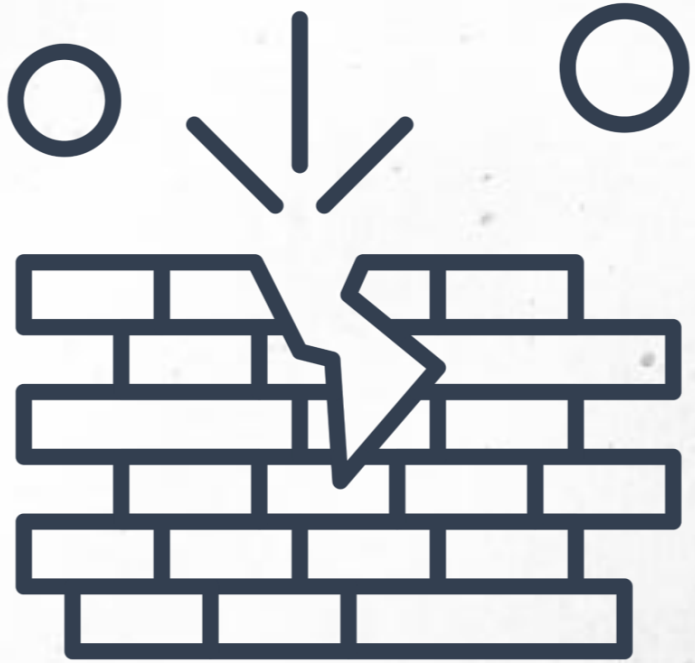
Zdroj: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-list-of-top-15-threats

Zraniteľnosť (I.)

- slabé miesto v oblasti vývoja, implementácie, prevádzky alebo vnútorného riadenia procesu, ktorá vplyvom udalostí hrozieb spôsobí stratu CIA alebo niektorého z aktív

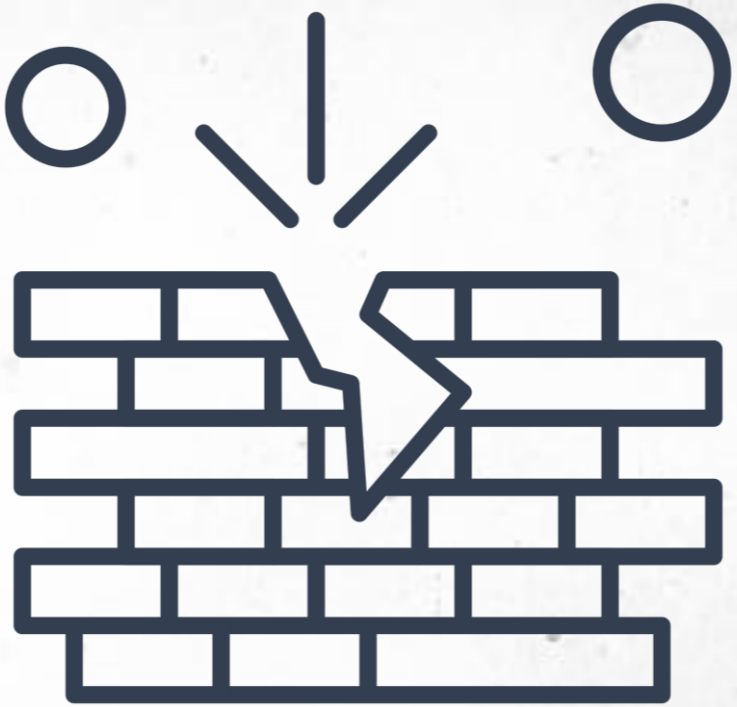
- niečo, čo umožňuje hrozbe prejaviť sa

- priesečník 3 prvkov:
  - slabosť alebo chyba systému,
  - útočníkov prístup k chybe a
  - útočníkova schopnosť zneužiť chybu



Zraniteľnosť (II.)

- podstata zraniteľného miesta môže byť:
  - **fyzická** – napr. umiestnenie informačného systému v mieste, ktoré umožňuje ľahké znehodnocovanie systému, výpadok napätia,
  - **fyzikálna** – vyžarovanie, útoky pri komunikácii na výmenu správy,
  - **v ľudskom faktore** – nesprávne zaškolenie operátorov, nedostatočné skúsenosti administrátorov.



Zraniteľnosť (III.)

Skupina	Príklady zraniteľností	Príklady hrozieb
Hardware	Nedodržanie pravidiel výmeny	Zničenie zariadenia
	Citlivosť na zmenu napätia	Prerušenie dodávky elektriny
	Citlivosť na zmenu teploty	Metorologický jav
	Nechránené uskladnenie	Krádež média alebo dokumentu
Software	Známe chyby v programe	Zneužitie oprávnení
	Žiadne logovanie udalostí	Zneužitie oprávnení
	Zložité používateľské rozhrania	Chyba použitia
	Nedostatočná dokumentácia	Chyba použitia
Siete	Nechránené komunikačné spojenia	Odposluch
	Nedostatočne bezpečná sieťová architektúra	Vzdialená špionáž
	Bod totálneho zlyhania	Zlyhanie komunikačného zariadenia
Zamestnanci	Nedostatočné bezpečnostné školenia	Chyba použitia
	Nedostatok kontrolných mechanizmov	Nezákonné spracovanie dát
	Nedostatočné povedomie o bezpečnosti	Chyba použitia
Lokality	Poloha v záplavovej časti	Povodeň
	Nestabilná elektrická sieť	Prerušenie dodávky elektriny

Zraniteľnosť (IV.)

CVE-2019-0708 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may resu
the information provided.

Current Description

A remote code execution vulnerability exists in Remote Desktop Services formerly known as Terminal Services when
attacker connects to the target system using RDP and sends specially crafted requests, aka 'Remote Desktop Services
Vulnerability'.

Source: MITRE

+View Analysis Description

Impact

CVSS v3.0 Severity and Metrics:

Base Score: 9.8 CRITICAL

Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H (V3.0 legend)

Impact Score: 5.9

Exploitability Score: 3.9

CVSS v2.0 Severity and Metrics:

Base Score: 10.0 HIGH

Vector: (AV:N/AC:L/Au:N/C:C/I:C/A:C) (V2 legend)

Impact Subscore: 10.0

Exploitability Subscore: 10.0

Zdroj: https://nvd.nist.gov/vuln/detail/CVE-2019-0708

Útok (I.)

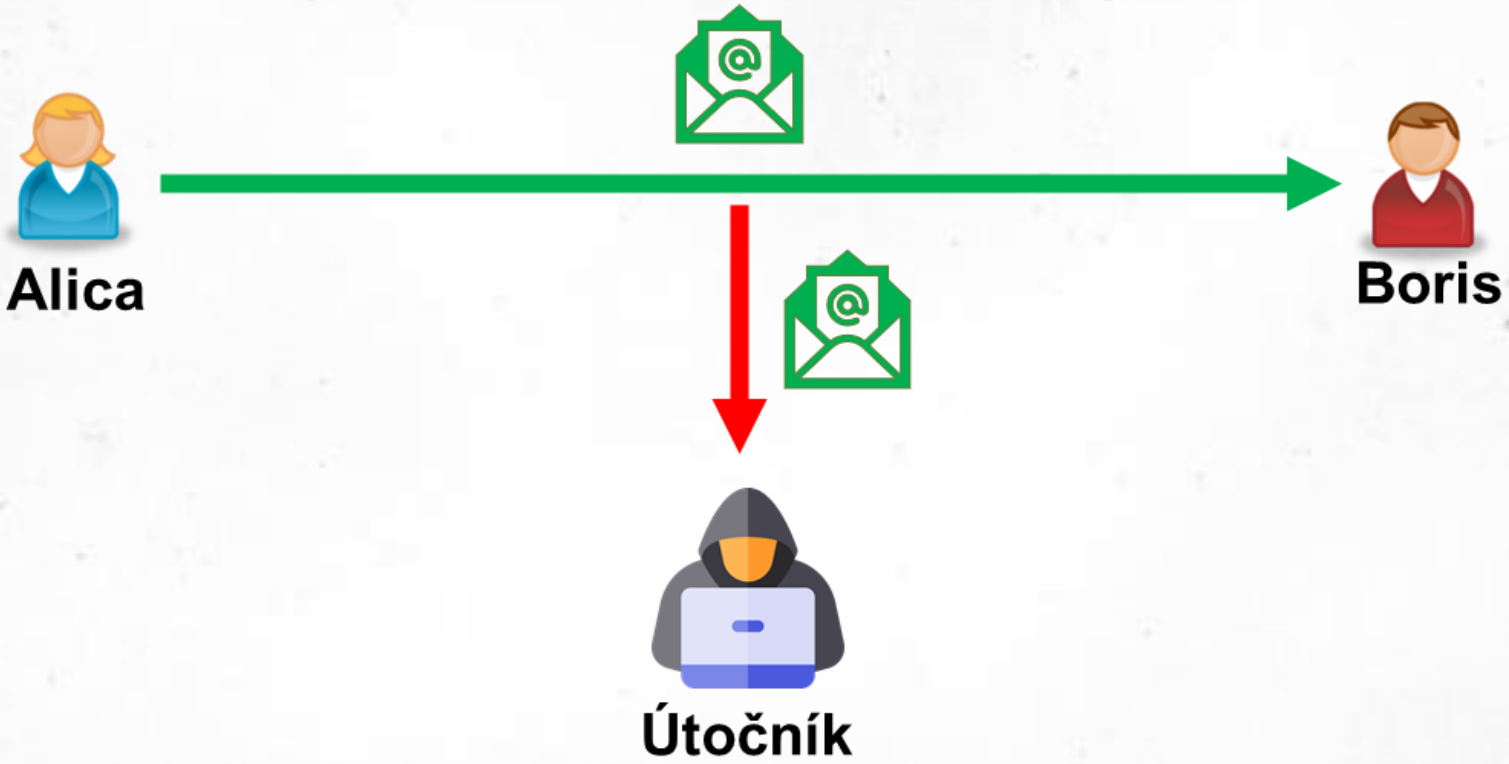
- pokus o zničenie, vystavenie hrozbe, zmenu, vyradenie z činnosti, odcudzeniu aktíva alebo získanie neoprávneného prístupu k aktívu alebo uskutočnenie neoprávneného použitia aktíva (ISO/IEC 27000: 2018)

- činnosti:
  - odpočúvanie (interception),
  - prerušenie (interruption),
  - modifikácia/úprava (modification)
  - výroba (fabrication)

C	**Odpočúvanie**
I	**Prerušenie** **Modifikácia** **Výroba**
A	**Prerušenie** **Modifikácia** **Výroba**

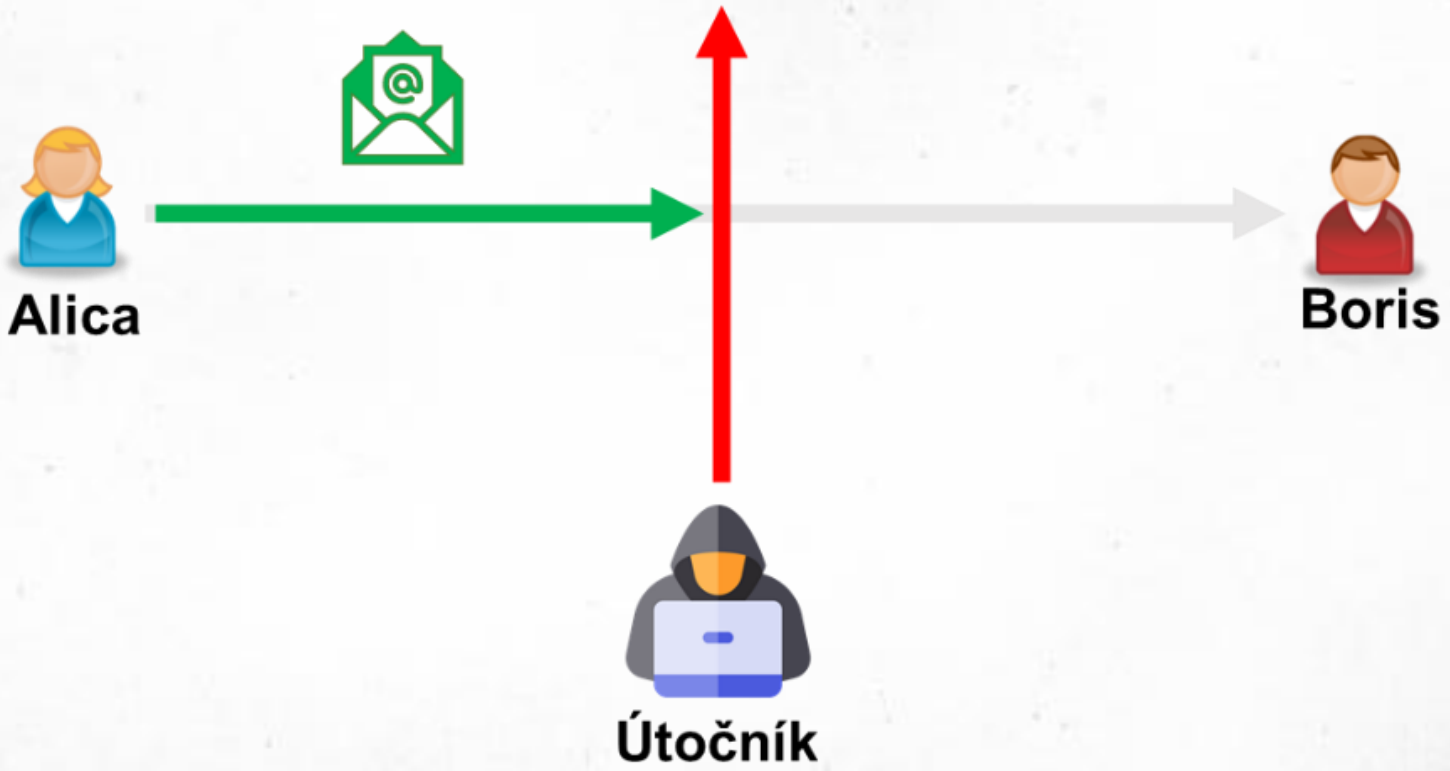
Útok (II.)

- odpočúvanie (interception)



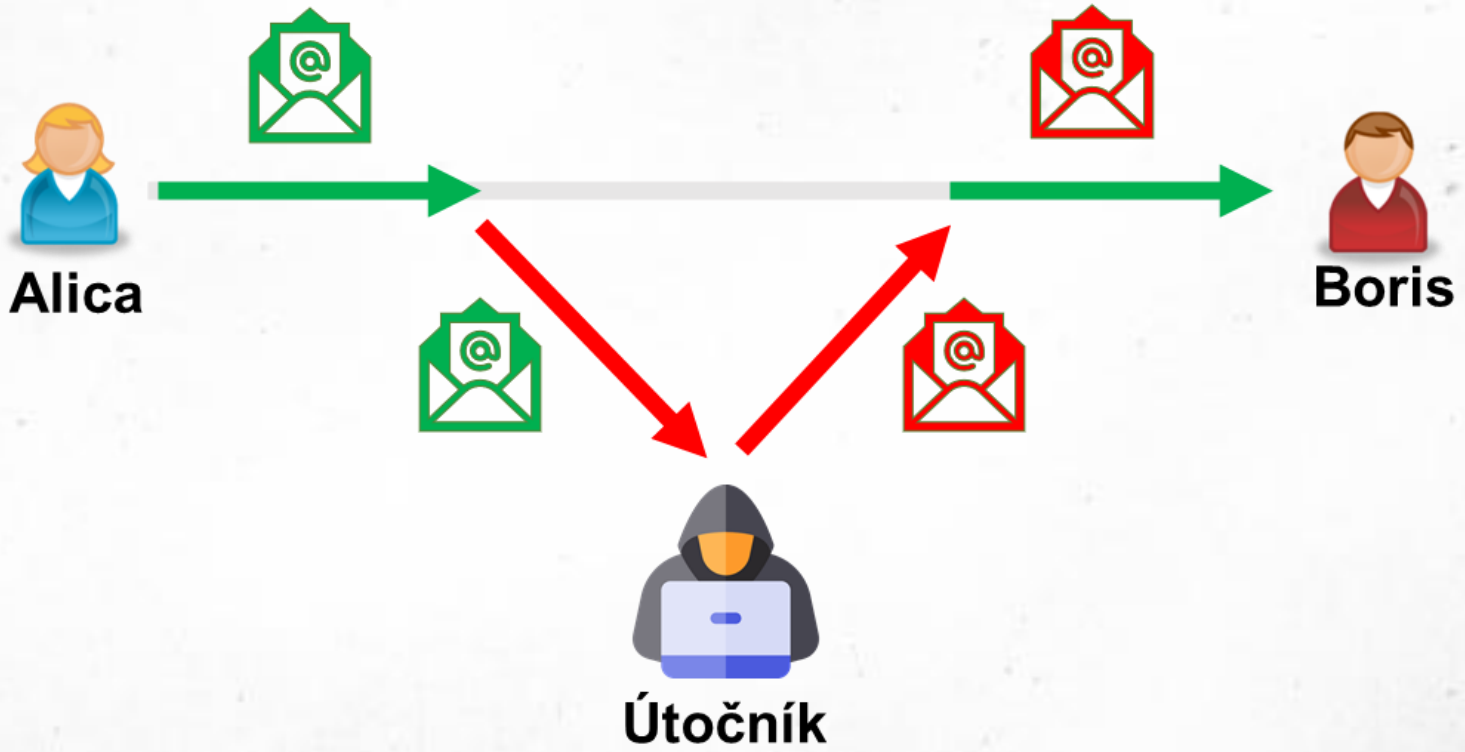
Útok (III.)

- prerušenie (interruption)



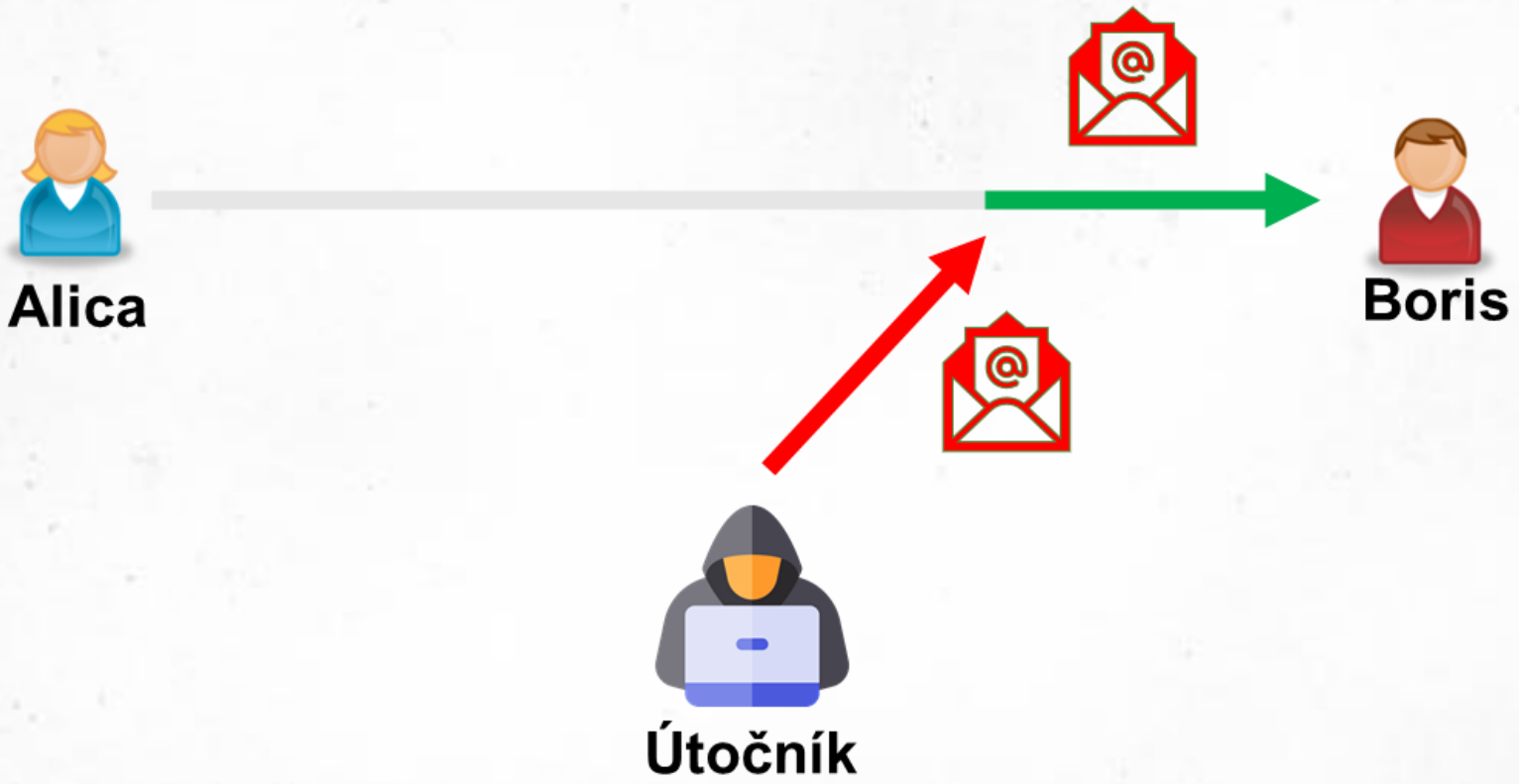
Útok (IV.)

- úprava (modification):
  - zmena – dochádza k zmene už existujúcich informácií
  - vloženie - pridanie informácií, ktoré predtým
  - vymazanie - odstránenie existujúcich informácií

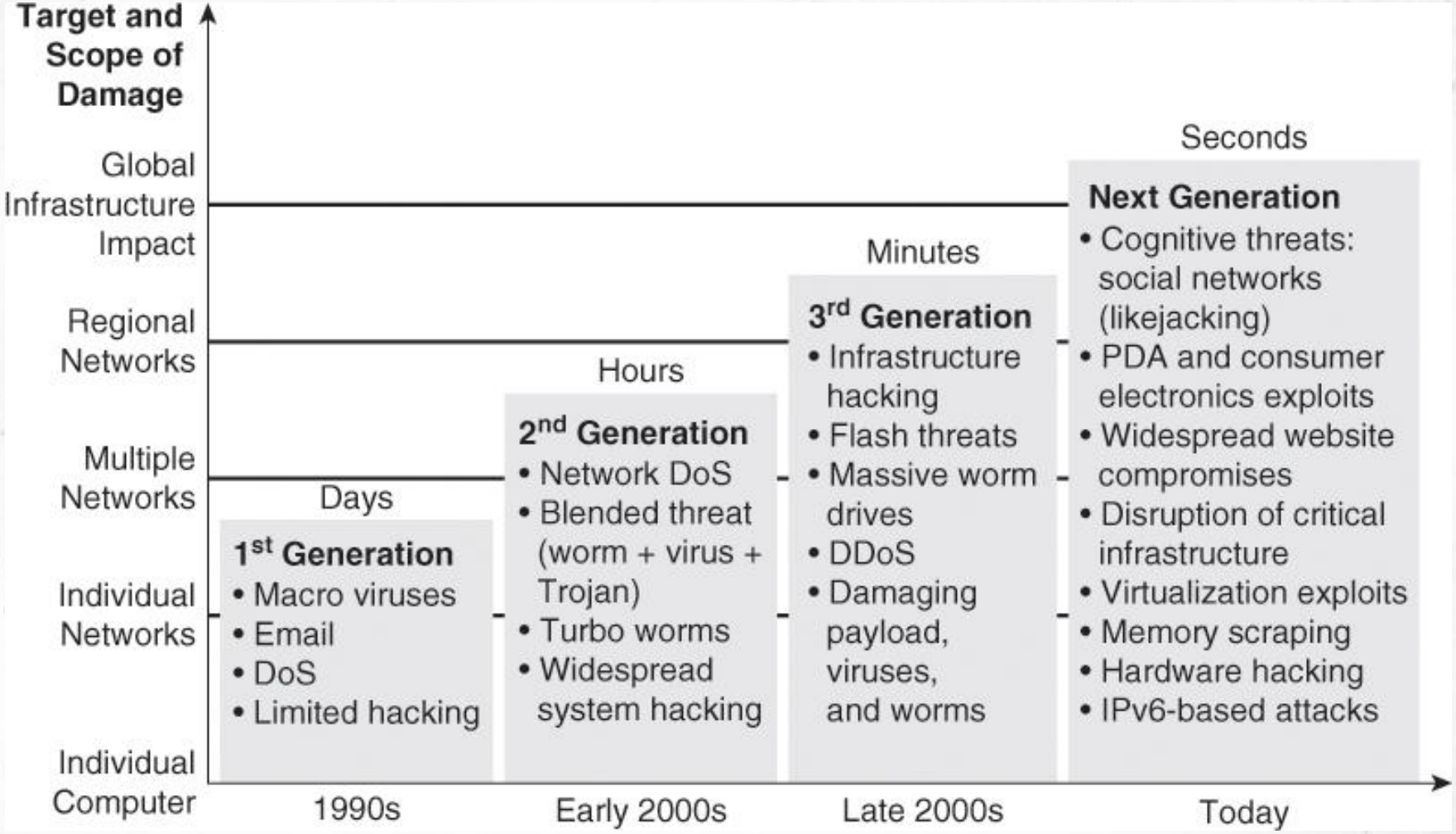


Útok (V.)

- výroba (fabrication)

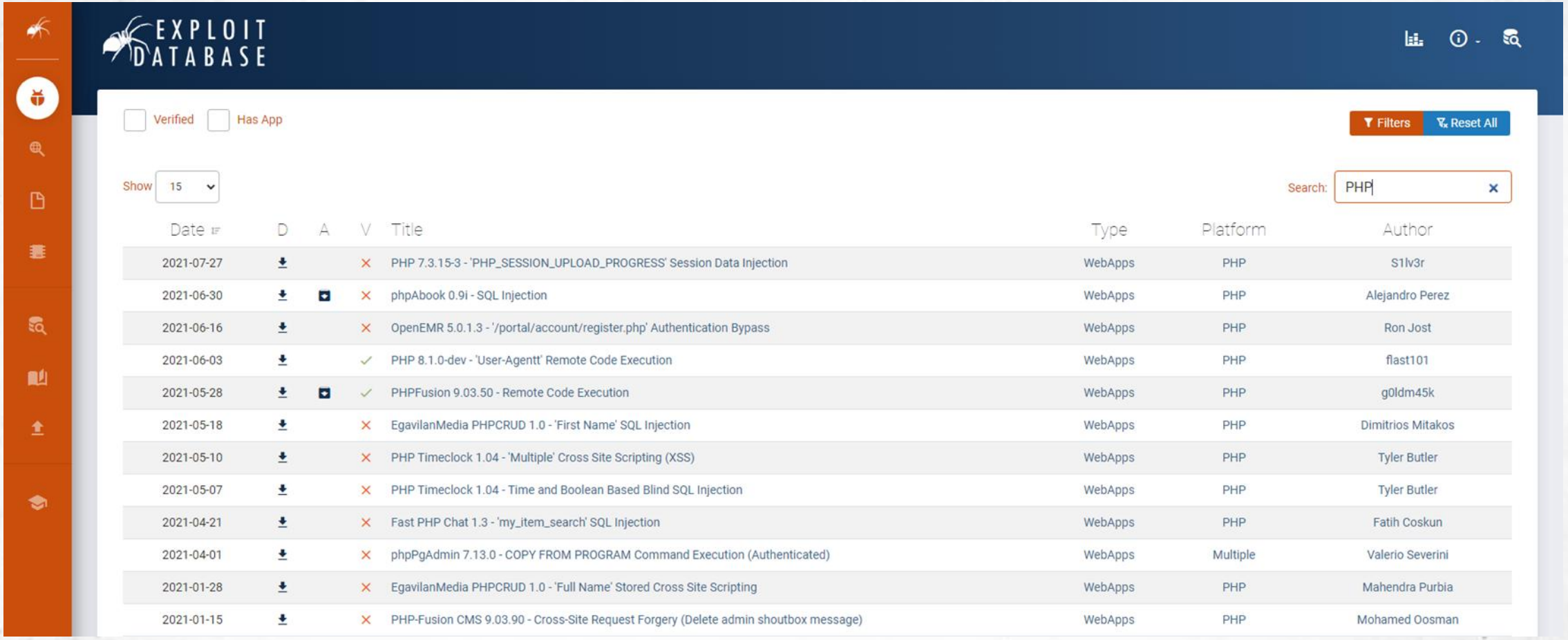


Útok (VI.)



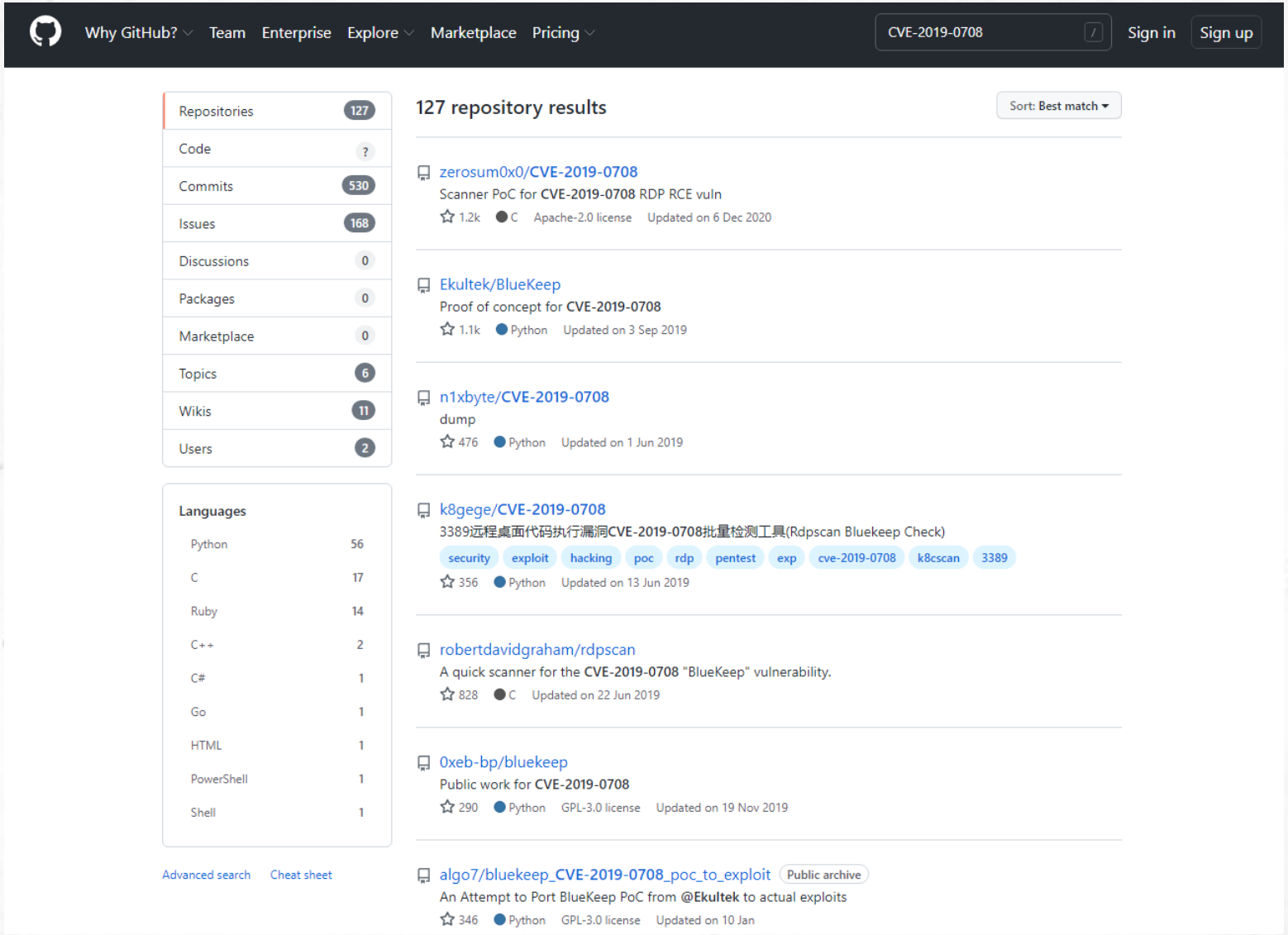
Zdroj: http://www.ciscopress.com/articles/article.asp?p=1998559

Útok (VII.)



Zdroj: https://www.exploit-db.com/

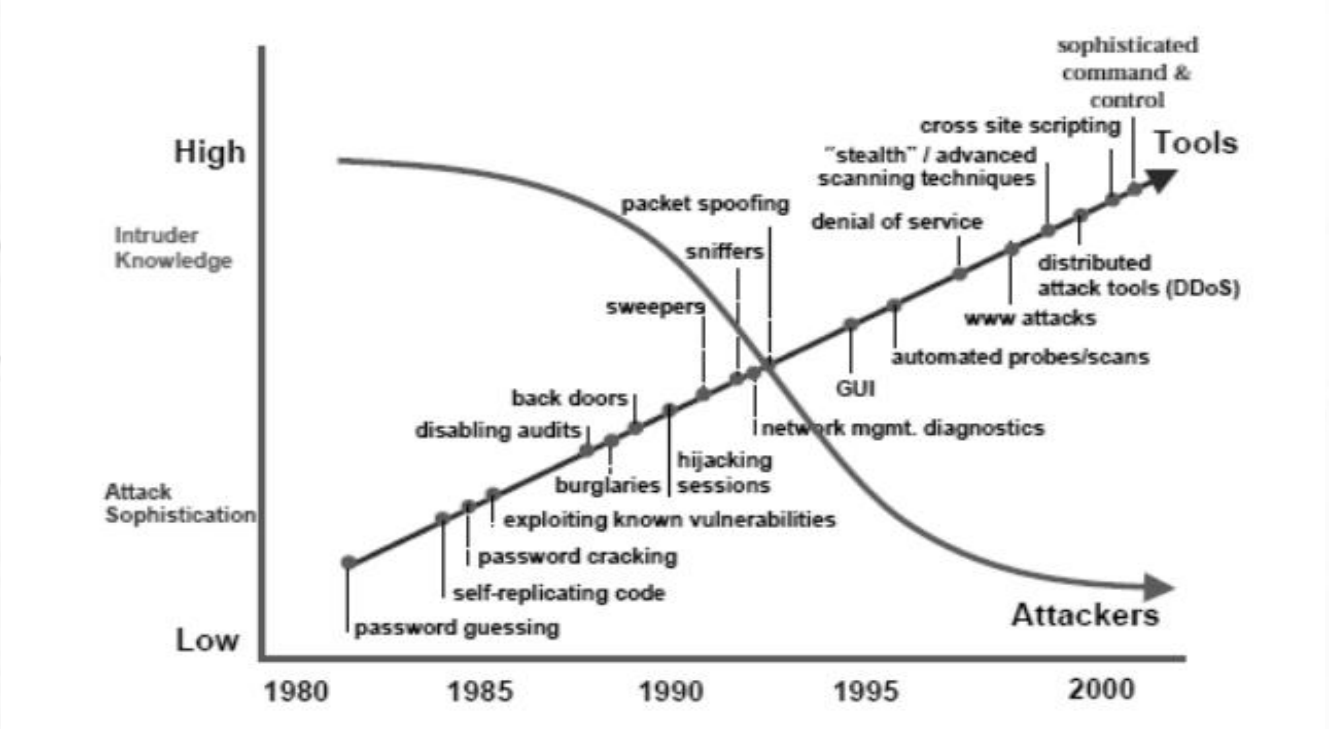
Útok (VIII.)



Zdroj: https://github.com/

Útočník (I.)

