Reaktívne a proaktívne činnosti

(Vzdelávanie pre zamestnancov verejnej správy v kategórii používateľov „IT manažér“, „informatik“, „zamestnanec v kybernetickej bezpečnosti“ – modul č. 4)

Meno a priezvisko

XX.XX.XXX

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

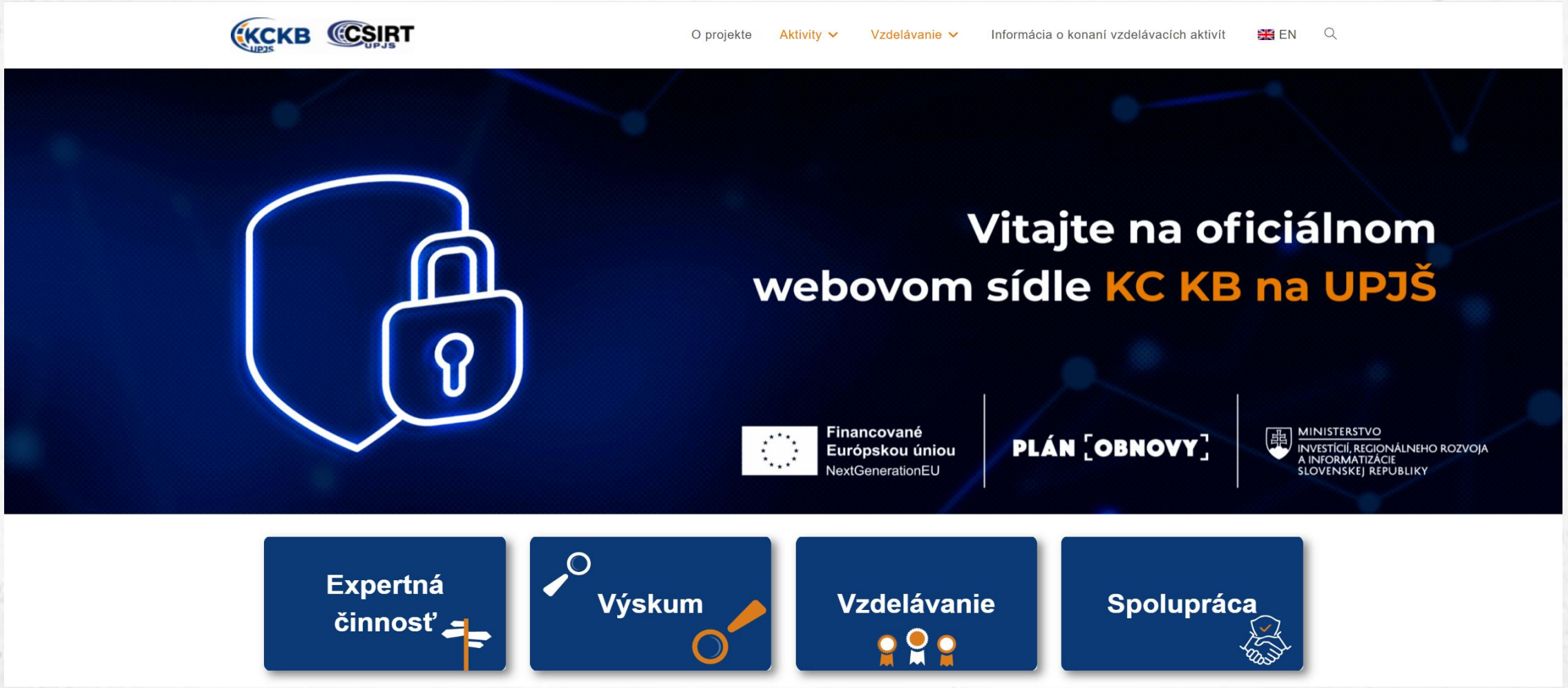
Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KC KB UPJŠ

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



Vzdelávacia aktivita (I.)

