KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

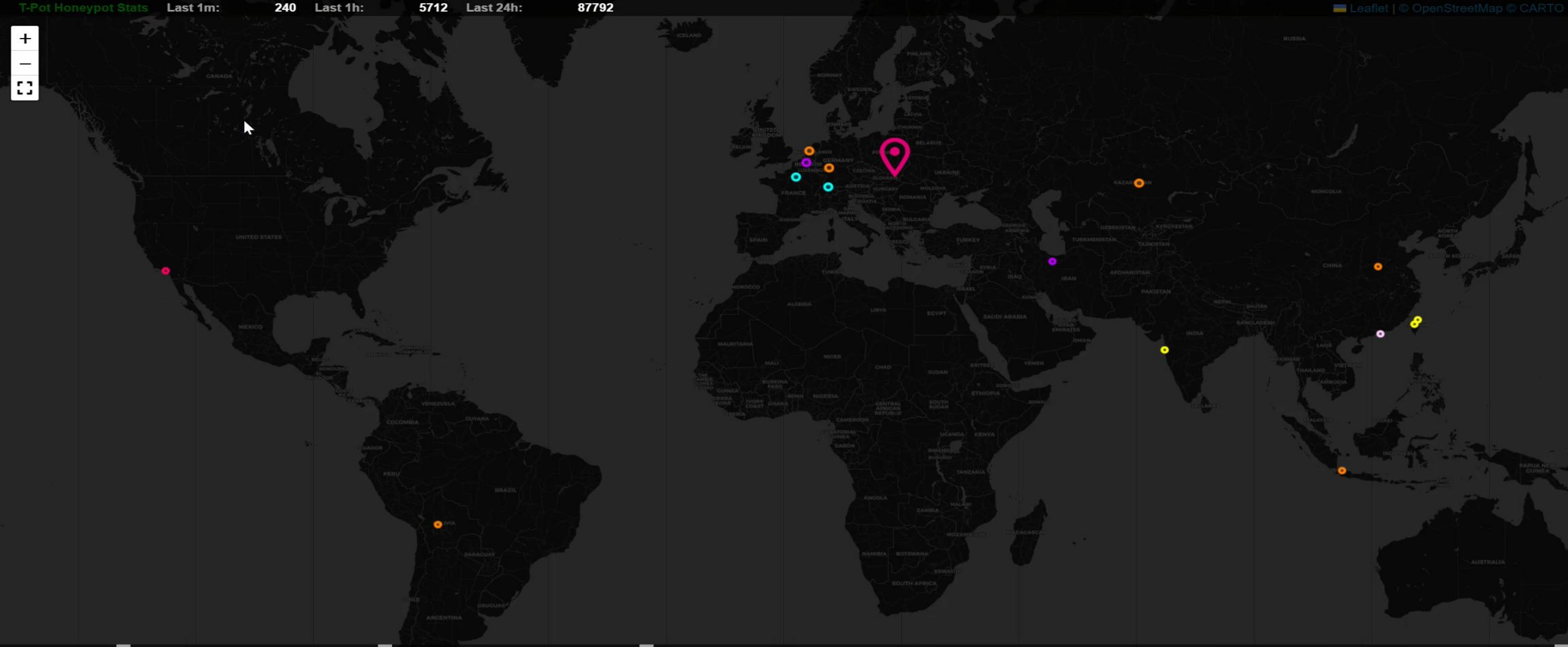
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Úvod do kybernetickej a informačnej bezpečnosti

KOPaHP/PKBaK/25 – Právo kybernetickej bezpečnosti a kyberkriminality

Meno a priezvisko
XX.XX.XXXX

KCKB UPJS CSIRT UPJS



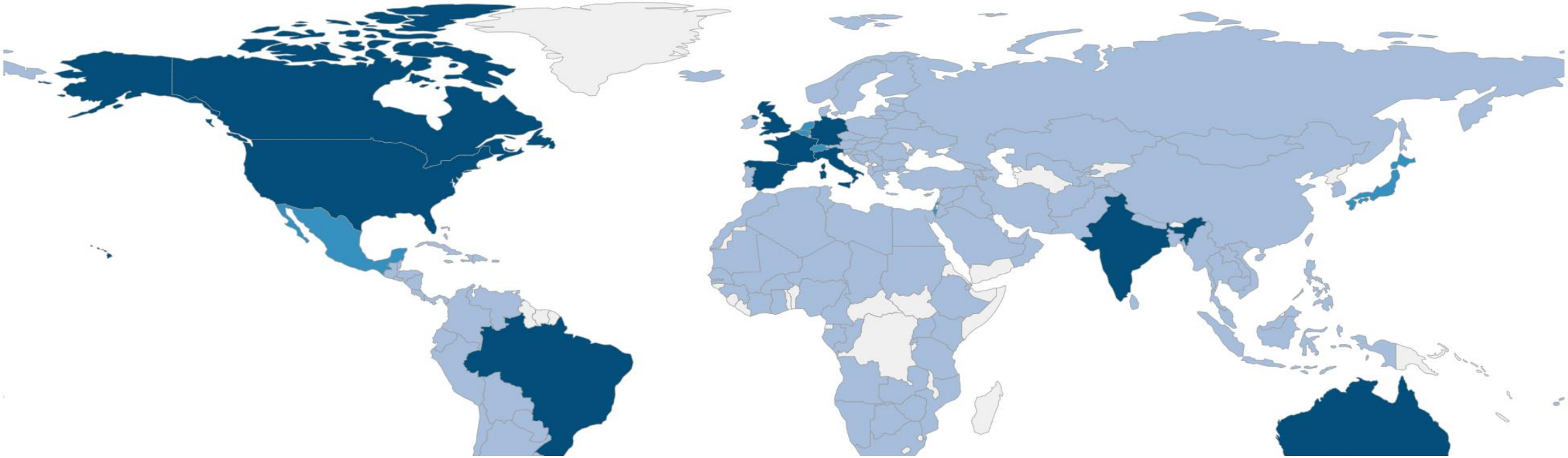
Color	Service
	FTP
	SSH
	TELNET
	EMAIL
	SQL
	DNS
	HTTP
	HTTPS

Hits	IP
4689	193.41.206.98
3672	193.37.69.157
3612	193.41.206.138
1993	193.37.69.205
236	170.64.199.171
235	209.38.30.136
108	54.89.203.179

Hits	Country
8380	France
5710	The Netherlands
565	United States
471	Australia
358	Taiwan
233	China
142	South Korea

Events	IP	Country	Honeypot	Service
2025-03-17 05:56:48	193.41.206.138	France	Tanner	HTTP
2025-03-17 05:56:48	193.41.206.138	France	Tanner	HTTP
2025-03-17 05:56:48	193.41.206.138	France	Tanner	HTTP
2025-03-17 05:56:47	193.41.206.138	France	Tanner	HTTP
2025-03-17 05:56:47	193.41.206.138	France	Tanner	HTTP
2025-03-17 05:56:48	193.41.206.138	France	Tanner	HTTP
2025-03-17 05:56:47	193.41.206.138	France	Tanner	HTTP

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**

živé 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/


100% bezpečnosť neexistuje

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.)

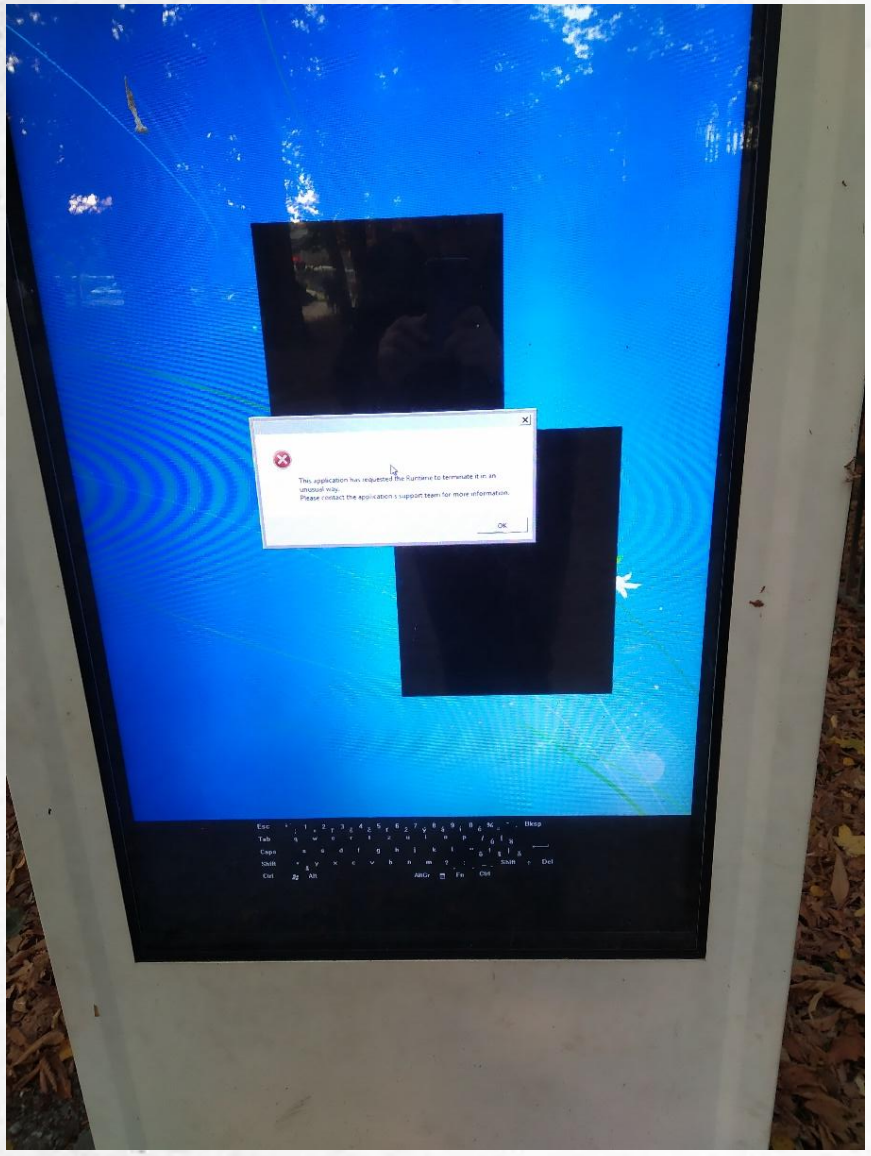
Vážený pane, vaše medicínske záznamy nám konečne zaslali späť a konečne poznáme príčinu vašich problémov

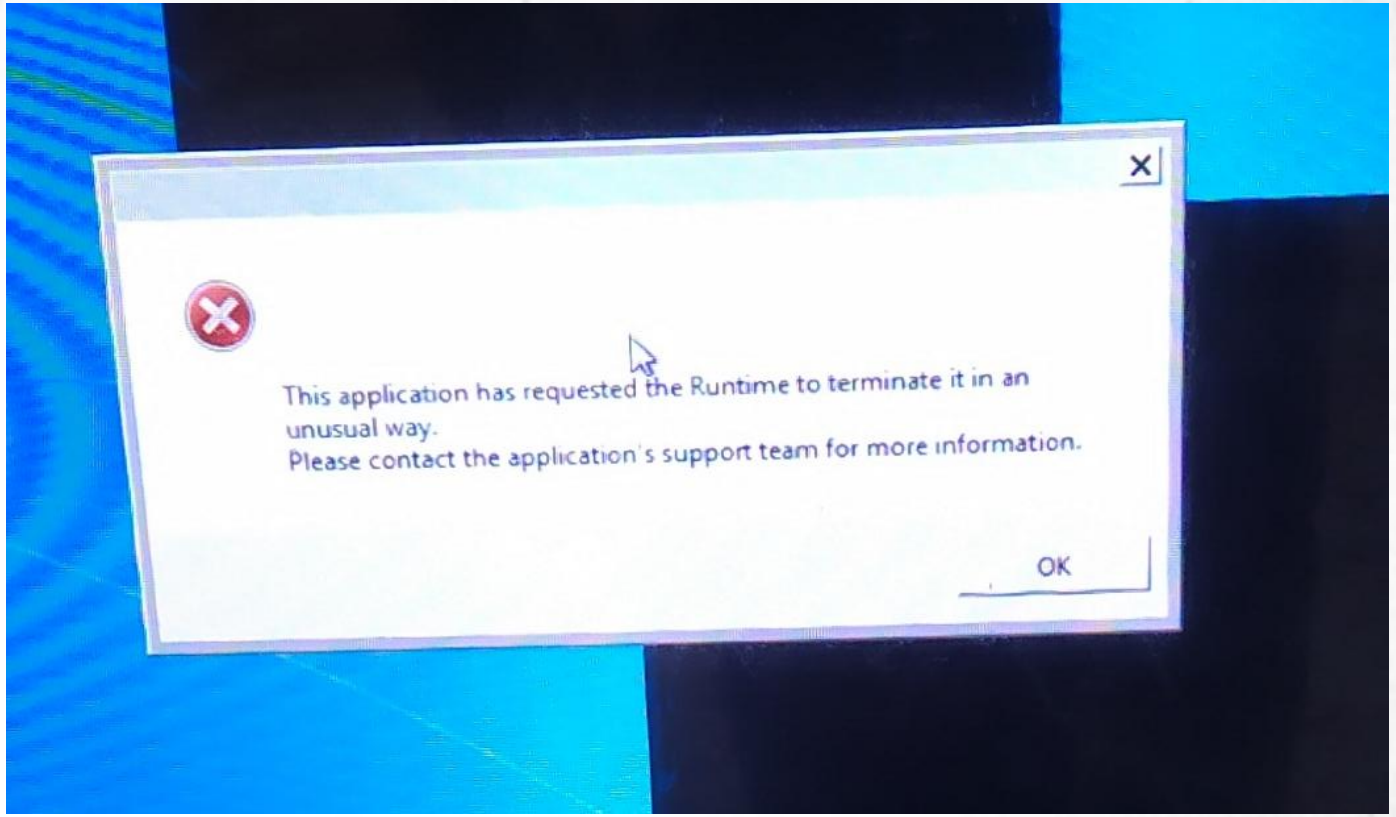
Ste tehotný!