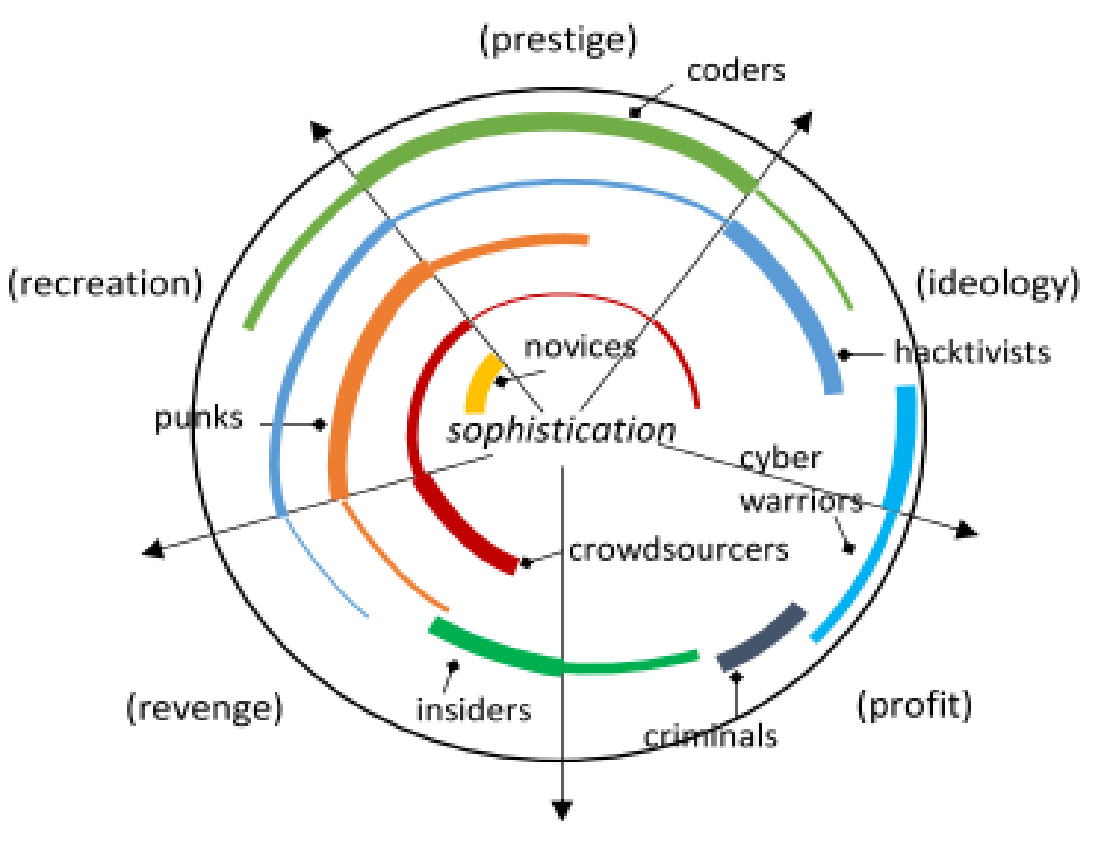
- jednotlivec, skupina, organizácia alebo vláda, ktorá vedie alebo má v úmysle vykonávať škodlivé činnosti (SP 800-30).



Zdroj: MEYERS, Carol; POWERS, Sarah; FAISSOL, Daniel. Taxonomies of cyber adversaries and attacks: a survey of incidents and approaches. Lawrence Livermore National Laboratory (April 2009), 2009, 7: 1-22,

Útočník (II.)

- motív pochádza z predtuchy, že systém, na ktorý sa útočník zameriava, uchováva alebo spracováva niečo cenné; to signalizuje, že systém môže byť ohrozený útokom
- Motív útokov (útočníkov):
  - narušenie obchodnej činnosti
  - krádež informácií a manipulácia s údajmi
  - vytváranie strachu a chaosu
  - šírenie náboženského alebo politického presvedčenia
  - poškodenie dobrého mena
  - pomsta
  - požadovanie výkupného



Zdroj: SEEBRUCK, Ryan. A typology of hackers: Classifying cyber malfeasance using a weighted arc circumplex model. Digital Investigation, 2015, 14: 36-45.

Útočník (III.)

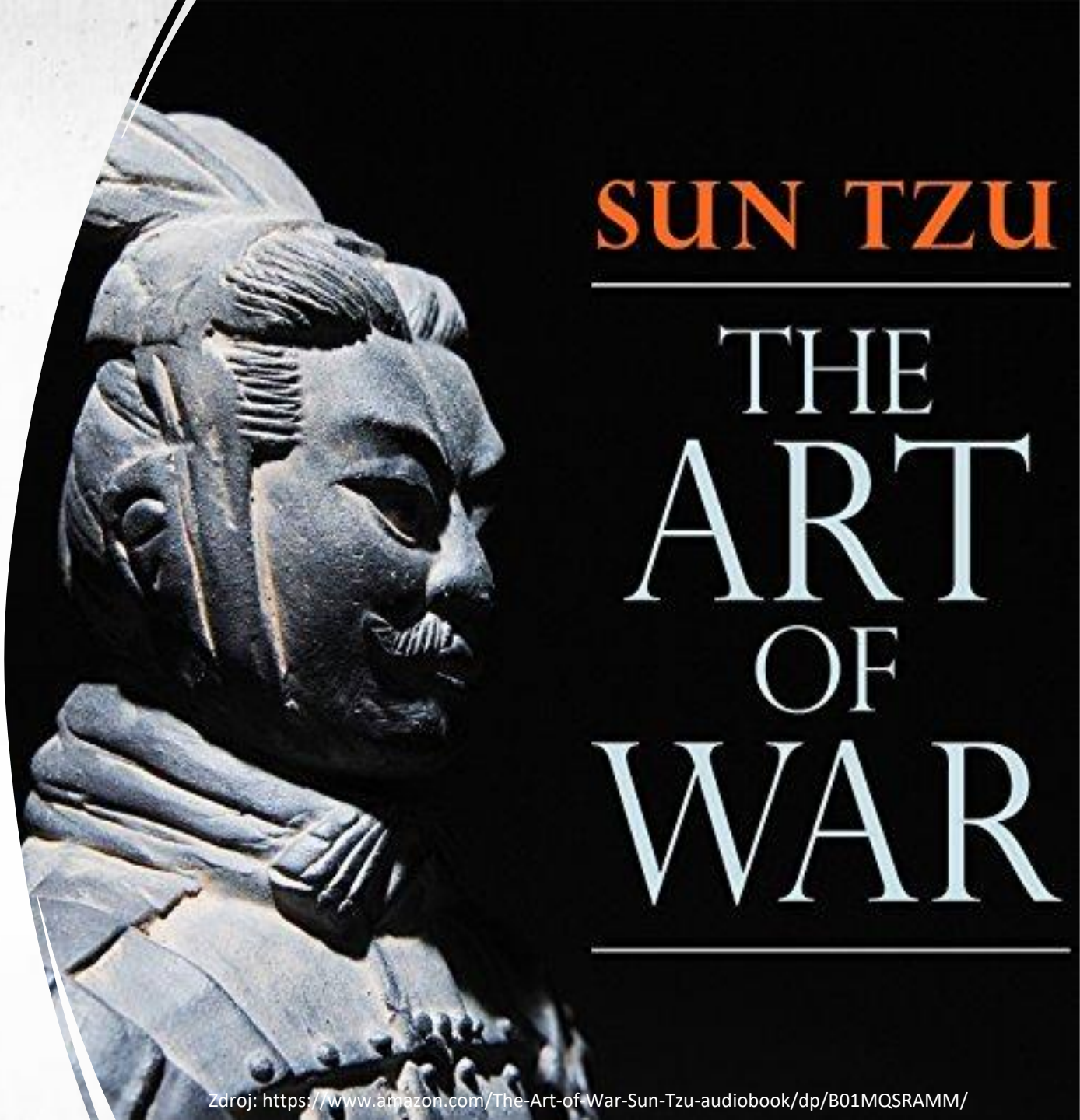
- **Script Kiddies** - nekvalifikovaný heker, ktorý kompromituje systém spustením skriptov, nástrojov a softvéru vyvinutého skutočnými hackermi
- **Organizovaní hackeri** - profesionálni hackeri, ktorí sa snažia zaútočiť na systém so ziskom
- **Hacktivisti** - jednotlivci, ktorí hackovaním propagujú politickú agendu, najmä poškodzovaním alebo deaktivovaním webových stránok
- **Útočníci sponzorovaní štátom** - jednotlivci zamestnaní vládou, aby prenikli a získali prísne tajné informácie alebo poškodili informačné systémy iných vlád
- **Insider Threat** - hrozba pochádzajúca od ľudí v organizácii, môžu to byť nespokojní zamestnanci, prepustení zamestnanci a nedostatočne školení zamestnanci

„Ak poznáš nepriateľa i seba samého, nebudeš porazený.

Ak nepoznáš nepriateľa, ale poznáš sám seba, máš 50% šancu na víťazstvo.

Ak nepoznáš sám seba, ani nepriateľa, prehráš.“

- Sun Tzu



Zdroj: https://www.amazon.com/The-Art-of-War-Sun-Tzu-audiobook/dp/B01MQSRAMM/

Zdroj: https://teachprivacy.com/the-funniest-hacker-stock-photos-5-0/

Zdroj: https://teachprivacy.com/the-funniest-hacker-stock-photos-5-0/

Zdroj: https://ciso.economictimes.indiatimes.com/news/ciso-strategies/ode-to-kevin-mitnick-a-legacy-of-cybersecurity-brilliance/102008065

WANTED
BY U.S. MARSHALS

NOTICE TO ARRESTING AGENCY: Before arrest, validate warrant through National Crime Information Center (NCIC).

United States Marshals Service NCIC entry number: (NIC/ W721460021).

NAME: .....MITNICK, KEVIN DAVID

AKS (S): .....MITNIK, KEVIN DAVID
MERRILL, BRIAN ALLEN

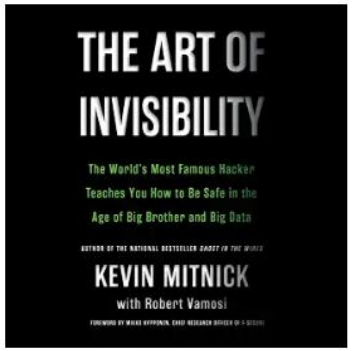
DESCRIPTION:

Sex: .....MALE
Race: .....WHITE
Place of Birth: .....VAN NUYS, CALIFORNIA
Date(s) of Birth: 08/06/63; 10/18/70
Height: .....5'11"
Weight: 190
Eyes: .....BLUE
Hair: .....BROWN
Skintone: .....LIGHT
Scars, Marks, Tattoos: .....NONE KNOWN

Showing results for *kevin mitnick*

Search instead for kevin metnick

Best Seller



The Art of Invisibility: The World's Most Famous Hacker Teaches You How Brother and Big Data

by Kevin Mitnick, Ray Porter, et al.

4.5 out of 5 stars ~ 163

Audible Audiobook

$0.00 ~~$35.58~~

Free with Audible trial

Paperback

$13.41 ~~$17.99~~

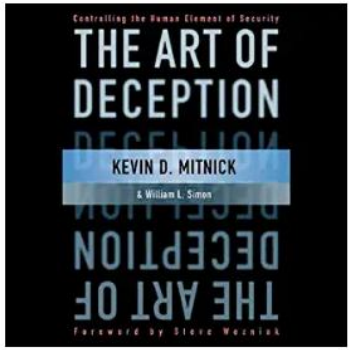
More Buying Choices

$11.96 (43 used & new offers)

Kindle

$10.98 ~~$28.00~~

Other formats: Hardcover , Mass Market Paperback , Audio CD



The Art of Deception: Controlling the Human Element of Security

by Kevin Mitnick, Nick Sullivan, et al.

4 out of 5 stars ~ 207

Audible Audiobook

$0.00 ~~$24.86~~

Free with Audible trial

Paperback

$12.47 ~~$16.95~~

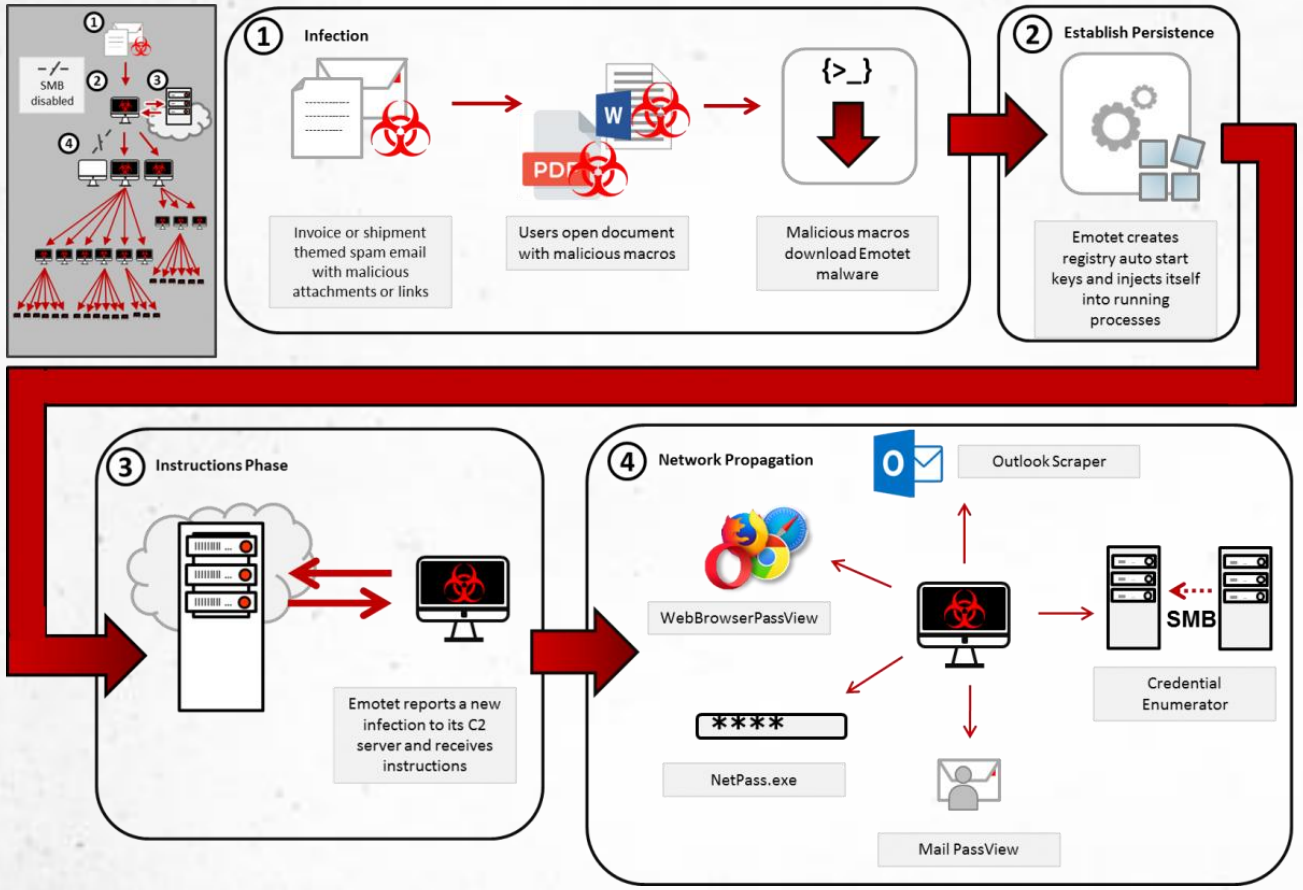
More Buying Choices

$1.94 (160 used & new offers)

Zdroj: https://cyber.tap.purdue.edu/blog/articles/kevin-mitnick-sound-familiar/

Emotet (I.)

- modus operandi



Media & Press

NEWS

World's most dangerous malware EMOTET disrupted through global action

27 JAN 2021

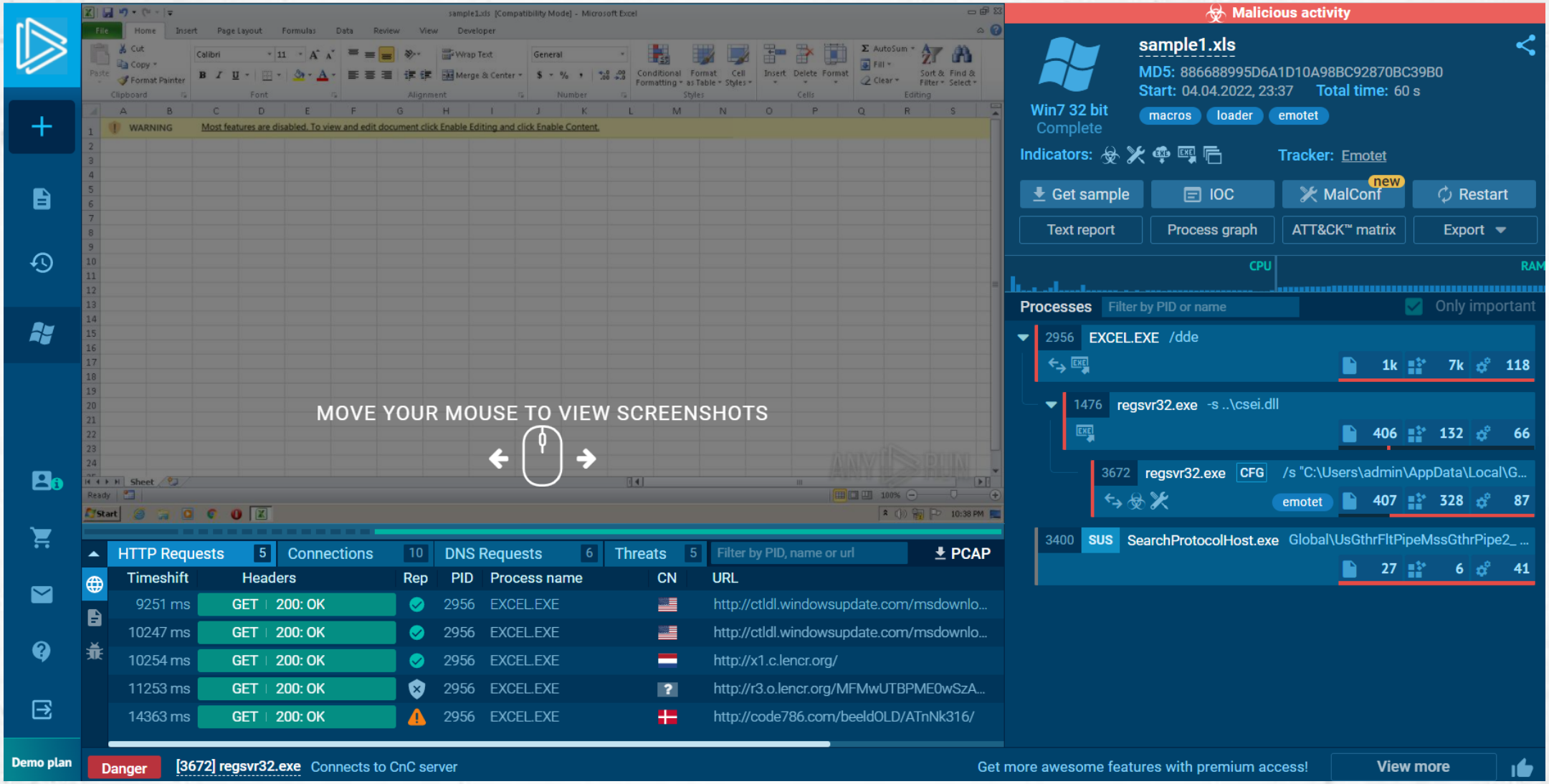
Law enforcement and judicial authorities worldwide have this week disrupted one of most significant botnets of the past decade: EMOTET. Investigators have now taken control of its infrastructure in an international coordinated action.

This operation is the result of a collaborative effort between authorities in the Netherlands, Germany, the United States, the United Kingdom, France, Lithuania, Canada and Ukraine, with international activity coordinated by Europol and Eurojust. This operation was carried out in the framework of the European Multidisciplinary Platform Against

EUROPOL

Zdroj: https://www.europol.europa.eu/media-press/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action, https://www.cisecurity.org/

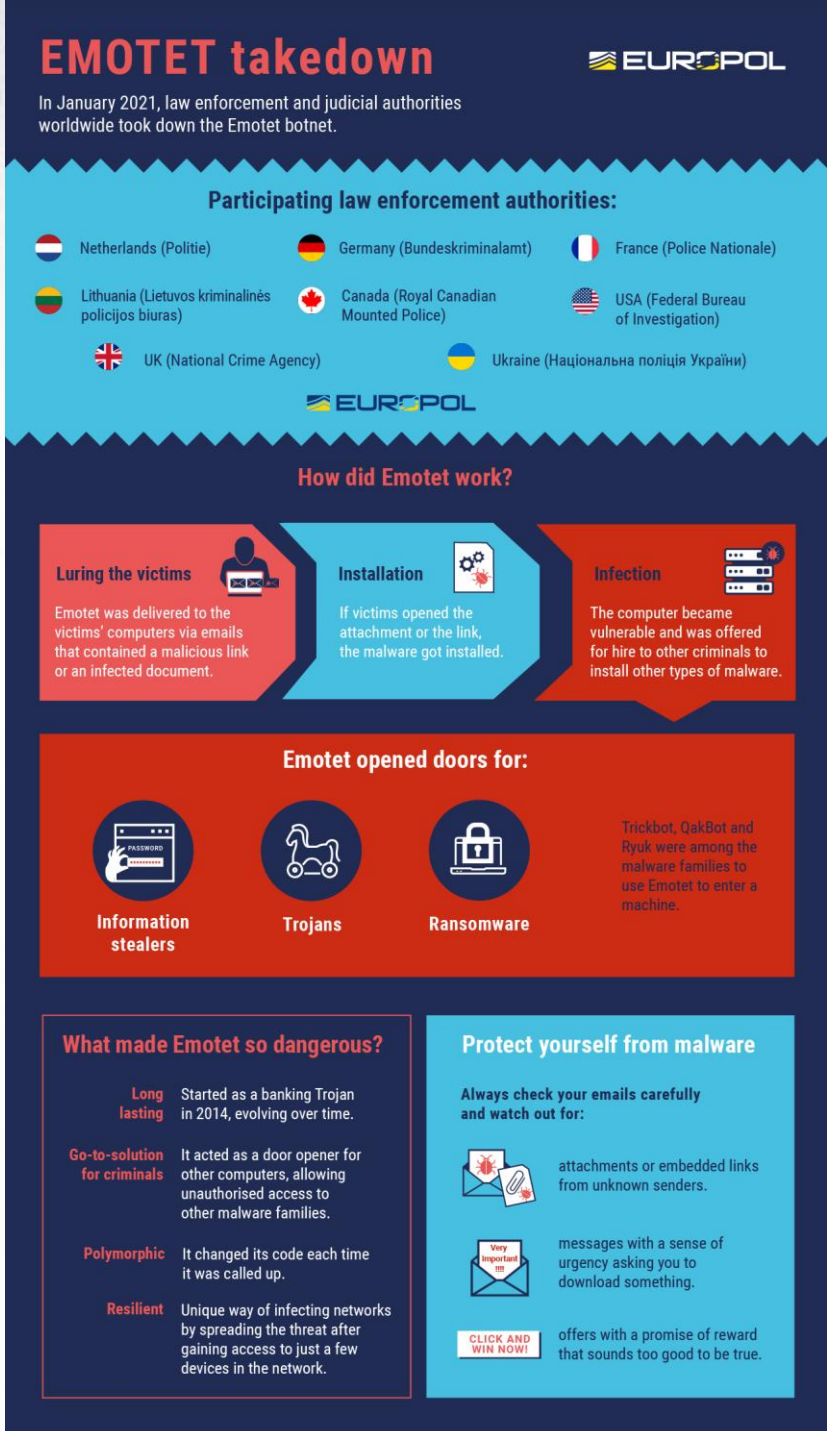
Emotet (II.)



Zdroj: https://app.any.run/tasks/093af2d6-3f5e-400d-9dcc-de2706a140ed/

Emotet (III.)

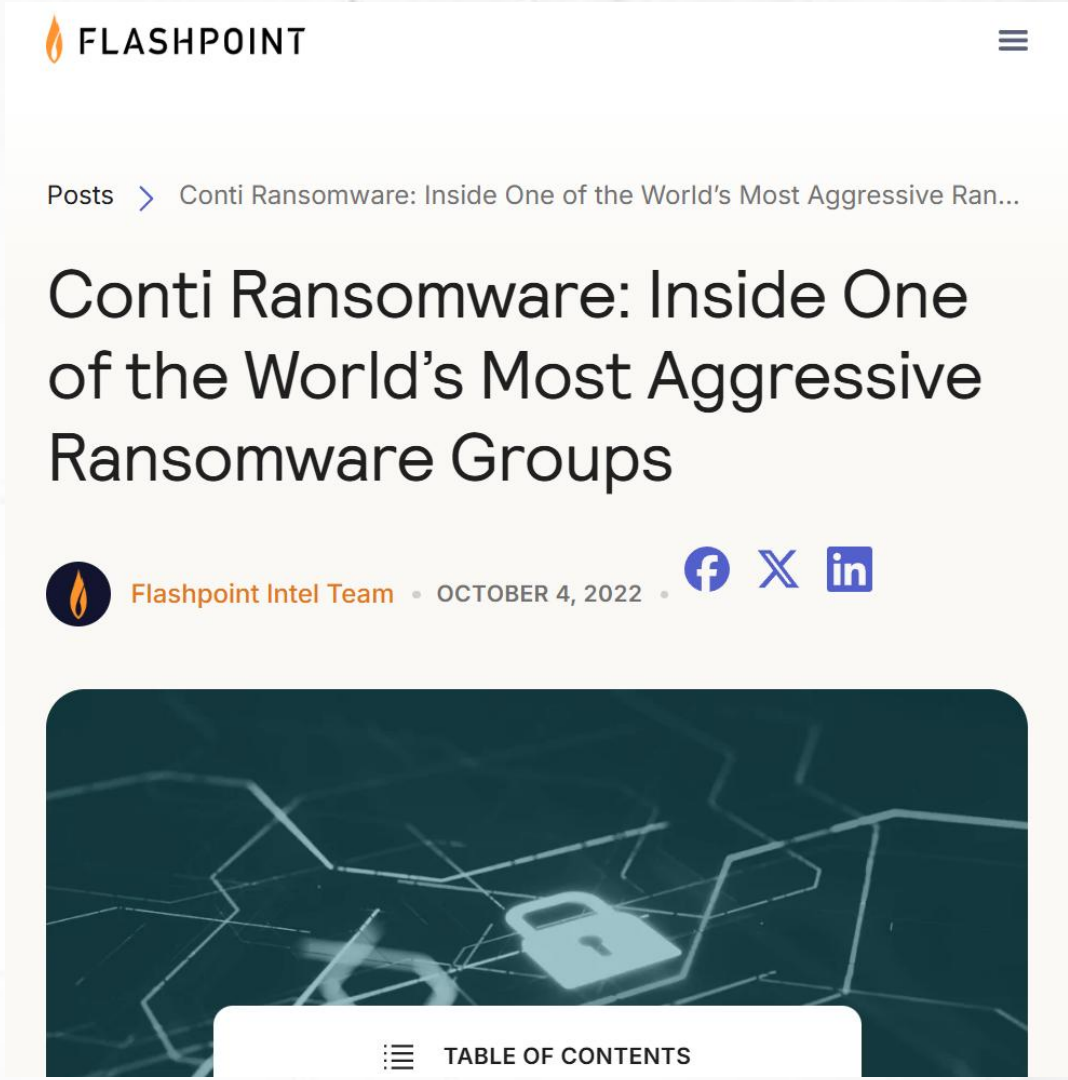
Medzinárodný policajný tím rozvrátil notoricky známy botnet Emotet



Zdroj: https://www.europol.europa.eu/media-press/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-d

Conti (I.)

- 1 z najväčších skupín
- únik údajov – nástroje, postupy, komunikácia



Zdroj: https://flashpoint.io/blog/history-of-conti-ransomware/

Conti (II.)

SIEŤOVÁ INFRAŠTRUKTÚRA

Takmer každú modernú sieť je možné hacknúť.

Dôvody sú nasledovné:

- **Nadbytočnosť sietí** – veľké množstvo služieb a rôzne vstupné body do tej istej siete.
- **Priorita pohodlia pred bezpečnosťou** – väznica je bezpečná, ale veľmi neefektívna na vykonávanie činností.
- **Ľudský faktor** – chyby v konfigurácii, sociálne inžinierstvo.

Conti (III.)

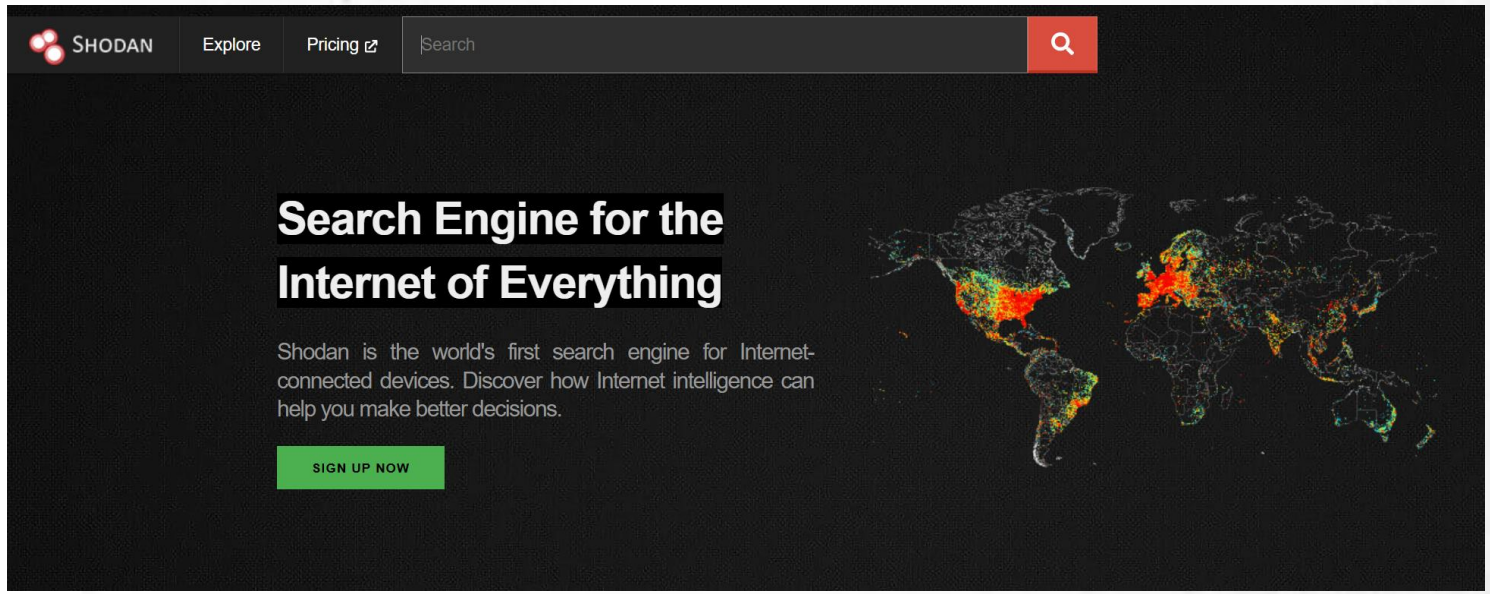
PRIESKUM A VÝBER CIEĽA

Ak nemáte konkrétny cieľ a disponujete exploitom, môžete skenovať sieť (celý internet alebo vybrané rozsahy IP adries) s cieľom nájsť zraniteľné služby.

Ak chcete ušetriť čas, použite známe služby ako Shodan.io, ale lepšie je mať vlastný skener.

Pri cielenom útoku je nevyhnutný prieskum:

1. Začnite analýzou domény
2. Veľké korporácie majú vlastné autonómne systémy (AS), ...
3. Použite OSINT nástroje na **získanie údajov o cieľovej organizácii a jej zamestnancoch.**



Zdroj: https://www.shodan.io/

Conti (IV.)

NÁSTROJE OSINT

Vyhľadávače informácií:

- theHarvester – zber emailov, subdomén, otvorených portov
- SpiderFoot – OSINT analýza
- hunter.io – zbiera emaily podľa domény

Vyhľadávanie firiem:

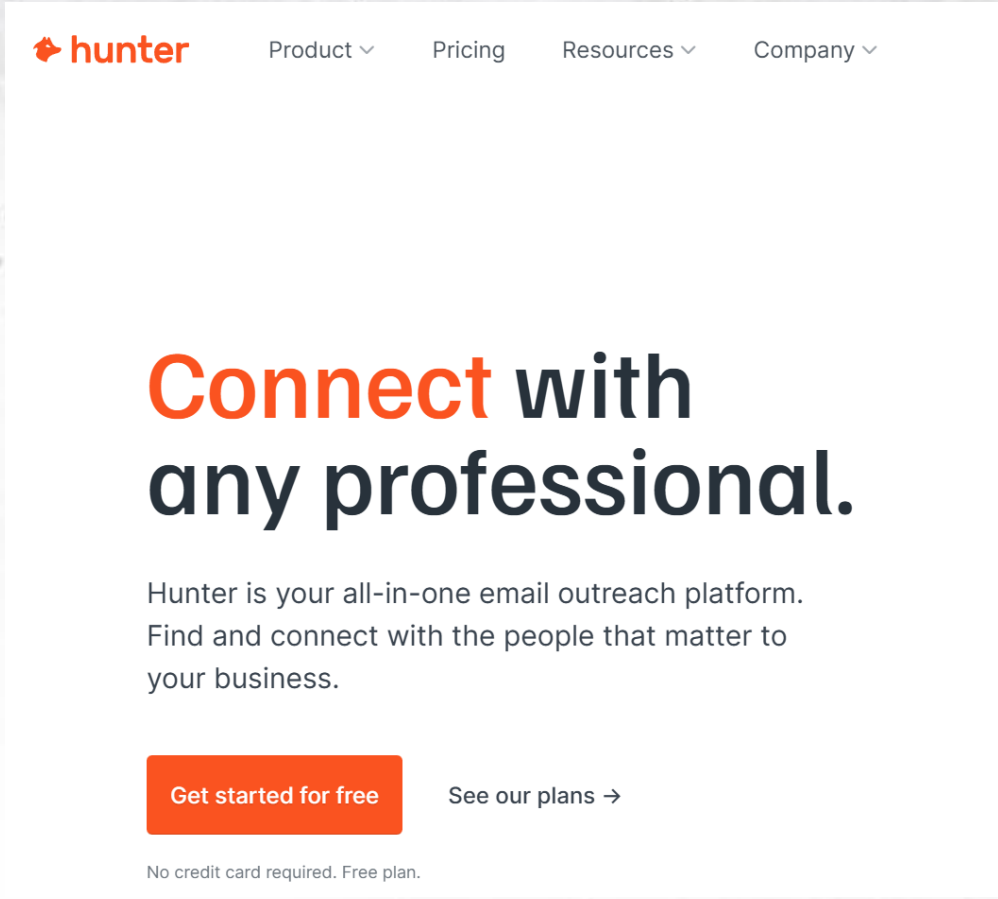
- ZoomInfo – firemné dáta
- OpenCorporates – databáza firiem

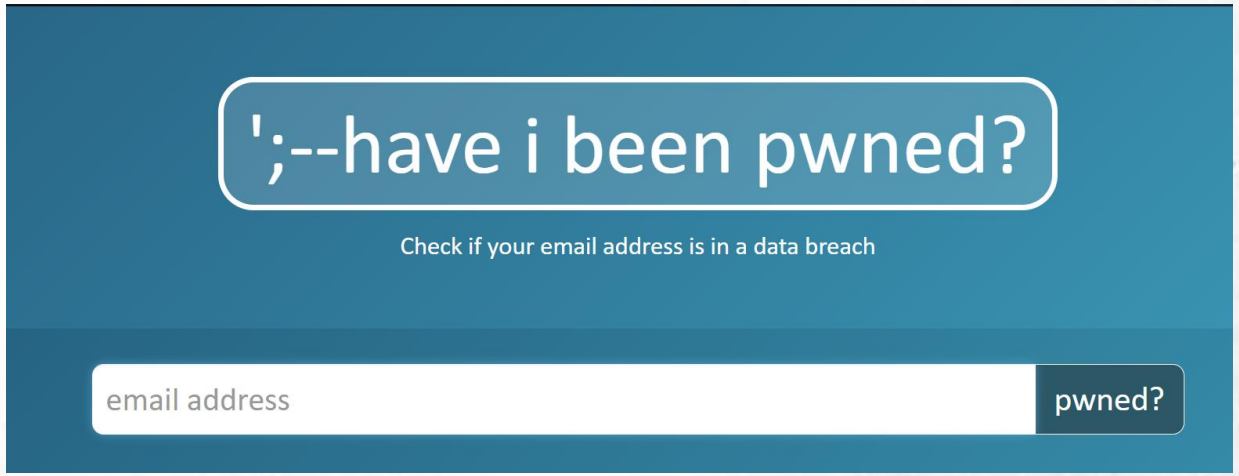
Vyhľadávanie používateľských mien:

- Namechk

Vyhľadávanie emailov:

- Have I Been Pwned





Zdroj: https://hunter.io/
https://haveibeenpwned.com/

Conti (V.)