- Časový harmonogram
  - 08:30 – 10:00 – 1. blok
  - 10:00 – 11:30 – 2. blok
  - 11:30 – 12:30 – obedňajšia prestávka
  - 12:30 – 14:00 – 3. blok
  - 14:00 – 15:30 – 4. blok

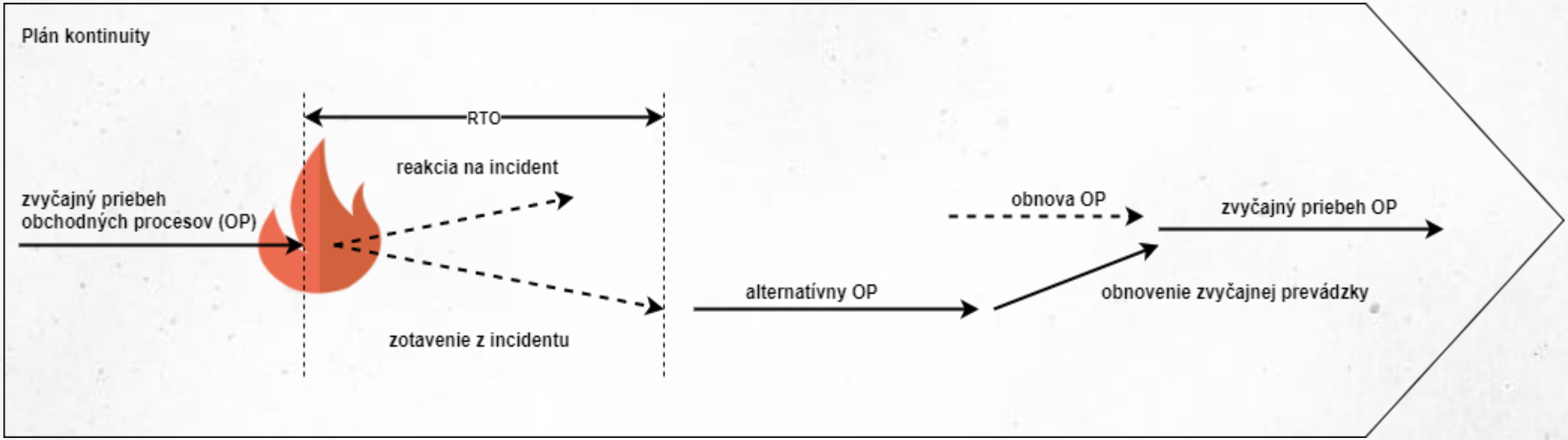
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Vzdelávacia aktivita (II.)

Číslo modulu	Názov modulu	Časová dotácia (45 min.)	Forma stretnutia
Modul č. 1	**Úvod do KIB a riadenie KIB**	8	Online / Prezenčne
Modul č. 2	**Vybrané kapitoly z kryptografie**	8	Prezenčne
Modul č. 3	**Vybrané kapitoly zo sieťovej bezpečnosti**	16	Prezenčne
Modul č. 4	**Reaktívne a proaktívne činnosti**	8	Prezenčne
Modul č. 5	**Reaktívne činnosti – komunikácia**	6	Prezenčne
Modul č. 6	**Vybrané kapitoly z práva informačných a komunikačných technológií I.**	8	Online / Prezenčne
Modul č. 7	**Vybrané kapitoly z práva informačných a komunikačných technológií II.**	8	Online / Prezenčne