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

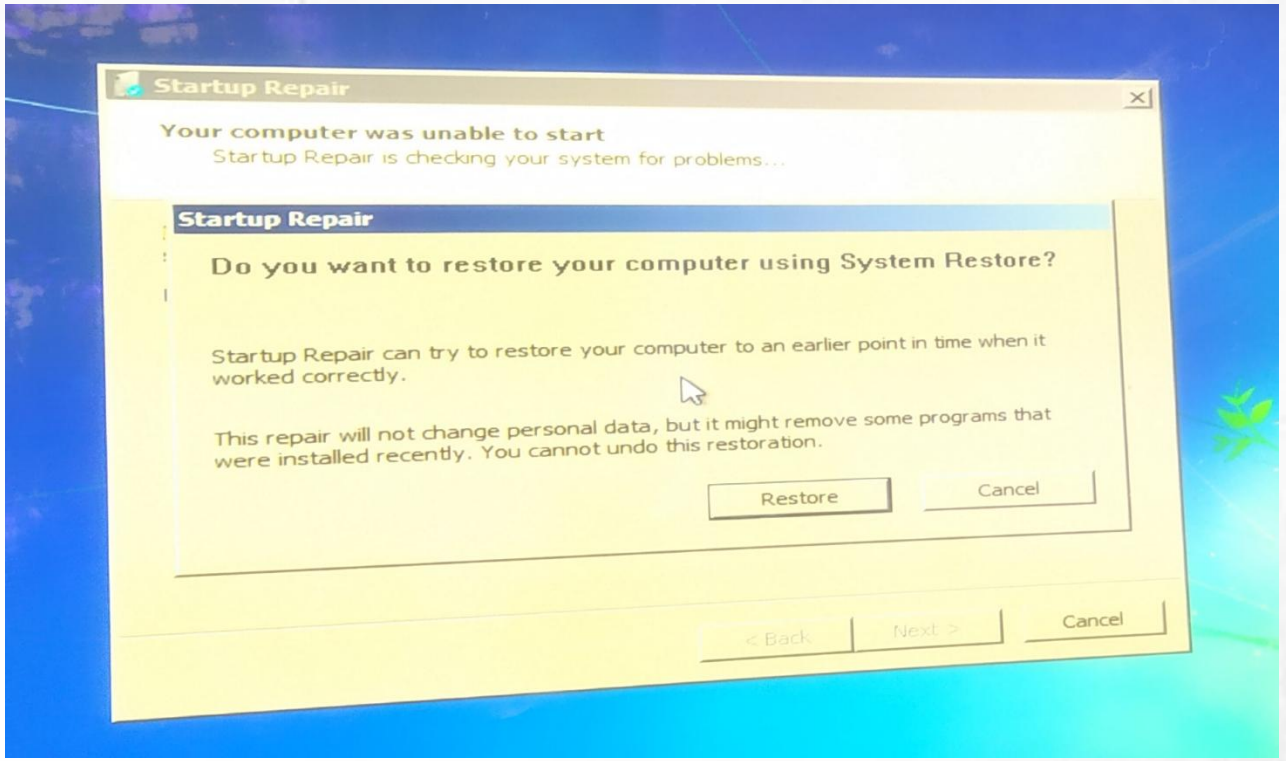

Search Google Maps
Stanične námestie
Košice, Košice Region
Google Street View
Apr 2024
See more dates
Košice
Stredná
škola že
Google
Image capture: Apr 2024
© 2024 Google
Slovakia
Terms
Privacy
Report a problem


Bez internetu



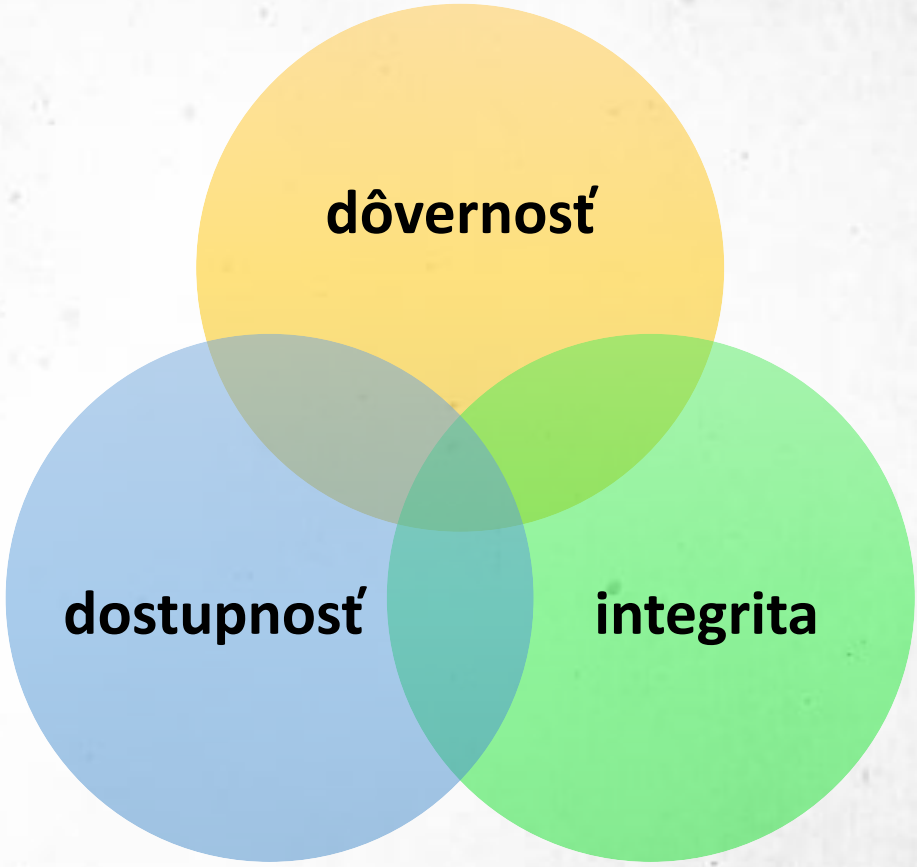

This application has requested the Runtime to terminate it in an unusual way.
Please contact the application's support team for more information.
OK


imotion

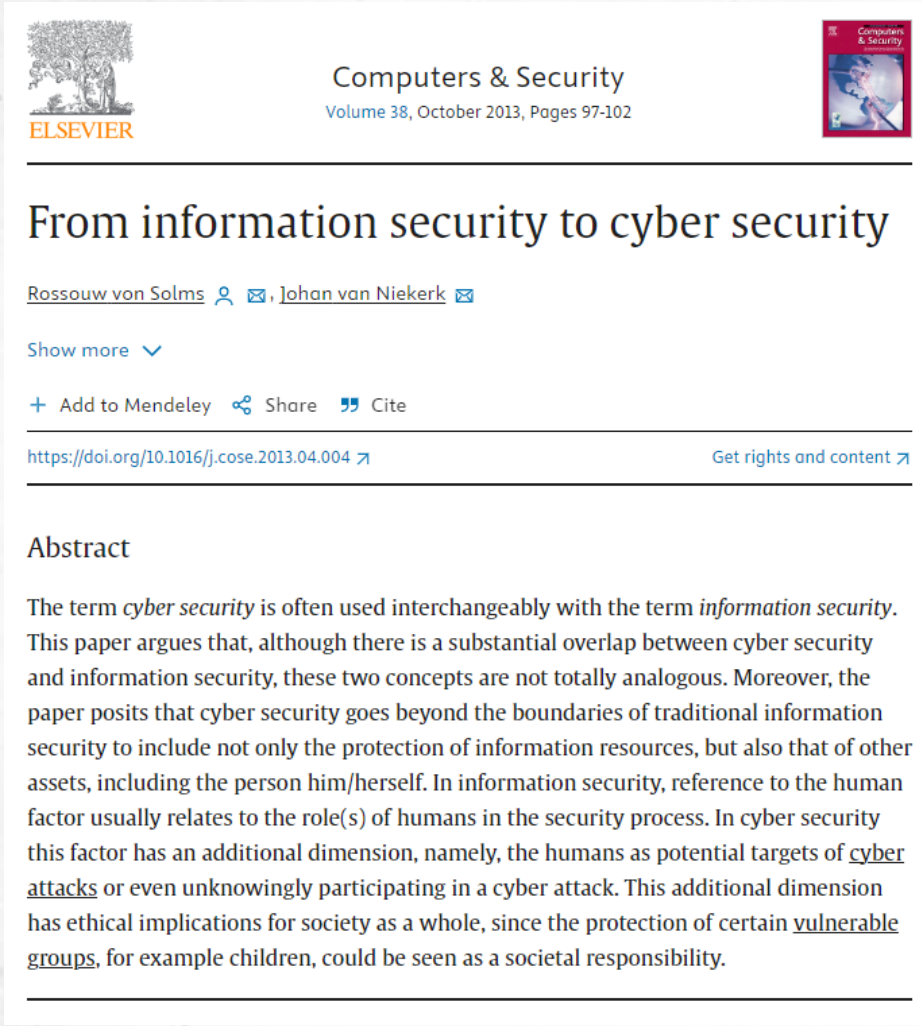

Startup Repair
Your computer was unable to start
Startup Repair is checking your system for problems...
Startup Repair
Do you want to restore your computer using System Restore?
Startup Repair can try to restore your computer to an earlier point in time when it worked correctly.
This repair will not 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

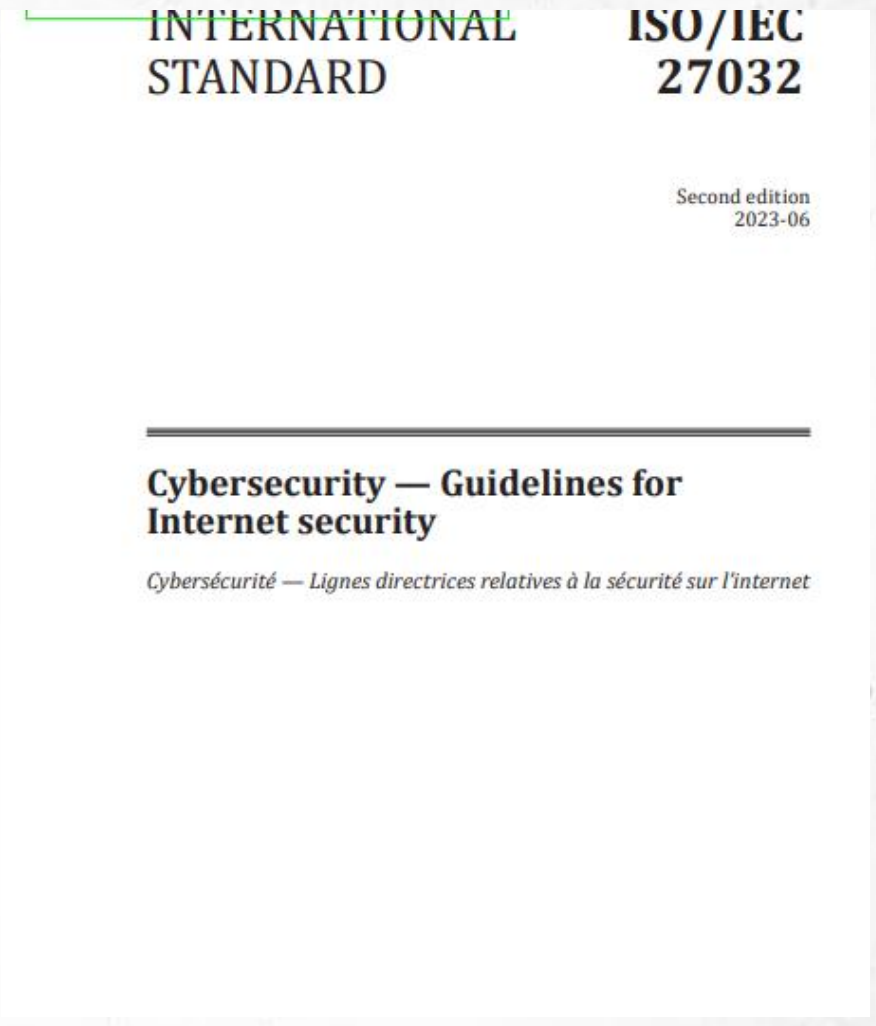
Show more

+ 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

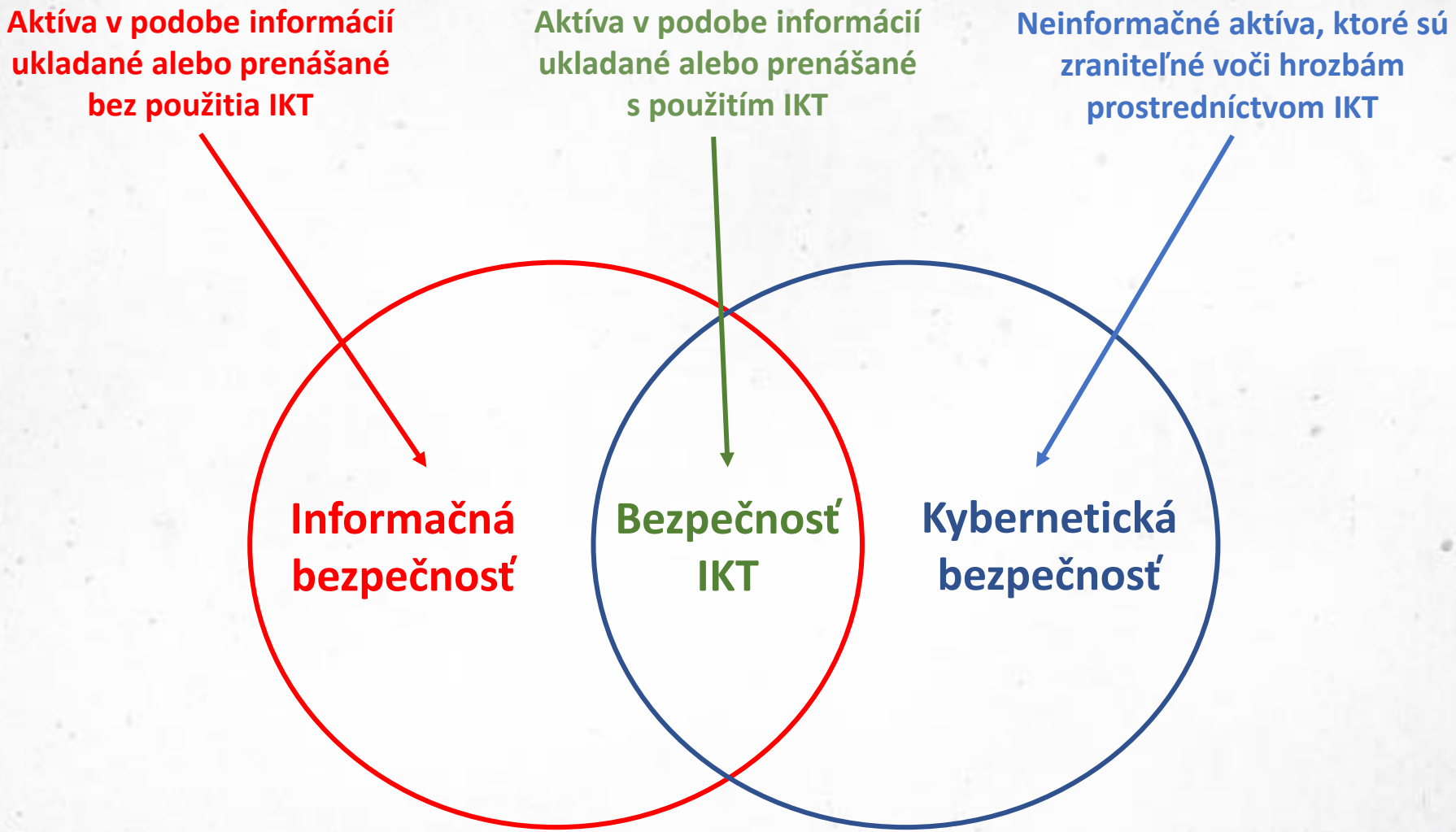
Second edition
2023-06

Cybersecurity — Guidelines for Internet security

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

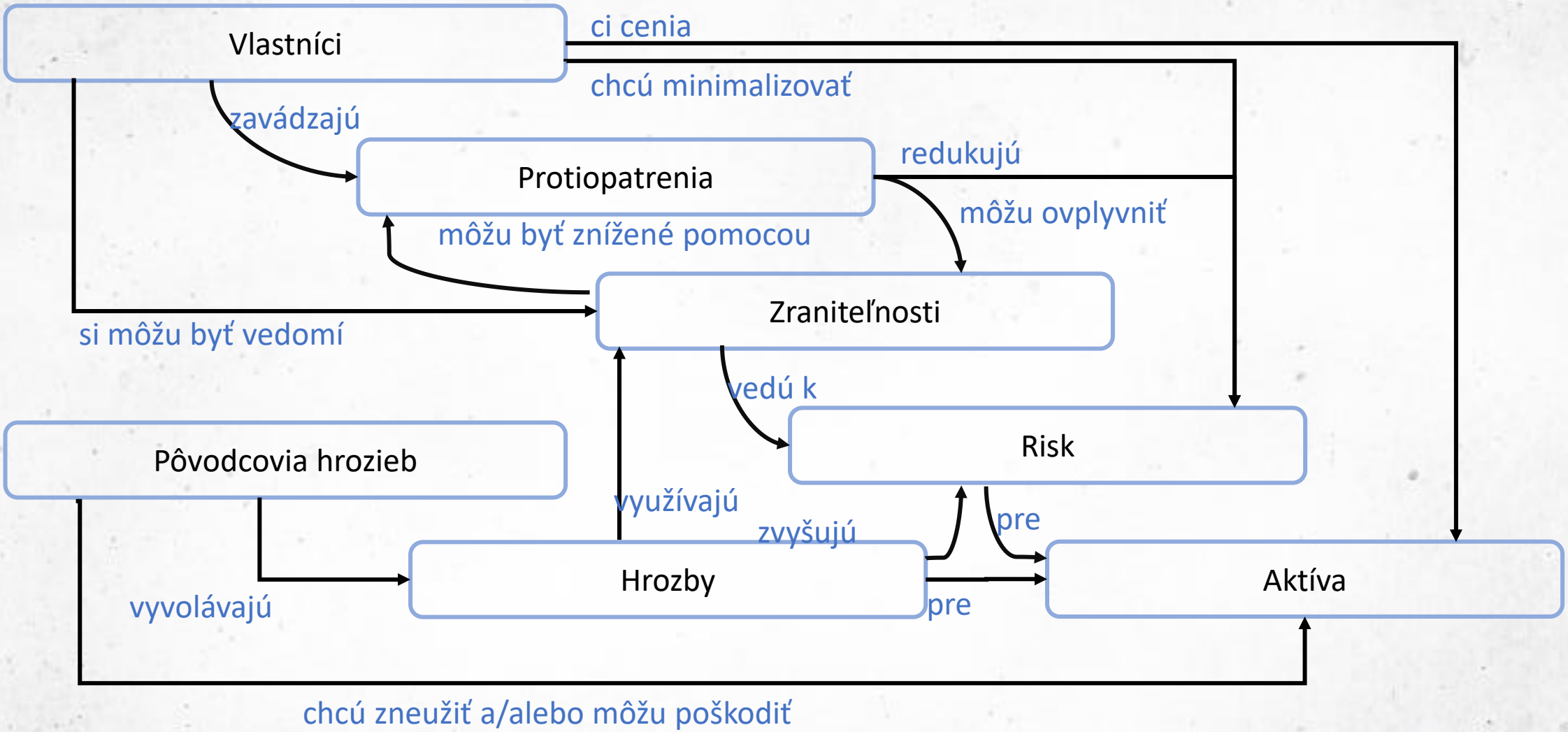
Zdroj: Von Solms, Rossouw, and Johan Van Niekerk. "From information security to cyber security." computers & security 38 (2013): 97-102.