Dátum: 2021-03-15T16:09:16.675Z
Od: Kalinka
Správa: Chlapi, viete mi povedať, ako vypnúť ESET File Security?

Dátum: 2021-03-15T15:14:23.771Z
Od: t3chnolog
Správa: dtssync je mizerná voľba v každom prípade)

Dátum: 2021-03-15T15:14:07.896Z
Od: Rosette
Správa: Zhromažďuje Sophos Windows logy? Je to len proti malvéru?

Dátum: 2021-03-15T15:13:30.907Z
Od: Slice
Správa: Ako nenápadná je možnosť vykonať DCSync na konkrétnych používateľoch, ak je na DC Sophos?

Dátum: 2021-03-15T14:39:56.903Z
Od: Andy
Správa: Jasné, vďaka, teraz to skúsim

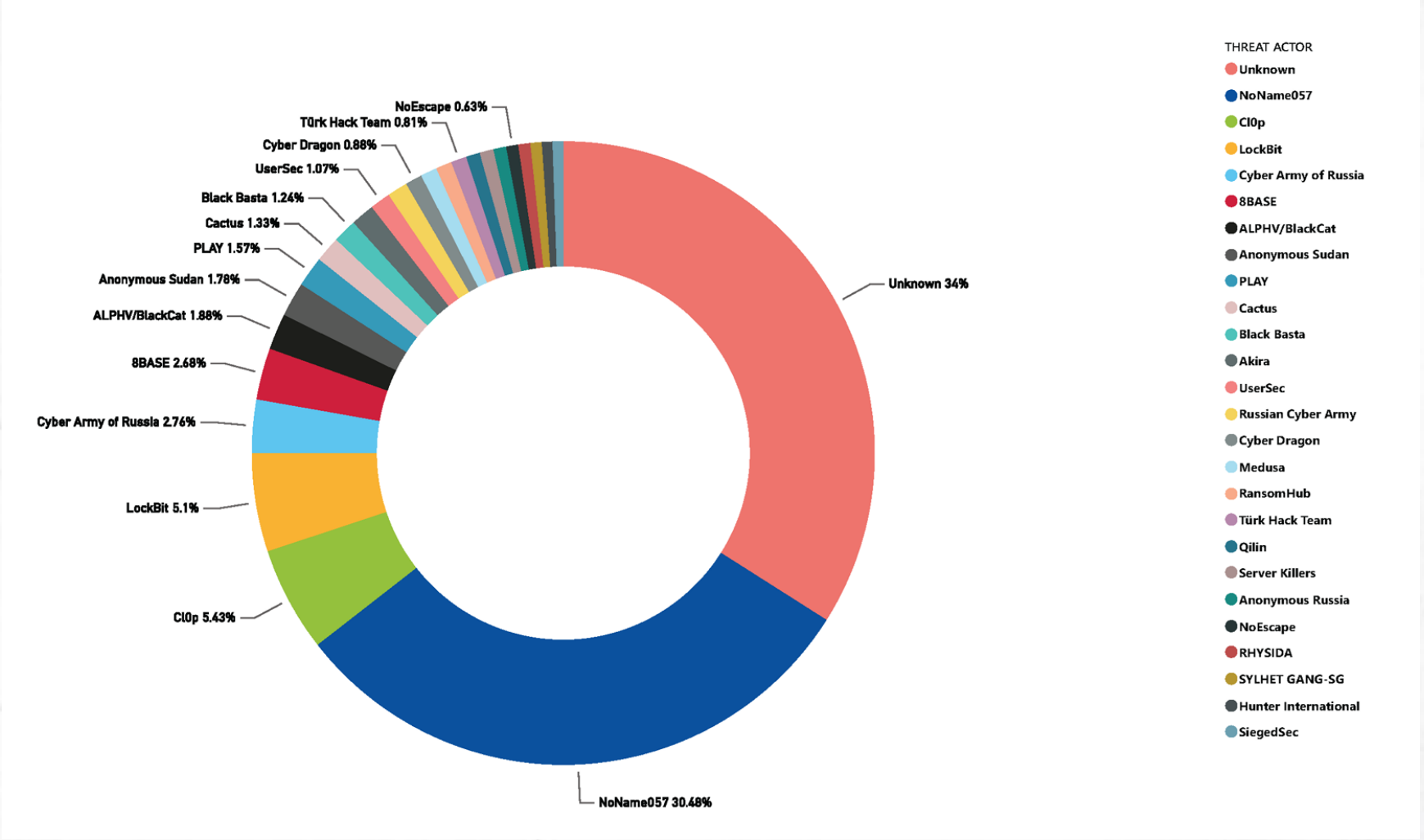
Conti (VI.)

Dátum: 2021-06-28T11:08:00.394568
Od: mango@q3.onion
Komu: stern@q3.onion
Správa:
Vyvinuli sme jednoduchší koncept analýzy dát a volaní\ vydierania. Navrhol som nasledovnú schému:
Máme samostatnú prieskumnú raketovú spoločnosť. Prenesieme ju na analytikov, ktorí vypracujú správu o spise. Ak sú potrebné vydierania\volania, túto úlohu pridelíme volajúcim. Aby volajúci pracovali efektívne a **nevolali len do prázdna, ako sa to deje teraz**, sú v kontakte s analytikmi a môžu si **od nich vyžiadať akékoľvek dodatočné údaje**,
povedzme časť zoznamu dátumov alebo nejaké informácie o počítačoch\heslách.

Ak **spoločnosť neodpovie, jej údaje sa odovzdajú na zverejnenie na stránke** (na to je potrebné pridať do tohto chatu buď manažéra, alebo niekoho z jeho podporného tímu).

Aktuálne štatistiky o skupinách (I.)

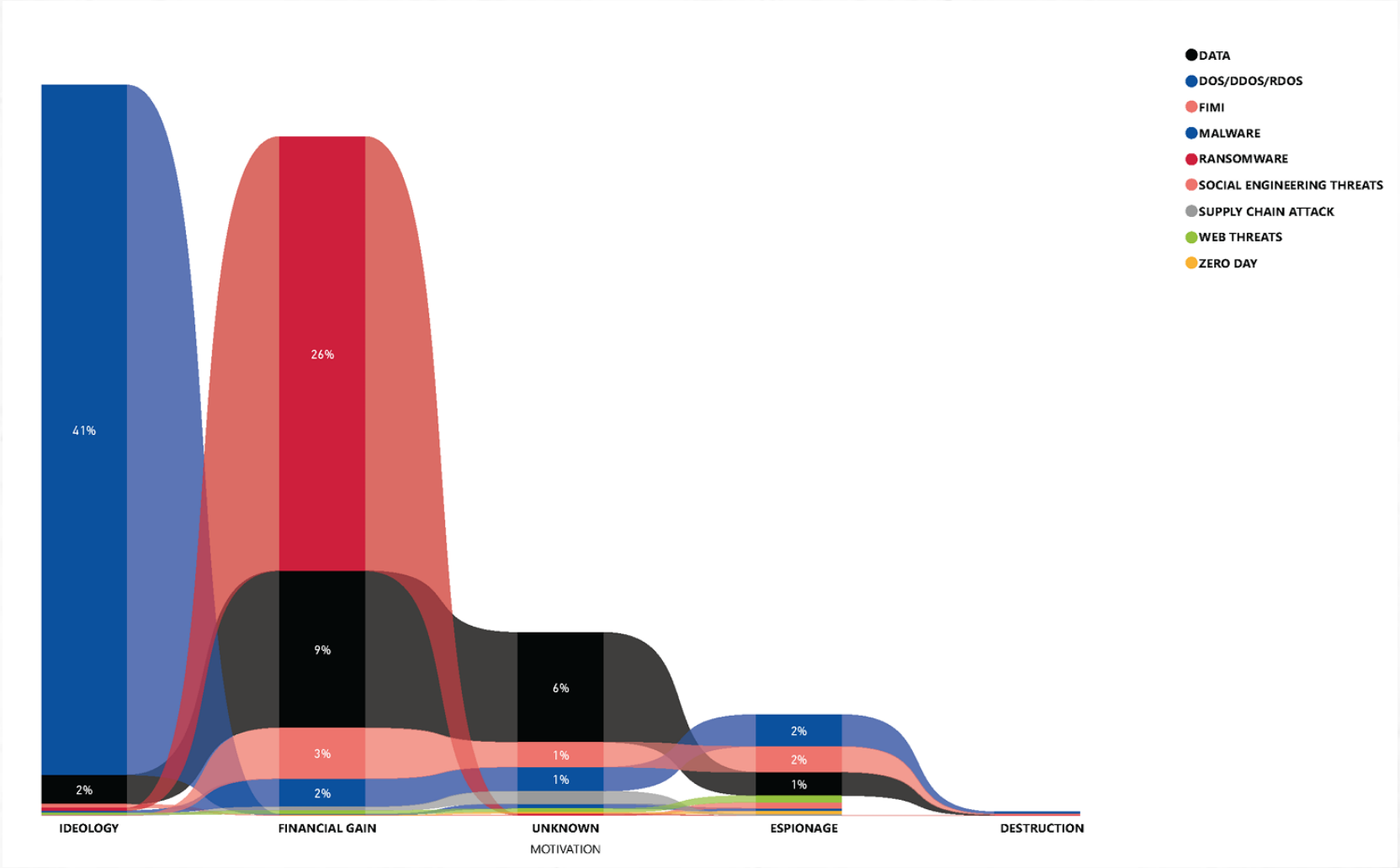
- skupiny útočníkov, júl 2023 – jún 2024



Zdroj: ENISA Landscape 2024, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

Aktuálne štatistiky o skupinách (II.)

- motivácia útočníkov, júl 2023 – jún 2024



Zdroj: ENISA Landscape 2024, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

Riziko (I.)

- úroveň vplyvu na organizačné operácie (vrátane cieľov, funkcie, alebo povesti), organizačné aktíva alebo jednotlivcov vyplývajúce z prevádzkovania informačného systému so zreteľom na potenciálny dopad hrozby a pravdepodobnosť, že sa táto hrozba vyskytne (FIPS 200).

- KB a IB založená na analýze rizík

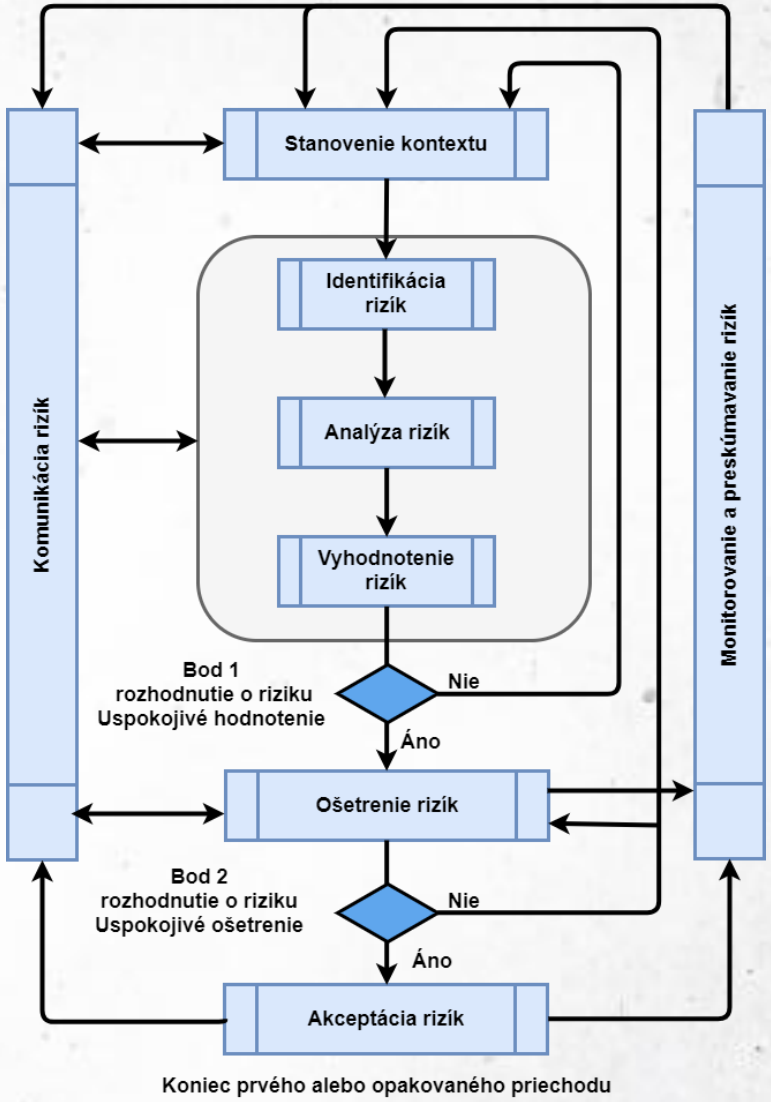
- denno-denná analýza rizík

Zdroj: http://www.securityinfowatch.com/blog/11288612/vidsys-2013-national-security-survey-shows-risk-becoming-a-bigger-priority-for-c-level-executives

Riziko (II.)

- metodika analýzy rizík kybernetickej bezpečnosti pre uplatnenie v procesoch riadenia rizika v zmysle požiadaviek zákona č. 69/2018 Z.´z. o kybernetickej bezpečnosti

- ISO/IEC 27005:2022 Informačné technológie – Bezpečnostné metódy – Riadenie rizík informačnej bezpečnosti

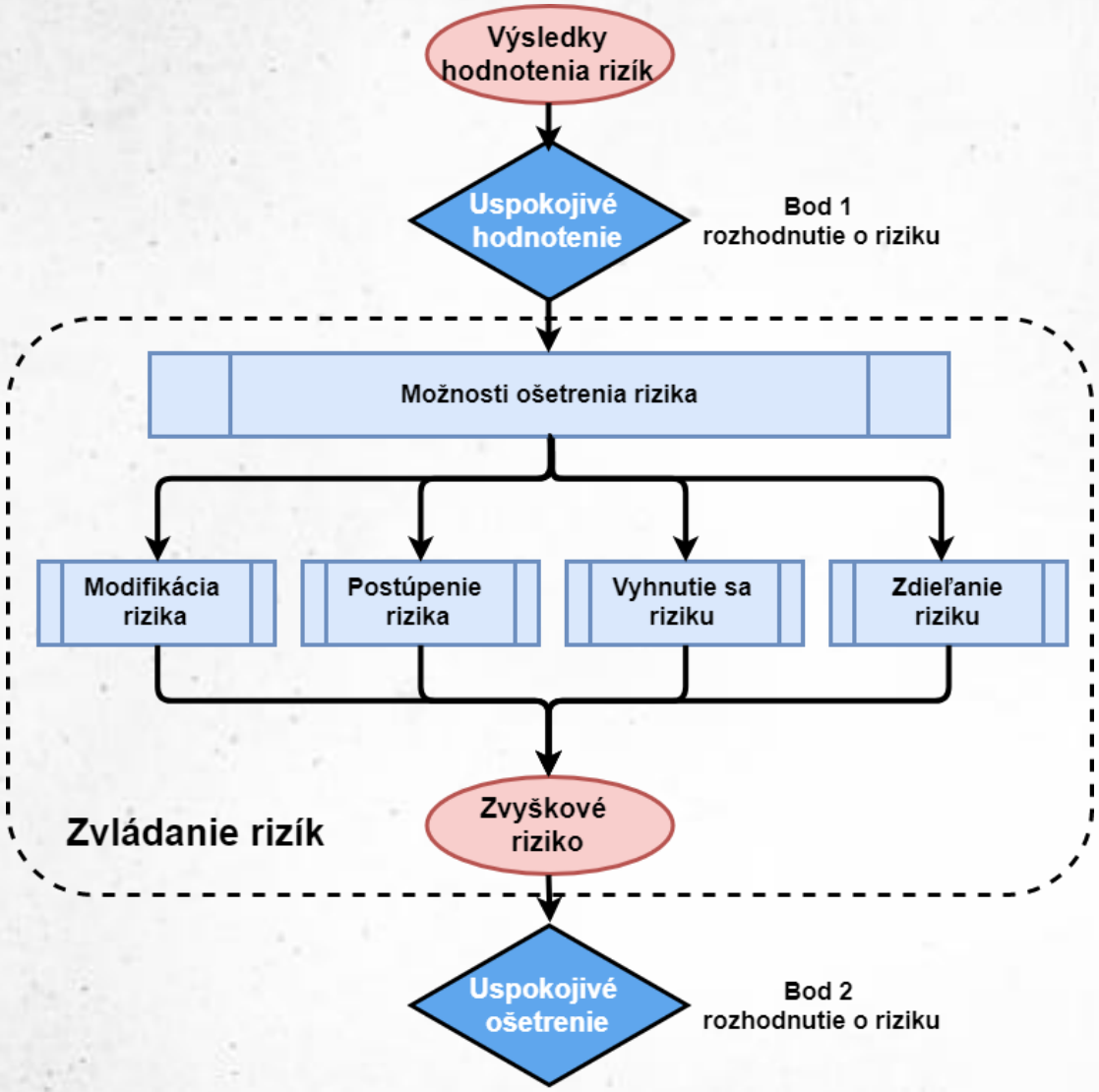


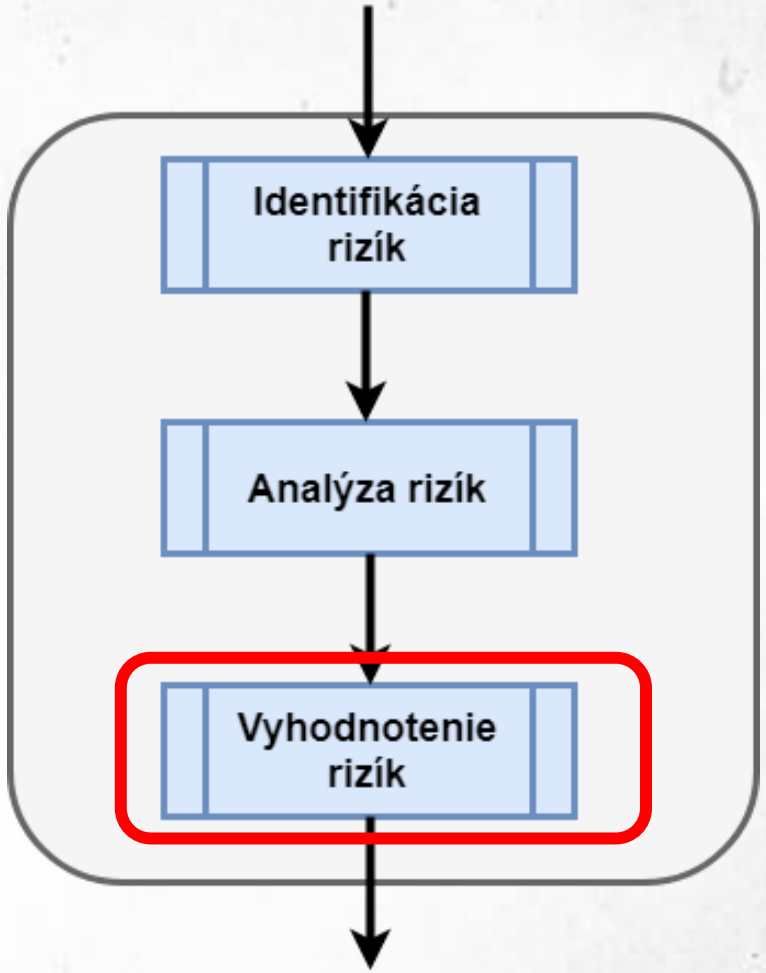
Riziko (III.)

Vyjadrenie rizika (kvalitatívny prístup)

Dopad → Pravdepodobnosť ↓	nízky	stredný	Vysoký
Nulová	Nulové	Nulové	Nulové
Nízka	Nízke	Nízke	Stredné
Stredná	Nízke	Stredné	Vysoké
Vysoká	Stredné	Vysoké	Vysoké

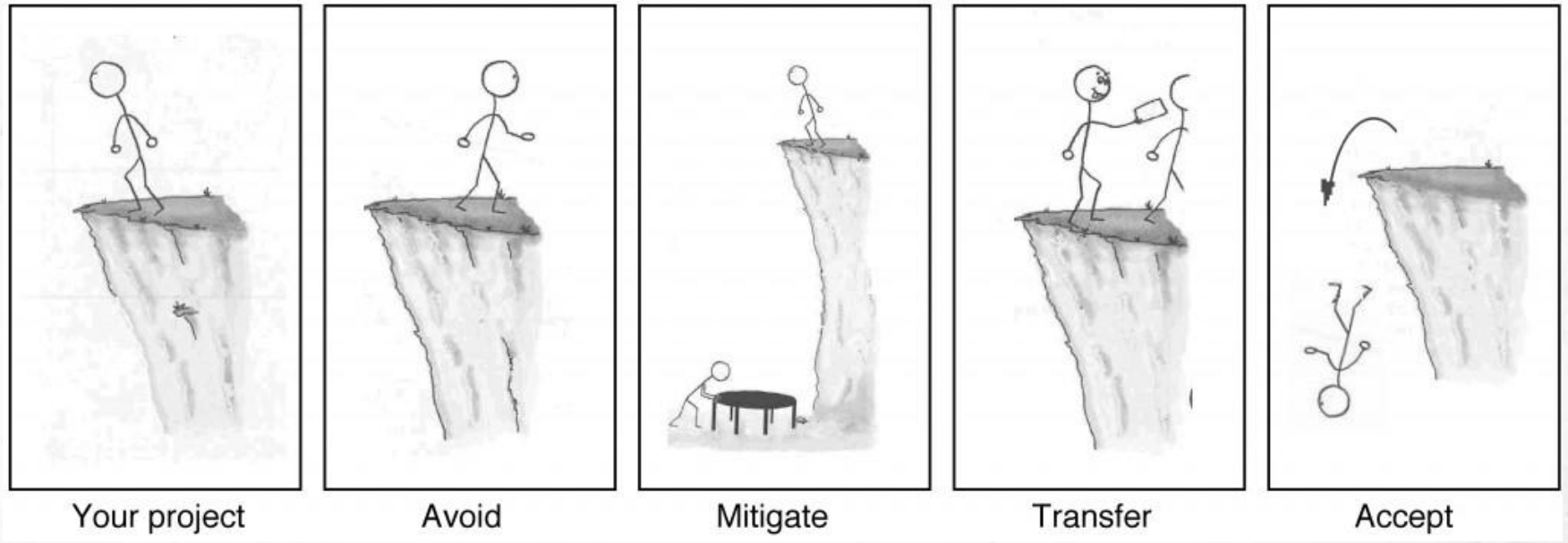
Riziko (IV.)


Výsledky hodnotenia rizík
Uspokojivé hodnotenie
Bod 1
rozhodnutie o riziku
Možnosti ošetrenia rizika
Modifikácia rizika
Postúpenie rizika
Vyhnutie sa riziku
Zdieľanie riziku
Zvyškové riziko
Zvládanie rizík
Uspokojivé ošetrenie
Bod 2
rozhodnutie o riziku


Identifikácia rizík
Analýza rizík
Vyhodnotenie rizík

Riziko (V.)

- Akceptovanie/Zachovanie rizika (Accept)
- Vyhnutie sa riziku (Avoid)
- Limitácia/Zníženie rizika (Mitigate / Limit)
- Presun rizika (Transfer)

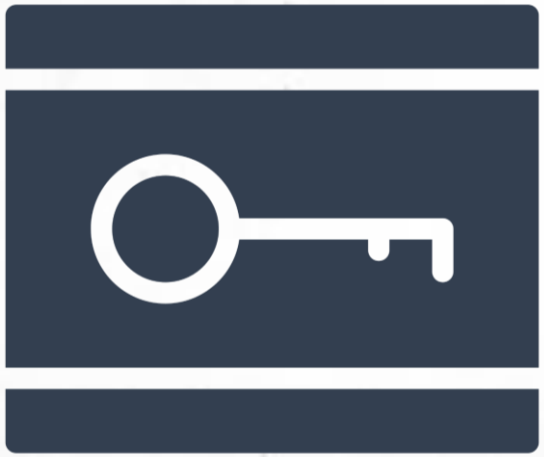


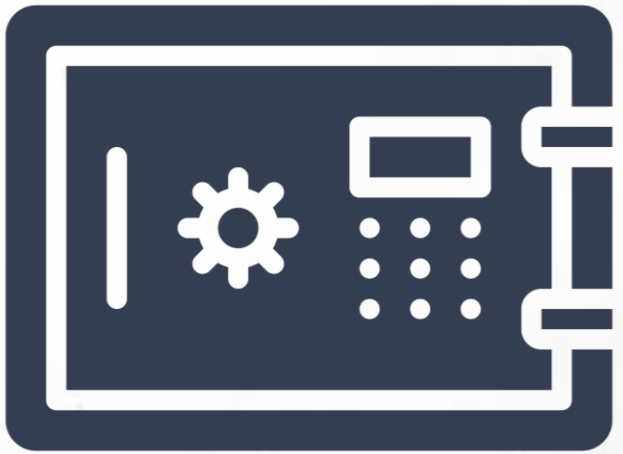
Zdroj: http://cnx.org/content/col11120/1.4/

Bezpečnostné opatrenia (I.)

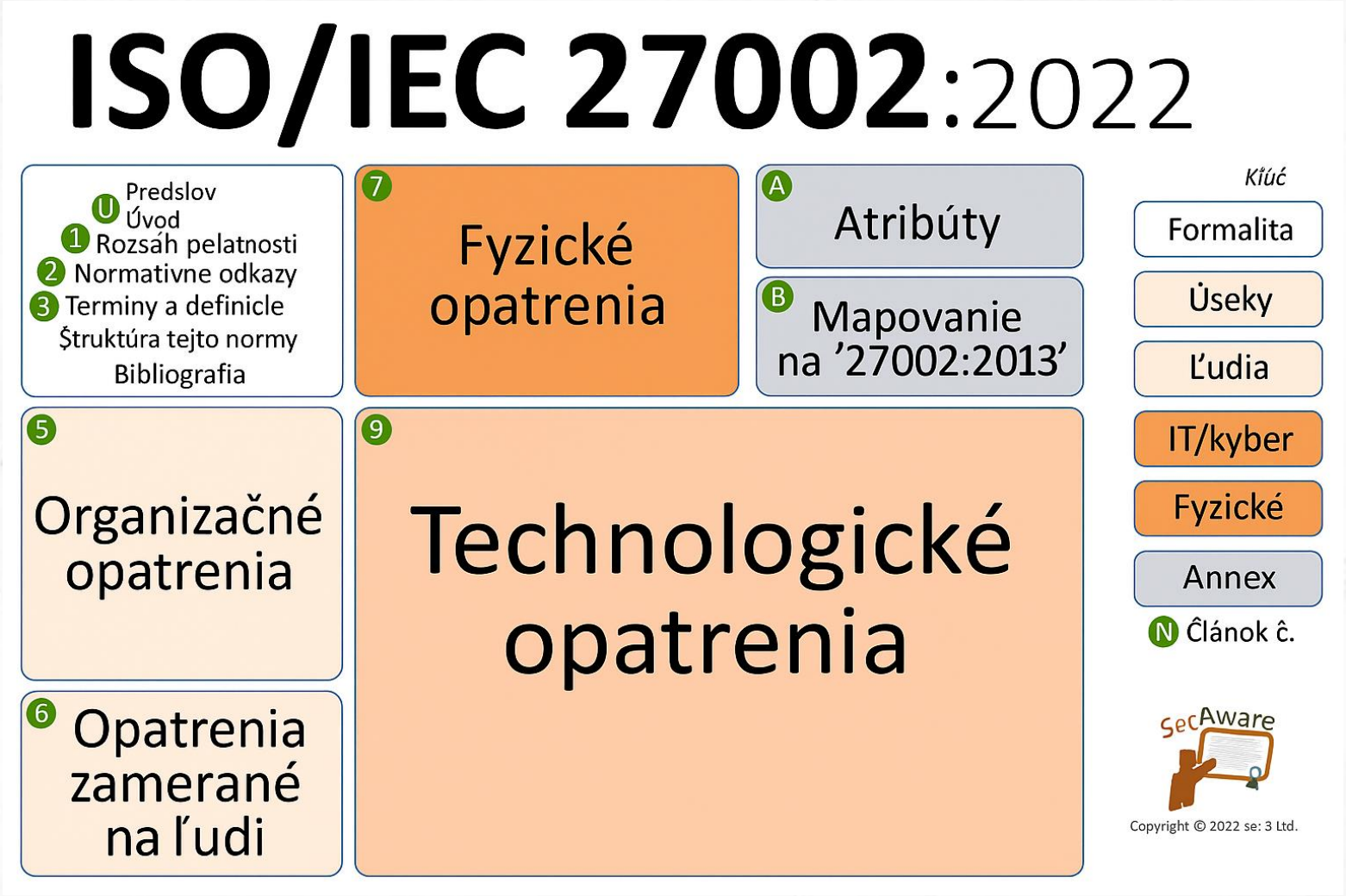
- akákoľvek činnosť, technické zariadenie, proces, mechanizmus, alebo čokoľvek, čo chráni informačný systém a jeho časti (aktíva) pred pôsobením konkrétnych hrozieb alebo hrozby.

- **Administratívne** – napr. politiky, odporúčania, štandardy
- **Fyzické** – napr. uzamykateľné dvere, náhradný zdroj napájania
- **Logické** – napr. heslá, firewally, prístupové zoznamy





Bezpečnostné opatrenia (II.)



Zdroj: https://www.iso27001security.com/html/27002.html

Bezpečnostné opatrenia (III.)

§ 20 ods. 2 Zákona o KB: Bezpečnostné opatrenia sa prijímajú a realizujú najmä pre oblasť

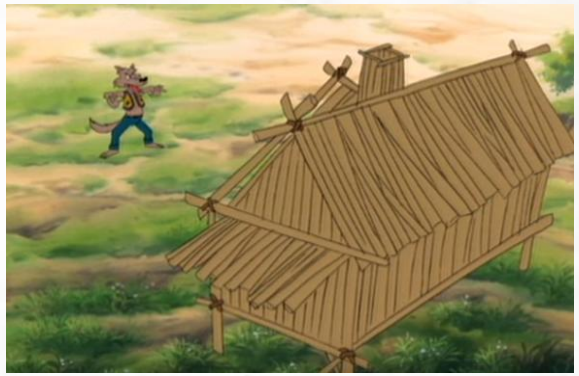
a) organizáciu a riadenie informačnej bezpečnosti a kybernetickej bezpečnosti,
b) správu zraniteľností a kybernetických hrozieb,
c) správu aktív a riadenie kybernetických hrozieb a rizík,
d) riadenie udalostí a kybernetických bezpečnostných incidentov,
e) riadenie kontinuity činností, zálohovanie, obnovu systémov po havárii a krízové riadenie,
f) bezpečnosť pri nadobúdaní, vývoji a údržbe siete, informačných systémov, aplikácií a konfigurácií,
g) postupy posudzovania účinnosti opatrení, riadenie súladu a kontrolné činnosti,
h) kryptografické opatrenia a zásady používania kryptografie,
i) bezpečnosť a spôsobilosti ľudských zdrojov,
j) správu identít a prístupov,
k) bezpečnosť pri prevádzke sietí a informačných systémov,
l) ochranu proti škodlivému kódu a nežiaducemu obsahu,
m) systémovú bezpečnosť, sieťovú bezpečnosť a komunikačnú bezpečnosť,
n) monitorovanie, zaznamenávanie a hlásenie udalostí,
o) fyzickú bezpečnosť, bezpečnosť prostredia a správu koncových zariadení,
p) ochranu záznamov, súkromia a označovanie informácií,
q) dodávateľský reťazec,
r) obstarávanie a využívanie certifikovaných produktov IKT, služieb IKT a procesov IKT.

Bezpečnostné opatrenia (IV.)

- **Minimálne bezpečnostná opatrenia** – príloha č. 2 Vyhlášky UPVII č. 179/2020 Z. z.

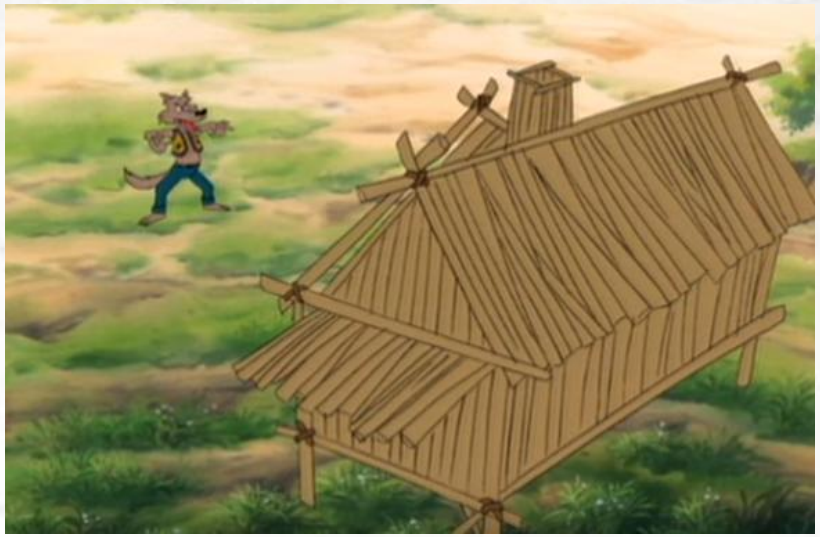
A. Organizácia kybernetickej bezpečnosti a informačnej bezpečnosti
B. Riadenie rizík kybernetickej bezpečnosti a informačnej bezpečnosti
C. Personálna bezpečnosť
D. Riadenie prístupov
E. Riadenie kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahoch s tretími stranami
F. Bezpečnosť pri prevádzke informačných systémov a sietí
G. Hodnotenie zraniteľností a bezpečnostné aktualizácie
H. Ochrana proti škodlivému kódu
I. Sieťová a komunikačná bezpečnosť
J. Akvizícia, vývoj a údržba informačných technológií verejnej správy
K. Zaznamenávanie udalostí a monitorovanie
L. Fyzická bezpečnosť a bezpečnosť prostredia
M. Riešenie kybernetických bezpečnostných incidentov
O. Kontinuita prevádzky informačných technológií verejnej správy
P. Audit a kontrolné činnosti

Aktivita (I.)



Aktivita (II.)

- Aktívum
- Hrozba
- Zraniteľnosť
- Útok
- Útočník
- Riziko
- Bezpečnostné opatrenie



Bezpečnostné hrozby (I.)

Zdroj: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-list-of-top-15-threats

Bezpečnostné hrozby (II.)