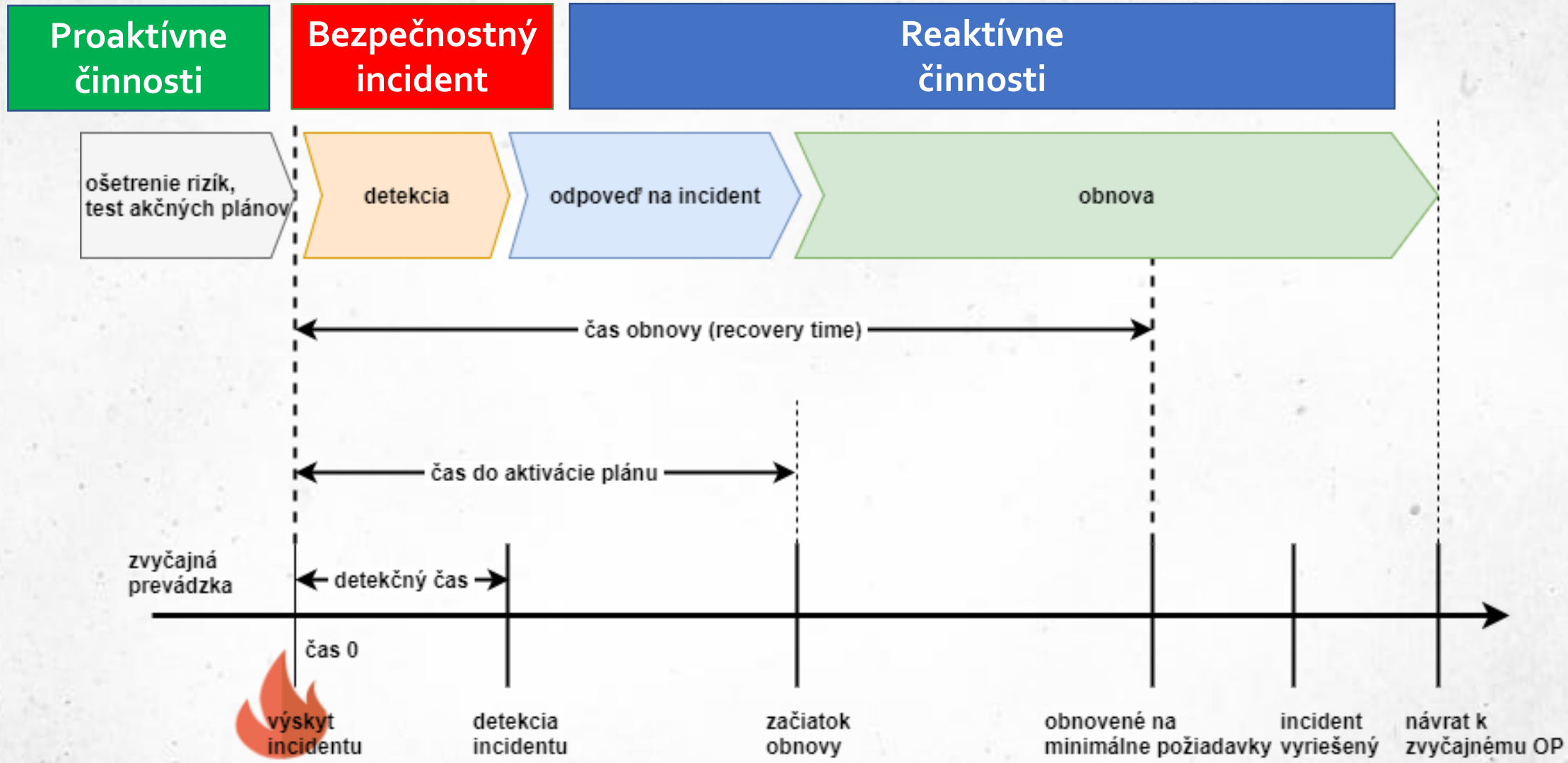
Kontinuita činností (I.)

- *schopnosť organizácie pokračovať v dodávke produktov a služieb v prijateľných časových rámcoch pri vopred definovanej kapacite počas narušenia* (ISO/IEC 22301:2019)



Zdroj: ISO/IEC 270035:2011

Kontinuita činností (II.)



Kontinuita činností (III.)