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.)

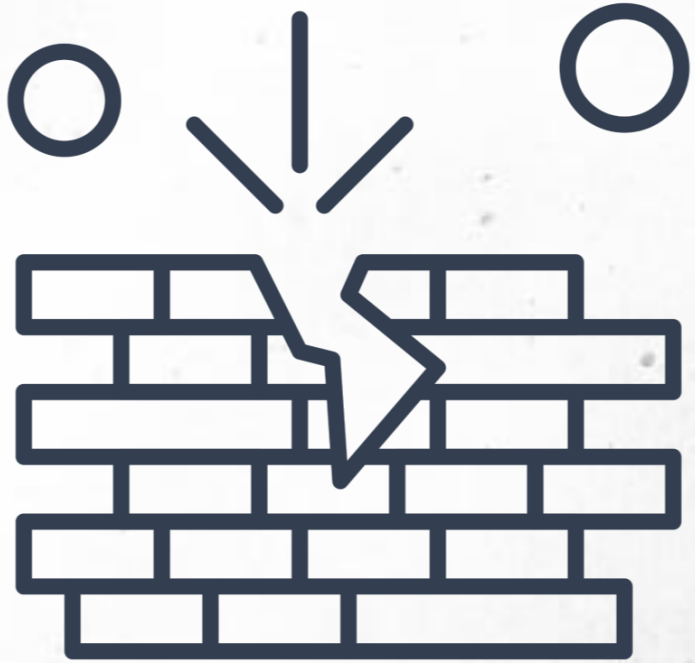
Typ	Hrozby	Zdroj
Fyzické poškodenie	Požiar	A,D,E
	Poškodenie vodou	A,D,E
	Znečistenie	A,D,E
	...	
Prírodná udalosť	Klimatický jav	E
	Povodeň	E
	...	
Strata základnej služby	Prerušenie dodávky elektriny	A,D,E
	...	
Ohrozenie informácií	Odposluch	D
	Krádež zariadenia	D
	...	
Neoprávnení činnosti	Neoprávnené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

Zraniteľnosť (I.)

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

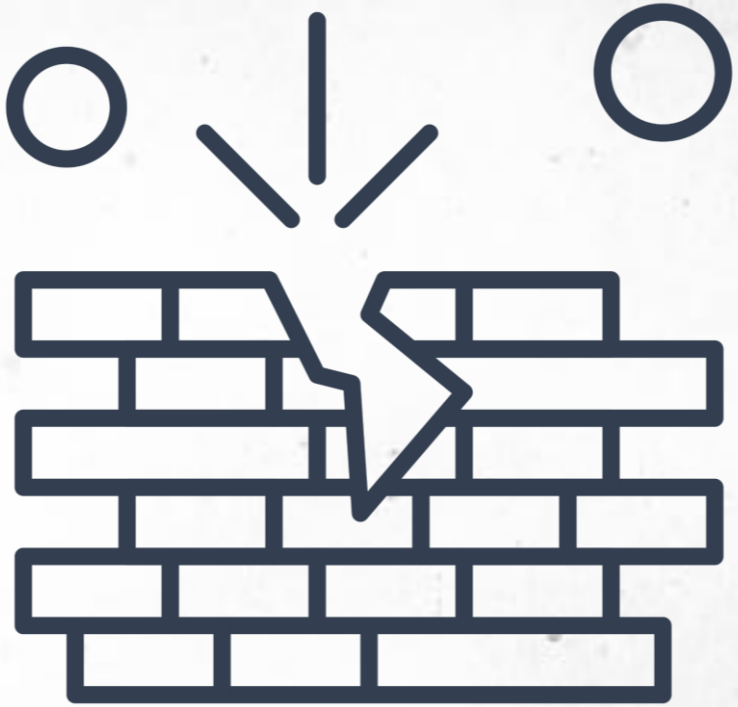
- niečo, čo umožňuje hrozbe prejaviť sa

- 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.)

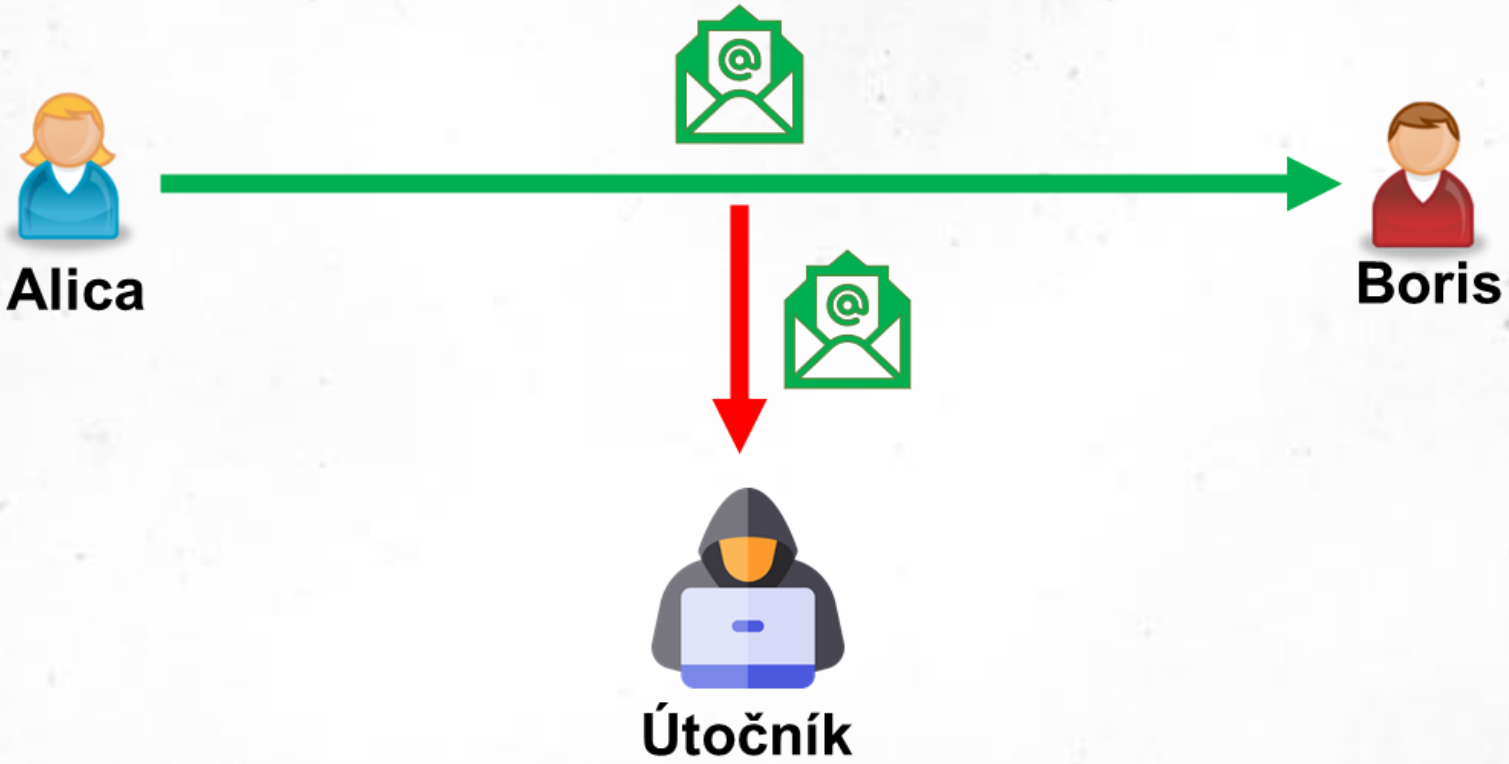
- pokus o zničenie, vystavenie hrozbe, zmenu, vyradenie z činnosti, odcudzeniu aktíva alebo získanie neoprávneného prístupu k aktívu alebo uskutočnenie neoprávneného použitia aktíva (ISO/IEC 27000: 2018)

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

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

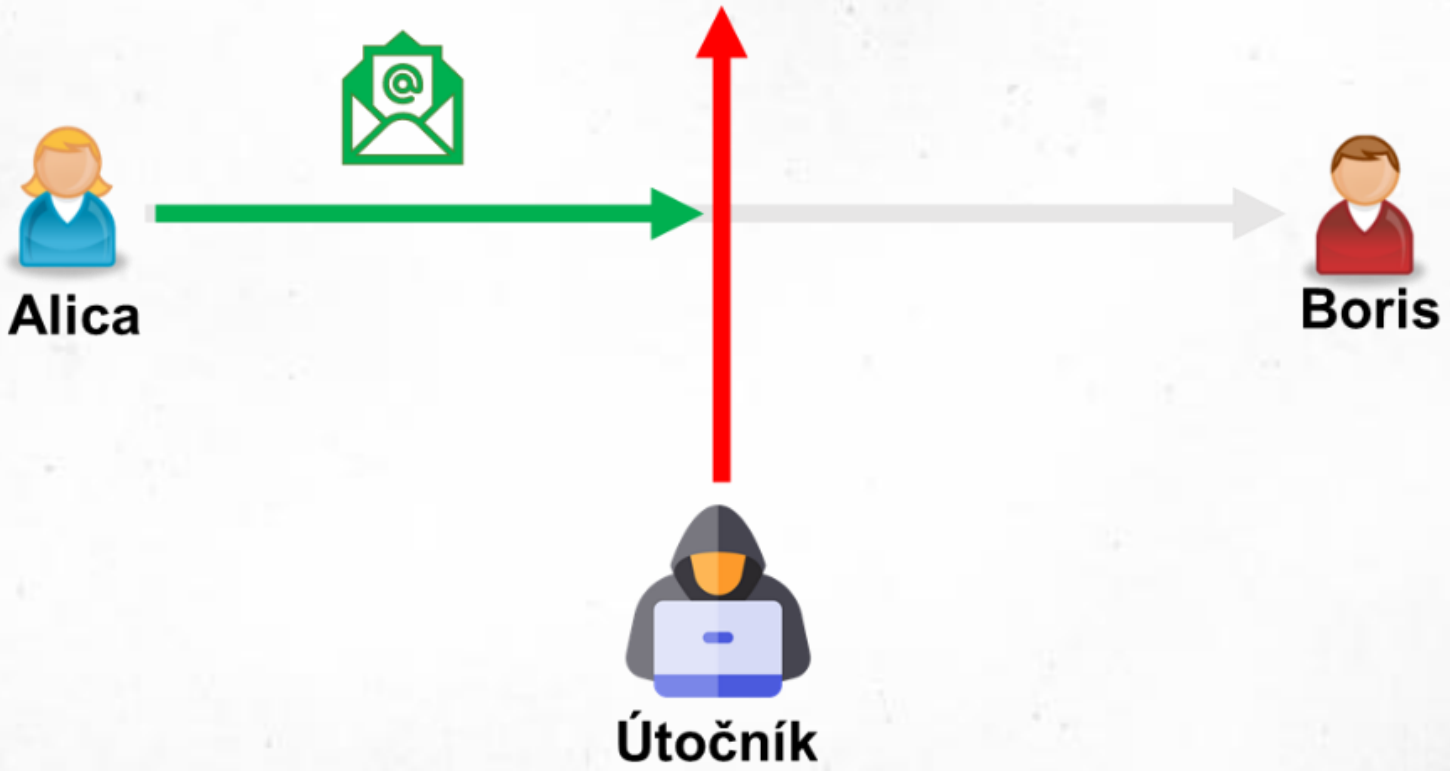
Útok (II.)

- odpočúvanie (interception)



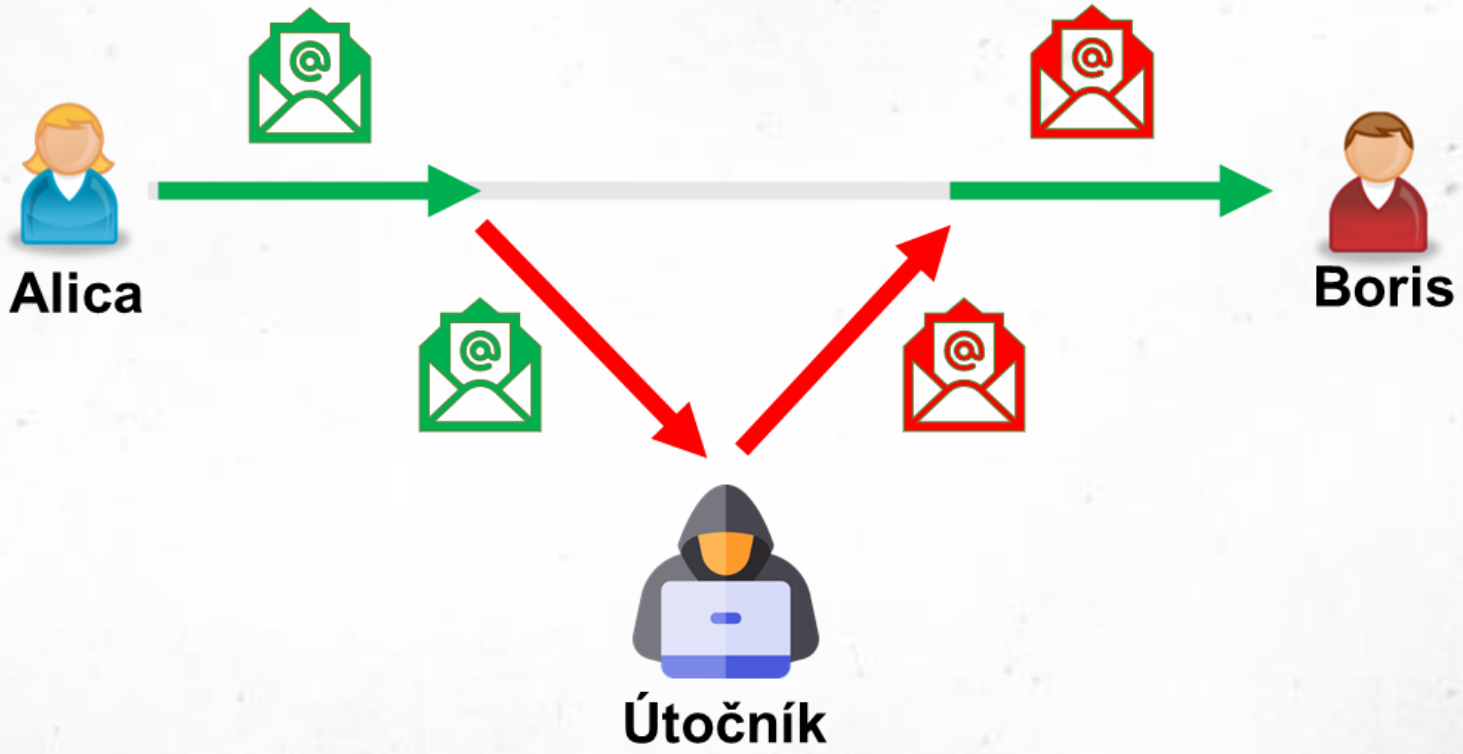
Útok (III.)