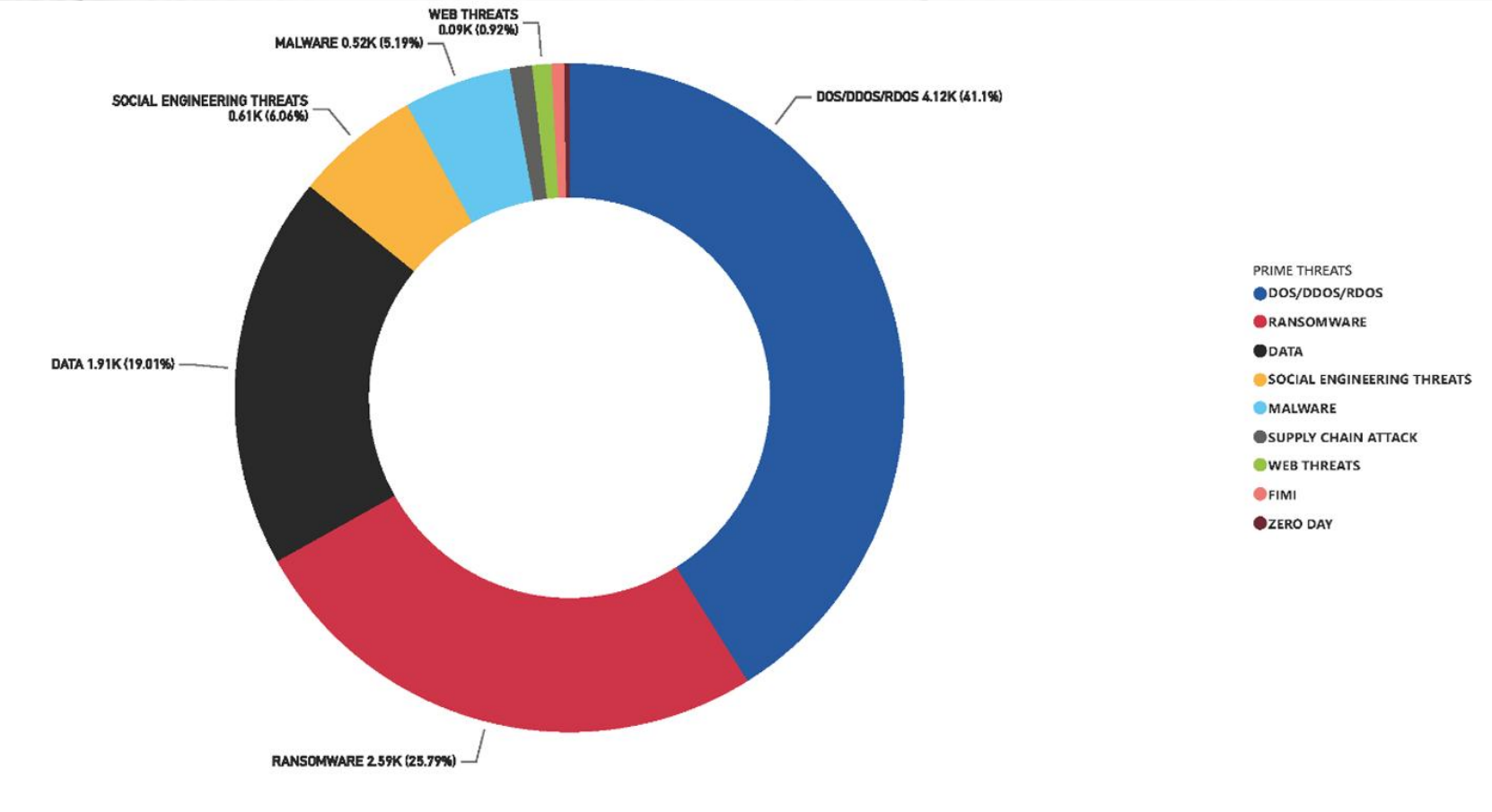
Zdroj: ENISA Landscape 2024, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

Bezpečnostné hrozby (III.)

Zdroj: https://www.enisa.europa.eu/publications/enisa-foresight-cybersecurity-threats-for-2030

Aktuálne bezpečnostné hrozby (I.)

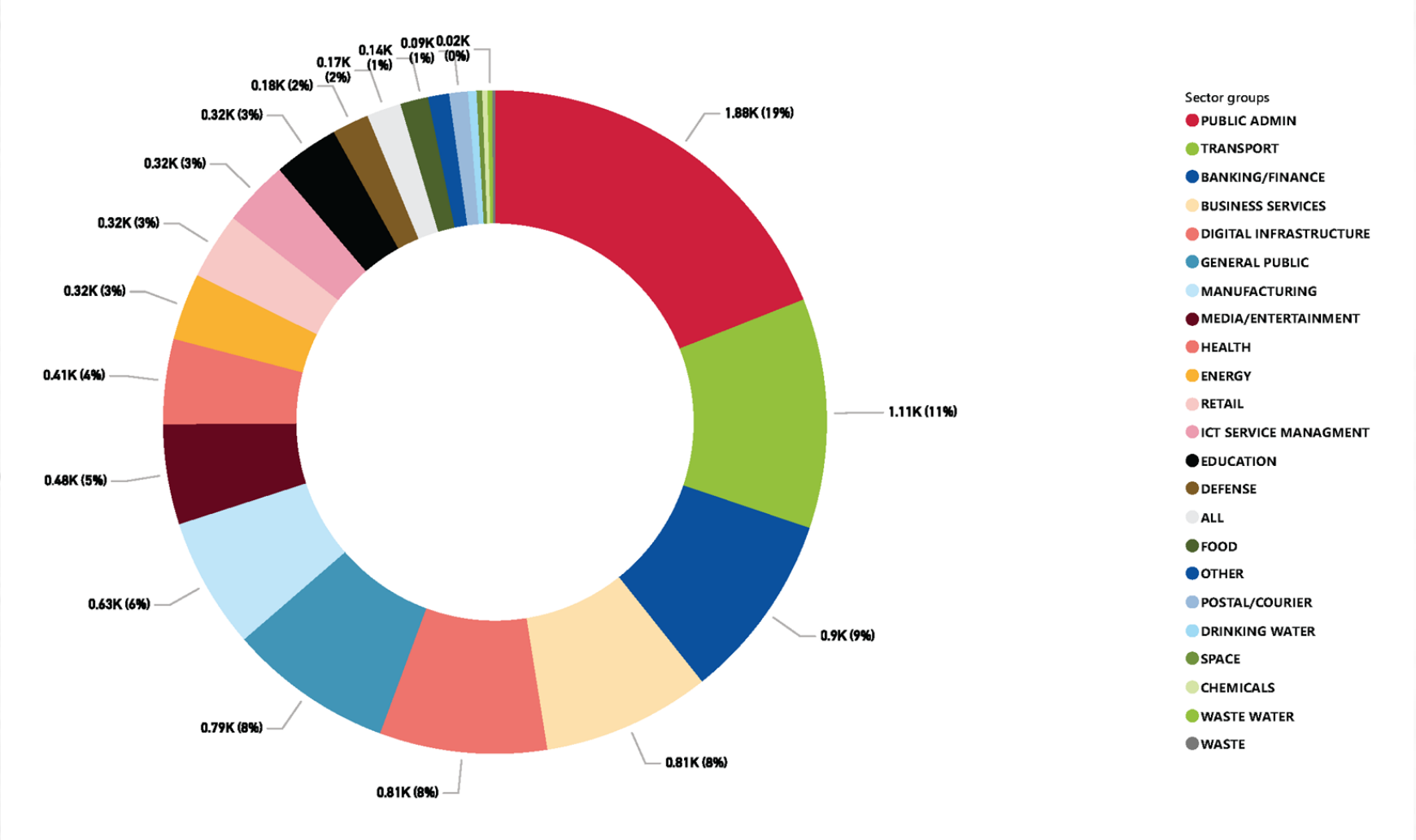
- bezpečnostné hrozby, júl 2023 – jún 2024



Zdroj: ENISA Landscape 2024, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

Aktuálne bezpečnostné hrozby (II.)

- cieľové sektory, júl 2023 – jún 2024



Zdroj: ENISA Landscape 2024, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

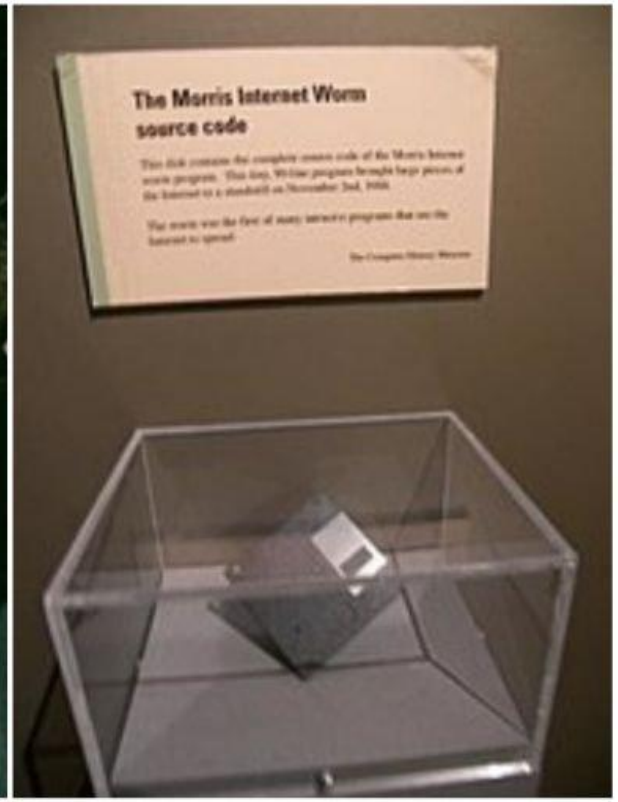
Škodlivý kód

3.11.2024 10:23 | Bezpečnosť

VIDEO Legendárny Morrisov červ má 36 rokov. Ochromil internet

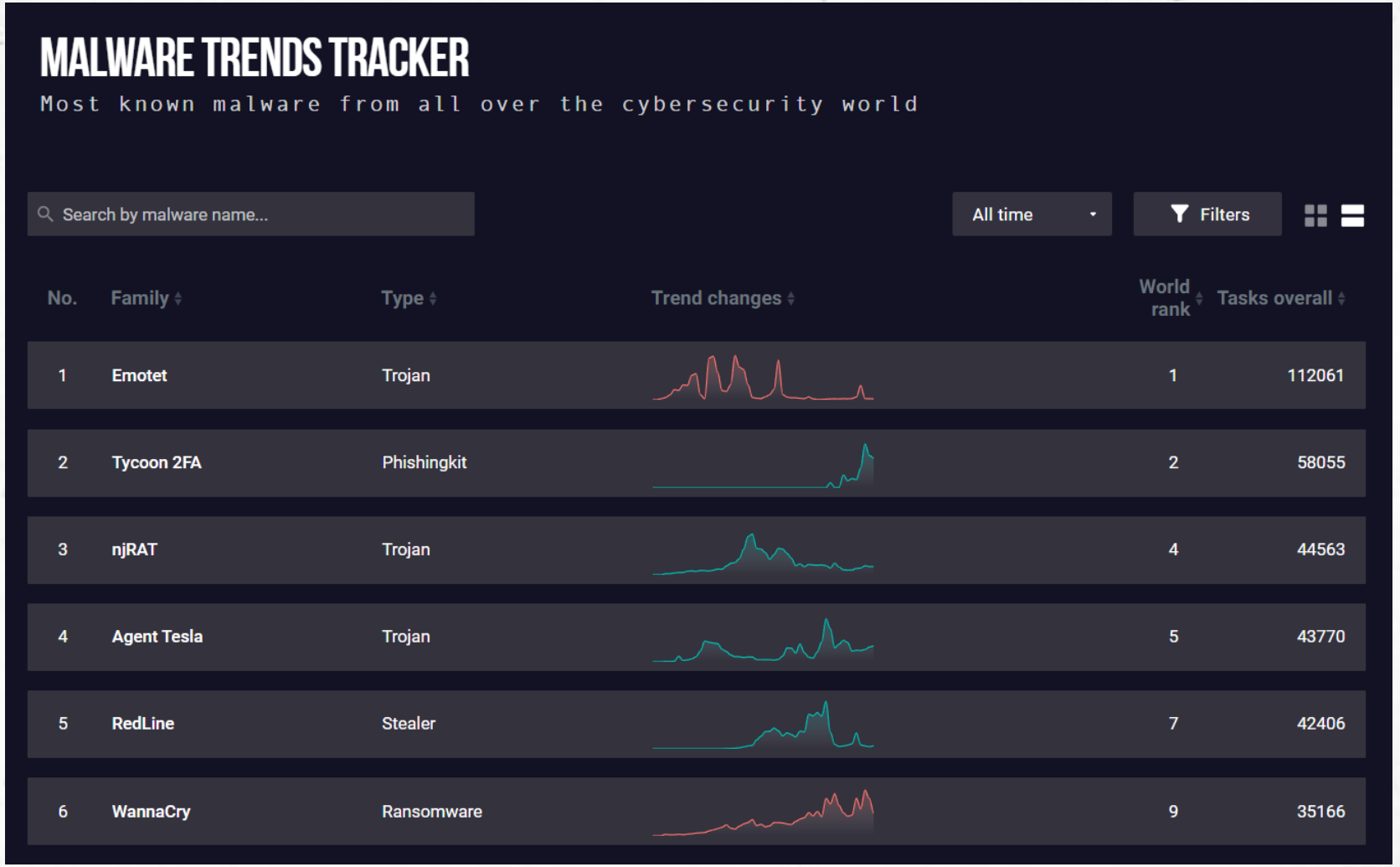
Zdroj: iStockphoto

Počítačová komunita v 80. rokoch zanedbávala bezpečnosť. Dostala nečakanú lekciu v podobe 99 riadkov kódu.



Zdroj: https://zive.aktuality.sk/clanok/135837/legendarny-morrisov-cerv-ma-36-rokov-ochromil-internet/ https://twitter.com/todayininfosec/status/926128404054777856

Vývoj malvéru (I.)



MALWARE TRENDS TRACKER

Most known malware from all over the cybersecurity world

Search by malware name...

All time

Filters

No.	Family	Type	Trend changes	World rank	Tasks overall
1	Emotet	Trojan		1	112061
2	Tycoon 2FA	Phishingkit		2	58055
3	njRAT	Trojan		4	44563
4	Agent Tesla	Trojan		5	43770
5	RedLine	Stealer		7	42406
6	WannaCry	Ransomware		9	35166

Zdroj: https://any.run/malware-trends/

Agent Tesla (I.)

AGENT TESLA

agenttesla trojan rat stealer

4	1 ↑	1	2423
Global rank	Month rank	Week rank	IOCs

Agent Tesla is spyware that collects information about the actions of its victims by recording keystrokes and user interactions. It is falsely marketed as a legitimate software on the dedicated website where this malware is sold.

Trojan
Type

Likely Turkey
Origin

1 January, 2014
First seen

20 March, 2024
Last seen

HOW TO ANALYZE AGENT TESLA WITH ANY.RUN

IOCs

IP addresses

66.29.151.236
198.23.221.13
76.74.235.200

Hashes

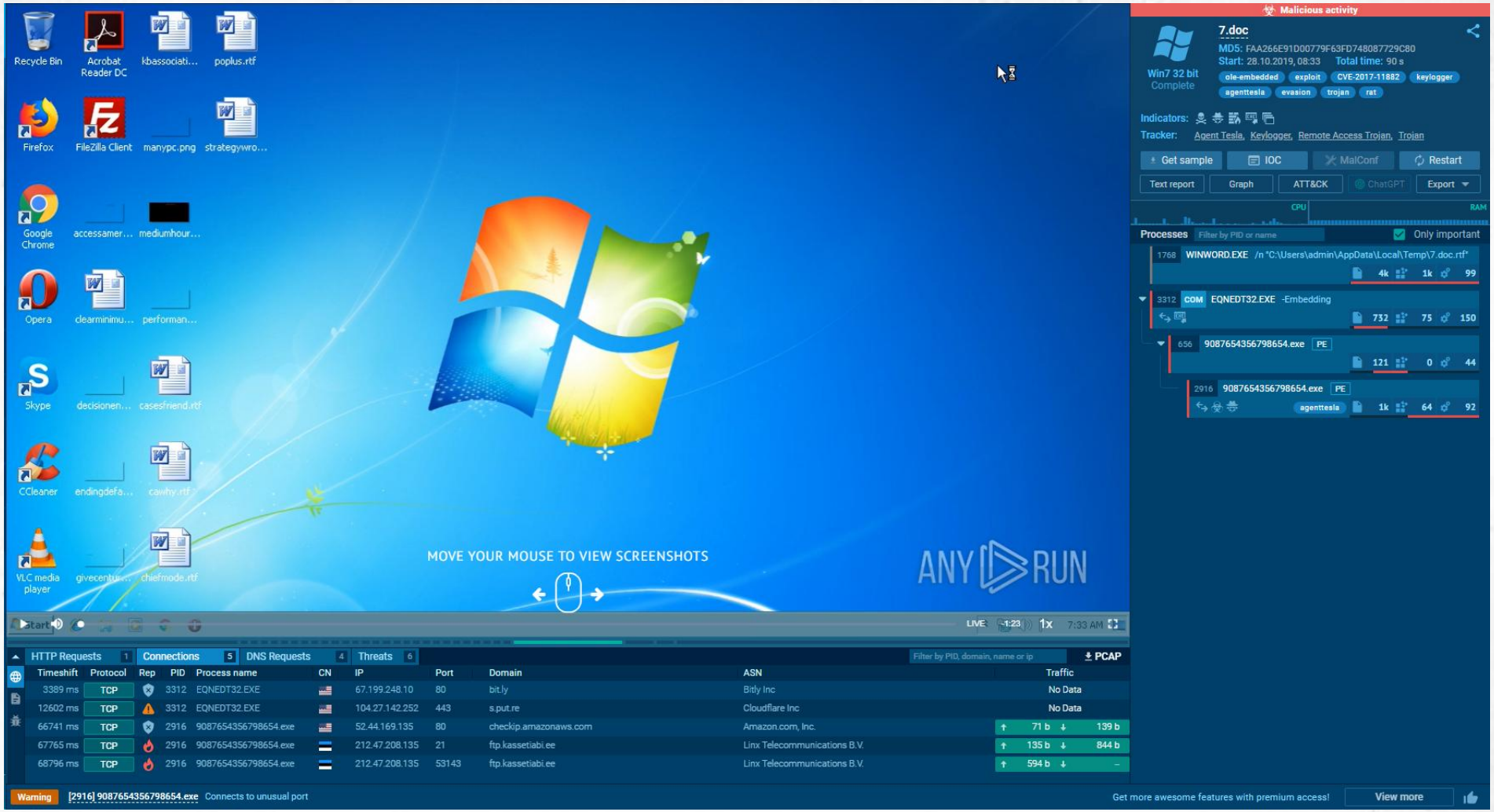
2A5D62B7DC7E761AF95740412AECCD4B5D7397BC7439859F781F6B03C47AA729
44DE0BEB798B850A37AC2FC193AD485891EDA952A428E237E3217420B5D45720
4910064584A83B348A17494B285F381EB9E6FABB59C528320BA90B31965C014C

Domains

mail.itresinc.com

Zdroj: https://any.run/malware-trends/agenttesla /

Agent Tesla (II.)



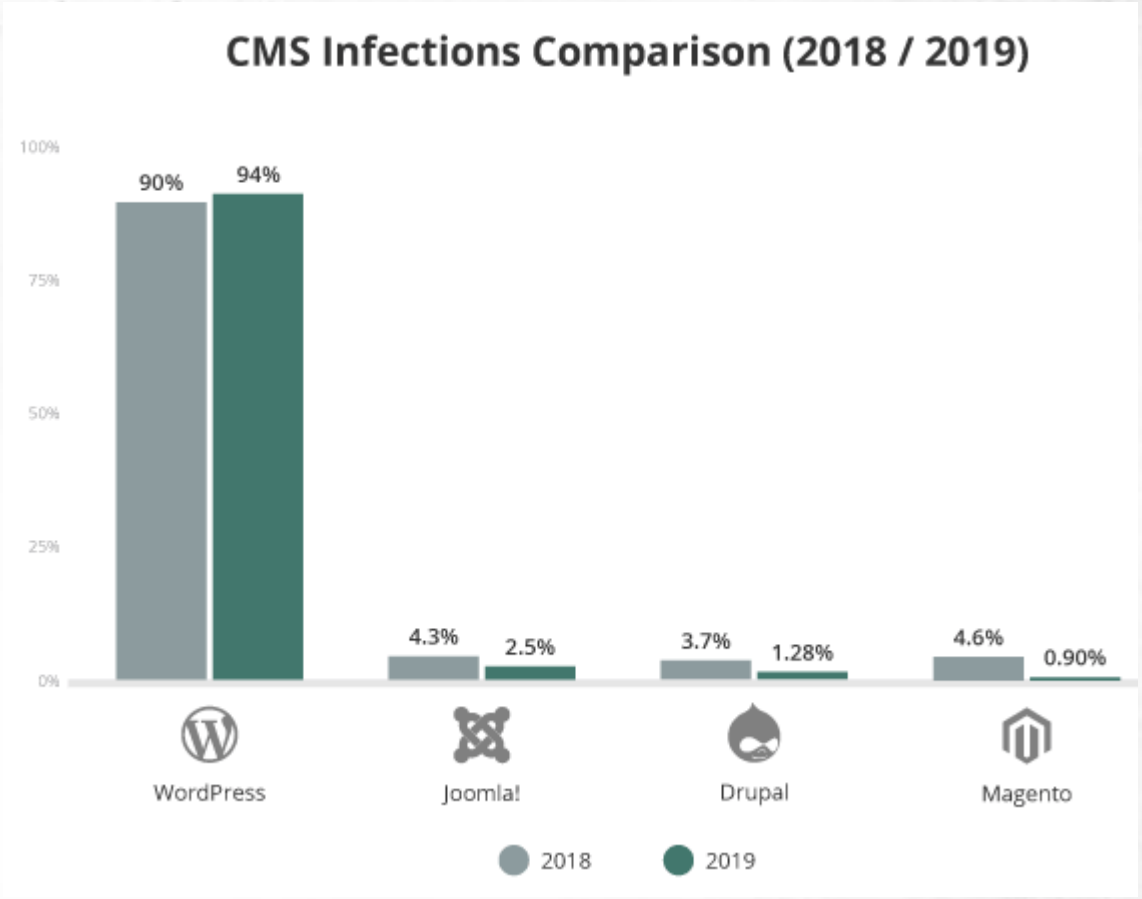
Zdroj: https://app.any.run/tasks/f5c4395c-3a53-47c8-9481-29caa2734c77/

Zneužitie webových sídel

Zdroj: https://hbr.org/2016/10/is-your-company-ready-for-a-ransomware-attack

Zneužitie webových sídel (I.)

- **exploity prehliadačov**
  - škodlivý kód môže zneužiť ActiveX, HTML, JavaScript, Flash
- **prevzaté súbory**
  - nezabezpečené webové stránky -> umiestnenie škodlivého skriptu do HTTP alebo kódu PHP
- **škodlivé URL**
  - na stiahnutie akéhokoľvek typu škodlivého softvéru do systémov
- **kompromitovaný systém na správu obsahu (CMS)**
  - odkazuje na pluginy a funkcie na zraniteľnom systéme

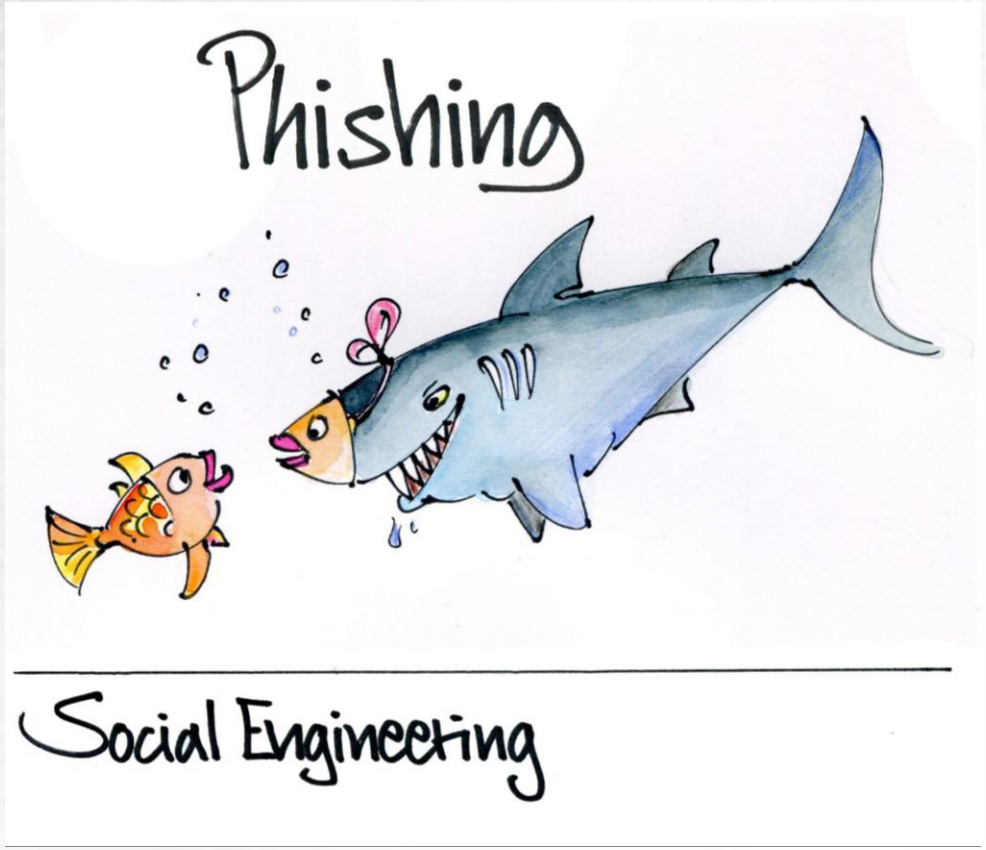


Zdroj: https://sucuri.net/reports/2019-hacked-website-report/

Sociálne inžinierstvo

Zdroj: www.freepik.com

Sociálne inžinierstvo (I.)



„Všetko závisí od toho, ako sa pozeráme na veci, a nie od toho, aké sú."

Carl Gustav Jung

Zdroj: https://mind42.com/public/2e72f1dd-08aa-46a7-b0fd-660634918dd3, https://baklol.com/baks/Funny/Forced-Perspective-Photography-_586/Eiffel-Tower-_7635

Sociálne inžinierstvo (II.)

Máte jednu novú správu

OB

OTP Banka Slovensko <sales@jezzamotors.com>

Komu Undisclosed recipients:

Odpovedať | Odpovedať všetkým | Preposlať | •••

po 6. 7. 2020 13:58

Ak chcete stiahnuť obrázky, kliknite sem. V záujme ochrany vašich osobných údajov program Outlook zabraňuje automatickému sťahovaniu niektorých obrázkov v tejto správe.

Vážený zákazník,

Máte dôležitú správu pre svoj bankový úcet.

Ak chcete cítat správy, prihlásit do internetového bankovníctva Nižšie si môžete precítat správy.

https://wwwotpdirekt.otpbanka.sk/Login

Dakujem,
OTP Banka Slovensko Account Team

Sociálne inžinierstvo (III.)

Dobrý deň, je tovar v dobrom stave?
Aká je cena ?
A odkiaľ si? 😊

Ok kupujem Na druhej strane, Vašu platbu uskutočním prostredníctvom DPD EXPRESSE doručenia v obálke hneď ako dostanete peniaze, pošlem dpd k Vám domov, aby s ch vyzdvihli?

OK, kupujem. Platbu však uskutočním prostredníctvom doručenia TNT EXPRESS v obálke, akonáhle dostanete peniaze, pošlem vám TNT na vyzdvihnutie?

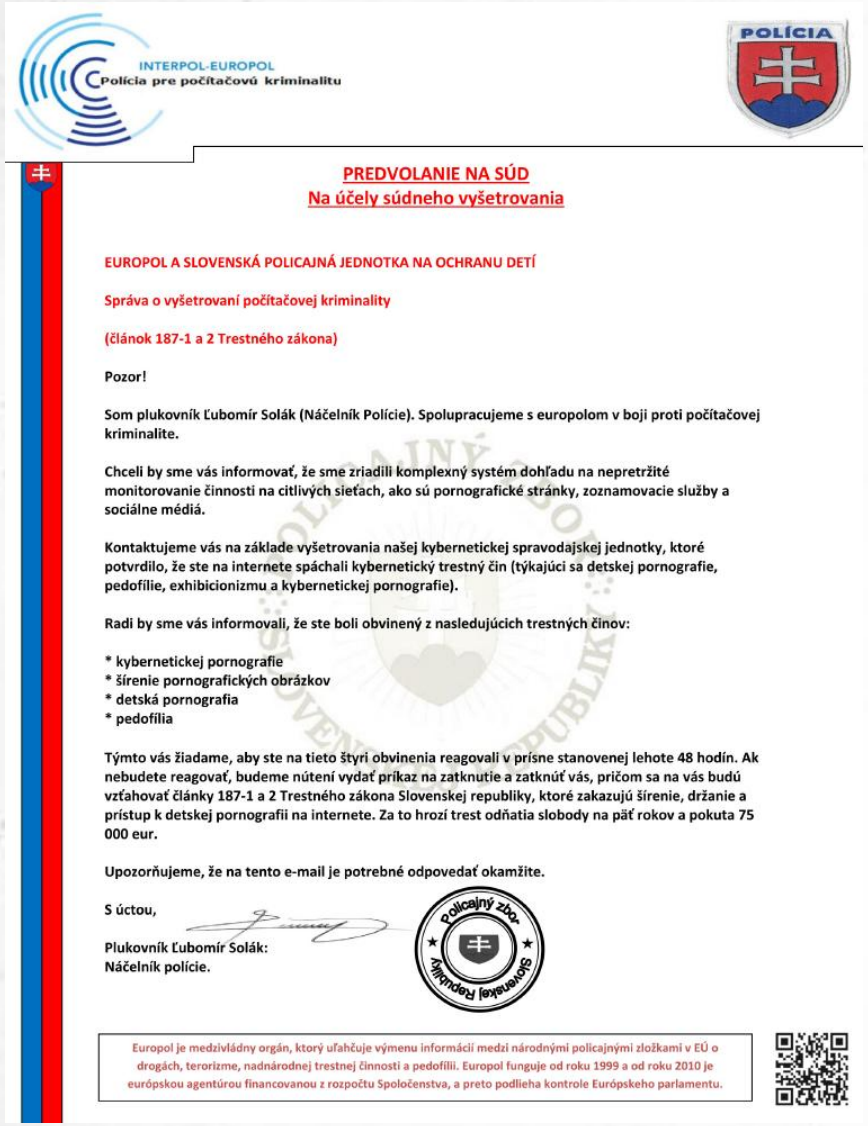
Ok Na dokončenie transakcie budem potrebovať vaše priezvisko/meno/adresu/ mesto:
PSČ / čiastka:
Emailová adresa :

Dobre, funguje to, budeš zajtra k dispozícii, o koľkej hodine, aby poštár TNT mohol prísť k tebe domov?

Ok Na dokončenie transakcie budem potrebovať vaše:

Je Priezvisko krstné meno:
Adresa Mesto PSČ
Cena položky:
Emailová adresa :
Telefónne čísla:

Sociálne inžinierstvo (IV.)



INTERPOL-EUROPOL
Polícia pre počítačovú kriminalitu

POLÍCIA

PREDVOLANIE NA SÚD
Na účely súdneho vyšetrovania

EUROPOL A SLOVENSKÁ POLICAJNÁ JEDNOTKA NA OCHRANU DETÍ

Správa o vyšetrovaní počítačovej kriminality

(článok 187-1 a 2 Trestného zákona)

Pozor!

Som plukovník Ľubomír Solák (Náčelník Polície). Spolupracujeme s europolom v boji proti počítačovej kriminalite.

Chceli by sme vás informovať, že sme zriadili komplexný systém dohľadu na nepretržité monitorovanie činnosti na citlivých sieťach, ako sú pornografické stránky, zoznamovacie služby a sociálne médiá.

Kontaktujeme vás na základe vyšetrovania našej kybernetickej spravodajskej jednotky, ktoré potvrdilo, že ste na internete spáchali kybernetický trestný čin (týkajúci sa detskej pornografie, pedofílie, exhibicionizmu a kybernetickej pornografie).

Radi by sme vás informovali, že ste boli obvinený z nasledujúcich trestných činov:

* kybernetickej pornografie
* šírenie pornografických obrázkov
* detská pornografia
* pedofília

Týmto vás žiadame, aby ste na tieto štyri obvinenia reagovali v prísne stanovenej lehote 48 hodín. Ak nebudete reagovať, budeme nútení vydať príkaz na zatknutie a zatknúť vás, pričom sa na vás budú vzťahovať články 187-1 a 2 Trestného zákona Slovenskej republiky, ktoré zakazujú šírenie, držanie a prístup k detskej pornografii na internete. Za to hrozí trest odňatia slobody na päť rokov a pokuta 75 000 eur.

Upozorňujeme, že na tento e-mail je potrebné odpovedať okamžite.

S úctou,

Plukovník Ľubomír Solák:
Náčelník polície.

Policajný zbor Slovenskej republiky

Europol je medzivládny orgán, ktorý uľahčuje výmenu informácií medzi národnými policajnými zložkami v EÚ o drogách, terorizme, nadnárodnej trestnej činnosti a pedofílii. Europol funguje od roku 1999 a od roku 2010 je európskou agentúrou financovanou z rozpočtu Spoločenstva, a preto podlieha kontrole Európskeho parlamentu.

POLICAJNY ZBOR SLOVENSKEJ REPUBLIKY.

PREDVOLAJ NA SÚD

Na vyšetrenie (článok 331-1-22 Trestného zákona)

Slovenská polícia v spojení s medzinárodnou políciou (INTERPOL). Kontaktuje vás krátko po zabavení počítača kybernetickej infiltrácie (oprávnenej vrátane detskej pornografie, pornografických stránok, kybernetickej pornografie, aby vás informoval, že ste predmetom niekoľkých právnych konaní, ktoré zahŕňajú:

VÝPOČTY POPLATKOV:

*DETSKÁ PORNOGRAFIA.
*PORNOGRAFICKÁ STRÁNKA.
*CYBER PORNOGRAFIA.
*NESPRÁVNE VYUŽÍVANIE MALÝCHLÝCH.

Žiadame vás, aby ste sa vyjadrili e-mailom tak, že nám napíšete svoje odôvodnenia, aby sme ich preskúmali a skontrolovali, aby sa vyhodnotili sankcie; že v prísnom termíne 72 hodín. Po uplynutí tejto doby budeme povinní postúpiť naše oznámenie ktorémukoľvek prokurátorovi republiky v blízkosti súdu prvého stupňa a špecialistovi na počítačovú kriminalitu, aby na vás uvalil väzbu a budete zaregistrovaný ako sexuálny delikvent.

Te ste boli varovaní.