- prerušenie (interruption)



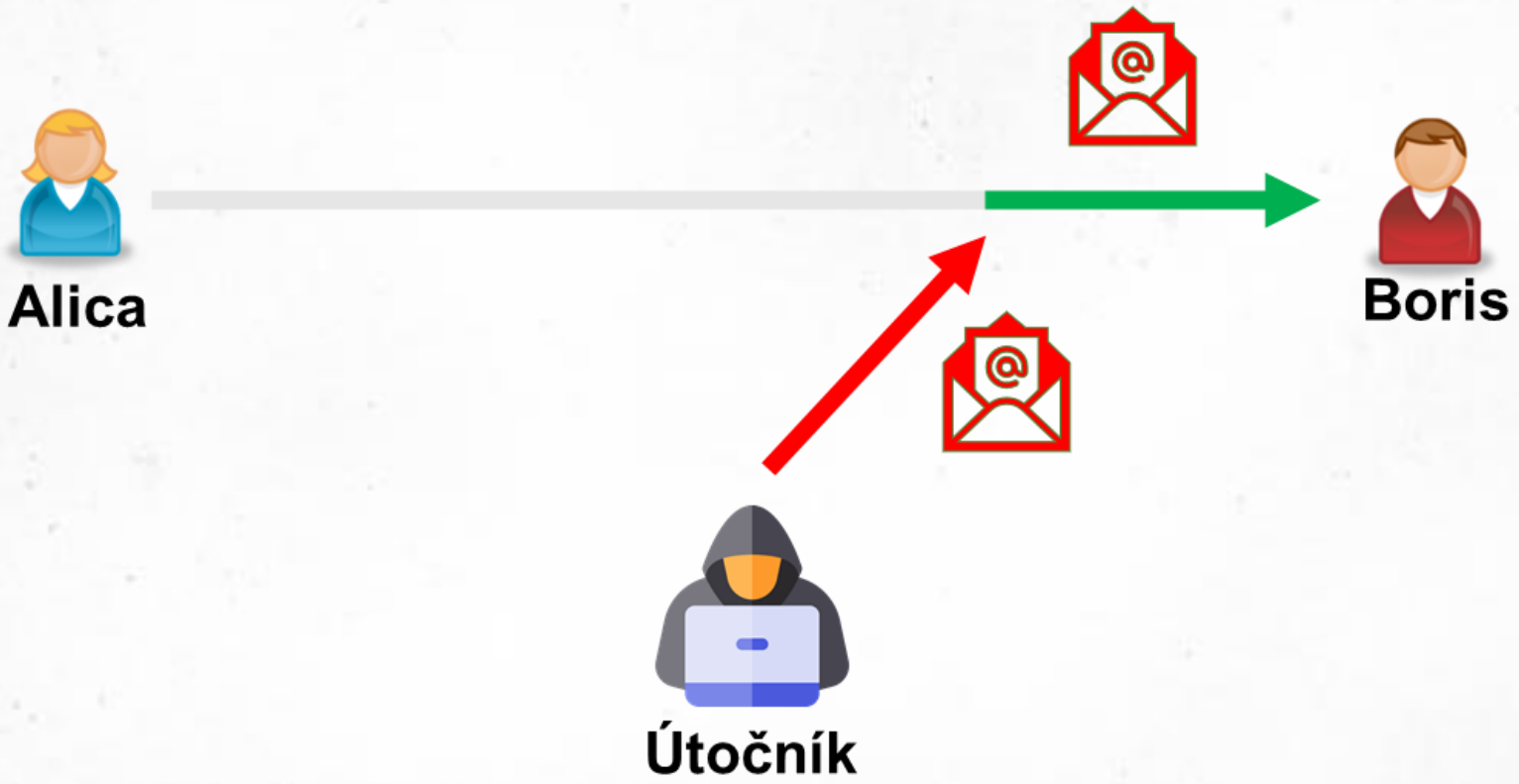
Útok (IV.)

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

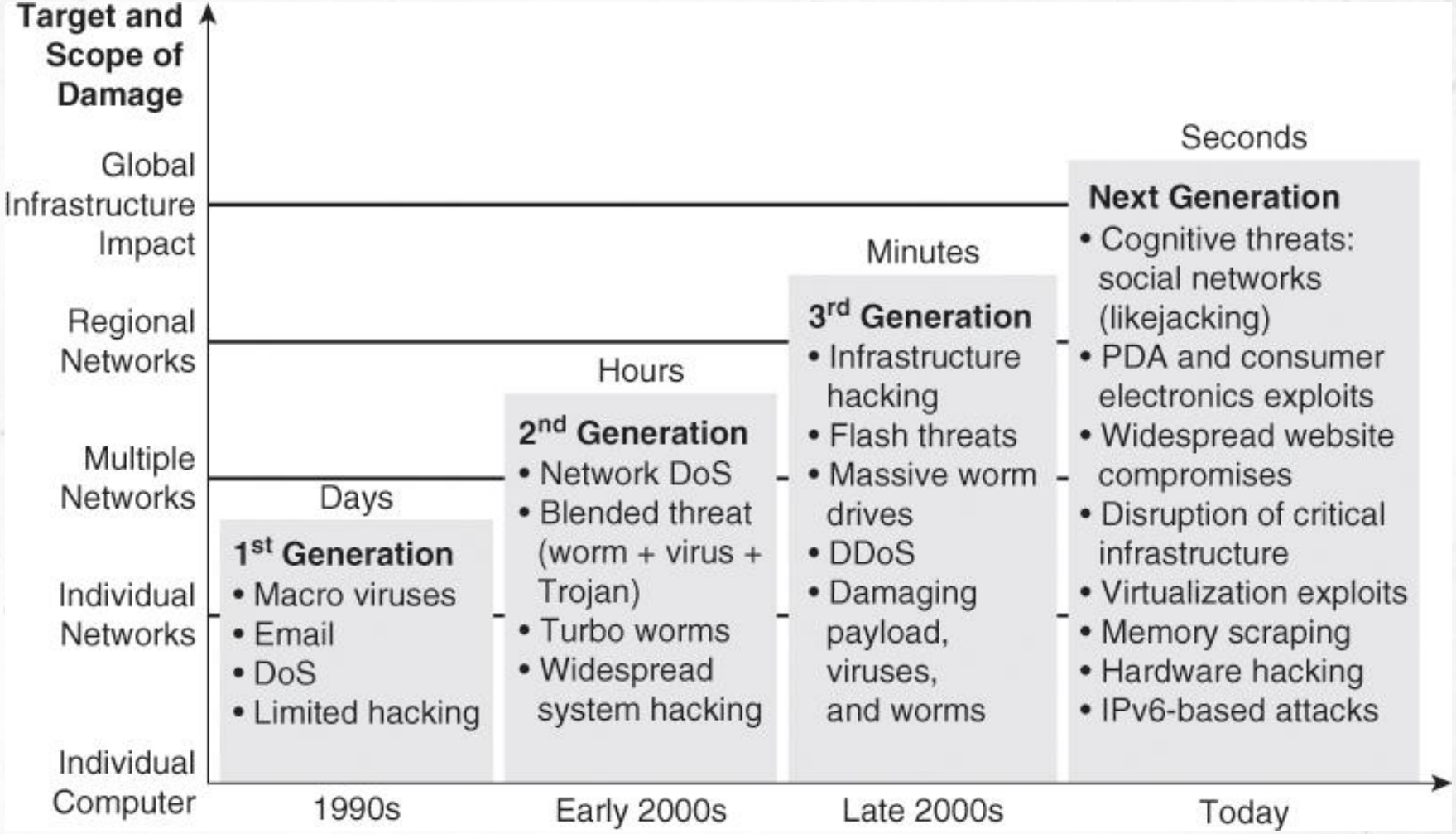


Útok (V.)

- výroba (fabrication)

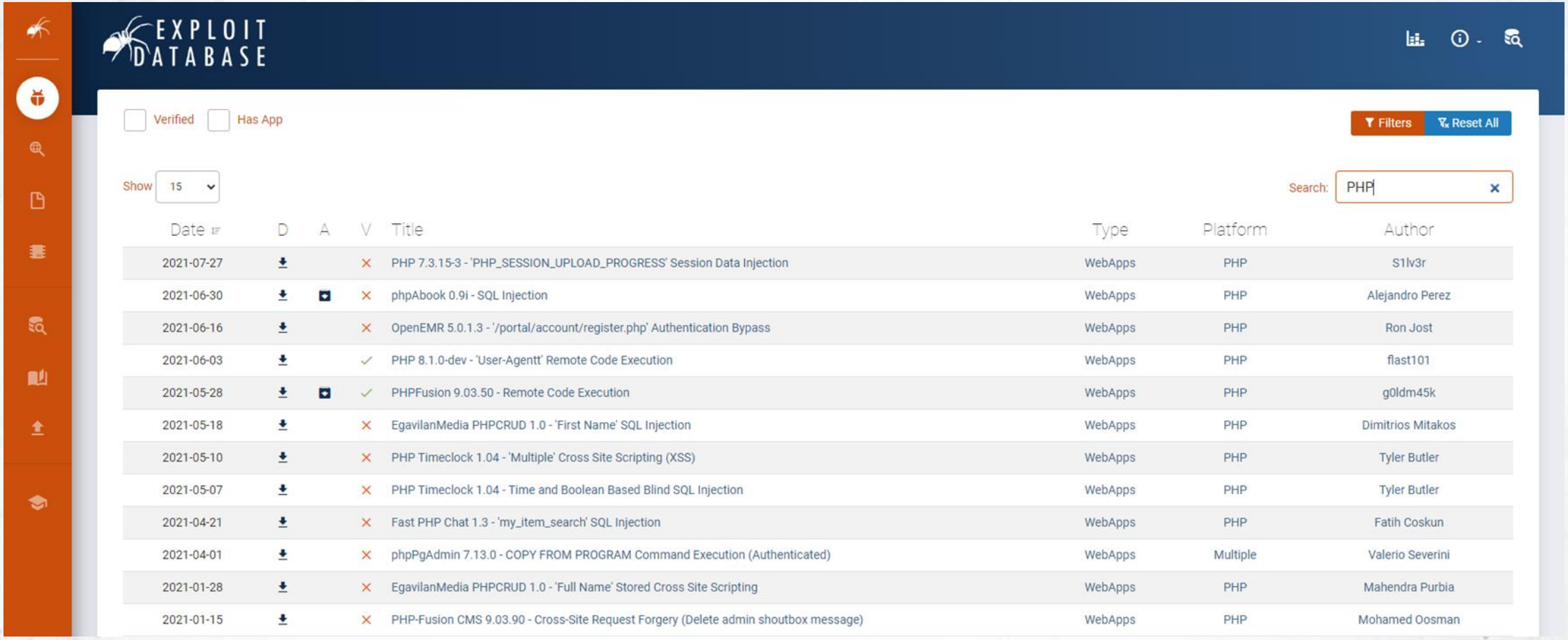


Útok (VI.)



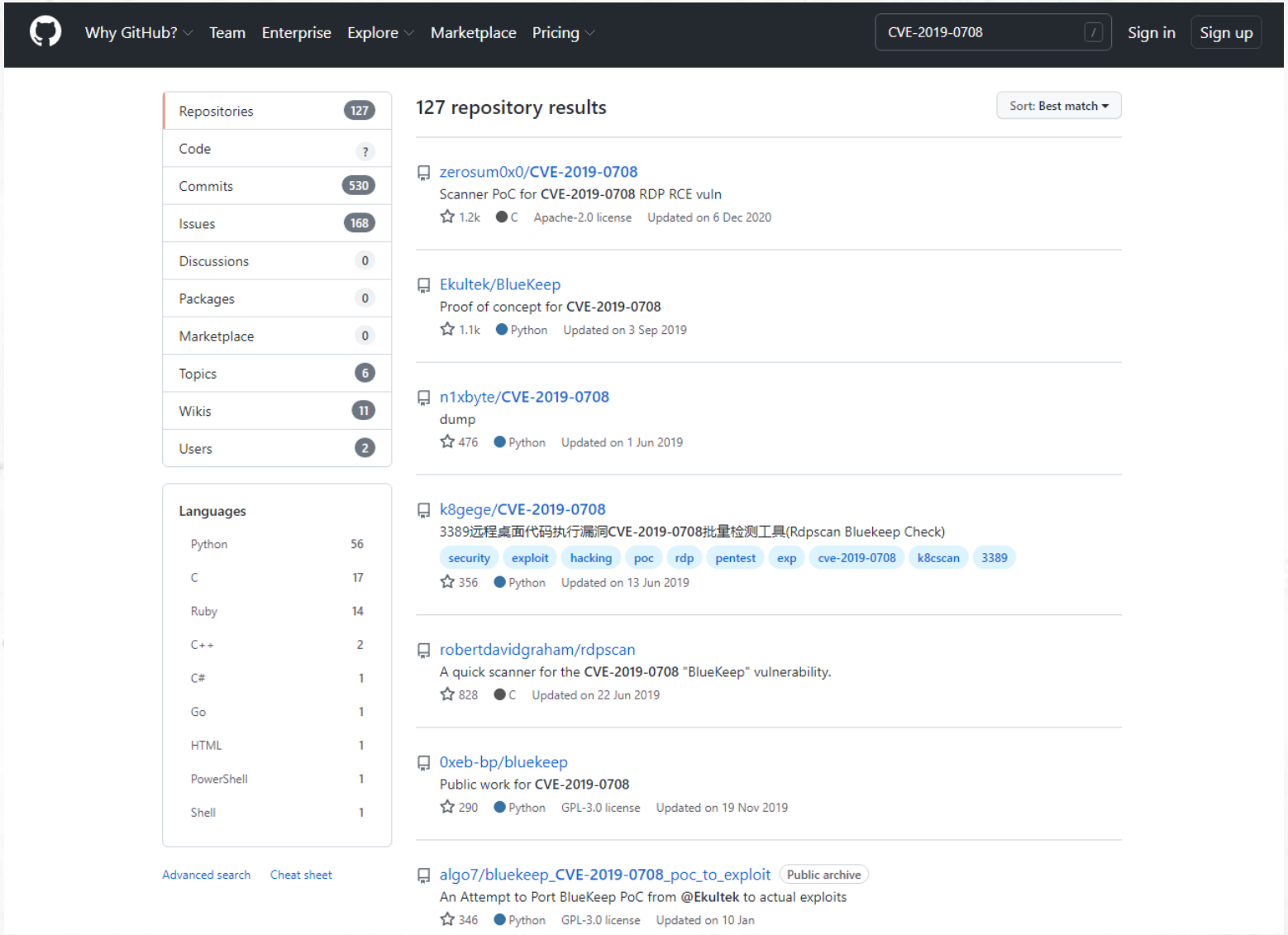
Zdroj: http://www.ciscopress.com/articles/article.asp?p=1998559

Útok (VII.)



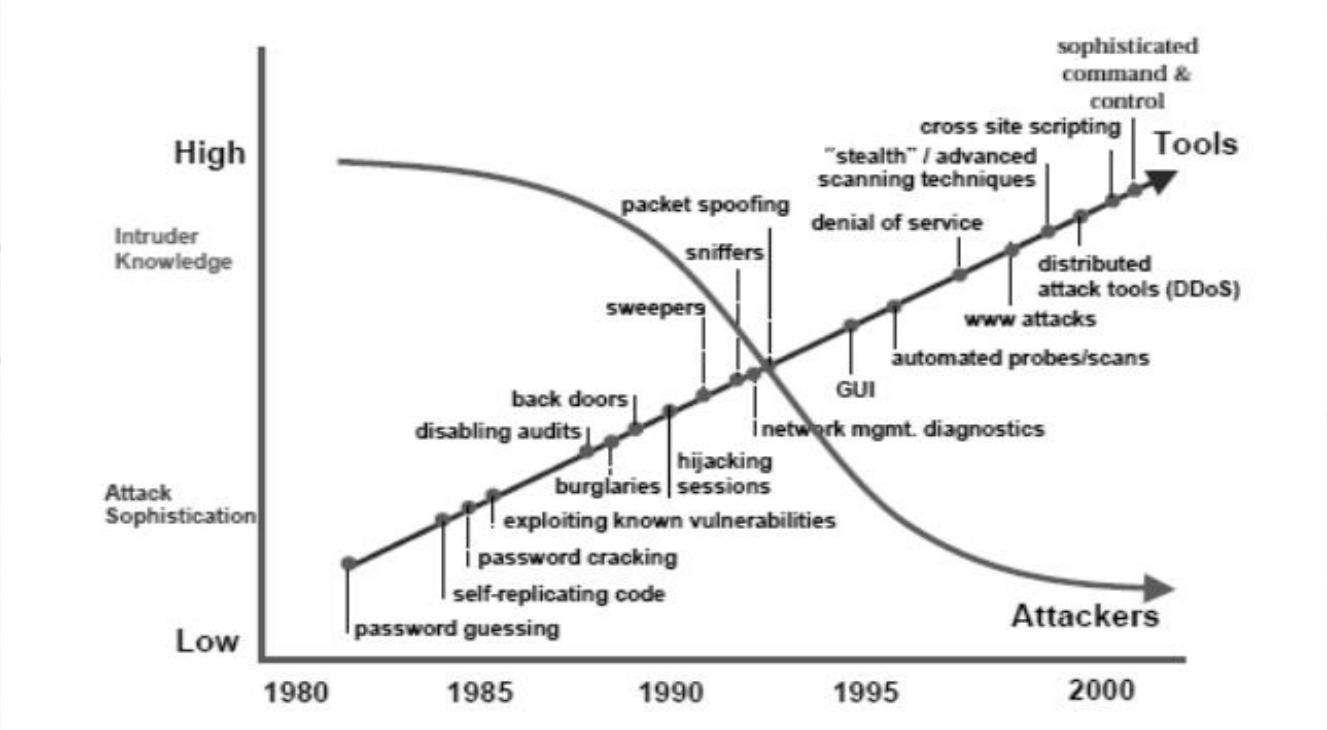
Date	D	A	V	Title	Type	Platform	Author
2021-07-27				PHP 7.3.15-3 - 'PHP_SESSION_UPLOAD_PROGRESS' Session Data Injection	WebApps	PHP	S1lv3r
2021-06-30				phpAbook 0.9i - SQL Injection	WebApps	PHP	Alejandro Perez
2021-06-16				OpenEMR 5.0.1.3 - '/portal/account/register.php' Authentication Bypass	WebApps	PHP	Ron Jost
2021-06-03				PHP 8.1.0-dev - 'User-Agentt' Remote Code Execution	WebApps	PHP	flast101
2021-05-28				PHPFusion 9.03.50 - Remote Code Execution	WebApps	PHP	g0ldm45k
2021-05-18				EgavilanMedia PHPCRUD 1.0 - 'First Name' SQL Injection	WebApps	PHP	Dimitrios Mitakos
2021-05-10				PHP Timeclock 1.04 - 'Multiple' Cross Site Scripting (XSS)	WebApps	PHP	Tyler Butler
2021-05-07				PHP Timeclock 1.04 - Time and Boolean Based Blind SQL Injection	WebApps	PHP	Tyler Butler
2021-04-21				Fast PHP Chat 1.3 - 'my_item_search' SQL Injection	WebApps	PHP	Fatih Coskun
2021-04-01				phpPgAdmin 7.13.0 - COPY FROM PROGRAM Command Execution (Authenticated)	WebApps	Multiple	Valerio Severini
2021-01-28				EgavilanMedia PHPCRUD 1.0 - 'Full Name' Stored Cross Site Scripting	WebApps	PHP	Mahendra Purbia
2021-01-15				PHP-Fusion CMS 9.03.90 - Cross-Site Request Forgery (Delete admin shoutbox message)	WebApps	PHP	Mohamed Oosman

Útok (VIII.)


Why GitHub?
Team
Enterprise
Explore
Marketplace
Pricing
CVE-2019-0708
Sign in
Sign up
Repositories 127
Code ?
Commits 530
Issues 168
Discussions 0
Packages 0
Marketplace 0
Topics 6
Wikis 11
Users 2
Languages
Python 56
C 17
Ruby 14
C++ 2
C# 1
Go 1
HTML 1
PowerShell 1
Shell 1
Advanced search
Cheat sheet
127 repository results
Sort: Best match
zerosum0x0/CVE-2019-0708
Scanner PoC for CVE-2019-0708 RDP RCE vuln
1.2k C Apache-2.0 license Updated on 6 Dec 2020
Ekultek/BlueKeep
Proof of concept for CVE-2019-0708
1.1k Python Updated on 3 Sep 2019
n1xbyte/CVE-2019-0708
dump
476 Python Updated on 1 Jun 2019
k8gege/CVE-2019-0708
3389远程桌面代码执行漏洞CVE-2019-0708批量检测工具(Rdpscan Bluekeep Check)
security exploit hacking poc rdp pentest exp cve-2019-0708 k8cscan 3389
356 Python Updated on 13 Jun 2019
robertdavidgraham/rdpscan
A quick scanner for the CVE-2019-0708 "BlueKeep" vulnerability.
828 C Updated on 22 Jun 2019
0xeb-bp/bluekeep
Public work for CVE-2019-0708
290 Python GPL-3.0 license Updated on 19 Nov 2019
algo7/bluekeep_CVE-2019-0708_poc_to_exploit Public archive
An Attempt to Port BlueKeep PoC from @Ekultek to actual exploits
346 Python GPL-3.0 license Updated on 10 Jan

Útočník (I.)

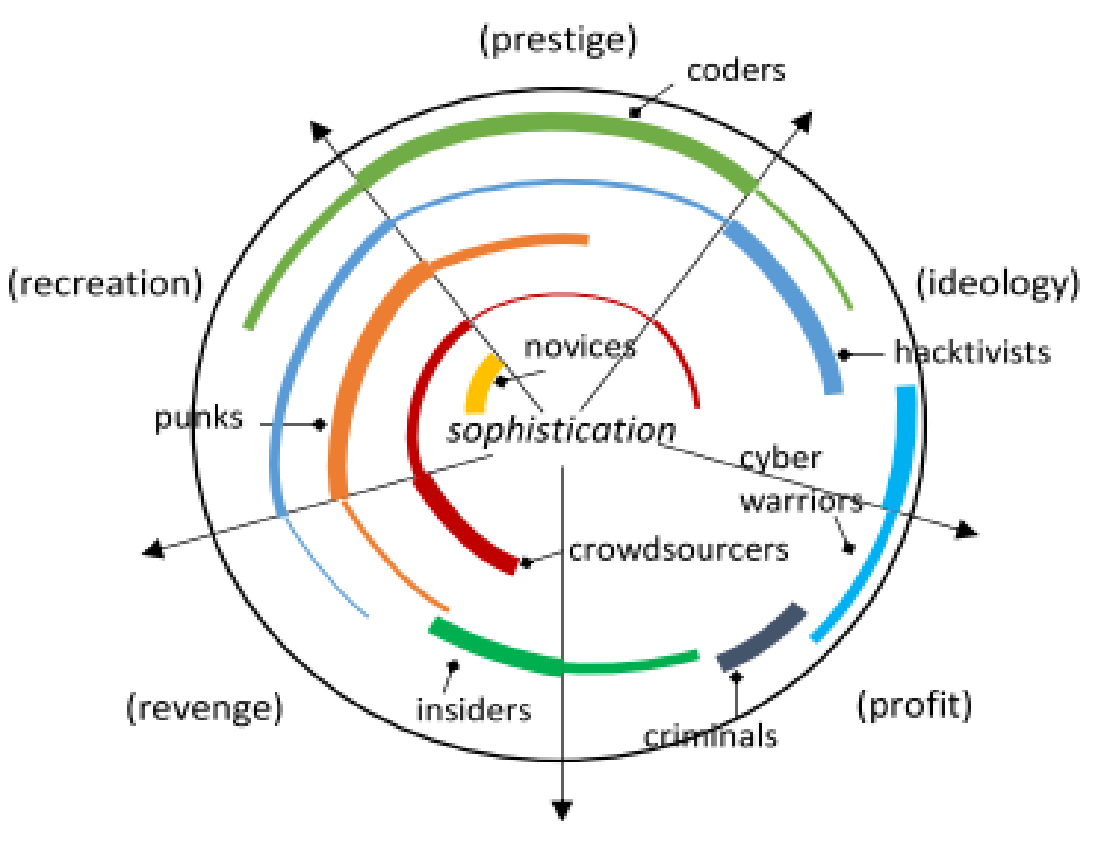
- jednotlivec, skupina, organizácia alebo vláda, ktorá vedie alebo má v úmysle vykonávať škodlivé činnosti (SP 800-30).



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.)

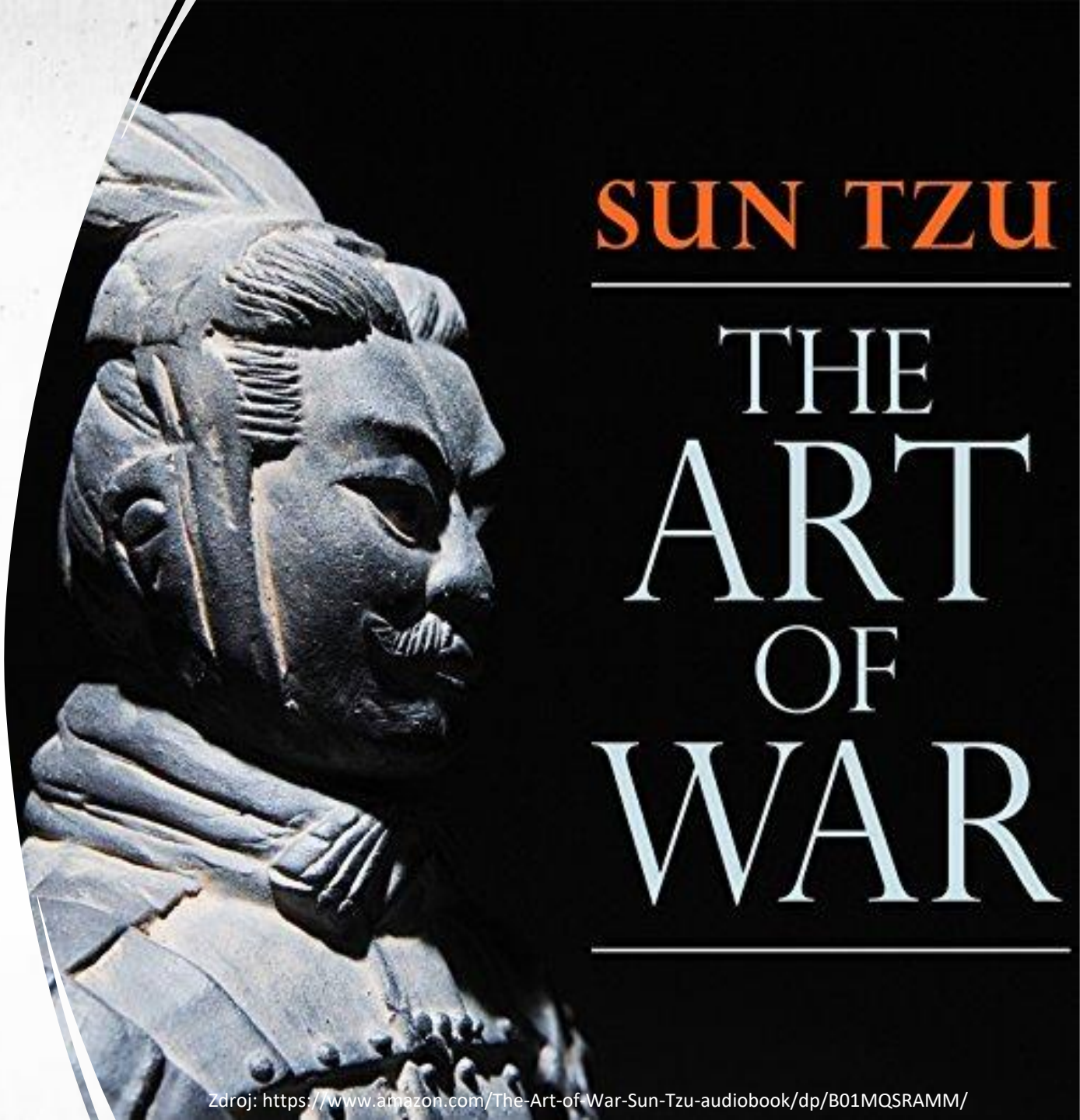
- **Script Kiddies** - nekvalifikovaný heker, ktorý kompromituje systém spustením skriptov, nástrojov a softvéru vyvinutého skutočnými hackermi
- **Organizovaní hackeri** - profesionálni hackeri, ktorí sa snažia zaútočiť na systém so ziskom
- **Hacktivisti** - jednotlivci, ktorí hackovaním propagujú 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://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

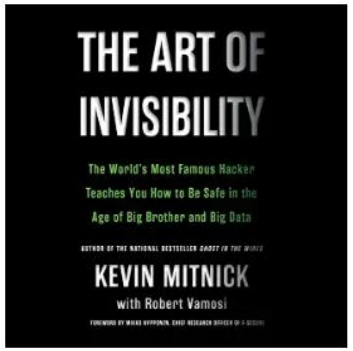
DESCRIPTION:

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~~

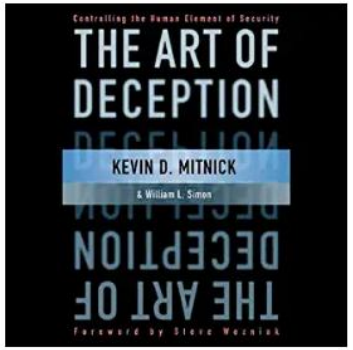
More Buying Choices

$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.

4.0 out of 5 stars 207

Audible Audiobook

$0.00 ~~$24.86~~

Free with Audible trial

Paperback

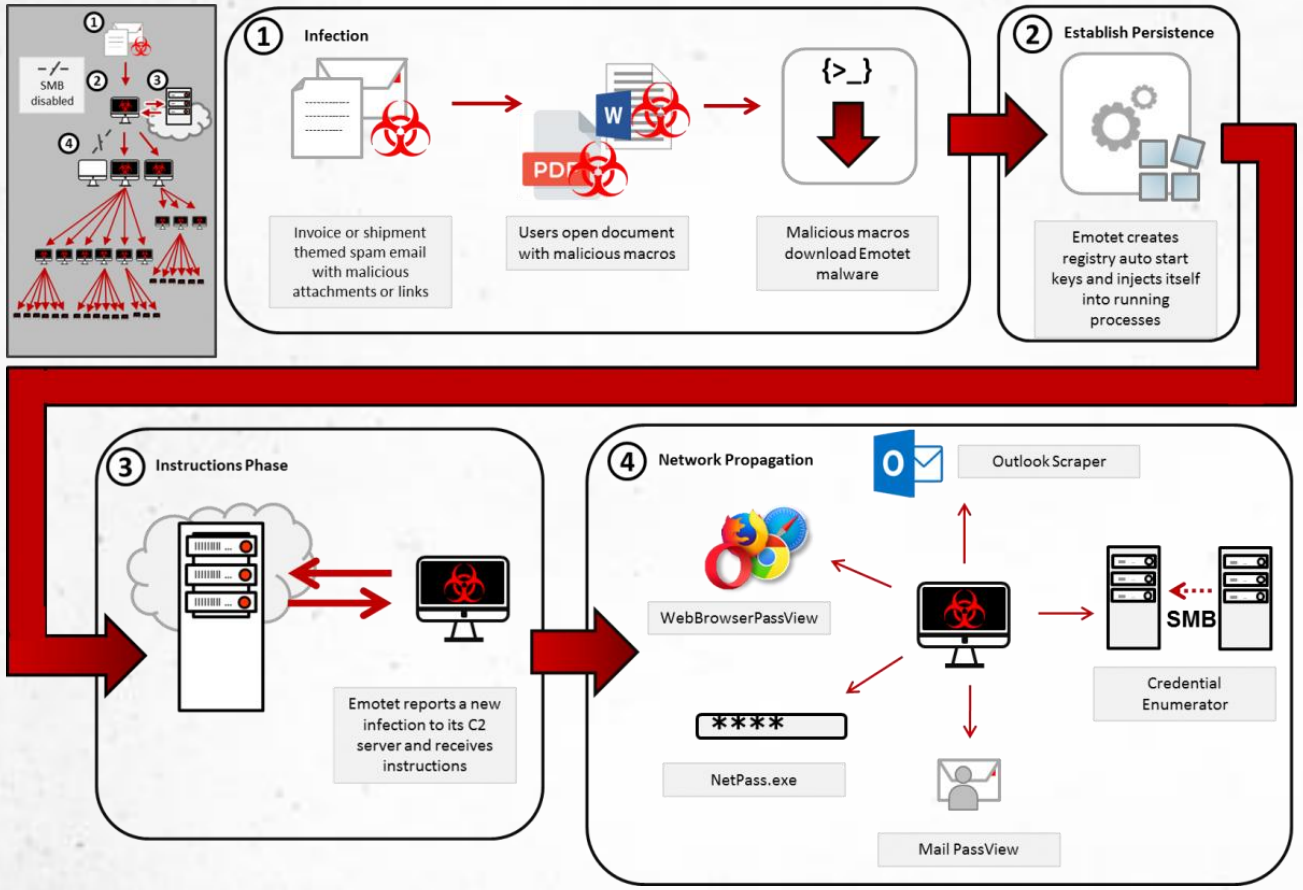
$12.47 ~~$16.95~~

More Buying Choices

$1.94 (160 used & new offers)

Emotet (I.)