POLICAJNÝ ZBOR

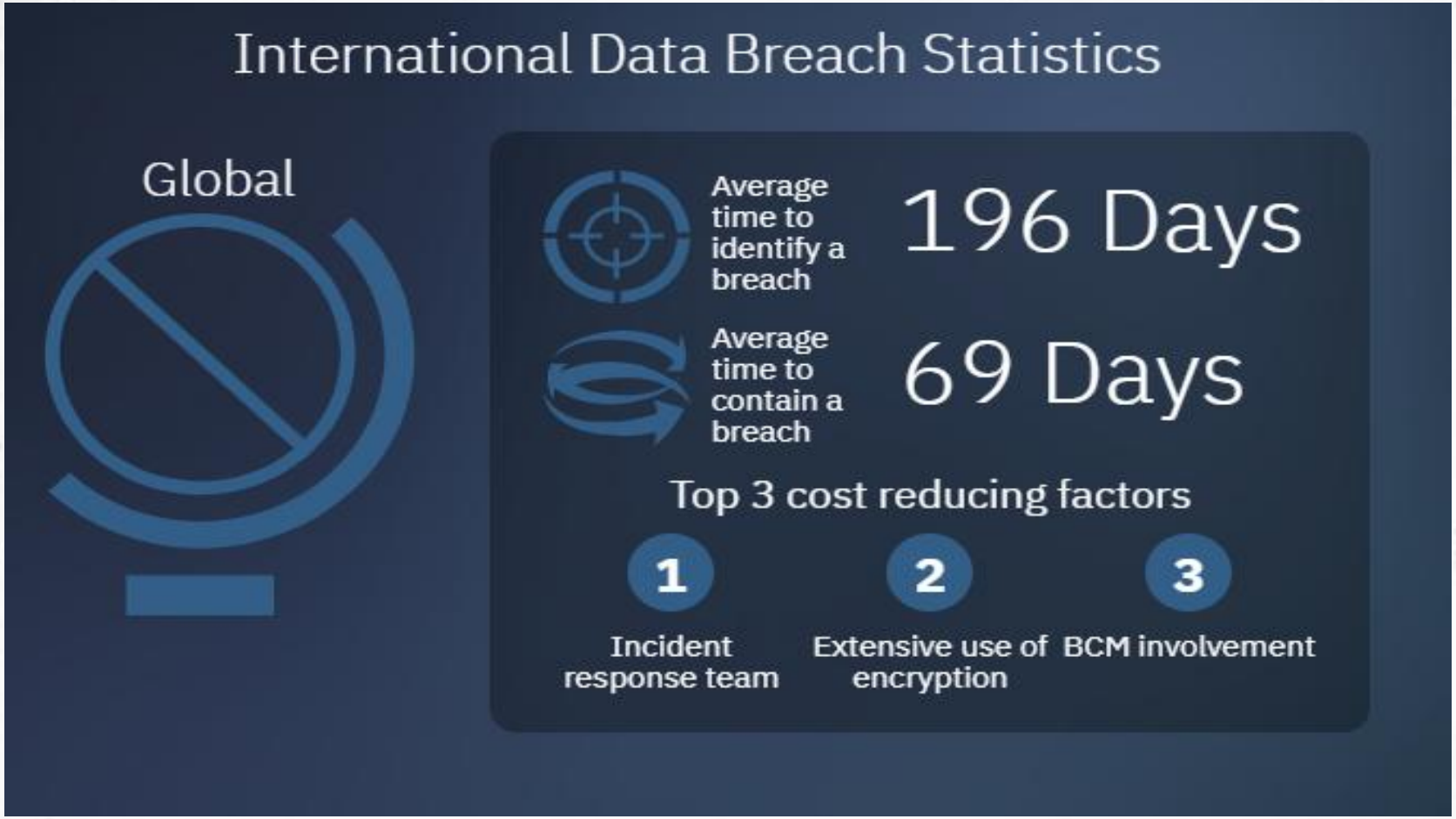
Zdroj: https://www.webpt.com/blog/protecting-patient-data-lessons-learned-from-the-anthem-and-equifax-data-breach

Únik údajov (I.)

- **Facebook** – 131 miliónoch používateľoch
- **Twitter (Hacking)** – 330 miliónov záznamov.
- **British Airways (Web)** – 380.000 záznamov.
- **Google (Web)** – 500.000 záznamov.

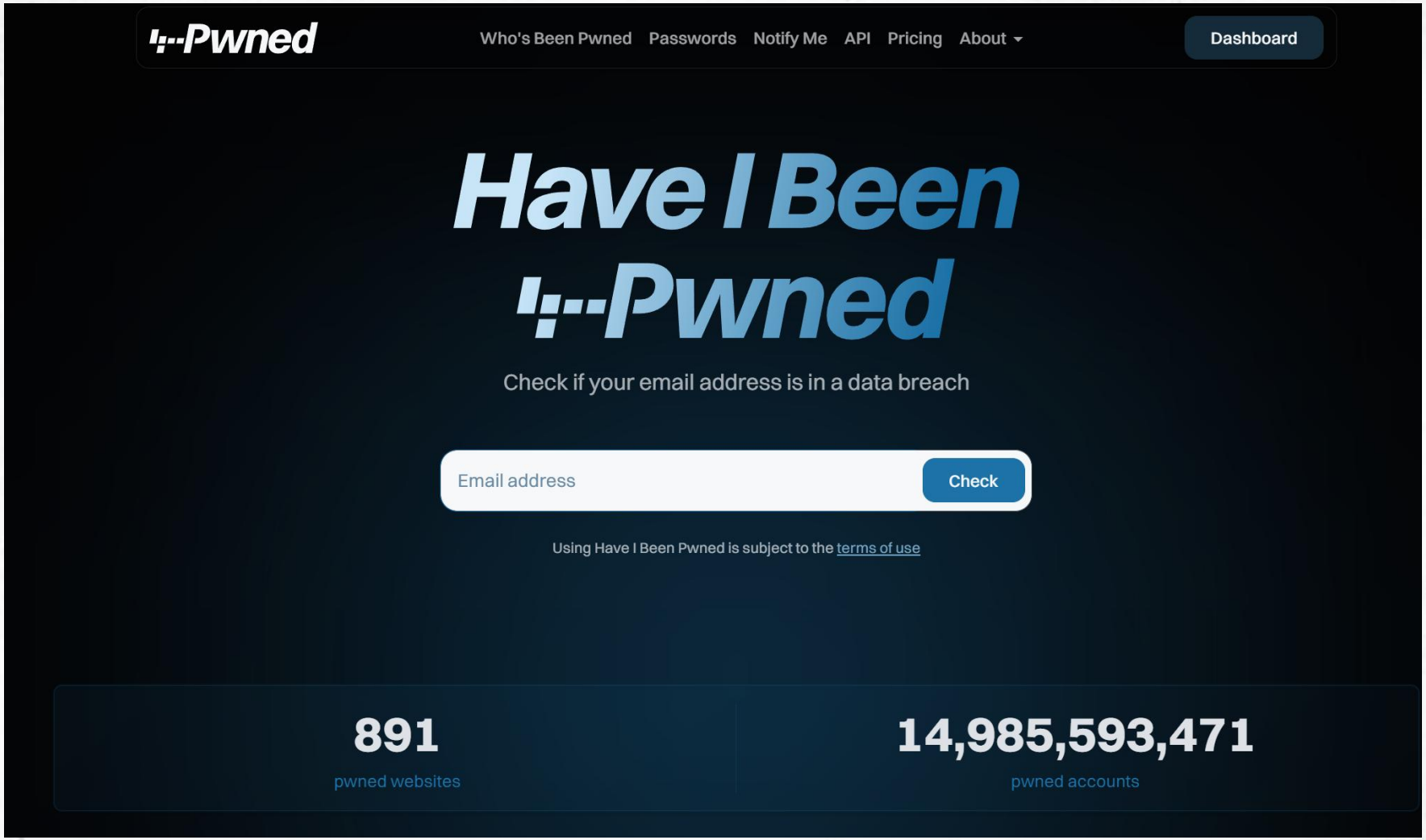
Zdroj: https://www.varonis.com/blog/data-breach-response-times/, Cost of a Data Breach Study: Benchmark research sponsored by IBM Security Independently conducted by Ponemon Institute LLC Global Overview (2018)

Únik údajov (II.)



Zdroj: https://www.varonis.com/blog/data-breach-response-times/, Cost of a Data Breach Study: Benchmark research sponsored by IBM Security Independently conducted by Ponemon Institute LLC Global Overview (2018)

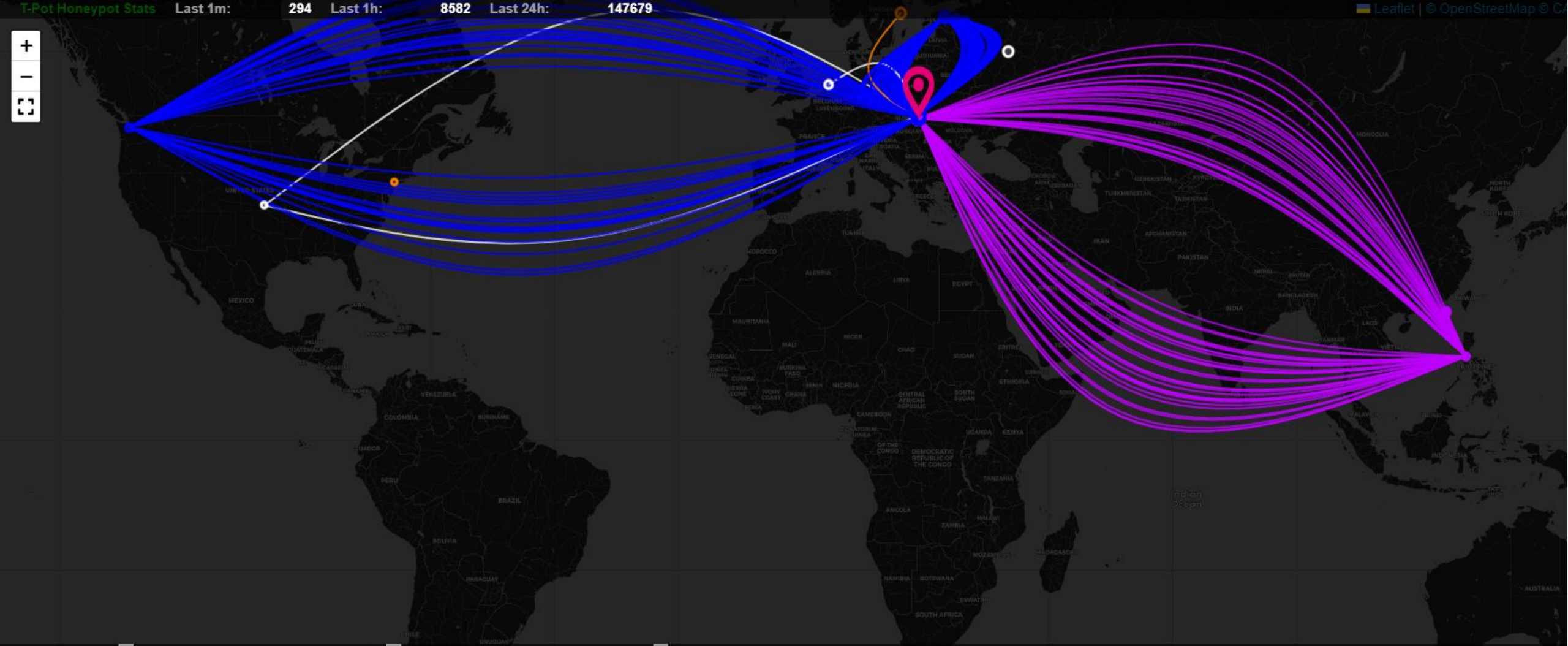
Únik údajov (III.)



Zdroj: https://haveibeenpwned.com/v

Sieťové útoky

Zdroj: https://hbr.org/2016/10/is-your-company-ready-for-a-ransomware-attack



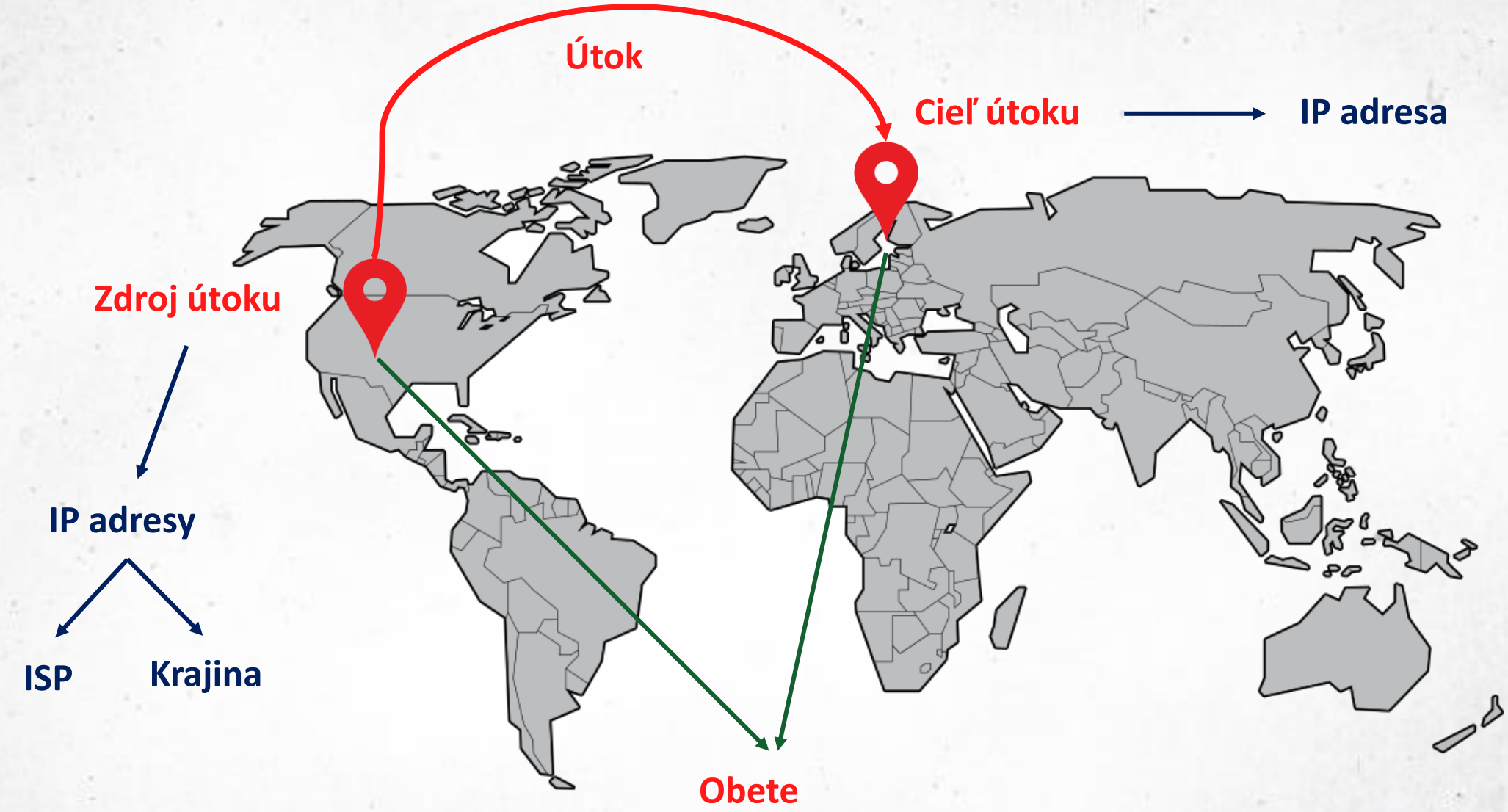
Color	Service
	FTP
	SSH
	TELNET
	EMAIL
	SQL
	DNS

Hits	IP
3686	185.73.125.23
1696	119.92.196.243
1284	66.94.123.164
962	80.66.88.148
43	79.137.222.62
31	50.31.21.8

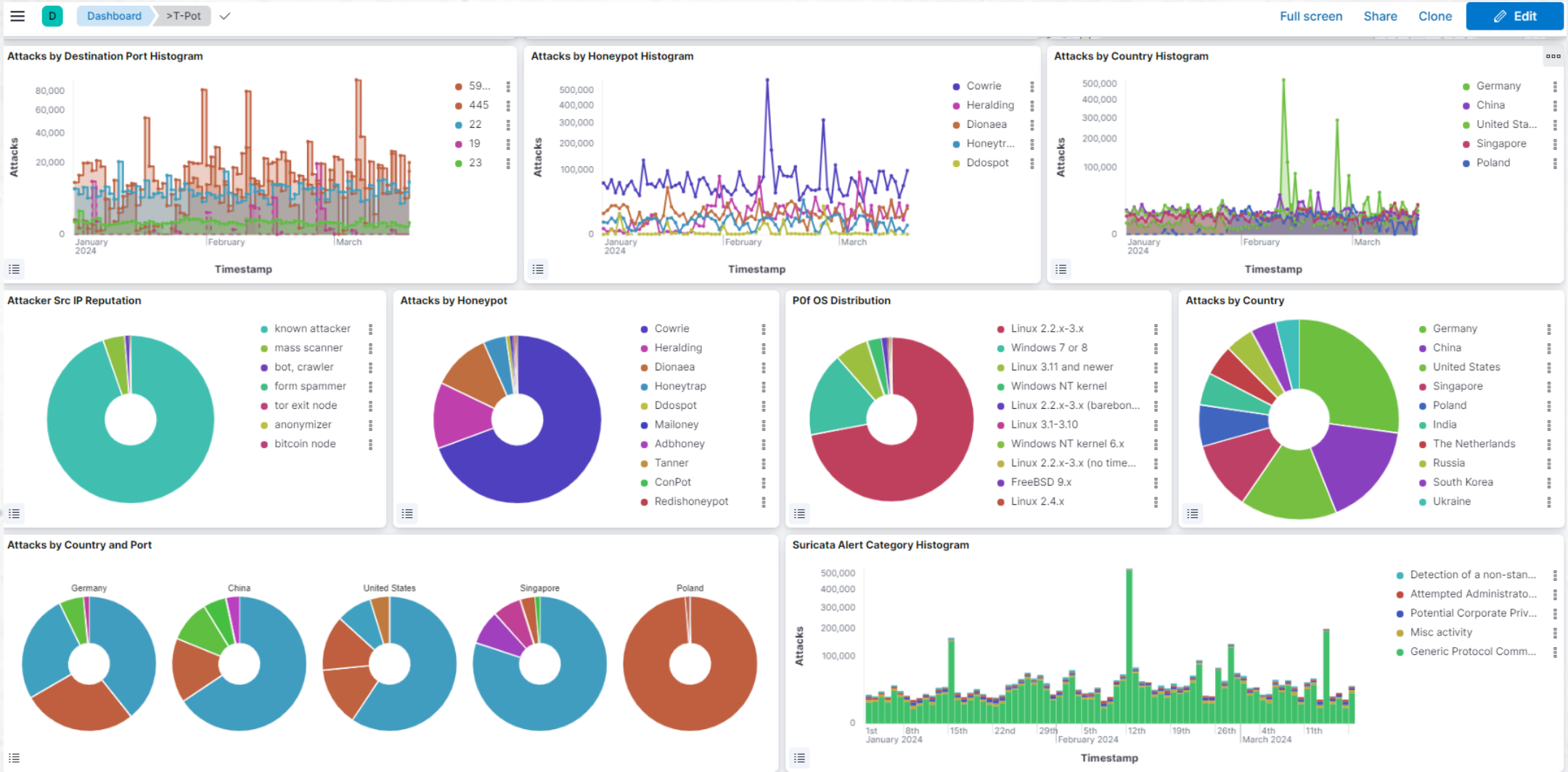
Hits	Country
3689	Estonia
1696	Philippines
1473	United States
1003	The Netherlands
82	Russia
52	China

Events	IP	Country	Honeypot	Service
2024-03-19 23:06:51	185.73.125.23	Estonia	Heralding	VNC
2024-03-19 23:06:51	185.73.125.23	Estonia	Heralding	VNC
2024-03-19 23:06:51	119.92.196.243	Philippines	Dionaea	SMB
2024-03-19 23:06:51	185.73.125.23	Estonia	Heralding	VNC
2024-03-19 23:06:51	66.94.123.164	United States	Heralding	VNC
2024-03-19 23:06:50	185.73.125.23	Estonia	Heralding	VNC

Sieťové útoky z pohľadu dát (I.)

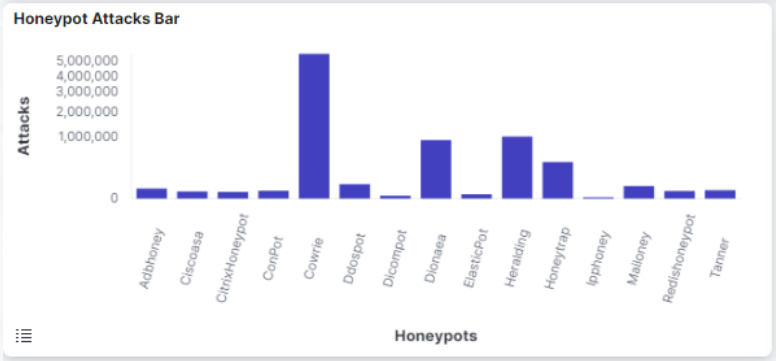


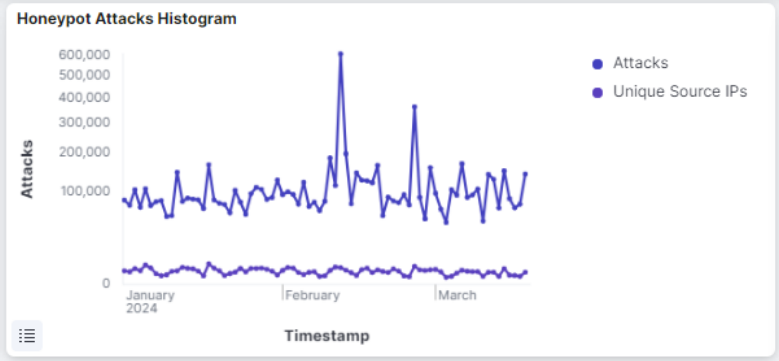
Situačné povedomie (I.)

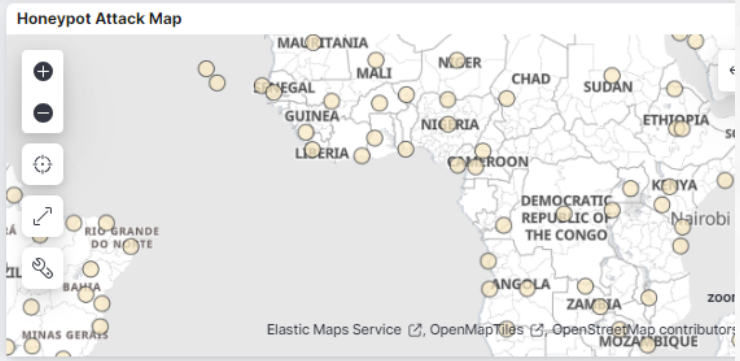


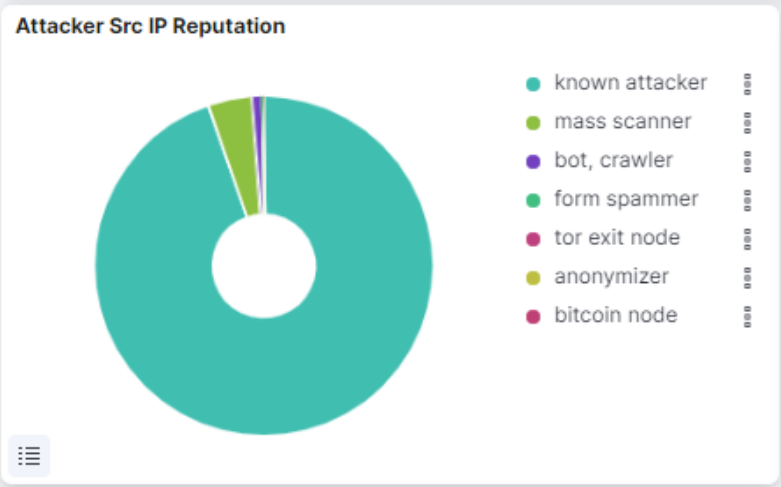
Situačné povedomie (II.)

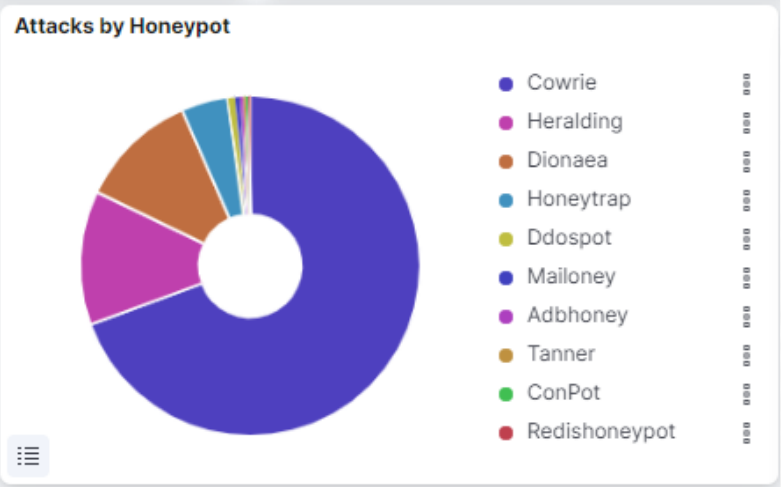
5,586,293	1,023,639	910,343	354,774	55,094	41,757	26,316	18,467	16,131	14,932
Cowrie - Attacks	Heralding - Attacks	Dionaea - Attacks	Honeytrap - Attacks	Ddospot - Attacks	Mailoney - Attacks	Adbhoney - Attacks	Tanner - Attacks	ConPot - Attacks	Redishoneypot - Attacks



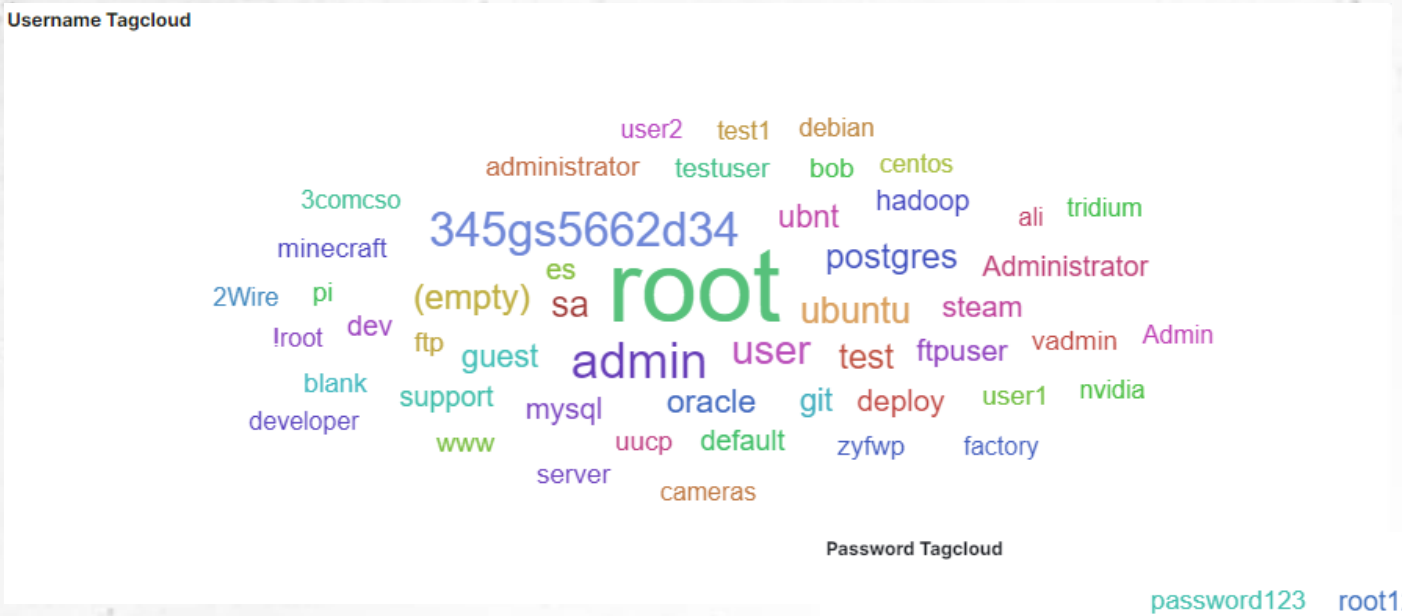






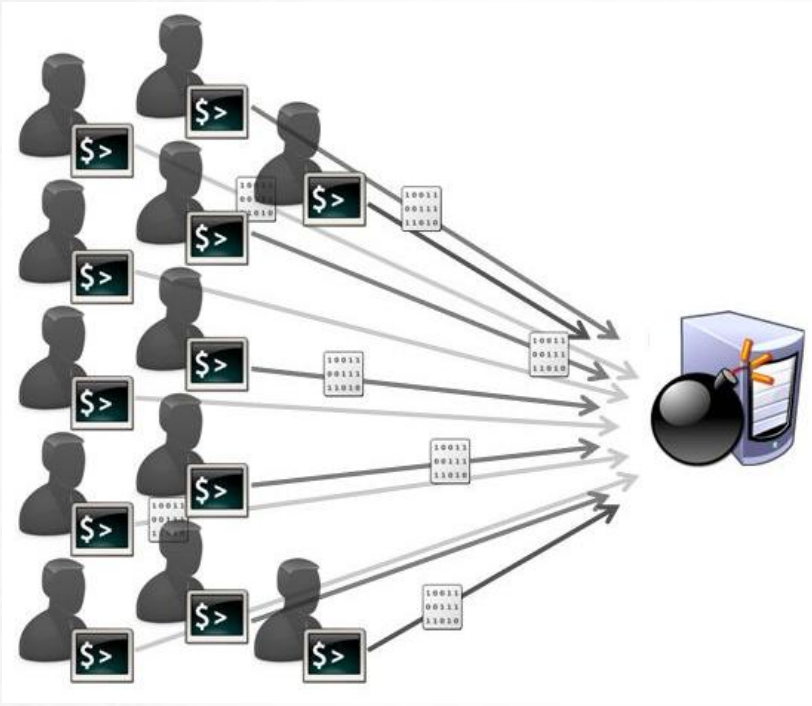


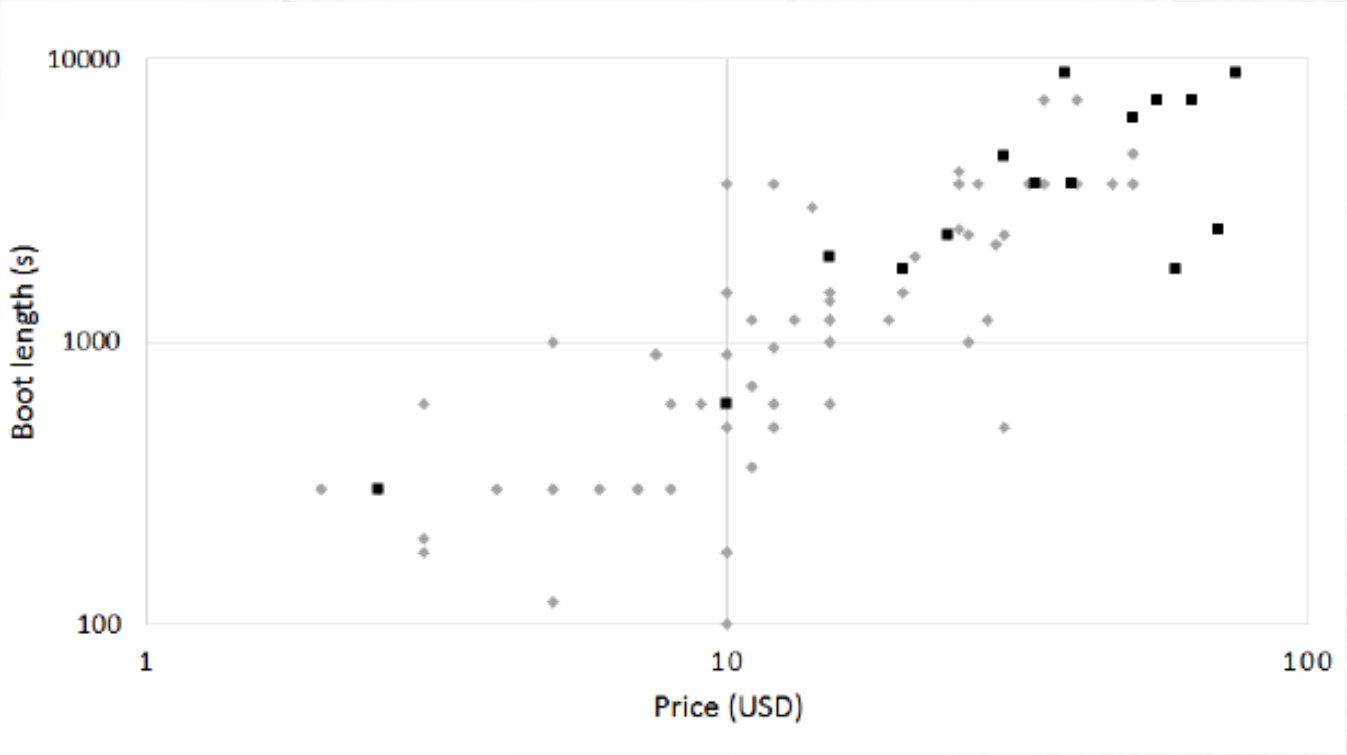
Situačné povedomie (III.)



Botnety a DDoS

- Infikované a vzdialene ovládateľné zariadenia – **boty (zombie)**
- botnet je zdroj mnohých hrozieb (click podvody, spam, phishing, disitribúcia malvéru, DoS)





Zdroj: http://ddosprogram.com/

BUKAC, Vit, et al. Service in Denial–Clouds Going with the Winds. In:*International Conference on Network and System Security*. Springer International Publishing, 2015. p. 130-143.

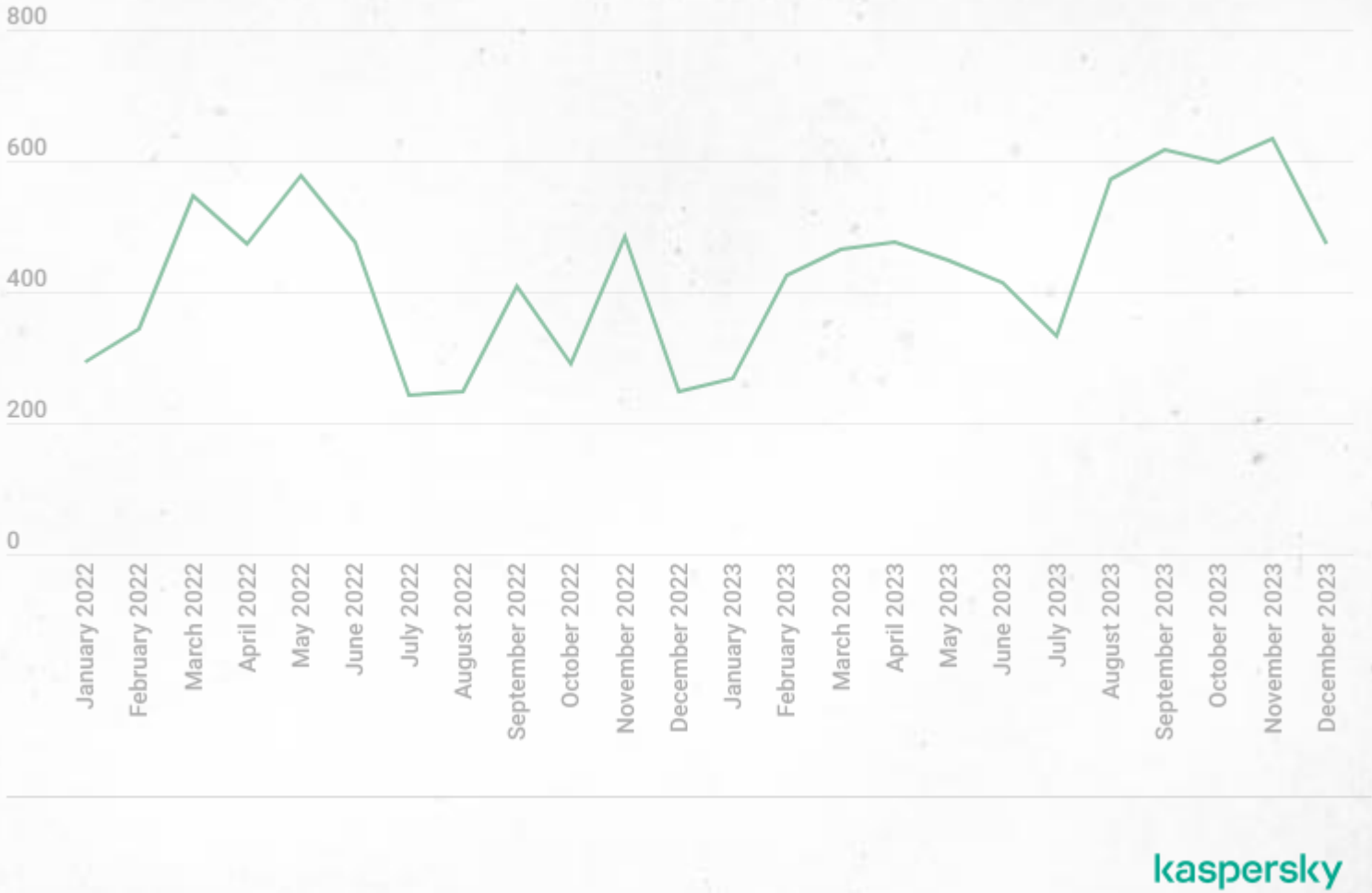
Zdroj: https://www.a-base.sk/sluzby/bezpecnost/

Vývoj ransomvéru (I.)

Zdroj: https://www.eset.com/sk/blog/firemna-it-bezpecnost/ransomver-sa-vyvija-zaplatte-inak-zverejnime-vase-data/

Vývoj ransomvéru (II.)

- Počet postov na ransomware blogoch, 2022 - 2023



Zdroj: https://securelist.com/darknet-predictions-for-2024/111763/

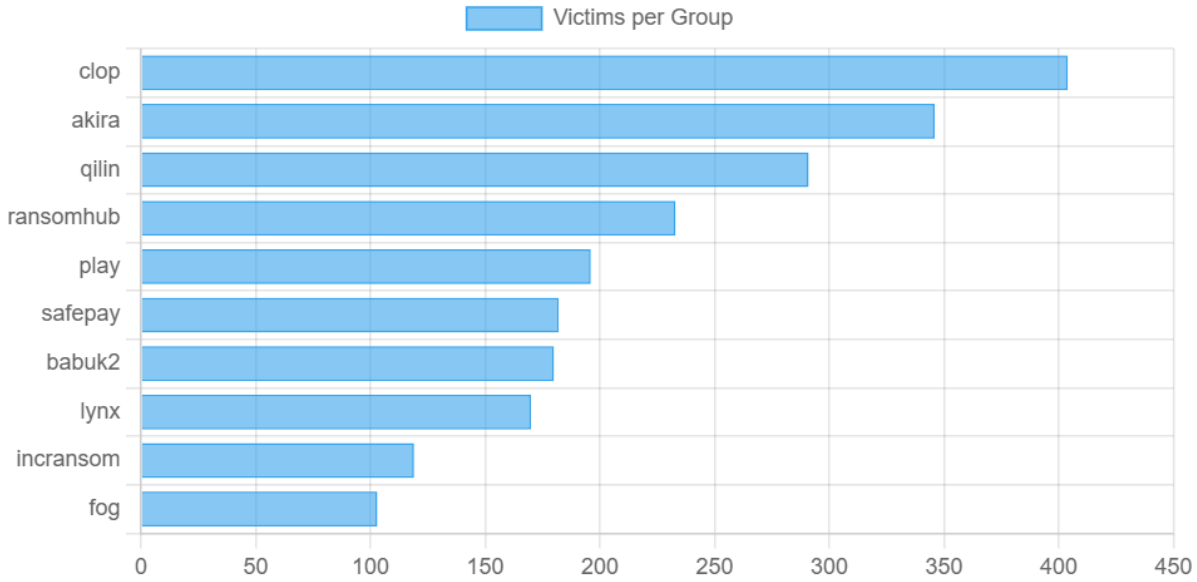
Vývoj ransomvéru (III.)

Ransomware Statistics for 2025

Total Victims for 2025: 3829

Total Groups: 268

Top 10 Groups



Zdroj: https://www.ransomware.live/

Vývoj ransomvéru (IV.)

All Groups

Group	Title	Status	Last seen	Location	Screenshot
0mega	0mega - Blog	🟢		omegalock5zxwbhswbisc42o2q2i54vdulyvtqqbudqousisjgc7j7yd.onion	📷
0mega	0mega - Blog	🟢		0mega.cc	📷
8base	Home	🔴	2023-11-03	basemmnnqwxevlymli5bs36o5ynti55xojzvn246spahniugwkff2pad.onion	📷
8base	Home	🔴	2024-03-19	xb6q2aggycmlcrjtbjendcnnwpmmwbosqaugxsqb4nx6cmod3emy7sad.onion	
Abrahams_Ax	Database Error	🔴	2024-02-09	abrahamm32umasogaqojib3ey2w2nwoafffrguq43tsyke4s3fz3w4yd.onion	📷
Abrahams_Ax		🔴	2024-02-09	abrahams-ax.se	📷
aGl0bGVyCg	Error Response Page	🔴	2022-10-30	hitleransomware.cf	
abyss	Abyss-data	🟢		3ev4metjirohtdpshsqlkrqcmxq6zu3d7obrdhglpy5jpbr7whmlfgqd.onion	📷
adminlocker	Admin Locker	🔴	2022-05-20	adminavf4cikzbv6mbbp7ujpwhygnn2t3egiz2pswldj32krrml42wyd.onion	
againstthewest	Threat Actors - Onion Forums - Internal Error	🔴	2023-01-07	giphvoitymatg4cv7bxqh5dz6sn6bfscywoat4qtslztkomf5lavrayd.onion	📷
akira		🟢		akiral2iz6a7qgd3ayp3l6yub7xx2uep76idk3u2kollpj5z3z636bad.onion	📷
akira		🔴	2021-05-01	akiralkzxzq2dsrzsrvbr2xgbbu2wgsmxryd4csgfameg52n7efvr2id.onion	
ako		🔴	2021-05-01	kwvhrdibgmmpkhkidrby4mccwqpds5za6uo2thcw5gz75qncv7rbhyad.onion	

Zdroj: https://www.ransomware.live/

Ransomware notes (I.)

All ransomware notes by groups

Note

> Ransomware notes are provided by Zscaler ThreatLabz under MIT License

8base	abysslocker	akira	alphv	atomsilo	avaddon	avoslocker	azov	beast	bianlian
biglock	bitpaymer	bitransomware	blackbasta	blackbyte	blackhunt	blackmatter	blacksnake	blacksuit	bluesky
cactus	cartel	cerber	chilelocker	cloak	clop	conti	cryptnet	cryptomix	cryptxxx
crytox	ctblocker	cuba	dagonlocker	darkangels	darkbit	darkpower	darkside	dataleak	deadbydawn
dharma	diavol	donut	doppelpaymer	dragonforce	ech0raix	esxiargs	ftcode	gandcrab	grief
gwisinlocker	h0lygh0st	hades	hive	hunters	icefire	inc	incransom	jaff	karakurt
karma	knight	lapiovra	lilith	lockbit	locky	lorenz	luckbit	lv	magniber
makop	mallox	maze	medusa	medusalocker	moneymessage	monti	nefilim	nemty	netwalker
nevada	noescape	nokoyawa	noname	novagroup	phobos	play	prometheus	qilin	qlocker
quantumlocker	ragnarlocker	ragnarok	rancoz	ransomexx	ransomhouse	ransomhub	ranzy	raworld	redalert
relic	revil	rhysida	rook	royal	rtmlocker	ryuk	scarecrow	schoolboys	shadow
slug	snatch	stop	sugar	suncrypt	teslacrypt	trigona	u-bomb	underground	vicesociety
vohuk	wastedlocker	xorist	yanluowang	zeon					

ast update : *Thursday 14/03/2024 20.59 (UTC)*

Zdroj: https://www.ransomware.live/

Ransomware notes (II.)

Ransom notes for group play

play

- ReadMe.txt

```
PLAY
news portal, tor network links:
mbrlkbtq5jonaqkurjwmxftytyn2ethqvbxfu4rgjbkkknndqwae6byd.onion
k7kg3jqxang3wh7hnmaiokchk7qoebupfgoik6rha6mjpzwupwtj25yd.onion
derdiarikucisv@gmx.de
```

- play.txt

```
PLAY
teilightomemaucd@gmx.com
```

Ransom notes for group medusa

medusa medusa

- !!!READ_ME_MEDUSA!!!.txt

```
$$\      $$\ $$$$$$$$\ $$$$$$$\  $$\   $$\  $$$$$$\   $$$$$$\
$$$\    $$$ |$$  _____|$$  __$$\ $$ |  $$ |$$  __$$\ $$  __$$\
$$$$\  $$$$ |$$ |      $$ |  $$ |$$ |  $$ |$$ /  \__|$$ /  $$ |
$$\$$\$$ $$ |$$$$$\    $$ |  $$ |$$ |  $$ |\$$$$$$\  $$$$$$$$ |
$$ \$$$  $$ |$$  __|   $$ |  $$ |$$ |  $$ | \____$$\ $$  __$$ |
$$ |\$  /$$ |$$ |      $$ |  $$ |$$ |  $$ |$$\   $$ |$$ |  $$ |
$$ | \_/ $$ |$$$$$$$$\ $$$$$$$  |\$$$$$$  |\$$$$$$  |$$ |  $$ |
\__|     \__|\________|\_______/  \______/  \______/ \__|  \__|
------------------------------[ Hello, [snip] !!! ]--------------------------

WHAT HAPPEND?
-------------------------------------------------------------
1. We have PENETRATE your network and COPIED data.
* We have penetrated entire network including backup system and researched all about your data.
* And we have extracted all of your networks including sub offices and your service clients networks valual

2. We have ENCRYPTED some your files.
While you are reading this message, it means you found your files and data has been ENCRYPTED by world's st
We have access to all of your sub offices and client service networks but didn't lock them all for your bra
We can solve this issue sliently and smoothly without 3rd parties and we decided lock only some of your ma:
But don't worry, we can restore everything to the original without harming your business.

There is only one possible way to get back your systems and business - CONTACT us via LIVE CHAT and pay fo
MEDUSA DECRYPTOR and DECRYPTION KEYs, Data deletion, Keep silent in media.
This MEDUSA DECRYPTOR will restore your entire network, This will take less than 1 business day.
```

Zdroj: https://www.ransomware.live/

Play (I.)

Ransom notes for group play

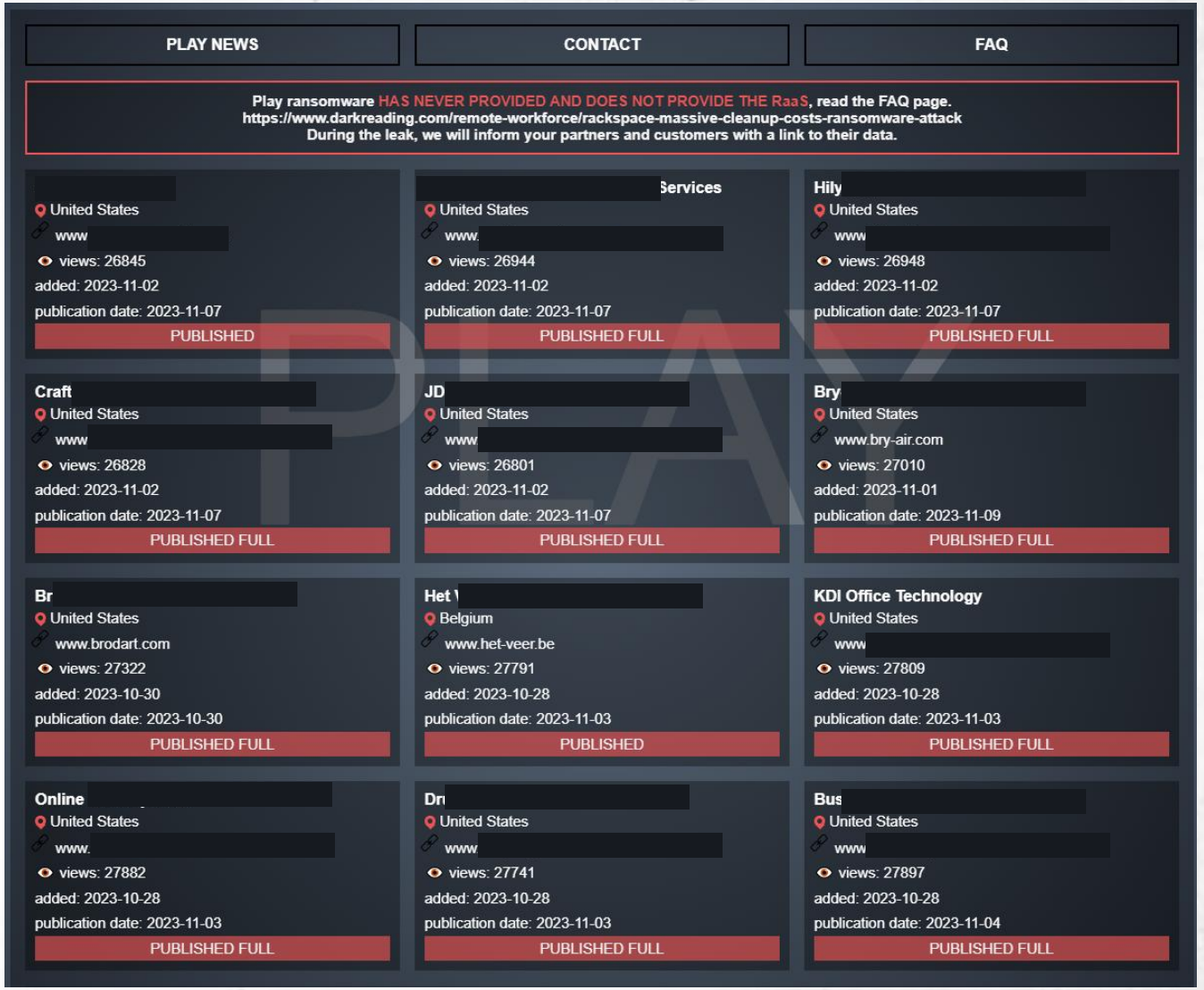
play

- ReadMe.txt

```
PLAY
news portal, tor network links:
mbrlkbtq5jonaqkurjwmxftytyn2ethqvbxfu4rgjbkkknndqwae6byd.onion
k7kg3jqxang3wh7hnmaiokchk7qoebupfgoik6rha6mjpzwupwtj25yd.onion
derdiarikucisv@gmx.de
```

- play.txt

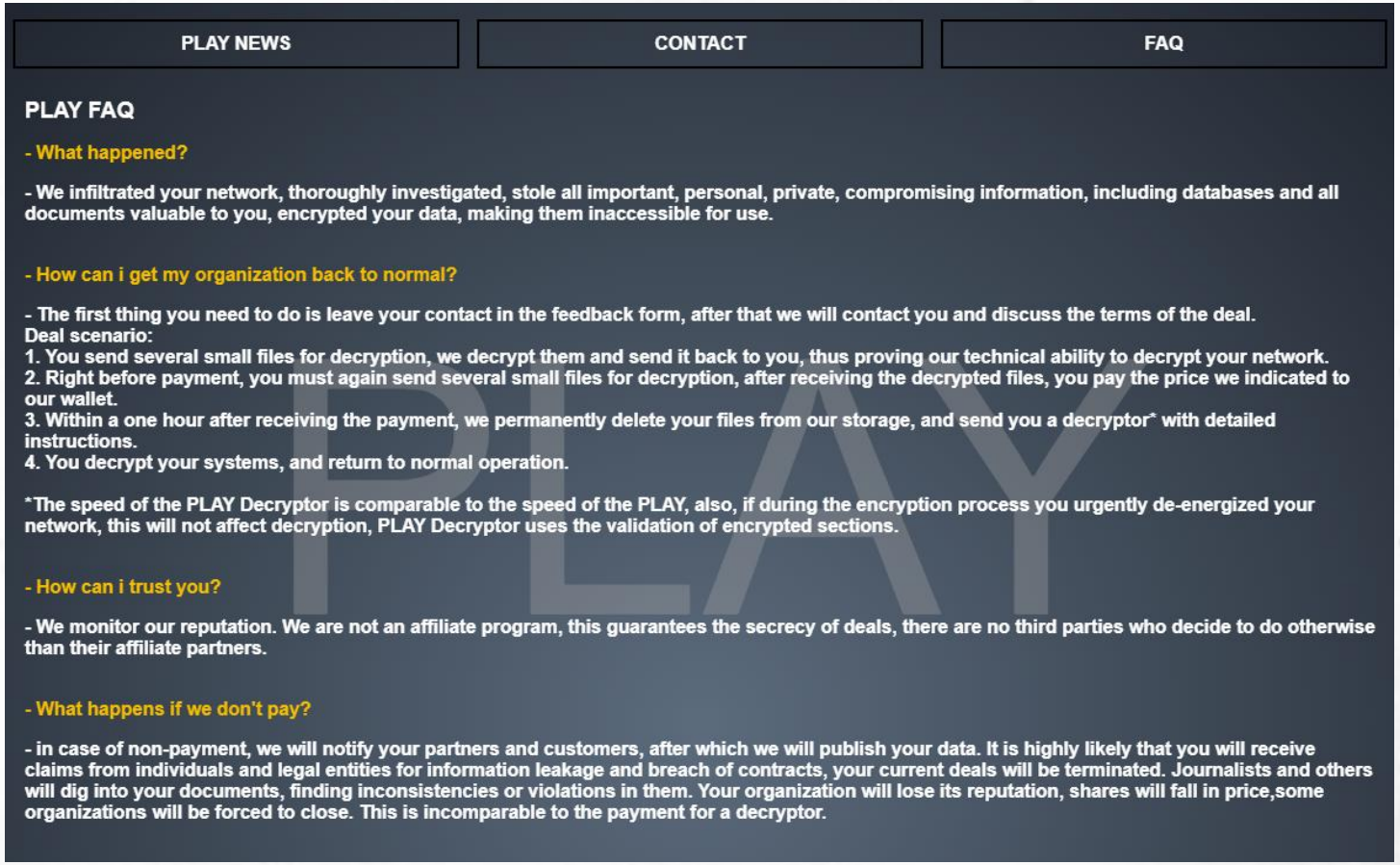
```
PLAY
teilightomemaucd@gmx.com
```



Zdroj: https://www.ransomware.live/

Play (II.)

- „Do not contact the FBI, police, or other government agencies. They do not care about your organization, they will not let you pay the ransom, which will entail the publication of files, after which courts, lawsuits, fines will begin.“



PLAY NEWS | CONTACT | FAQ

PLAY FAQ

- What happened?

- We infiltrated your network, thoroughly investigated, stole all important, personal, private, compromising information, including databases and all documents valuable to you, encrypted your data, making them inaccessible for use.

- How can i get my organization back to normal?

- The first thing you need to do is leave your contact in the feedback form, after that we will contact you and discuss the terms of the deal.
Deal scenario:
1. You send several small files for decryption, we decrypt them and send it back to you, thus proving our technical ability to decrypt your network.
2. Right before payment, you must again send several small files for decryption, after receiving the decrypted files, you pay the price we indicated to our wallet.
3. Within a one hour after receiving the payment, we permanently delete your files from our storage, and send you a decryptor* with detailed instructions.
4. You decrypt your systems, and return to normal operation.

*The speed of the PLAY Decryptor is comparable to the speed of the PLAY, also, if during the encryption process you urgently de-energized your network, this will not affect decryption, PLAY Decryptor uses the validation of encrypted sections.

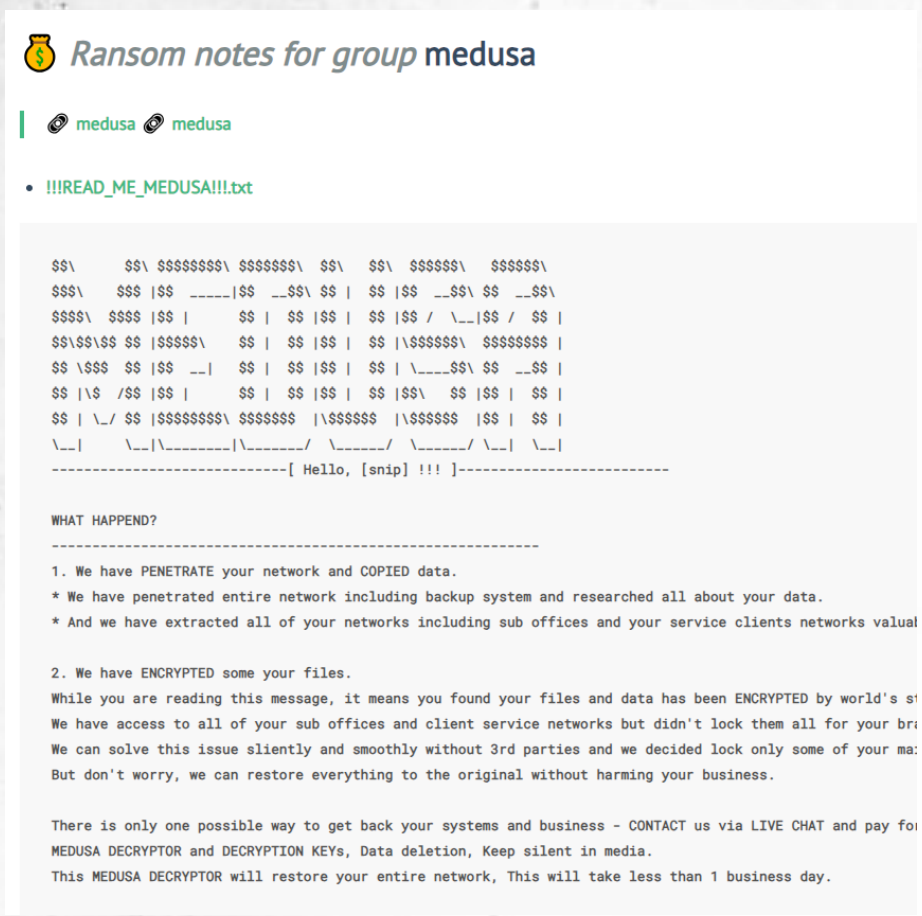
- How can i trust you?

- We monitor our reputation. We are not an affiliate program, this guarantees the secrecy of deals, there are no third parties who decide to do otherwise than their affiliate partners.

- What happens if we don't pay?

- in case of non-payment, we will notify your partners and customers, after which we will publish your data. It is highly likely that you will receive claims from individuals and legal entities for information leakage and breach of contracts, your current deals will be terminated. Journalists and others will dig into your documents, finding inconsistencies or violations in them. Your organization will lose its reputation, shares will fall in price,some organizations will be forced to close. This is incomparable to the payment for a decryptor.

Medusa



Ransom notes for group medusa

medusa medusa

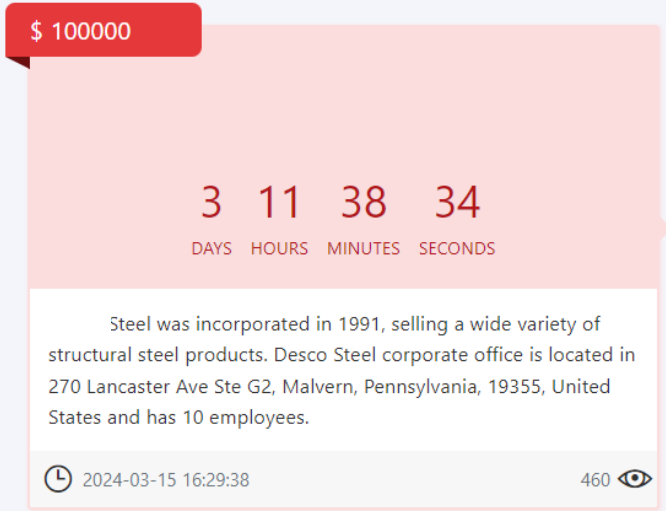
- !!!READ_ME_MEDUSA!!!.txt

```
$$\      $$\ $$$$$$$$\ $$$$$$$\  $$\   $$\  $$$$$$\   $$$$$$\
$$$\    $$$ |$$  _____|$$  __$$\ $$ |  $$ |$$  __$$\ $$  __$$\
$$$$\  $$$$ |$$ |      $$ |  $$ |$$ |  $$ |$$ /  \__|$$ /  $$ |
$$\$$\$$ $$ |$$$$$\    $$ |  $$ |$$ |  $$ |\$$$$$$\  $$$$$$$$ |
$$ \$$$  $$ |$$  __|   $$ |  $$ |$$ |  $$ | \____$$\ $$  __$$ |
$$ |\$  /$$ |$$ |      $$ |  $$ |$$ |  $$ |$$\   $$ |$$ |  $$ |
$$ | \_/ $$ |$$$$$$$$\ $$$$$$$  |\$$$$$$  |\$$$$$$  |$$ |  $$ |
\__|     \__|\________|\_______/  \______/  \______/ \__|  \__|
------------------------------[ Hello, [snip] !!! ]--------------------------

WHAT HAPPEND?
-------------------------------------------------------------
1. We have PENETRATE your network and COPIED data.
* We have penetrated entire network including backup system and researched all about your data.
* And we have extracted all of your networks including sub offices and your service clients networks valual

2. We have ENCRYPTED some your files.
While you are reading this message, it means you found your files and data has been ENCRYPTED by world's s
We have access to all of your sub offices and client service networks but didn't lock them all for your br
We can solve this issue sliently and smoothly without 3rd parties and we decided lock only some of your ma
But don't worry, we can restore everything to the original without harming your business.

There is only one possible way to get back your systems and business - CONTACT us via LIVE CHAT and pay fo
MEDUSA DECRYPTOR and DECRYPTION KEYs, Data deletion, Keep silent in media.
This MEDUSA DECRYPTOR will restore your entire network, This will take less than 1 business day.
```

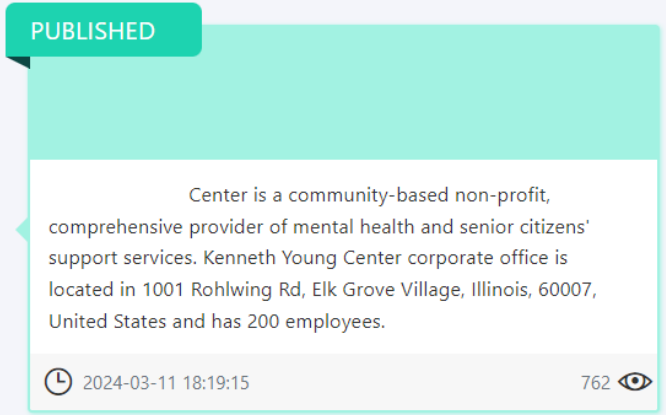


$ 100000

3 DAYS 11 HOURS 38 MINUTES 34 SECONDS

Steel was incorporated in 1991, selling a wide variety of structural steel products. Desco Steel corporate office is located in 270 Lancaster Ave Ste G2, Malvern, Pennsylvania, 19355, United States and has 10 employees.

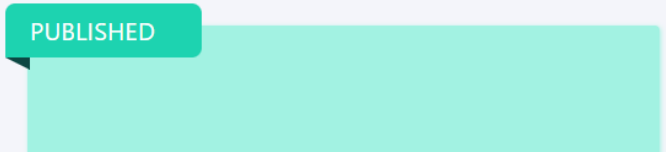
2024-03-15 16:29:38 460



PUBLISHED

Center is a community-based non-profit, comprehensive provider of mental health and senior citizens' support services. Kenneth Young Center corporate office is located in 1001 Rohlwing Rd, Elk Grove Village, Illinois, 60007, United States and has 200 employees.

2024-03-11 18:19:15 762



PUBLISHED

Zdroj: https://www.ransomware.live/

Zdroj: https://pentest-tools.com/blog/supply-chain-attacks

Dodávateľské vzťahy (I.)

živé Predplatné

20.1.2021 20:00 | Bezpečnosť

Útoky SolarWinds získali ďalší cenný skalp. Prienik priznal aj bezpečnostný špecialista Malwarebytes

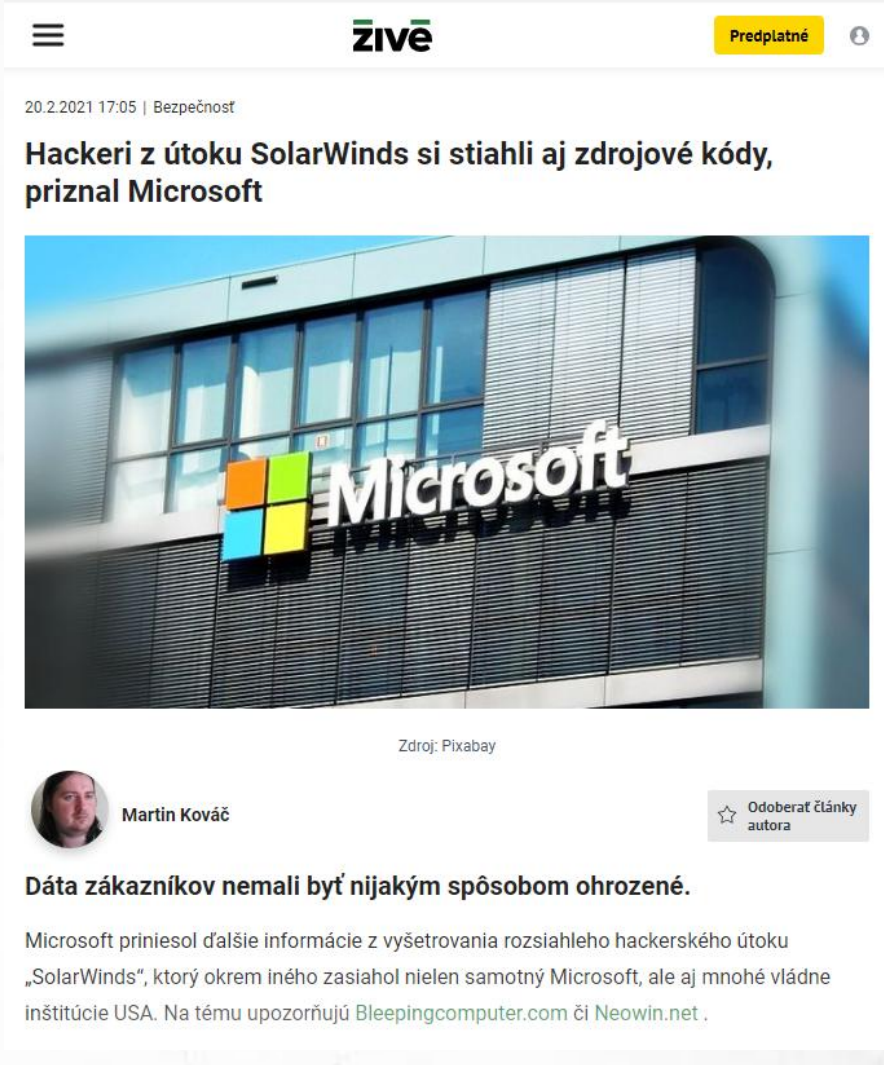
Zdroj: iStockphoto

Martin Kováč

Odoberať články autora

Medzi obeťami nájdeme aj Microsoft.

Bezpečnostná spoločnosť Malwarebytes s určitým oneskorením (napríklad voči priznaniu firmy Microsoft) oficiálne potvrdila , že sa taktiež stala obeťou takzvaného SolarWinds útoku.



živé Predplatné

20.2.2021 17:05 | Bezpečnosť

Hackeri z útoku SolarWinds si stiahli aj zdrojové kódy, priznal Microsoft

Zdroj: Pixabay

Martin Kováč

Odoberať články autora

Dáta zákazníkov nemali byť nijakým spôsobom ohrozené.

Microsoft priniesol ďalšie informácie z vyšetrovania rozsiahleho hackerského útoku „SolarWinds“, ktorý okrem iného zasiahol nielen samotný Microsoft, ale aj mnohé vládne inštitúcie USA. Na tému upozorňujú Bleepingcomputer.com či Neowin.net .

Zdroj: https://zive.aktuality.sk/clanok/150677/utoky-solarwinds-ziskali-dalsi-cenny-skalp-prienik-priznal-aj-bezpecnostny-specialista-malwarebytes/
https://zive.aktuality.sk/clanok/151230/hackeri-z-utoku-solarwinds-si-stiahli-aj-zdrojove-kody-priznal-microsoft/

Dodávateľské vzťahy (II.)

20.2.2021 17:05 | Bezpečnosť

Hackeri z útoku SolarWinds si stiahli aj zdrojové kódy, priznal Microsoft

Zdroj: Pixabay

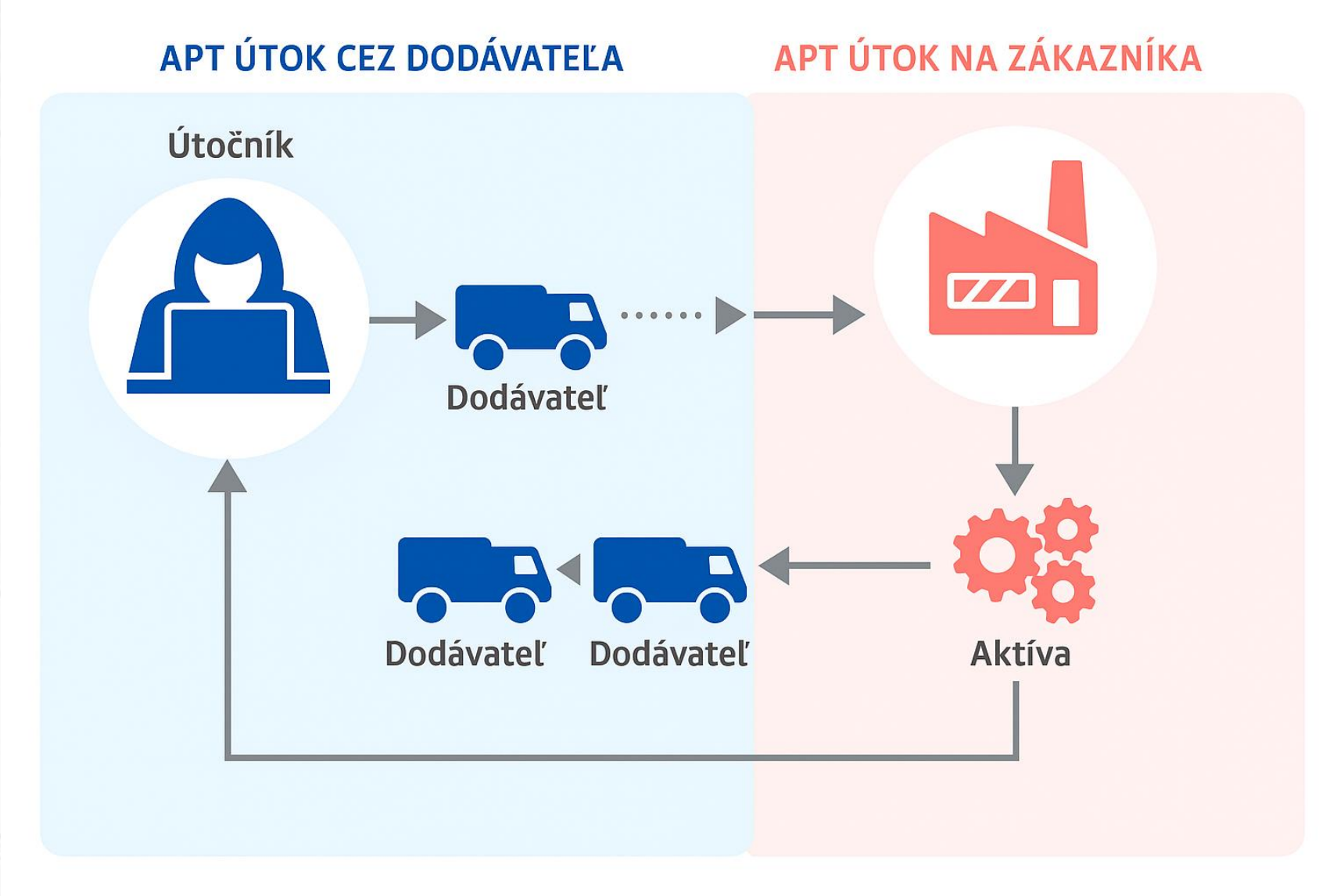
Martin Kováč

Dáta zákazníkov nemali byť nijakým spôsobom ohrozené.