- modus operandi



Media & Press

NEWS

World's most dangerous malware EMOTET disrupted through global action

27 JAN 2021

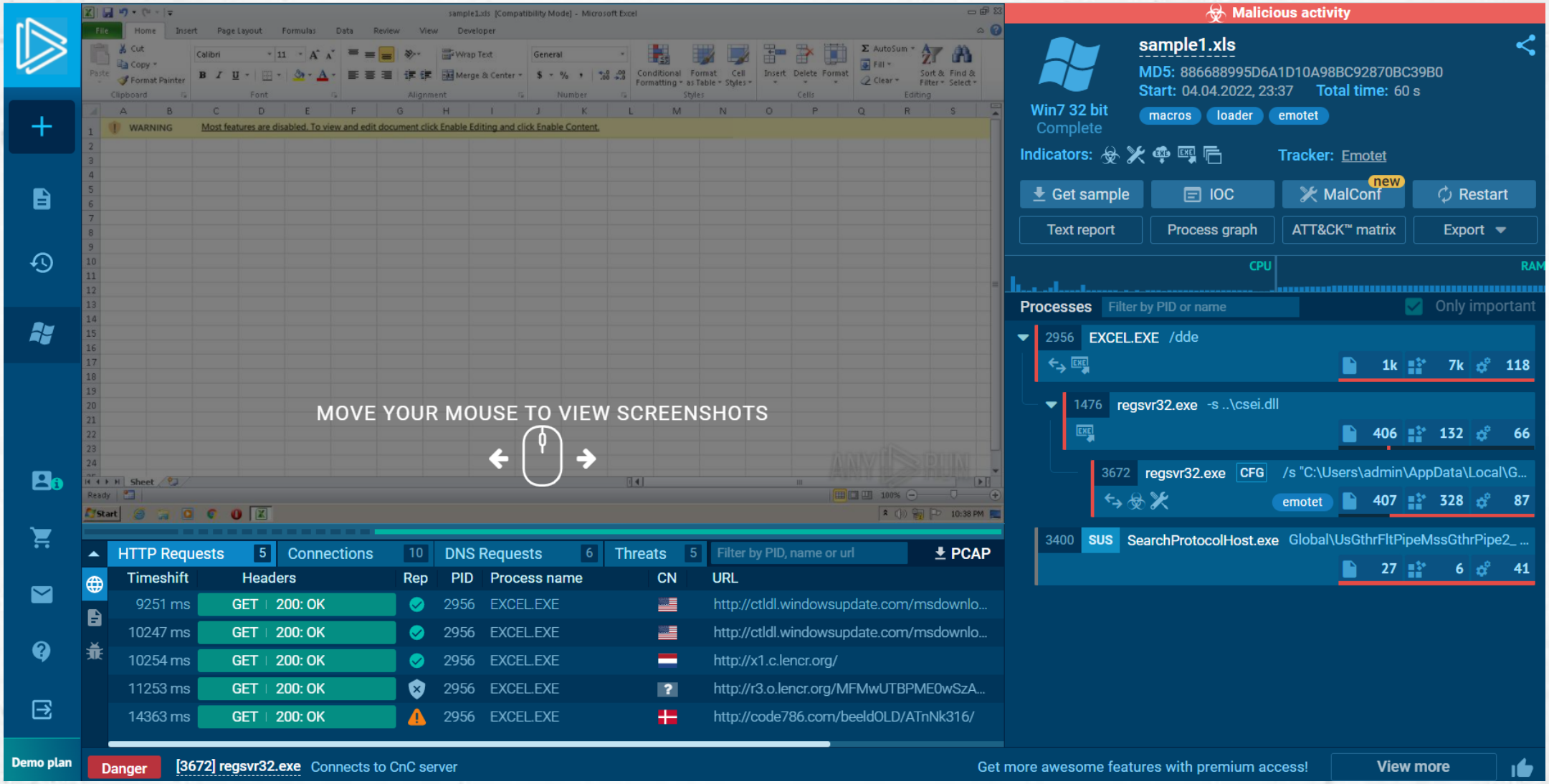
Law enforcement and judicial authorities worldwide have this week disrupted one of most significant botnets of the past decade: EMOTET. Investigators have now taken control of its infrastructure in an international coordinated action.

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/

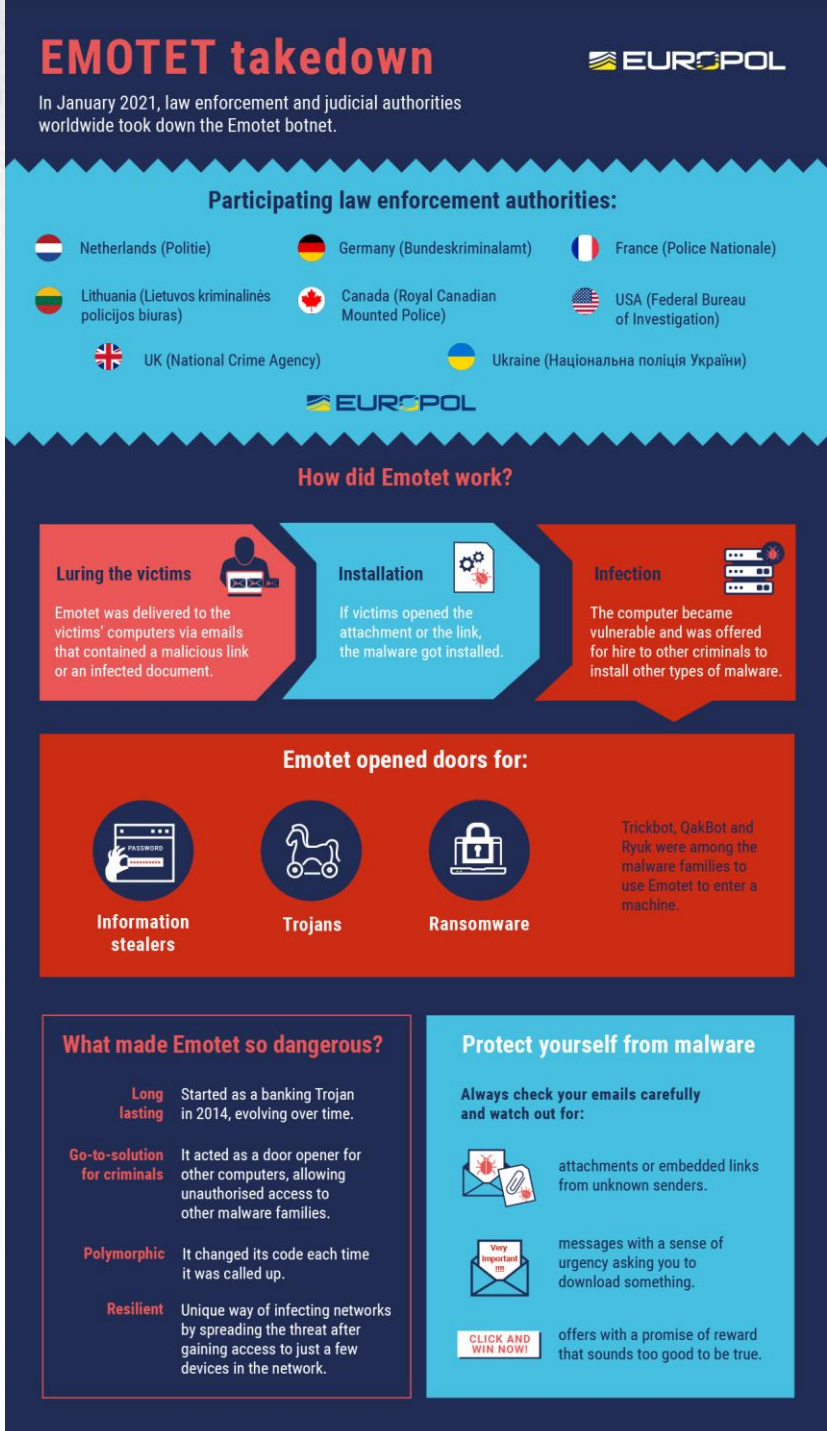
Emotet (II.)



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

Emotet (III.)

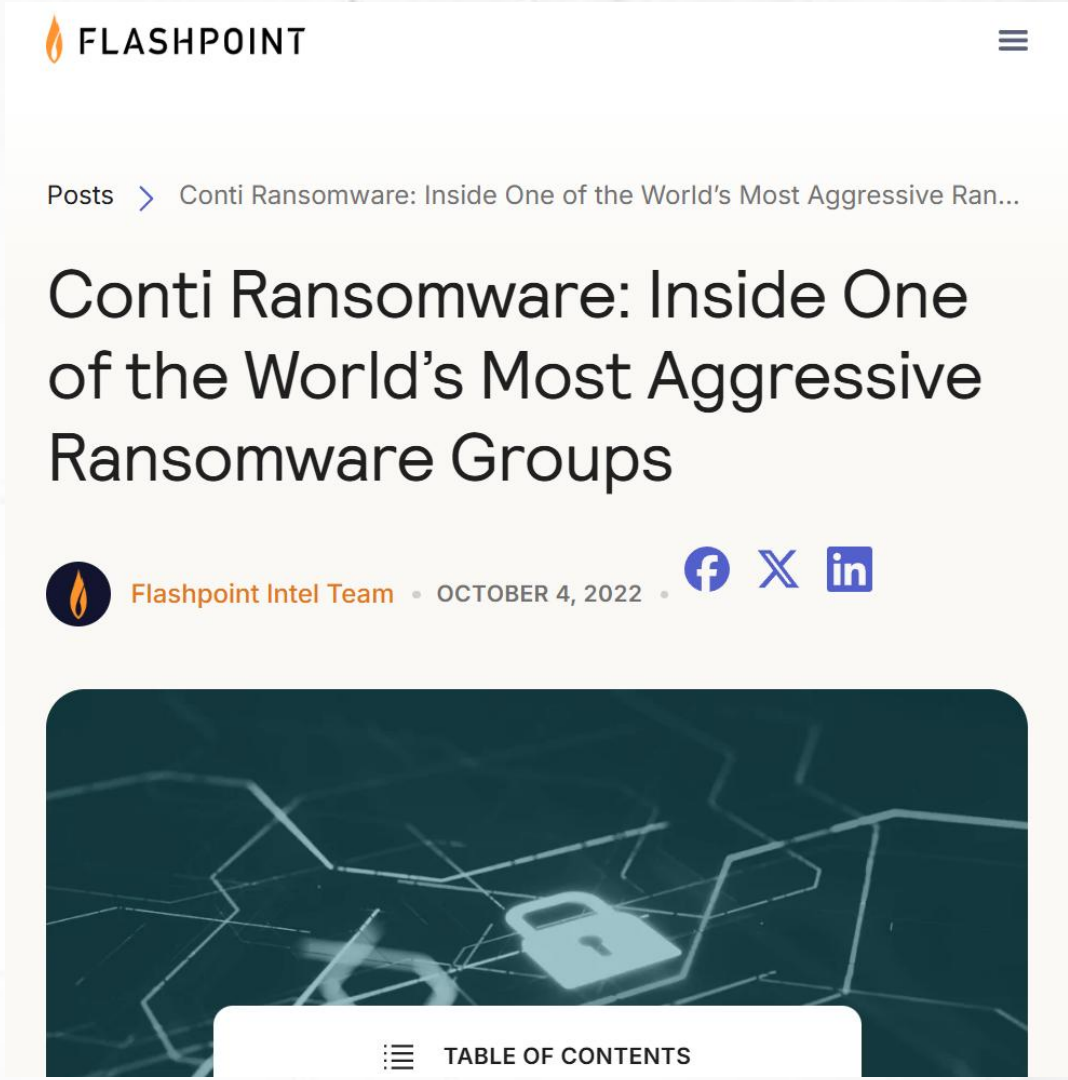
Medzinárodný policajný tím rozvrátil notoricky známy botnet Emotet



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



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.)

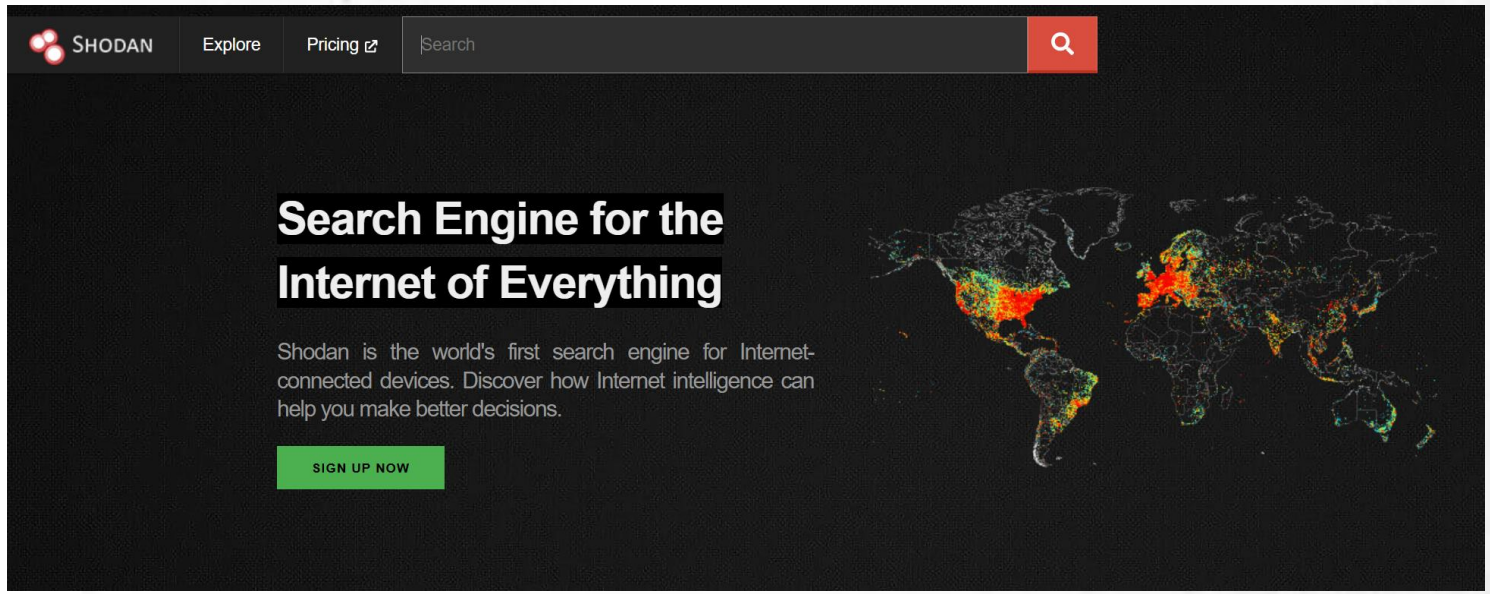
PRIESKUM A VÝBER CIEĽA

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.**



Conti (IV.)