Microsoft priniesol ďalšie informácie z vyšetrovania rozsiahleho hackerského útoku „SolarWinds“, ktorý okrem iného zasiahol nielen samotný Microsoft, ale aj mnohé vládne

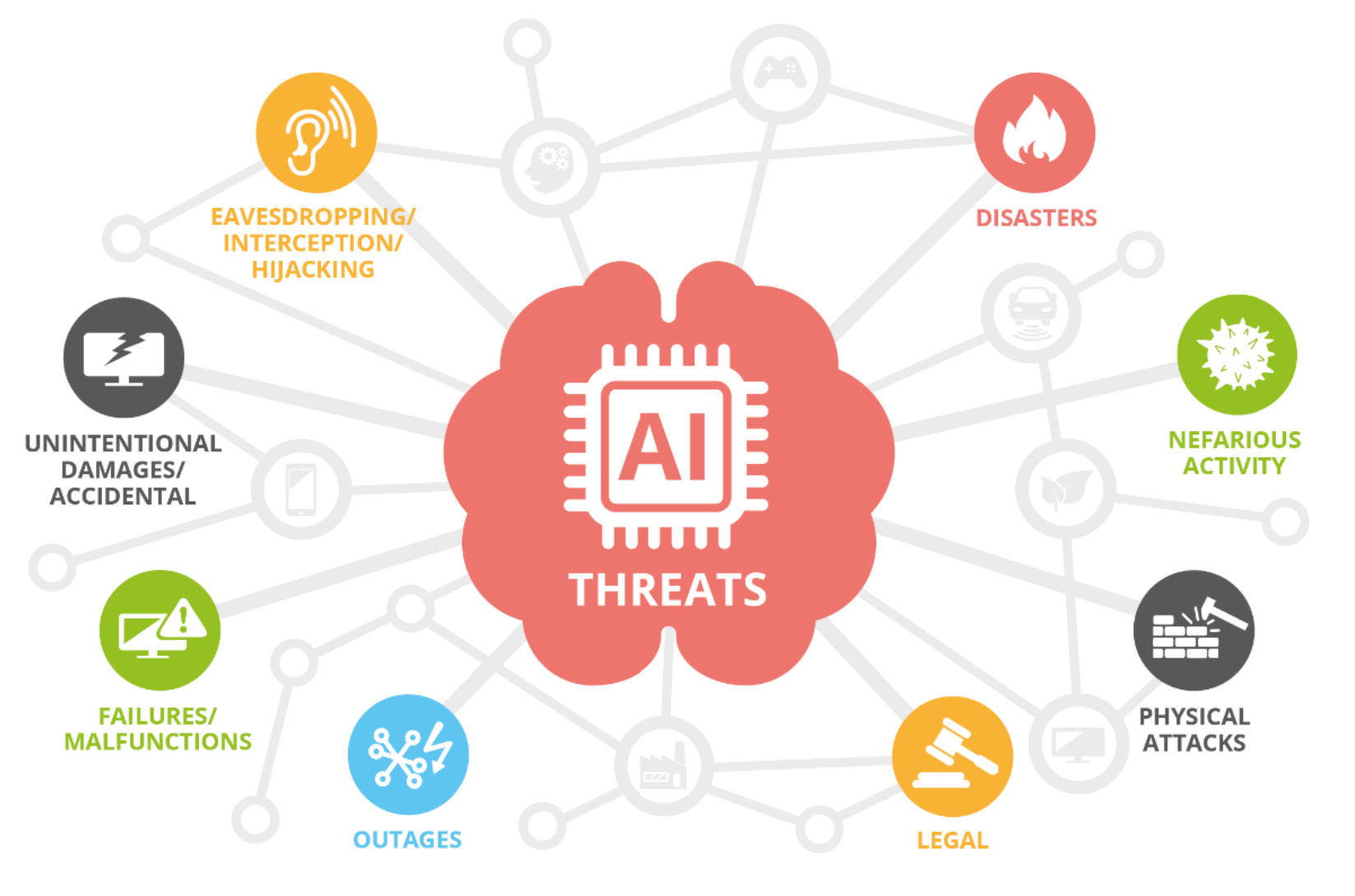
Zdroj: https://www.solarwinds.com/product-comparison/network-monitoring-solutions, https://zive.aktuality.sk/clanok/151230/hackeri-z-utoku-solarwinds-si-stiahli-aj-zdrojove-kody-priznal-microsoft/

Dodávateľské vzťahy (III.)



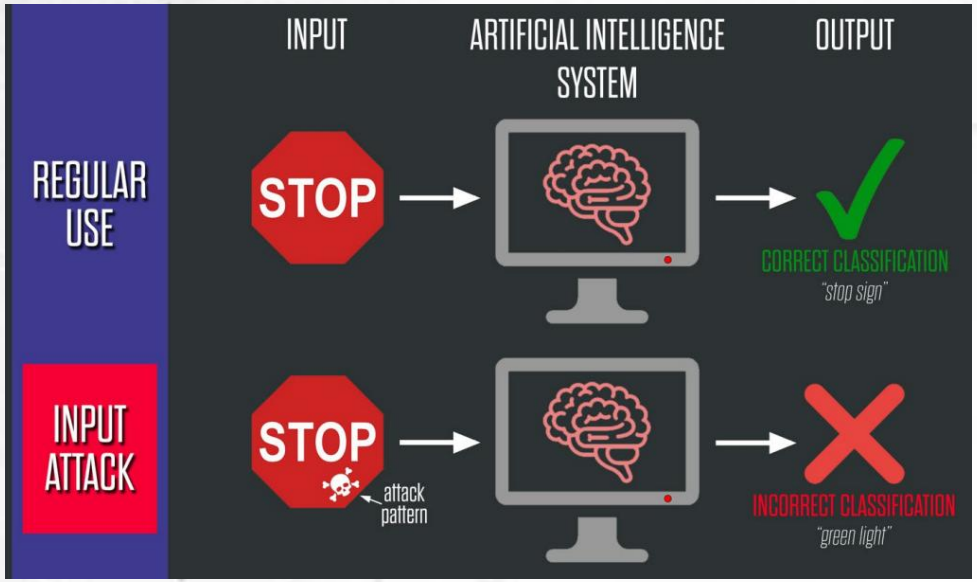
Zdroj: https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

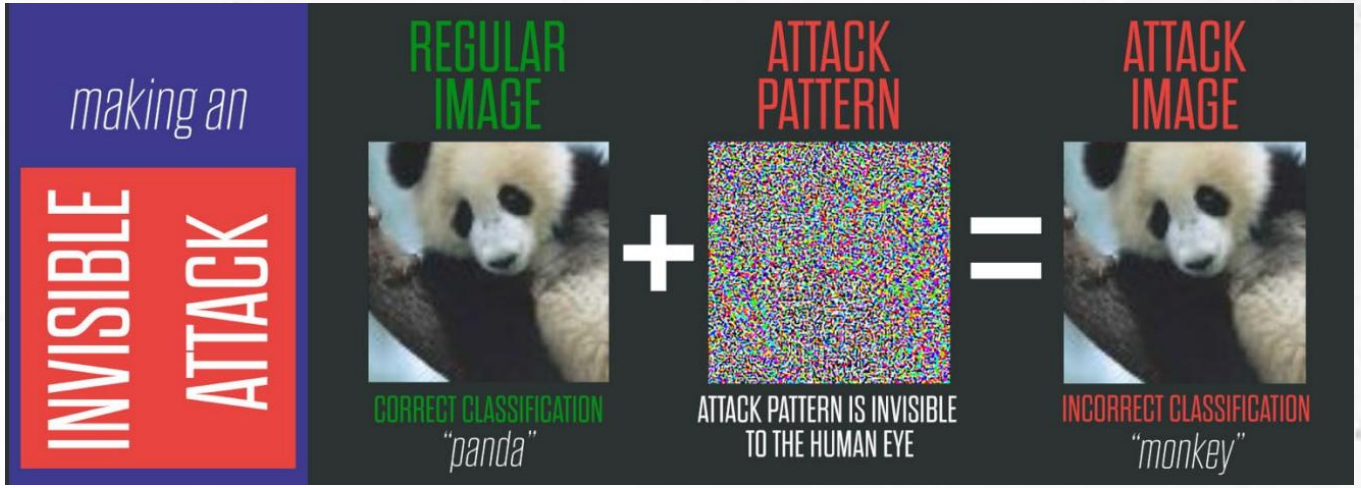
Bezpečnosť AI (I.)



Zdroj: https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges

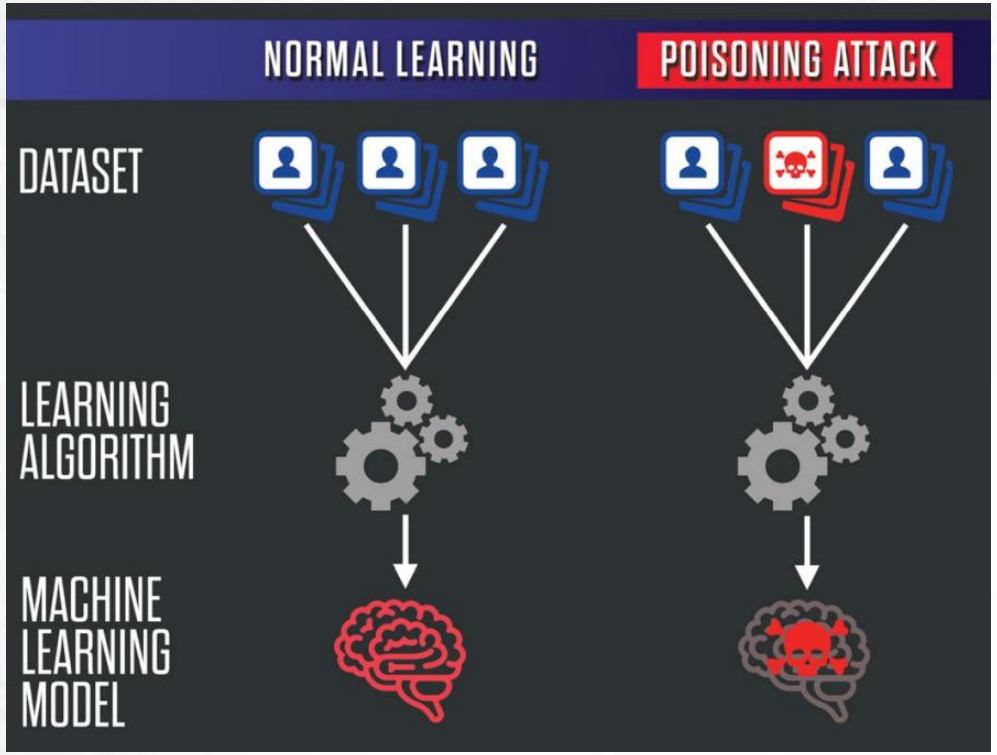
Bezpečnosť AI (II.)





Zdroj: https://www.belfercenter.org/sites/default/files/2019-08/AttackingAI/AttackingAI.pdf

Bezpečnosť AI (III.)



Dezinformačnej sieti sa podarilo úspešne ovplyvniť populárne AI nástroje

Tomas Valenta
Country Leader at Check Point Software Technologies Slovakia

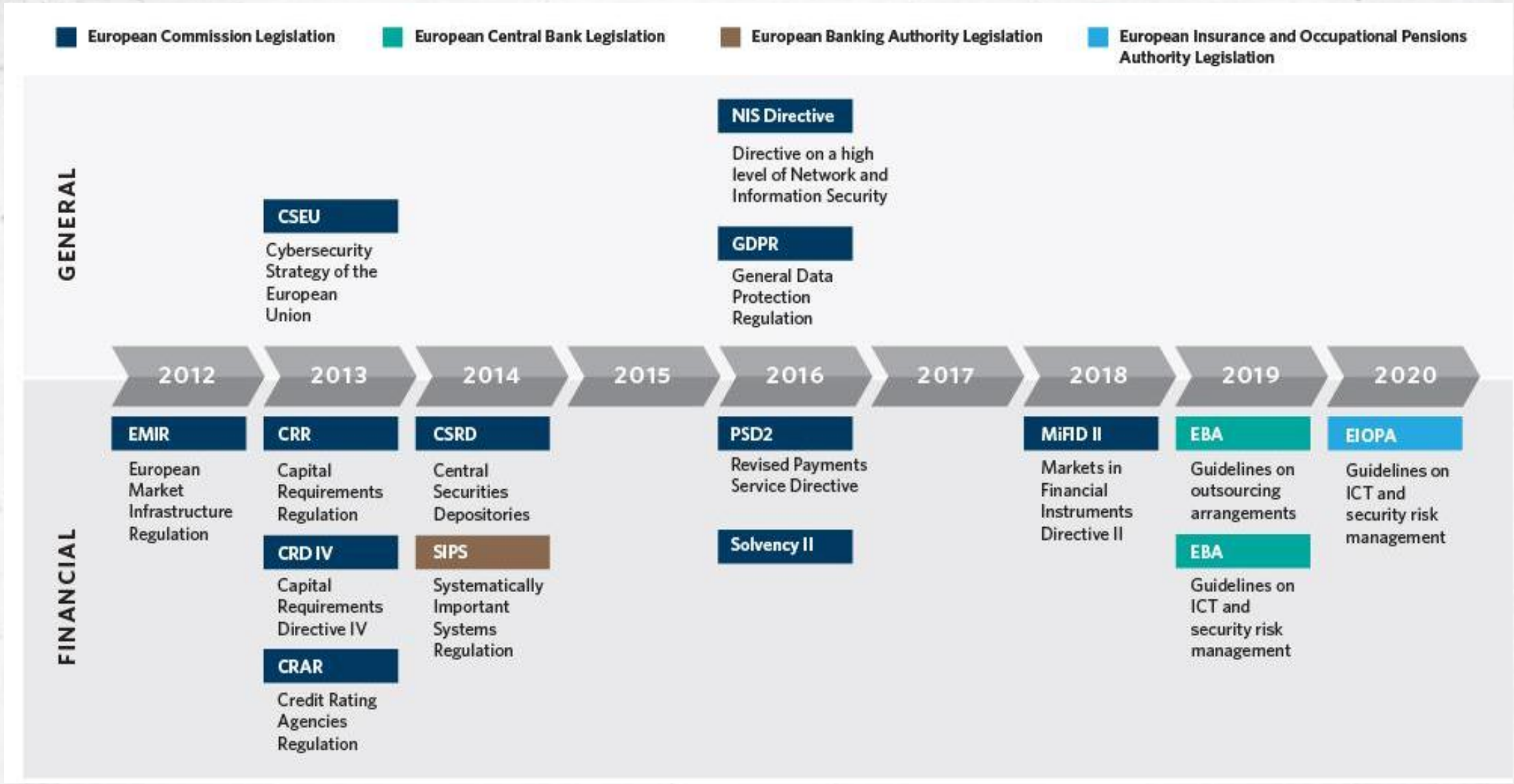
March 18, 2025

ChatGPT, Copilot, Meta AI, Gemini alebo Grok opakujú v tretine prípadov prokremeľské dezinformácie. Informuje o tom analýza spoločnosti NewsGuard.

Rozsiahla aktivita siete narúša spôsob, ako veľké jazykové modely spracúvajú informácie. Prenikanie ruskej propagandy do systémov umelej inteligencie spôsobuje šírenie nepravdivých

Zdroj: https://www.belfercenter.org/sites/default/files/2019-08/AttackingAI/AttackingAI.pdf, https://www.linkedin.com/pulse/dezinforma%C4%8Dnej-sieti-pravda-sa-podarilo-%C3%BAspe%C5%A1ne-ai-n%C3%A1stroje-valenta-qcjme/

Právna úprava KB (I.)



Zdroj: https://carnegieendowment.org/2021/03/16/european-union-cybersecurity-and-financial-sector-primer-pub-84055

Európska právna úprava (I.)

- Zmluva o EÚ a Zmluva o fungovaní EÚ
- Charta základných práv EÚ

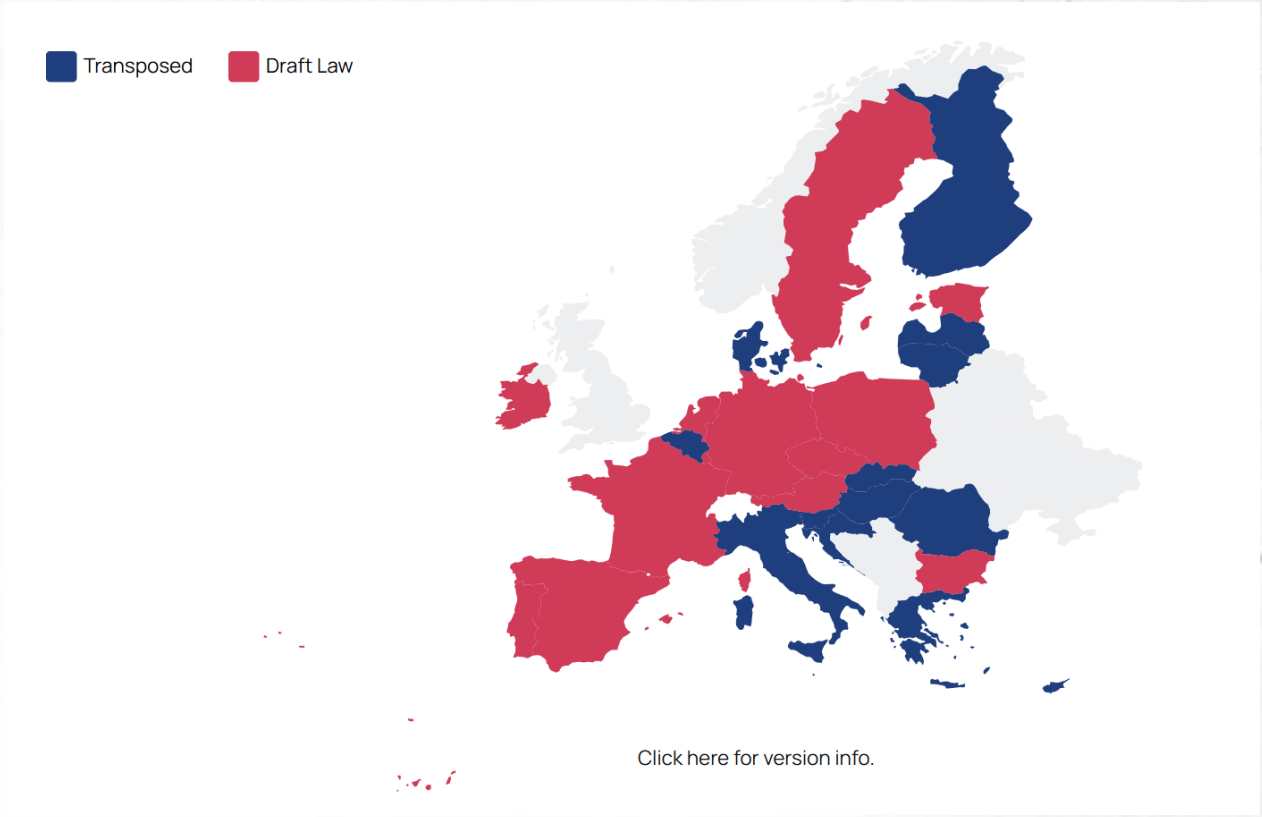
- NARIADENIE EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (**všeobecné nariadenie o ochrane údajov - GDPR**)

- SMERNICA EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2022/2555 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (**smernica NIS 2**)

Európska právna úprava (II.)

- smernica sa musí transponovať do právneho poriadku (nariadenie platí priamo)
- členské štáty mali transponovať smernicu do 17. októbra 2024 (SR – od 1.1.2025)
- implementácia do právnej úpravy v členských štátoch - organizácie sa musia prispôsobiť až po prijatí v danej krajine

- spolupráca pri zvládaní incidentov
- koordinované zverejňovanie zraniteľností
- riadenie kybernetických rizík



Zdroj: https://ecs-org.eu/activities/nis2-directive-transposition-tracker/

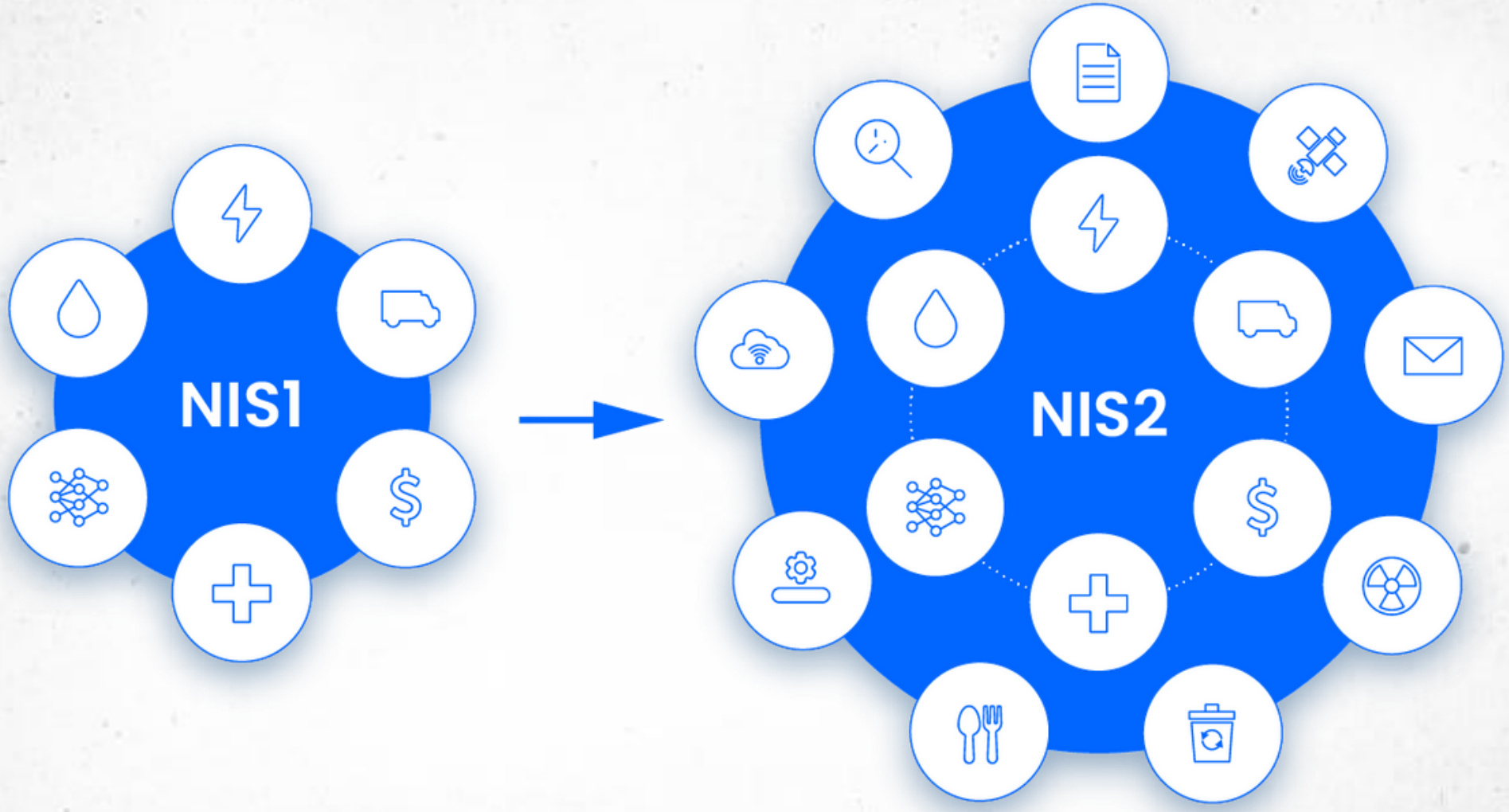
Európska právna úprava (III.)

Ciele:

- členské štáty boli primerane vybavené. Napríklad s tímom reakcie na incidenty počítačovej bezpečnosti (CSIRT)
- spoluprácu medzi všetkými členskými štátmi
- kultúra bezpečnosti v sektoroch, ktoré sú životne dôležité pre naše hospodárstvo a spoločnosť

- sprísniť uložené bezpečnostné požiadavky,
- riešiť bezpečnosť dodávateľského reťazca,
- zefektívniť ohlasovanie incidentov,
- posilniť opatrenia v oblasti dohľadu,
- zaviesť požiadavky na vymáhanie práva s harmonizovanými sankciami vo všetkých členských štátoch EÚ.

Európska právna úprava (IV.)



Zdroj: https://nis2directive.eu/

28.11.2024 12:05 | Bezpečnosť

Úroveň kybernetickej bezpeč sa zvýši

Zdroj: istock

TASR

Novela bude účinná od 1. januára 2

Zvýšenie úrovne kybernetickej bezpečnosti

rizík, ktoré sú spôsobené rýchlym technologickým vývojom a

Ako ovplyvní smernica NIS2 možnosť používať druhotný softvér?

redakcia touchIT 25. februára 2025

Tento článok je tlačová správa a je publikovaný bez redakčných úprav.

V decembri 2022 schválila Európska únia smernicu NIS2 (Network and Information System Directive 2), ktorá stanovuje pravidlá a požiadavky na kybernetickú bezpečnosť ICT systémov a sietí. Členské štáty EÚ mali implementovať NIS2 do svojich právnych poriadkov do 18. októbra 2024. Na Slovensku smernica nadobudla účinnosť 1. januára 2025. Ovplyvnia nové prísnejšie pravidlá

žnosť používania druhotného softvéru?

nyc digitalizáciou. To sú hlavné ciele novely zákona o kybernetickej

platná od 16. januára 2023.

Zdroj: https://zive.aktuality.sk/clanok/zpNPdfB/uroven-kybernetickej-bezpecnosti-na-slovensku-sa-zvysi/, https://touchit.sk/ako-ovplyvni-smernica-nis2-moznost-pouzivat-druhotny-softver/698207, https://touchit.sk/je-vasa-firma-pripravena-na-nis2/620047, https://zive.aktuality.sk/clanok/JExEku3/prezident-podpisal-novelu-zakona-o-kybernetickej-bezpecnosti-co-sa-meni/

Slovenská právna úprava (I.)

- Zákon č. 69/2018 Z. z. o **kybernetickej bezpečnosti** a o zmene a doplnení niektorých zákonov
  - Prevádzkovatelia základných služieb a prevádzkovatelia kritických základných služieb

- Zákon č. 95/2019 Z. z. o **informačných technológiách vo verejnej správe** a o zmene a doplnení niektorých zákonov (ZoITVS)
  - verejná správa – ministerstvá, mestá, obce, školy ...

- Zákon č. 18/2018 Z. z. o **ochrane osobných údajov** a o zmene a doplnení niektorých zákonov
  - Prevádzkovateľ, ktorý spracúva osobné údaje

- zákon č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (**zákon o e-Governmente**)
- zákon č. 452/2021 Z. Z. **o elektronických komunikáciách**
- zákon č. 215/2004 Z. z. o **ochrane utajovaných skutočností**

Slovenská právna úprava (II.)

- novela zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti

- rozšírenie povinných subjektov
- zrušenie dopadových a špecifických kritérií
- bezpečnosť dodávateľského reťazca

- neboli novelizované vykonávacie právne predpisy, resp. osobitná právna úprava

13.12.2024 18:40 | Bezpečnosť

Prezident podpísal novelu zákona o kybernetickej bezpečnosti, čo sa mení

Zdroj: istock

TASR

Novela bude účinná od 1. januára 2025.

Zdroj: https://zive.aktuality.sk/clanok/JExEku3/prezident-podpisal-novelu-zakona-o-kybernetickej-bezpecnosti-co-sa-meni/

Slovenská právna úprava (III.)

- § 17 ods. 1 písm. e) zákona o KB - osoba, ktorá spĺňa najmenej podmienky **veľkosti pre stredný podnik** a vykonáva činnosť v niektorom zo sektorov podľa prílohy č. 1 alebo prílohy č. 2 zákona o KB

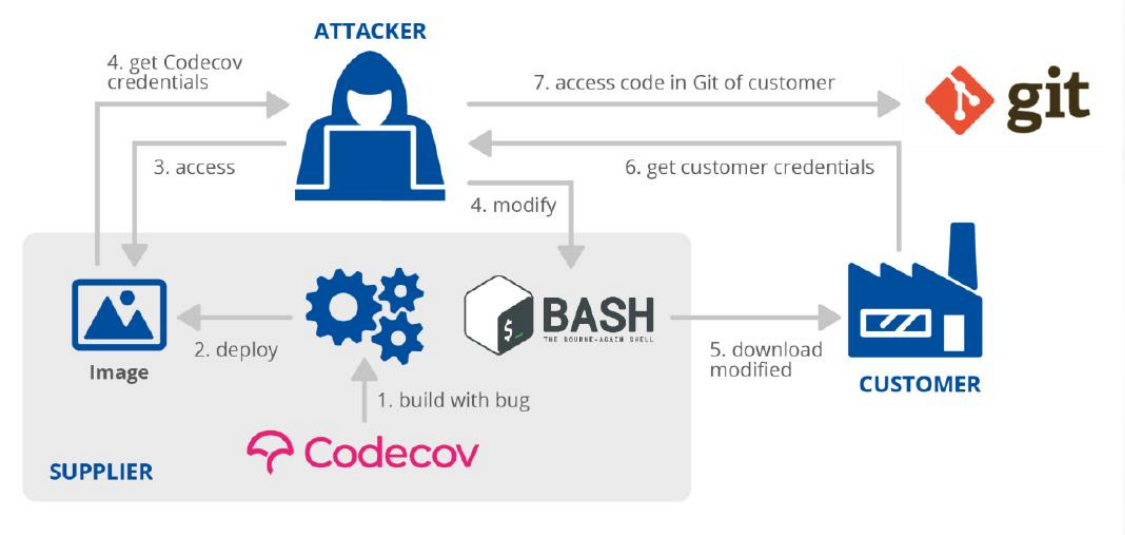
- odporúčanie Komisie 2003/361/ES
- **viac ako 50** zamestnancov a
- obrat alebo súvaha **nad 10 mil. €**

Zdroj: https://www.nbu.gov.sk/novela-kyberzakona-je-predo-dvermi-nbu-zverejnil-pomocku-pre-organizacie/

Slovenská právna úprava (IV.)

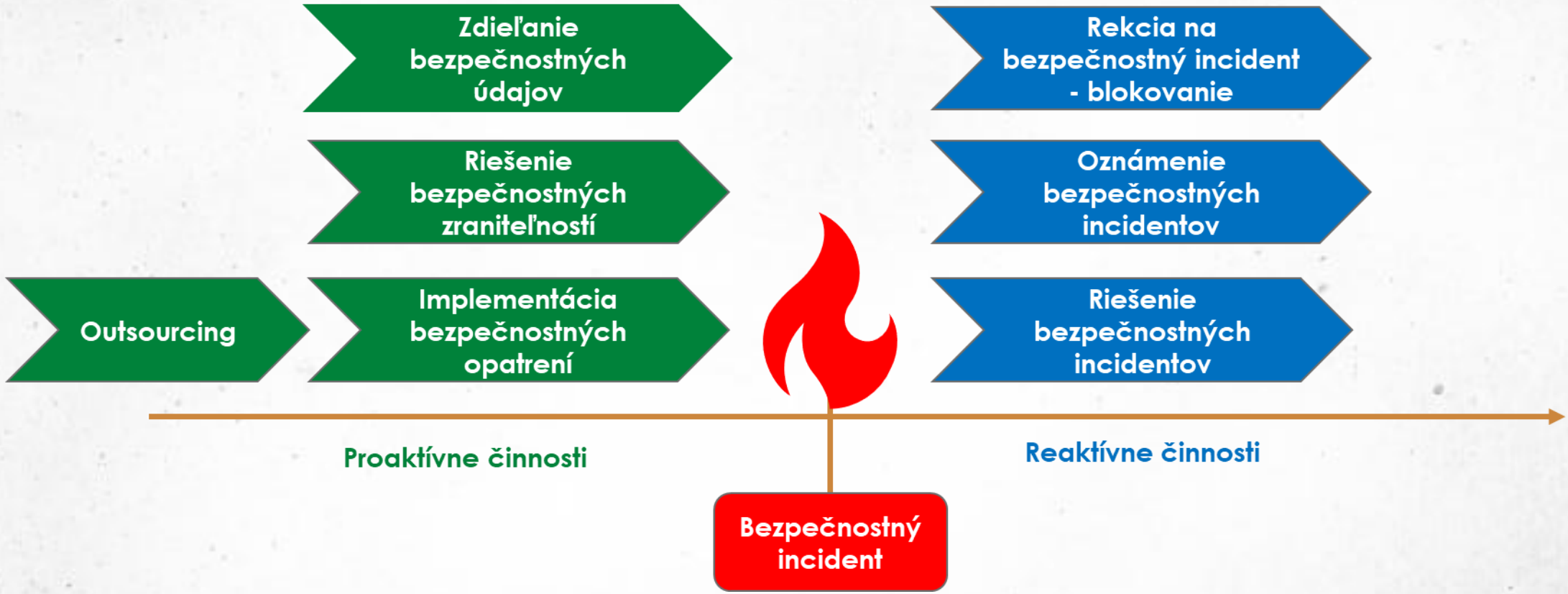
- rozšírenie pôsobnosti na **dodávateľské reťazce**

- § 17 ods. 1 písm. i) zákona o KB - tretia strana, ktorá má významný vplyv pri zabezpečovaní kybernetickej bezpečnosti, a má uzatvorenú zmluvu s prevádzkovateľom základnej služby, ktorý prevádzkuje kritickú základnú službu



Zdroj: https://thehackernews.com/2021/05/rapid7-source-code-breached-in-codecov.html

Slovenská právna úprava (V.)



Slovenská právna úprava (VI.)

- **§ 15 ods. 2 ZoKB - preventívne služby:**
  - vytváraním bezpečnostného povedomia,
  - výcvikom,
  - spoluprácou s ostatnými jednotkami CSIRT,
  - monitorovaním a evidenciou zraniteľností, kybernetických hrozieb, kybernetických kríz a kybernetických bezpečnostných incidentov,
  - pripojením na jednotný informačný systém kybernetickej bezpečnosti,
  - poskytovaním informácií a údajov do jednotného informačného systému kybernetickej bezpečnosti,
  - prijímaním a zasielaním včasného varovania pred kybernetickými bezpečnostnými incidentmi prostredníctvom jednotného informačného systému kybernetickej bezpečnosti,
  - poskytovaním pomoci s monitorovaním siete a informačného systému alebo vykonávaním takéhoto monitorovania po dohode so správcom siete alebo prevádzkovateľom siete alebo prevádzkovateľom informačného systému,

Slovenská právna úprava (VII.)

§ 15 ods. 3 ZoKB - reaktívne služby:

- výstraha a varovanie,
- detekcia kybernetických bezpečnostných incidentov,
- analýza kybernetických bezpečnostných incidentov,
- odozva, ohraničenie, riešenie a náprava následkov kybernetických bezpečnostných incidentov,
- asistencia pri riešení kybernetického bezpečnostného incidentu na mieste,
- reakcia na kybernetický bezpečnostný incident,
- podpora reakcií na kybernetické bezpečnostné incidenty,
- koordinácia reakcií na kybernetické bezpečnostné incidenty,
- návrh opatrení na zabránenie ďalšiemu pokračovaniu, šíreniu a opakovanému výskytu kybernetických bezpečnostných incidentov.

Mýtus – KB je súčasný fenomén

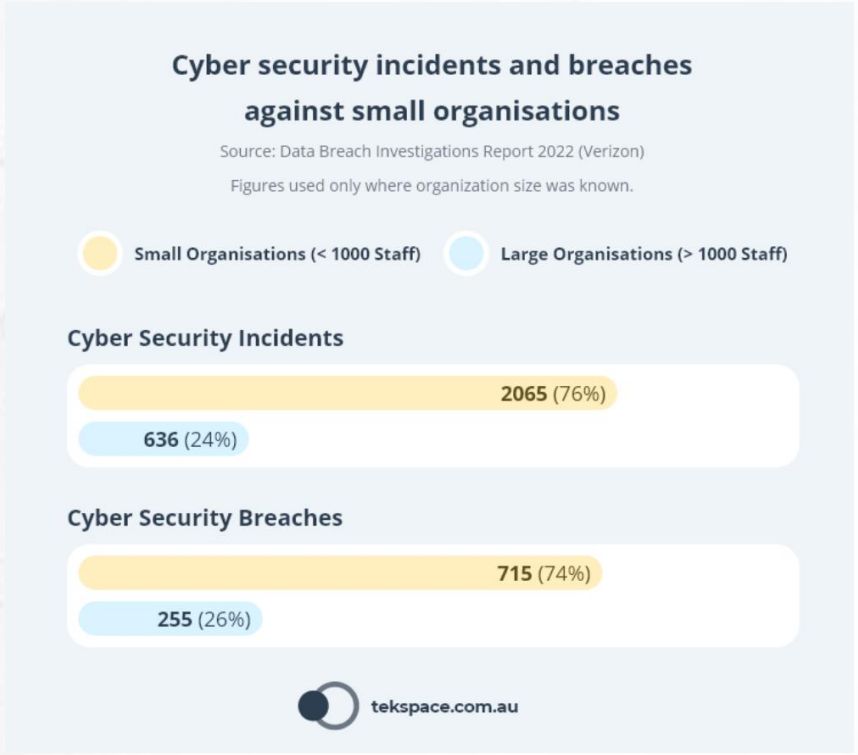
- bezpečnostné hrozby a bezpečnostné opatrenia existovali aj pred smernicou NIS, smernicou NIS 2 a zákonom o kybernetickej bezpečnosti

- povinnosť venovať sa informačnej a kybernetickej bezpečnosti bola už predtým
- rok 2000 - ISO/IEC 17799:2000
- rok 2022 - ISO/IEC 27002:2022

Zdroj: https://advisera.com/27001academy/explanation-of-11-new-iso-27001-2022-controls/

Mýtus – KB je problém veľkých a známych (I.)