NÁSTROJE OSINT

Vyhľadávače informácií:

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

Vyhľadávanie firiem:

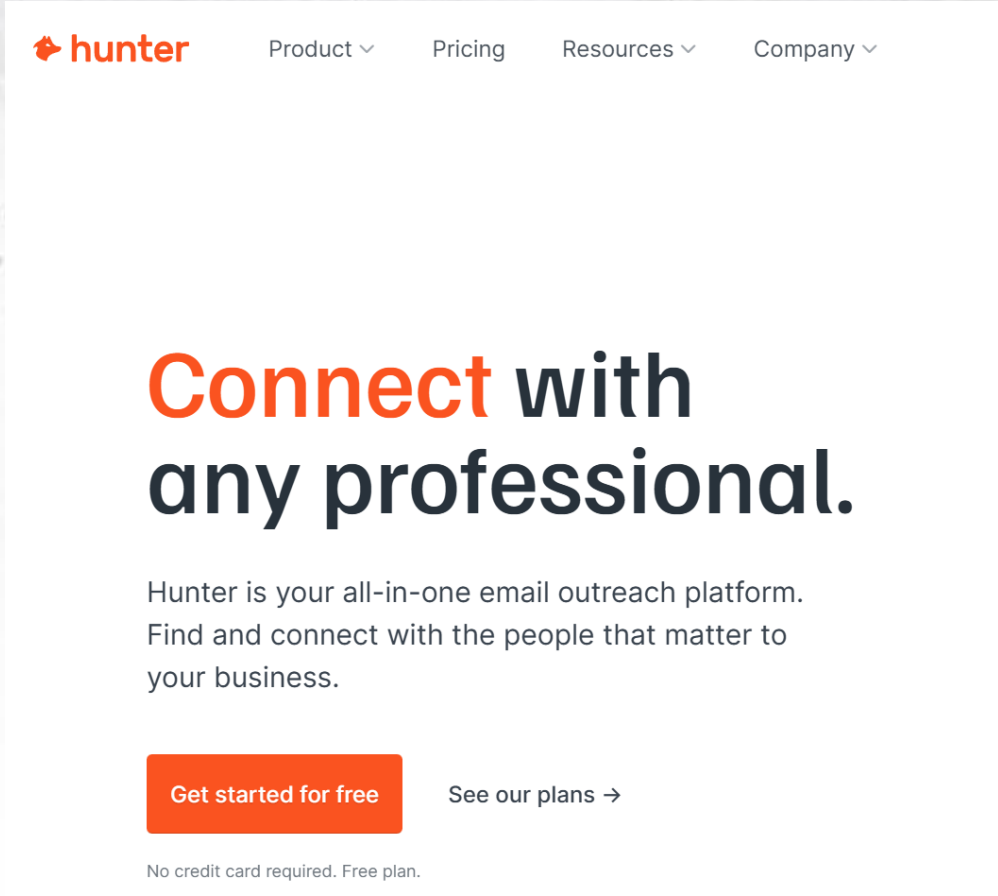
- ZoomInfo – firemné dáta
- OpenCorporates – databáza firiem

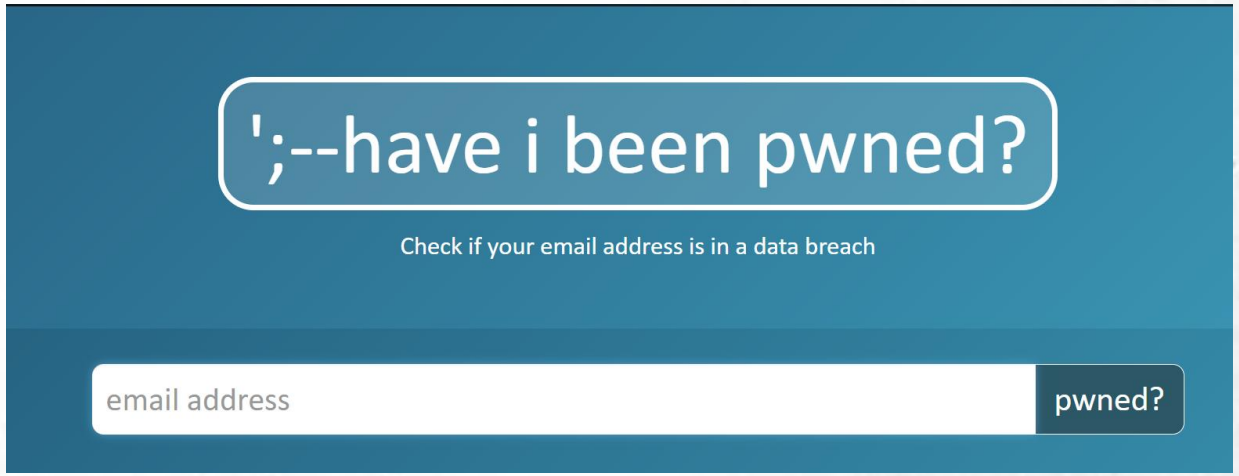
Vyhľadávanie používateľských mien:

- Namechk

Vyhľadávanie emailov:

- Have I Been Pwned





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

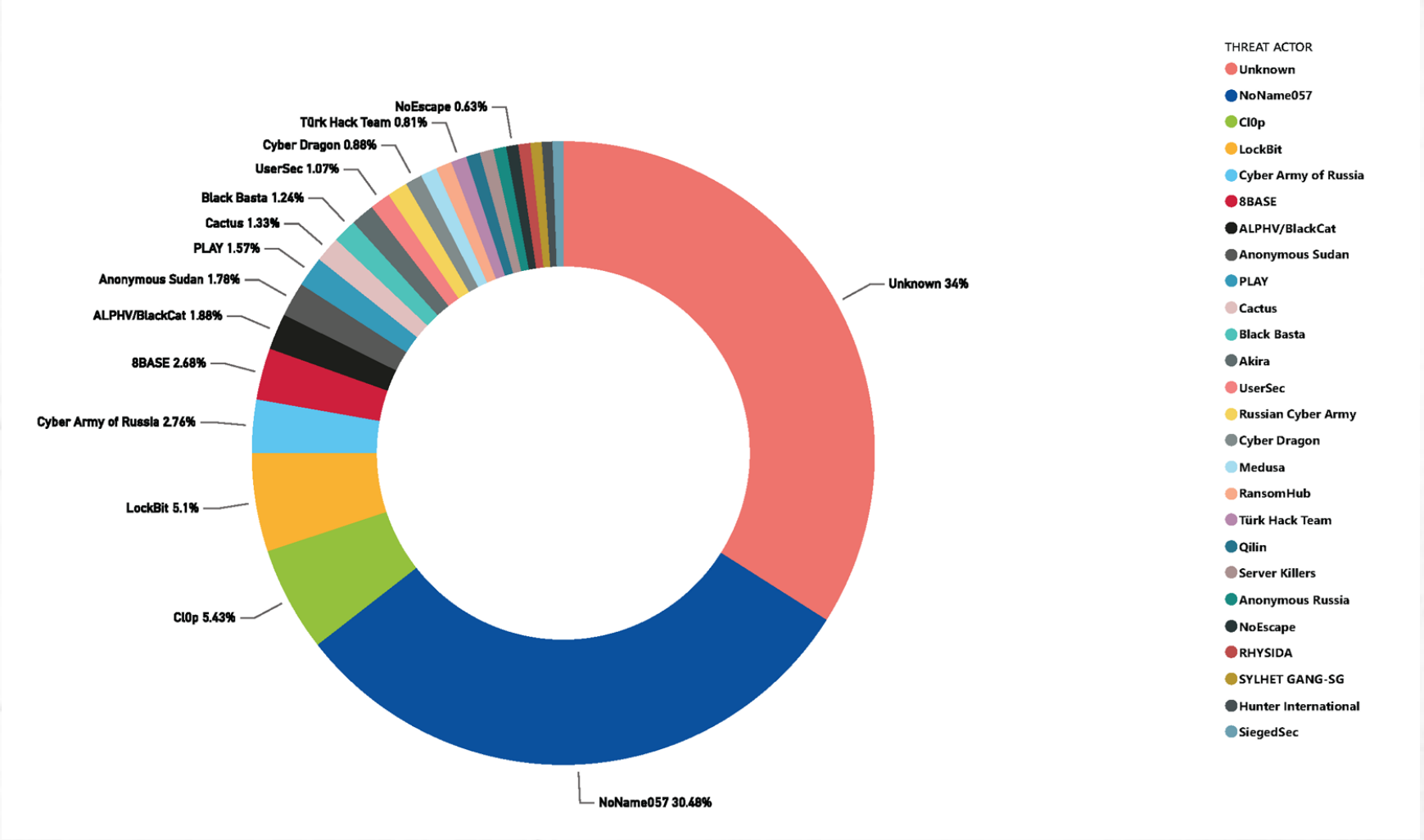
Conti (VI.)

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.)

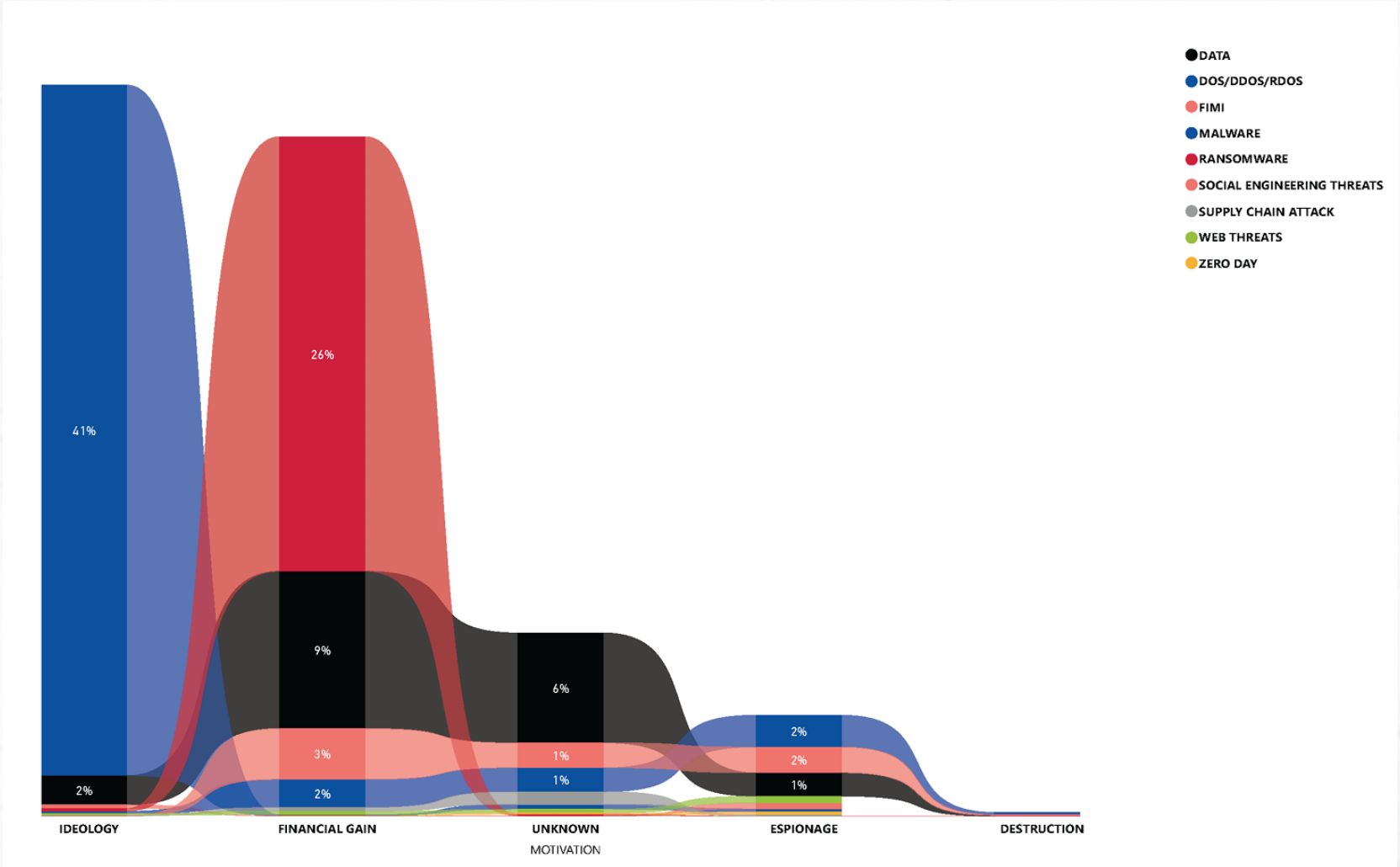
- skupiny útočníkov, júl 2023 – jún 2024