- menšie podniky sú tiež cieľmi útokov
- útočníci sa zameriavajú na každého z nás



Zdroj: https://tekspace.com.au/articles/cyber-security-myths-misconceptions/, https://tvnoviny.sk/domace/clanok/932340-novy-typ-podvodu-cieli-na-seniorov-na-vylakanie-penazi-zneuzivaju-telefony

Mýtus – KB je problém veľkých a známych (II.)

- aj menšie podniky spadajú pod regulácie smernice NIS 2 a zákona o KB

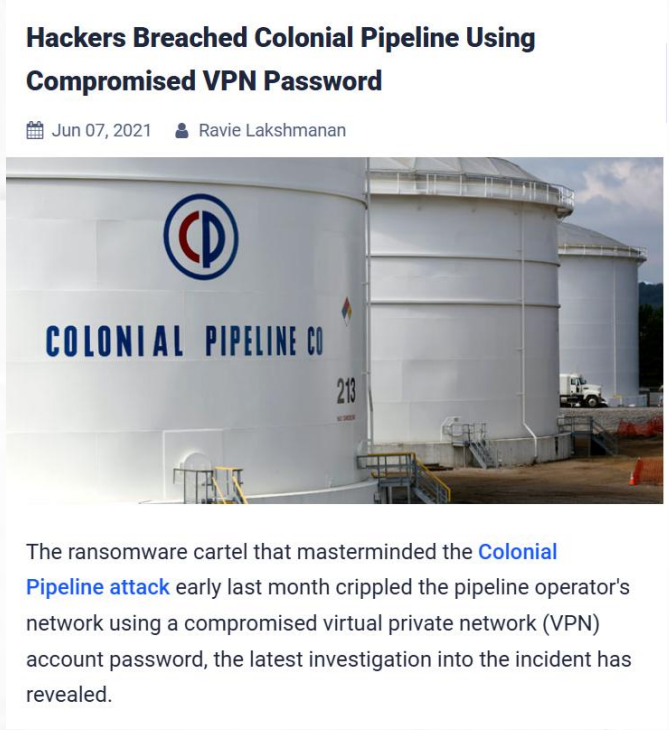
- § 17 ods. 1 písm. e) zákona o KB - osoba, ktorá spĺňa najmenej podmienky **veľkosti pre stredný podnik** a vykonáva činnosť v niektorom zo sektorov podľa prílohy č. 1 alebo prílohy č. 2 zákona o KB

- odporúčanie Komisie 2003/361/ES
- **viac ako 50** zamestnancov a
- obrat alebo súvaha **nad 10 mil. €**

Zdroj: https://www.nbu.gov.sk/novela-kyberzakona-je-predo-dvermi-nbu-zverejnil-pomocku-pre-organizacie/

Mýtus – KB je zodpovednosť len IT a MKB (I.)

- manažér kybernetickej bezpečnosti a zamestnanci IT nedokážu zabezpečiť všetko sami
- právna úprava vyžaduje integráciu kybernetickej bezpečnosti do riadenia organizácie
- zodpovednosť – štatutárny orgán



Hackers Breached Colonial Pipeline Using Compromised VPN Password

Jun 07, 2021 Ravie Lakshmanan

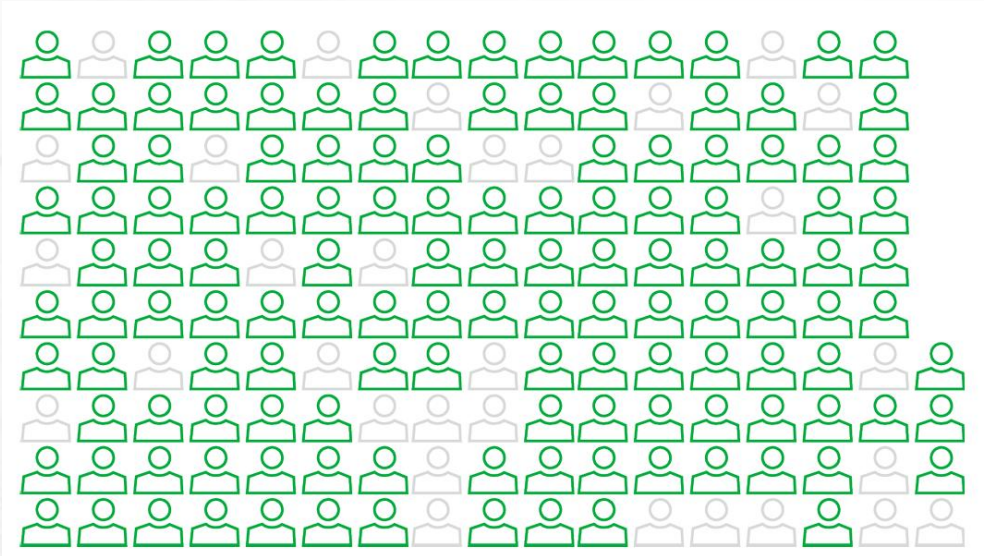
The ransomware cartel that masterminded the Colonial Pipeline attack early last month crippled the pipeline operator's network using a compromised virtual private network (VPN) account password, the latest investigation into the incident has revealed.

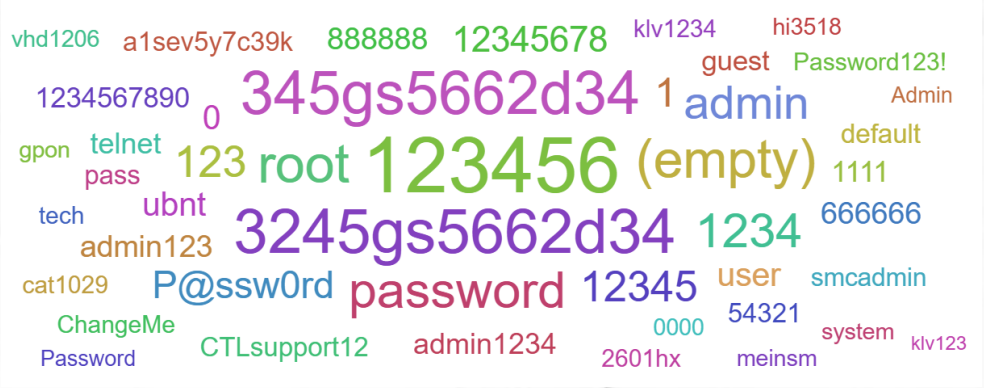
Zdroj: https://thehackernews.com/2021/06/hackers-breached-colonial-pipeline.html

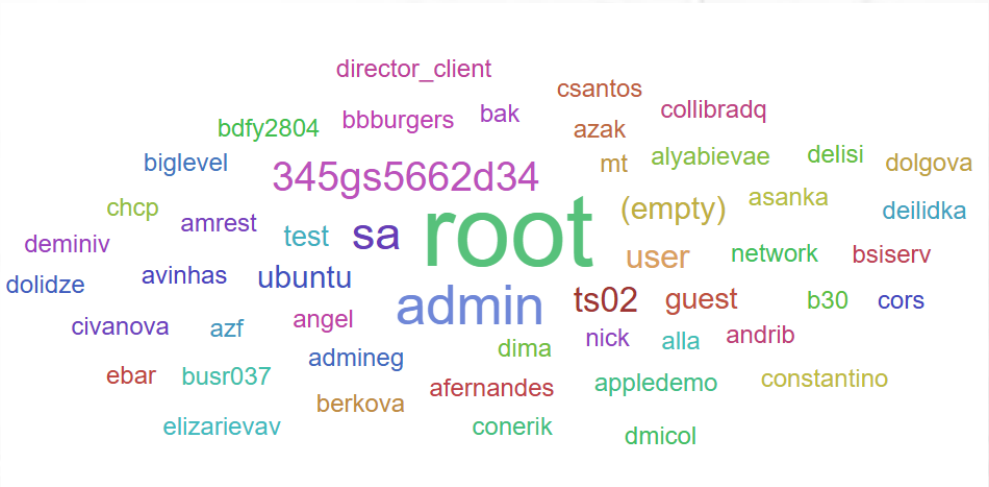
Mýtus – KB je zodpovednosť len IT a MKB (II.)

- každý zamestnanec nesie svoju mieru zodpovednosti.
- prevencia cez pravidelné školenia a budovanie bezpečnostnej kultúry.

82 %



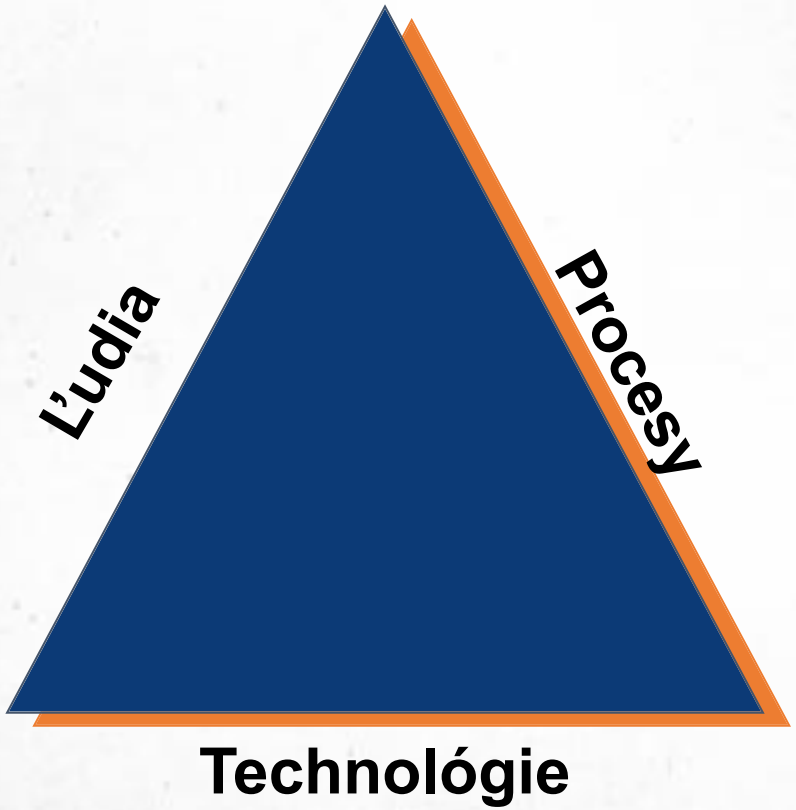


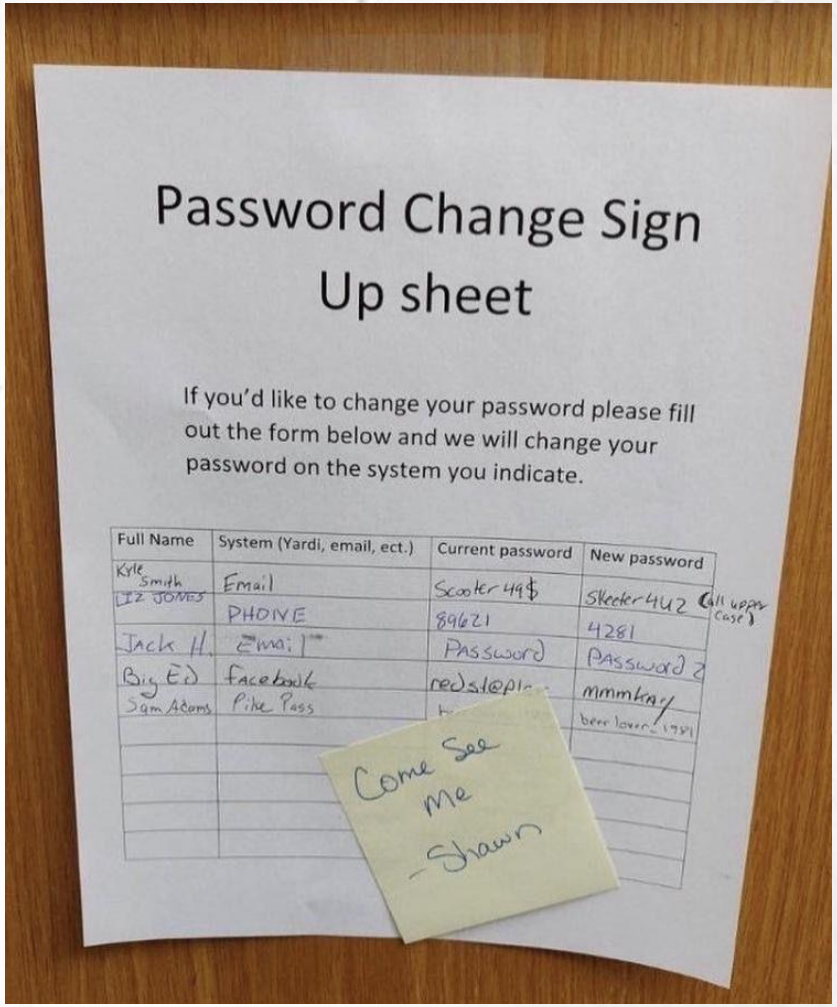


Zdroj: Verizon: DBIR Data Breach Investigations Report, 2022.

Mýtus – KB je jednorazový projekt (I.)

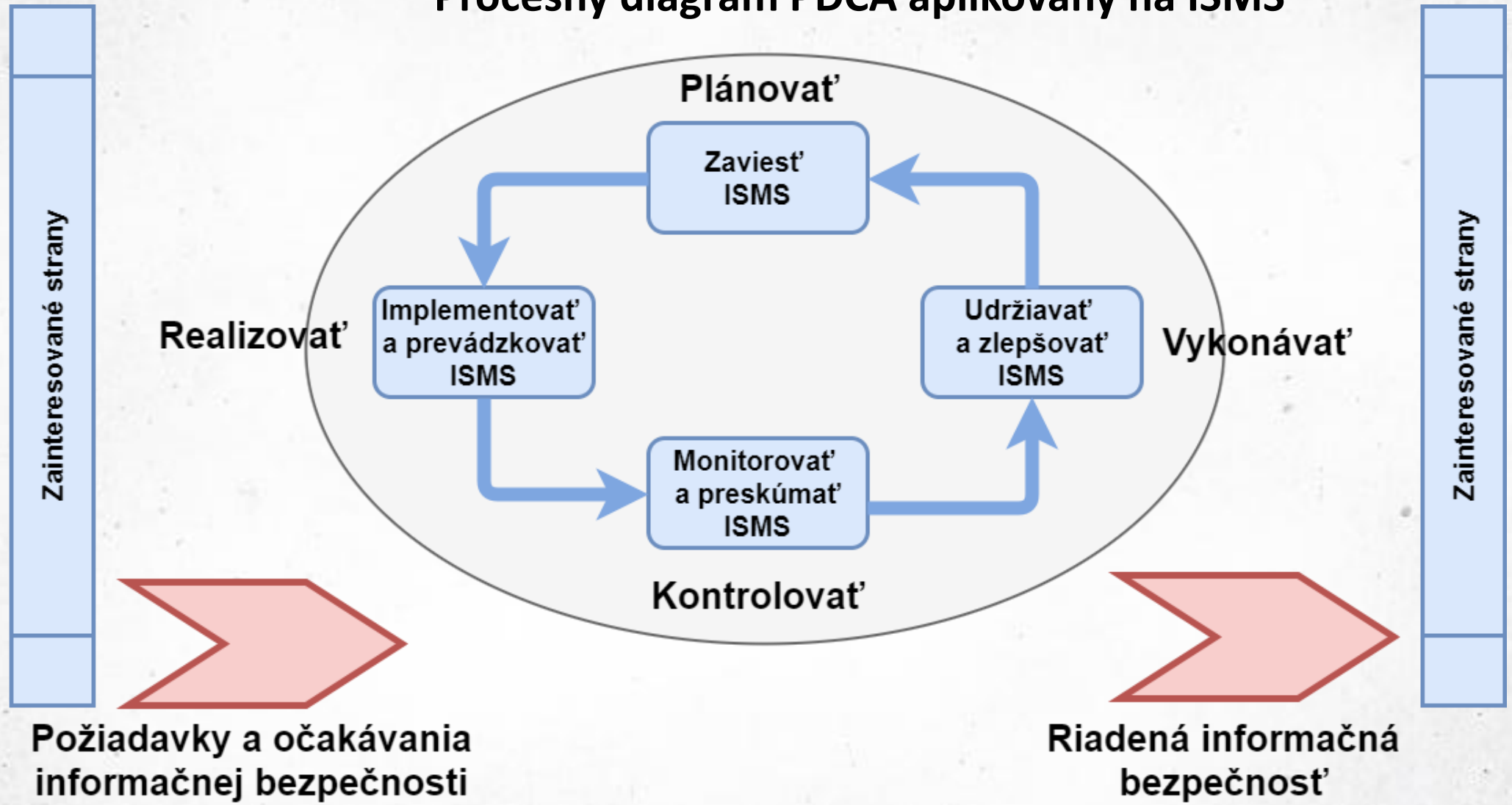
- kybernetická bezpečnosť je neustály proces, nie stav
- ide o prepojenie procesov, ľudí a technológií
- požadujte kvalitu a nenechajte sa odbiť zložitými pojmami (BIA, RTO, RPO, threat hunting, CTI, ...)



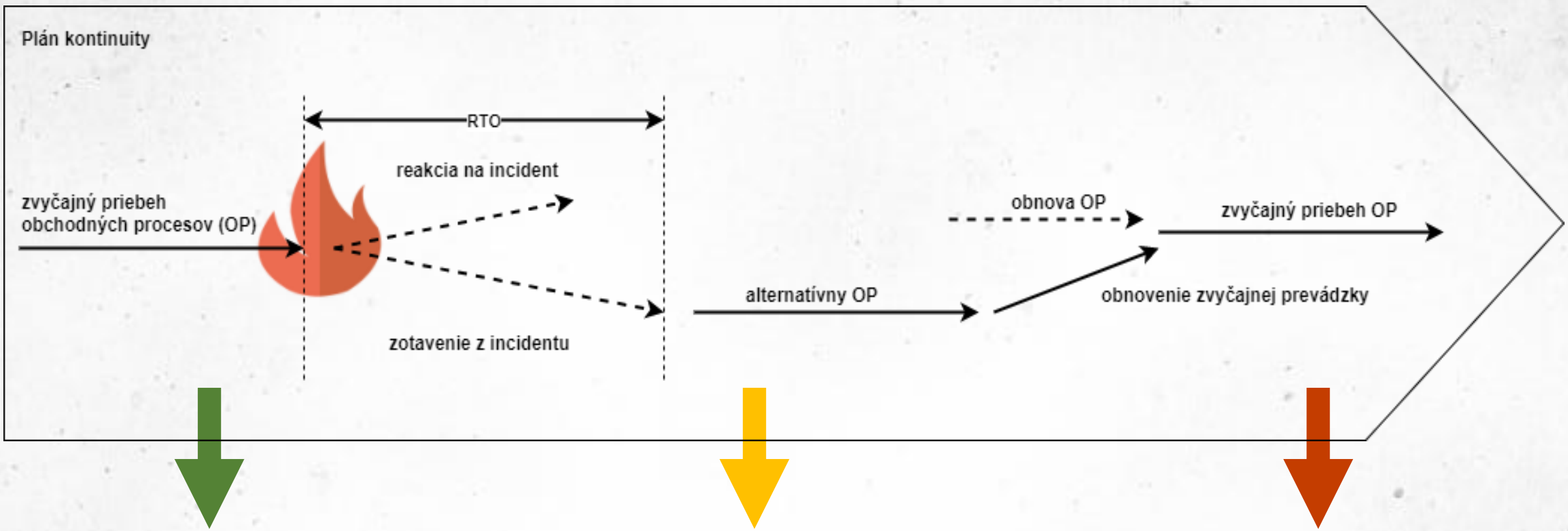


Mýtus – KB je jednorazový projekt (II.)

Procesný diagram PDCA aplikovaný na ISMS



Mýtus – KB je jednorazový projekt (III.)



Reakcia na incident

(IR)

Kontinuita činností

(BC)

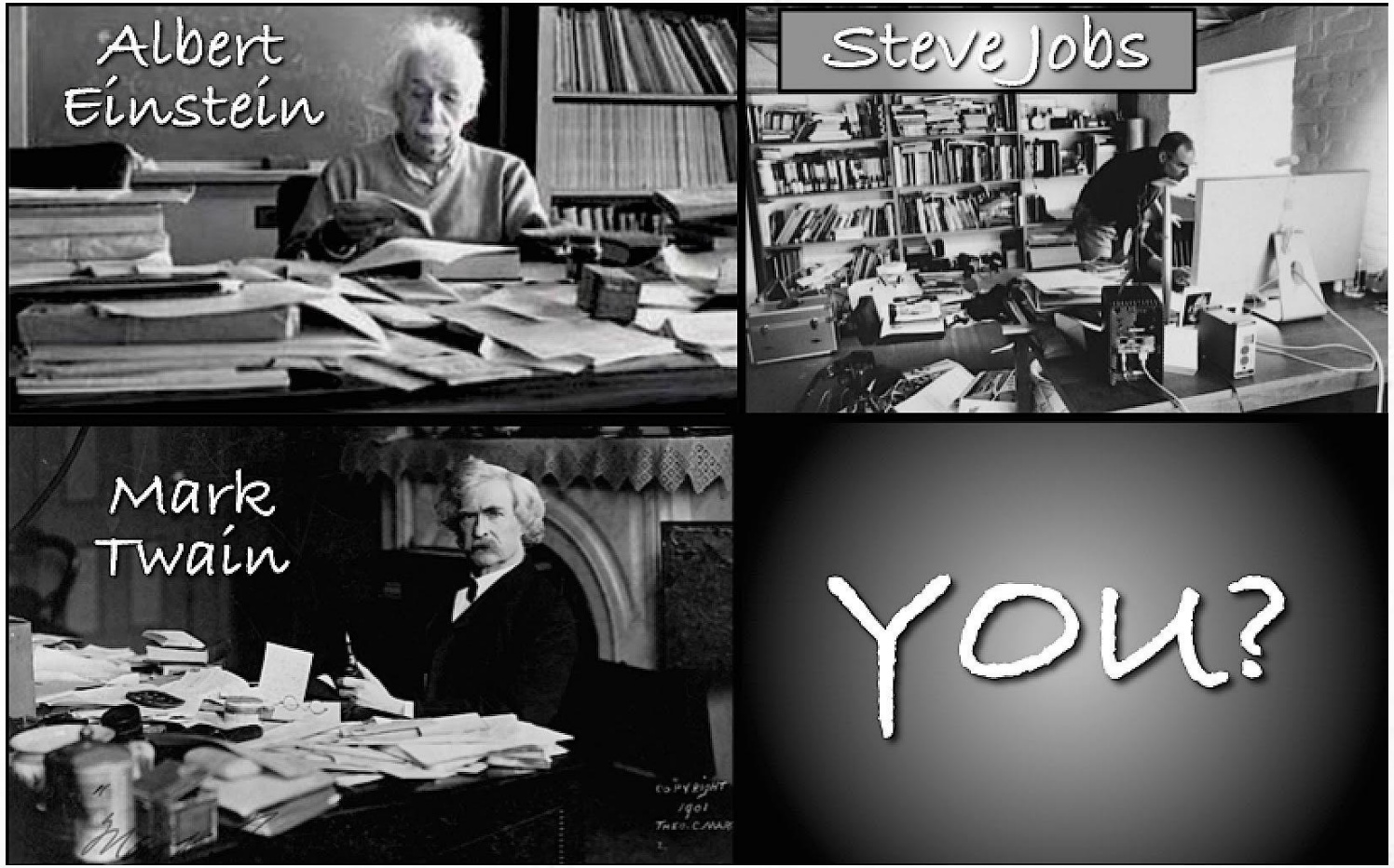
Obnova činností

(BR)

Zdroj: ISO/IEC 270035:2011

Pravidlá čistého stola (I.)

„Ak preplnený stôl znamená preťaženú myseľ, čo potom znamená prázdny stôl?“
Albert Eistein

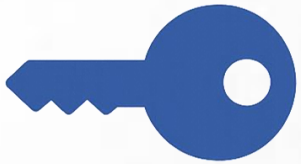


Zdroj: https://privacymatters.ubc.ca/desk-test-answers

Pravidlá čistého stola (II.)

(1) Na konci pracovnej doby odstrániť z povrchu pracovného stolu všetky zložky na dokumenty, pamäťové médiá a uložiť ich do uzamkýnateľného priestoru.

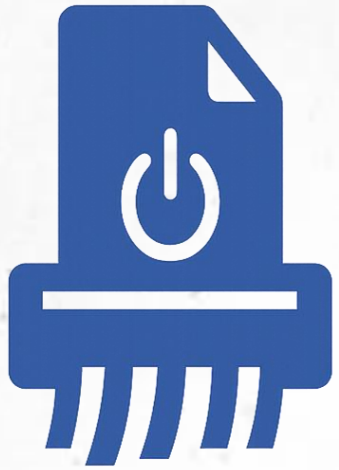
(2) Kľúče od uzamkýnateľných priestorov nesmú byť voľne dostupné.



(3) Okamžite po vytlačení odstrániť dokumenty z tlačiarní alebo kopírovacích zariadení.

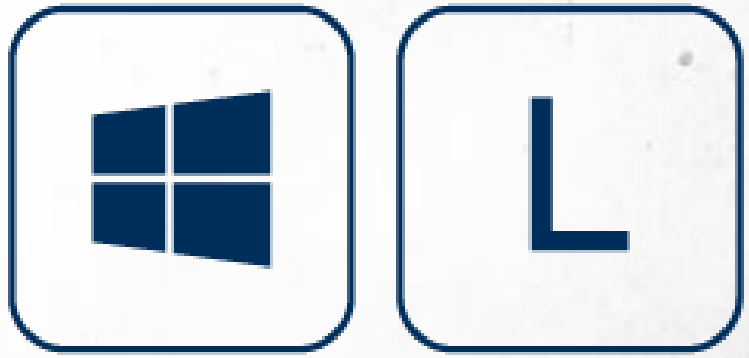
Pravidlá čistého stola (III.)

(4) Citlivé dokumenty musia byť zničené pomocou skartovacieho zariadenia.



(5) Po skončení práce vypnúť počítač.

(6) Pri každom opustení pracovného miesta uzamknúť počítač heslom.



(7) Otvorené programy po ukončení práce odhlásiť.

Pravidlá čistého stola (II.)

(8) Pri prenose notebookov, smartfonov a iných mobilných zariadení je zakázané ponechávať tieto zariadenia bez dozoru.

(9) Ponechať mobilné zariadenia v automobile (aj v uzamknutom) bez dozoru je prísne zakázané.

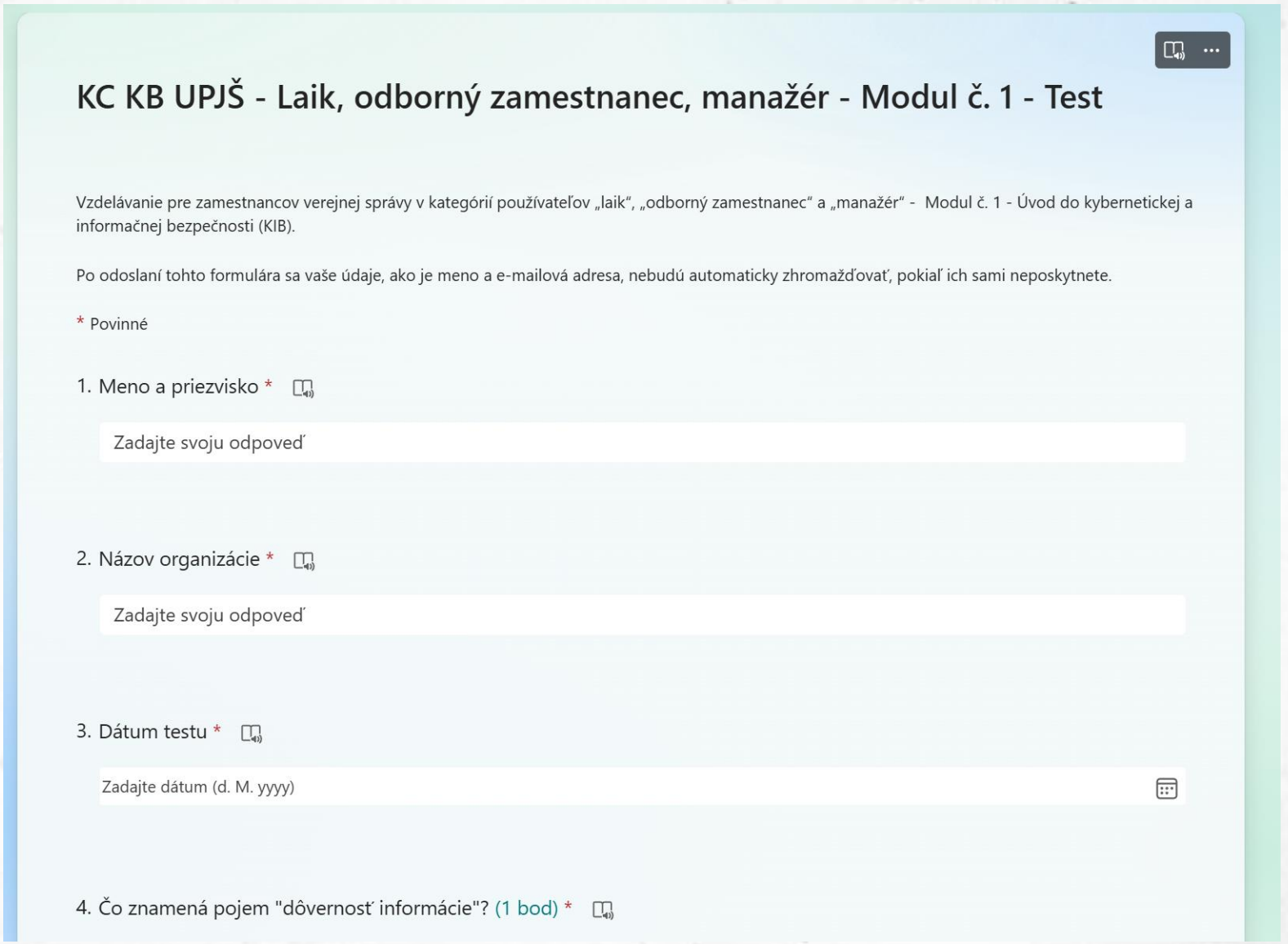
(10) Zatvárať dvere po vstupe do miestnosti chránenej prístupovým systémom.

Zdroj: https://privacymatters.ubc.ca/desk-test-answers

Zdroj: https://privacymatters.ubc.ca/desk-test-answers

Záverečný test

- Test: ...



KC KB UPJŠ - Laik, odborný zamestnanec, manažér - Modul č. 1 - Test

Vzdelávanie pre zamestnancov verejnej správy v kategórií používateľov „laik", „odborný zamestnanec" a „manažér" - Modul č. 1 - Úvod do kybernetickej a informačnej bezpečnosti (KIB).

Po odoslaní tohto formulára sa vaše údaje, ako je meno a e-mailová adresa, nebudú automaticky zhromažďovať, pokiaľ ich sami neposkytnete.

* Povinné

1. Meno a priezvisko *

Zadajte svoju odpoveď

2. Názov organizácie *

Zadajte svoju odpoveď

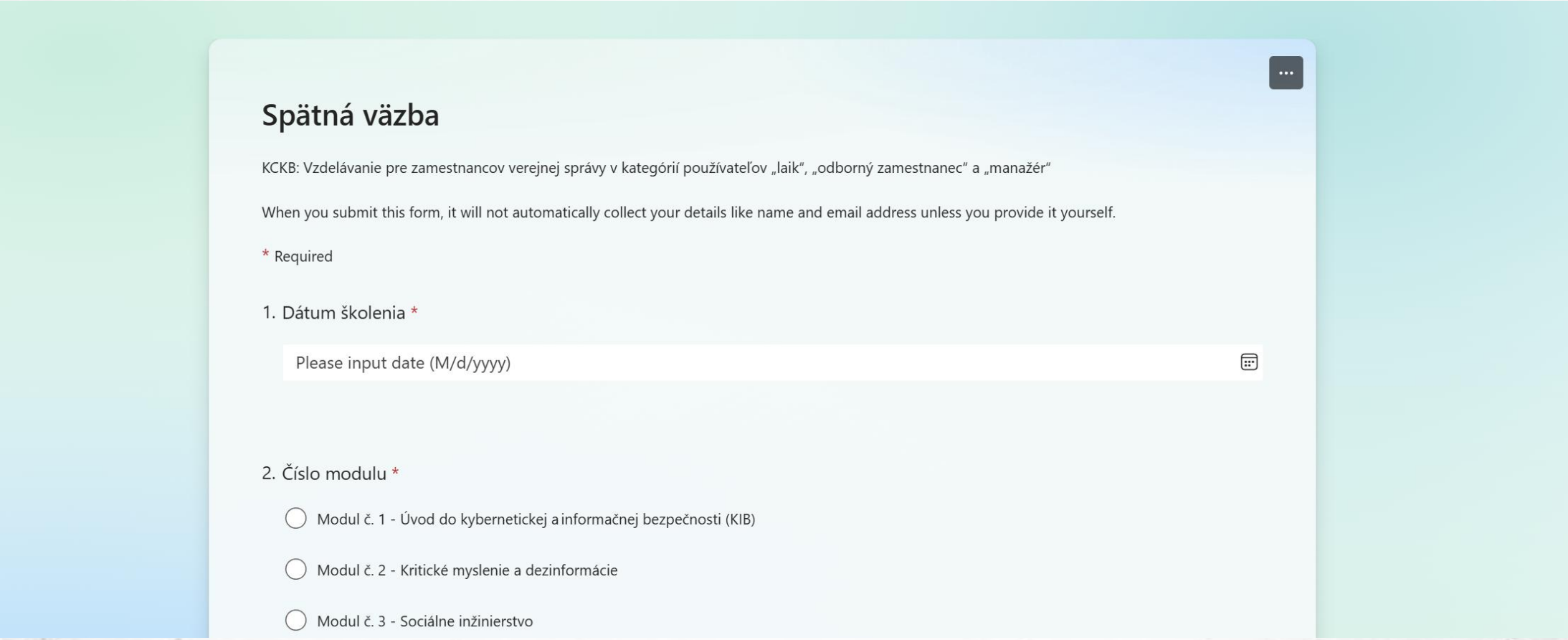
3. Dátum testu *

Zadajte dátum (d. M. yyyy)

4. Čo znamená pojem "dôvernosť informácie"? (1 bod) *

Spätná väzba

- Spätná väzba: ...



Spätná väzba

KCKB: Vzdelávanie pre zamestnancov verejnej správy v kategórií používateľov „laik“, „odborný zamestnanec“ a „manažér“

When you submit this form, it will not automatically collect your details like name and email address unless you provide it yourself.

* Required

1. Dátum školenia *

Please input date (M/d/yyyy)

2. Číslo modulu *

- Modul č. 1 - Úvod do kybernetickej a informačnej bezpečnosti (KIB)
- Modul č. 2 - Kritické myslenie a dezinformácie
- Modul č. 3 - Sociálne inžinierstvo

KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Ďakujem za pozornosť

meno.priezvisko@upjs.sk

https://cyberawareness.sk