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

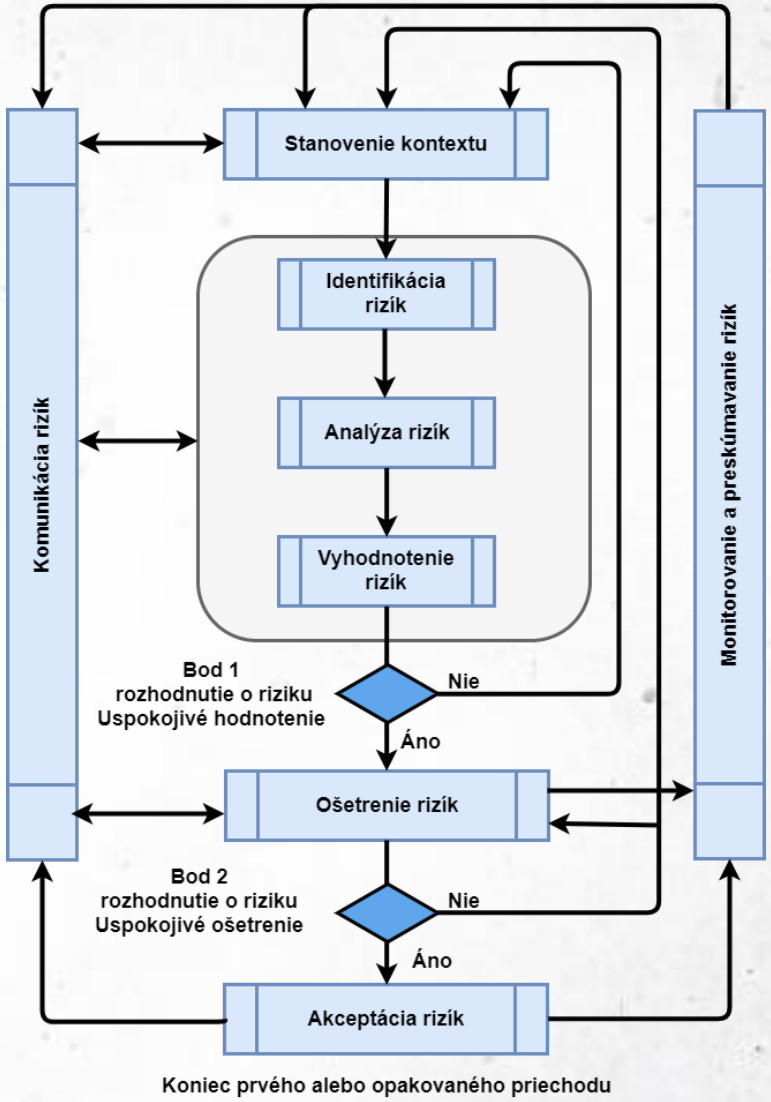
- denno-denná analýza rizík

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

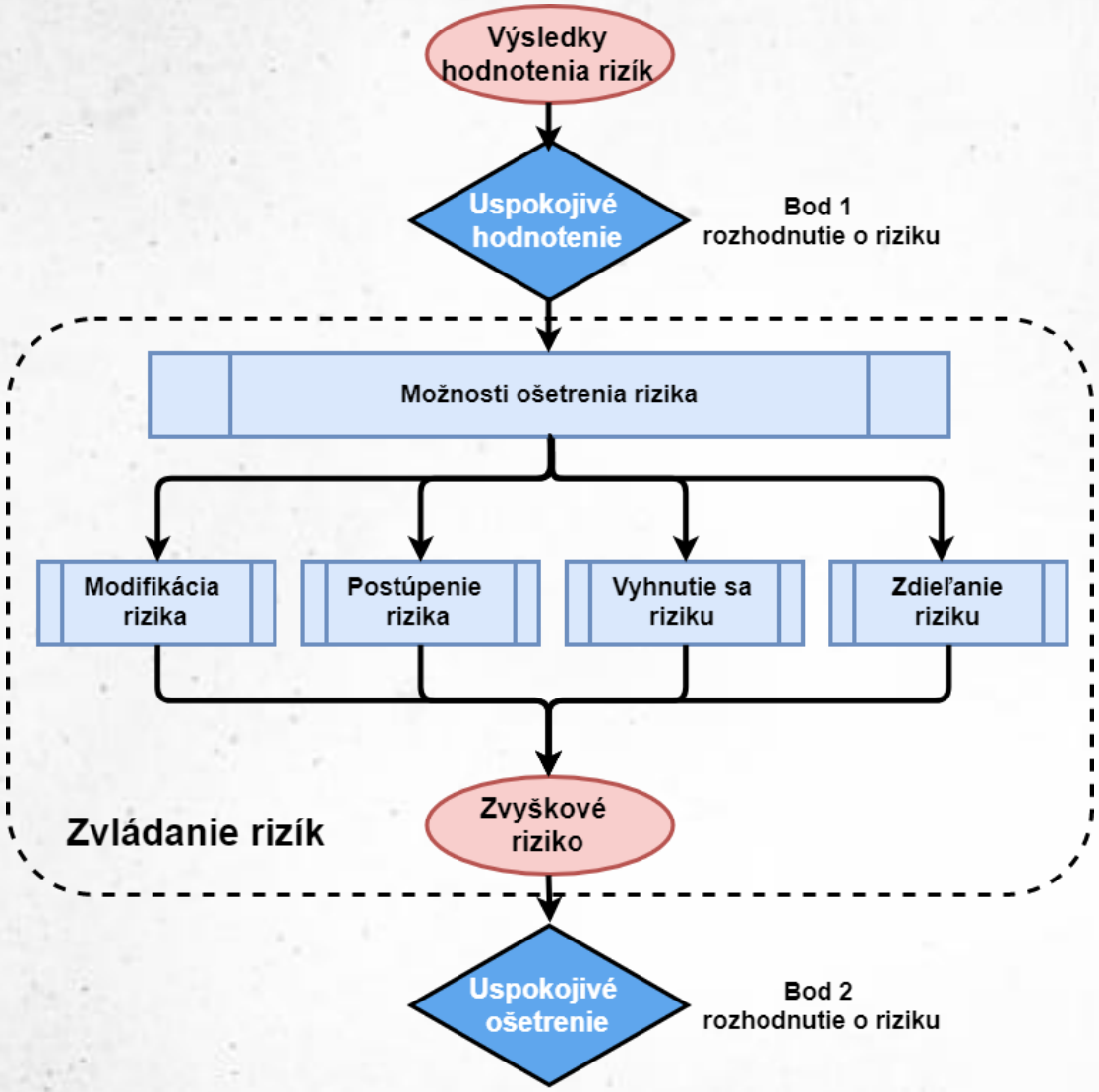


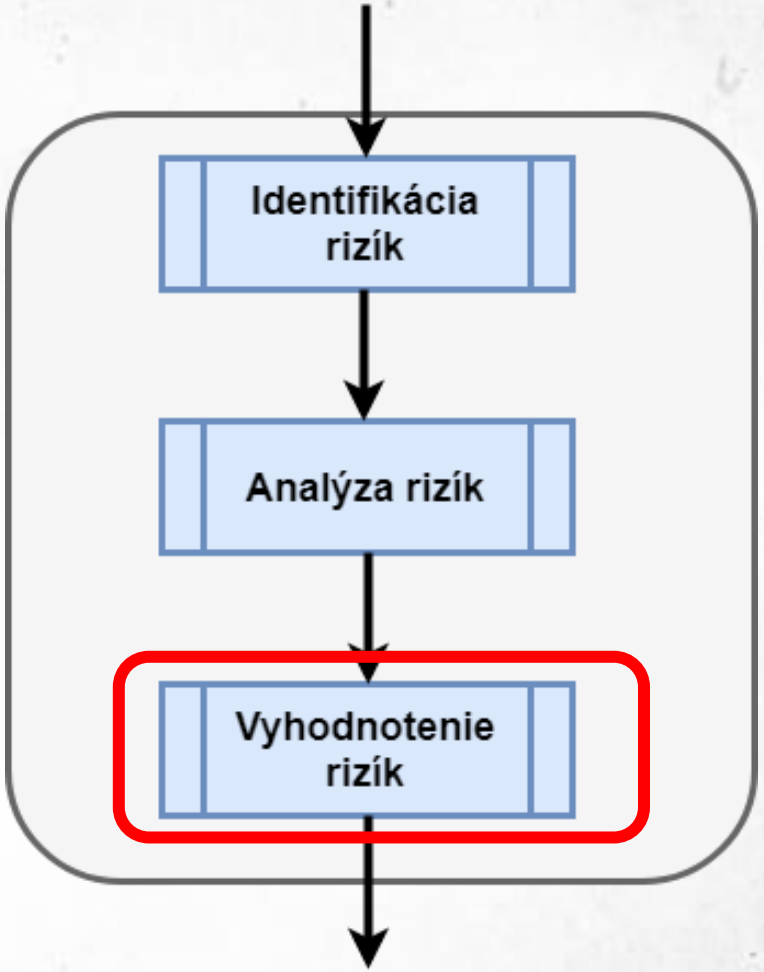
Riziko (III.)

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

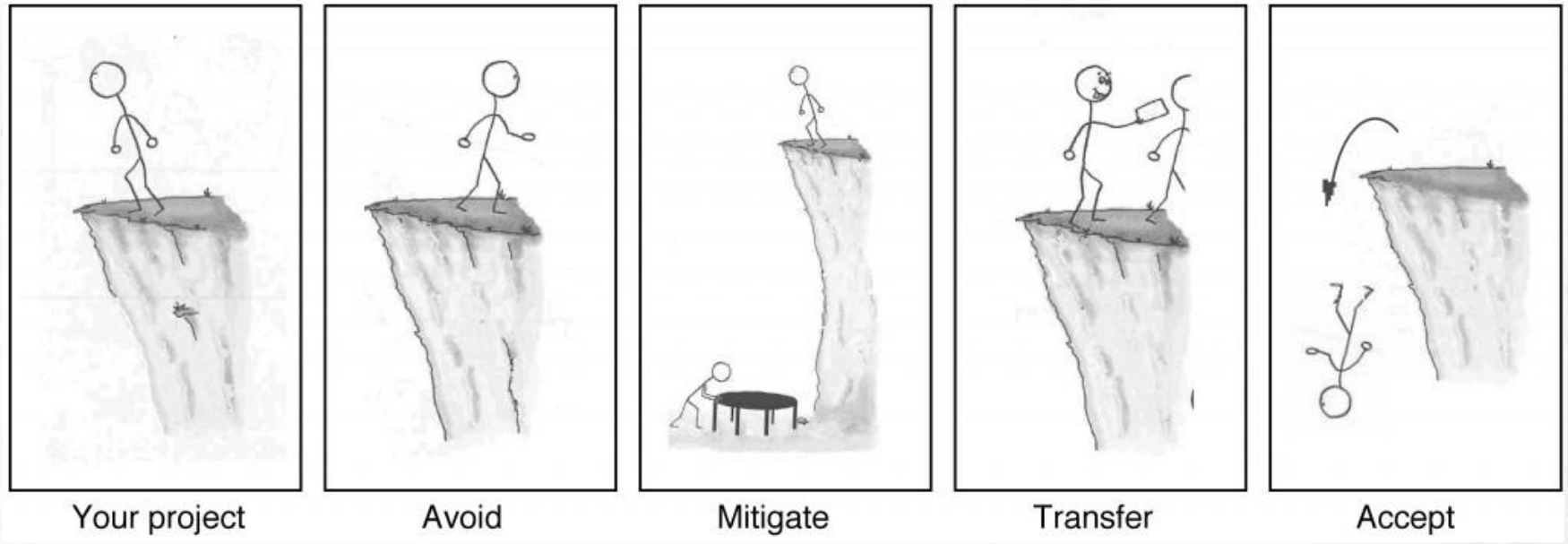
Riziko (IV.)


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)

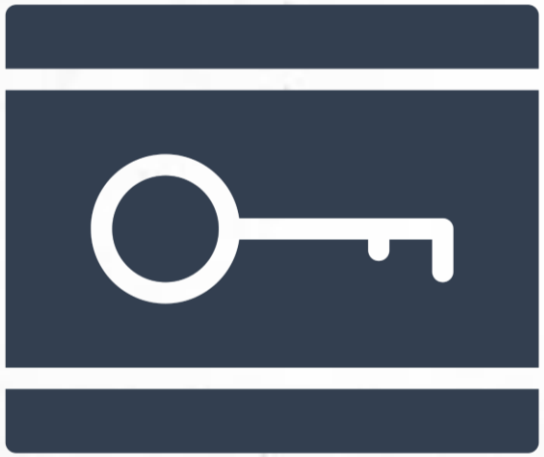


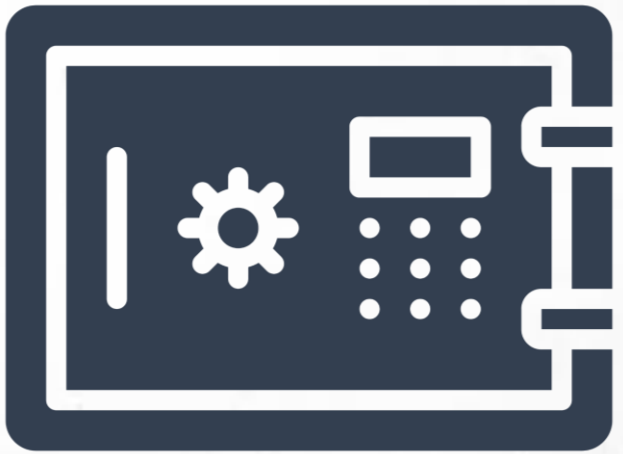
Zdroj: http://cnx.org/content/col11120/1.4/

Bezpečnostné opatrenia (I.)

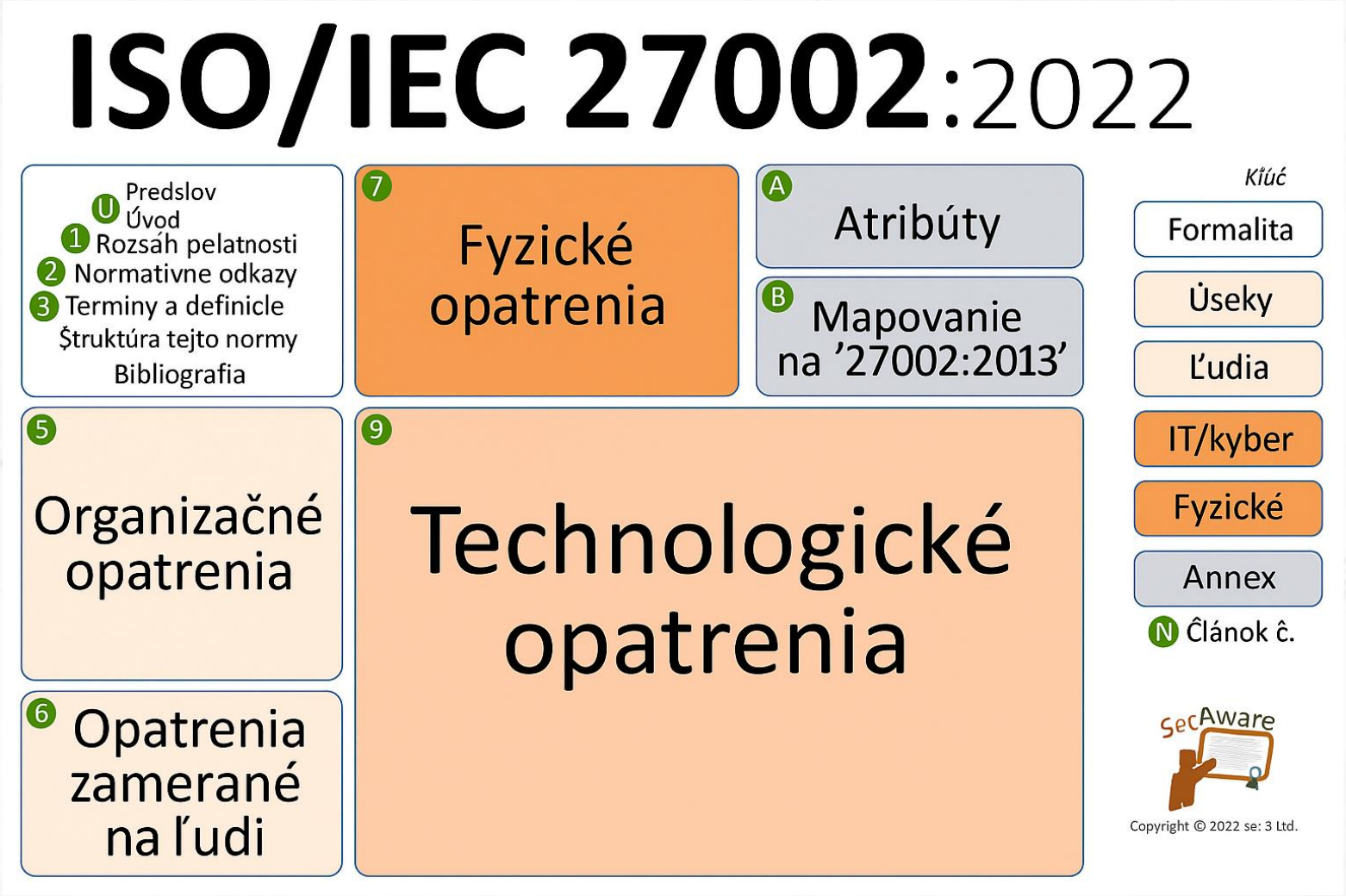
- akákoľvek činnosť, technické zariadenie, proces, mechanizmus, alebo čokoľvek, čo chráni informačný systém a jeho časti (aktíva) pred pôsobením konkrétnych hrozieb alebo hrozby.

- **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

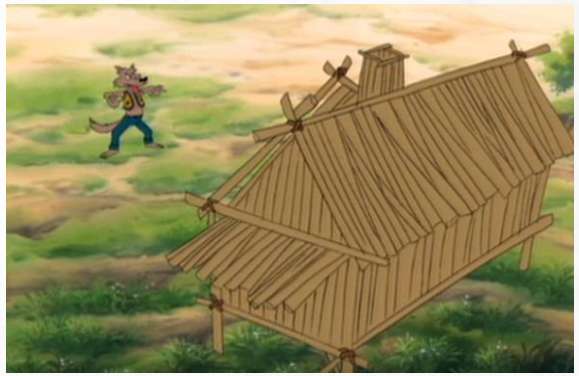
a) organizáciu a riadenie informačnej bezpečnosti a kybernetickej bezpečnosti,
b) správu zraniteľností a kybernetických hrozieb,
c) správu aktív a riadenie kybernetických hrozieb a rizík,
d) riadenie udalostí a kybernetických bezpečnostných incidentov,
e) riadenie kontinuity činností, zálohovanie, obnovu 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.

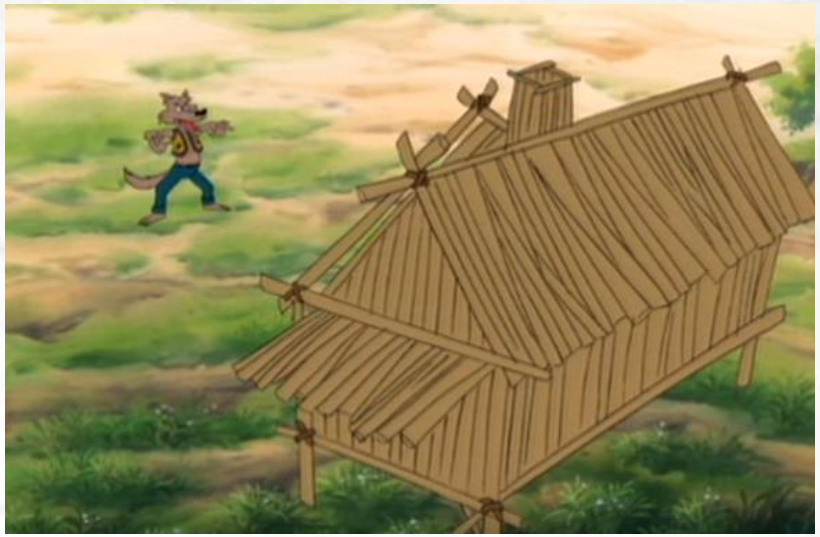
A. Organizácia kybernetickej bezpečnosti a informačnej bezpečnosti
B. Riadenie rizík kybernetickej bezpečnosti a informačnej bezpečnosti
C. Personálna bezpečnosť
D. Riadenie prístupov
E. Riadenie kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahoch s tretími stranami
F. Bezpečnosť pri prevádzke 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



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

monika.rapava@upjs.sk

https://cyberawareness.sk