Prevencia

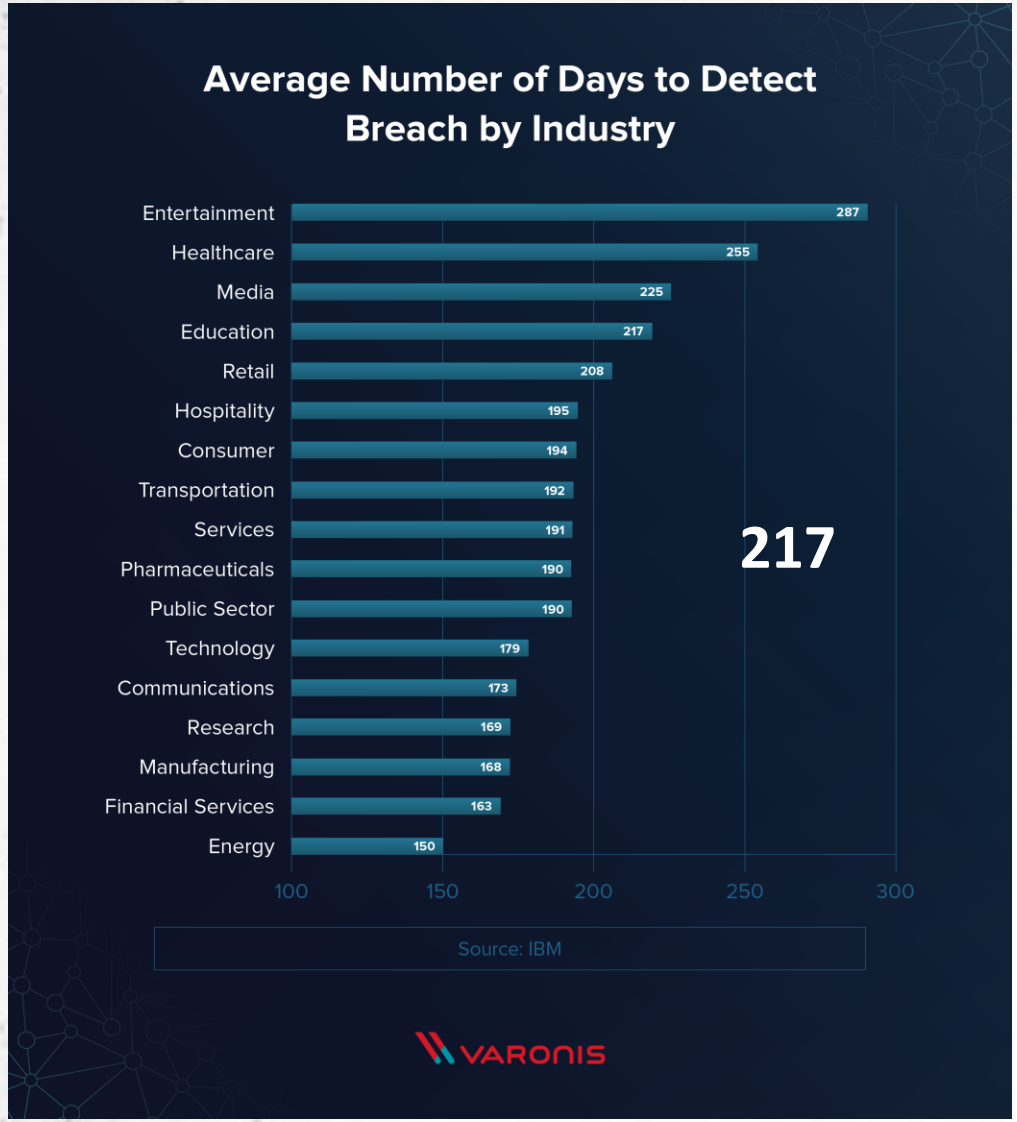
Detekcia

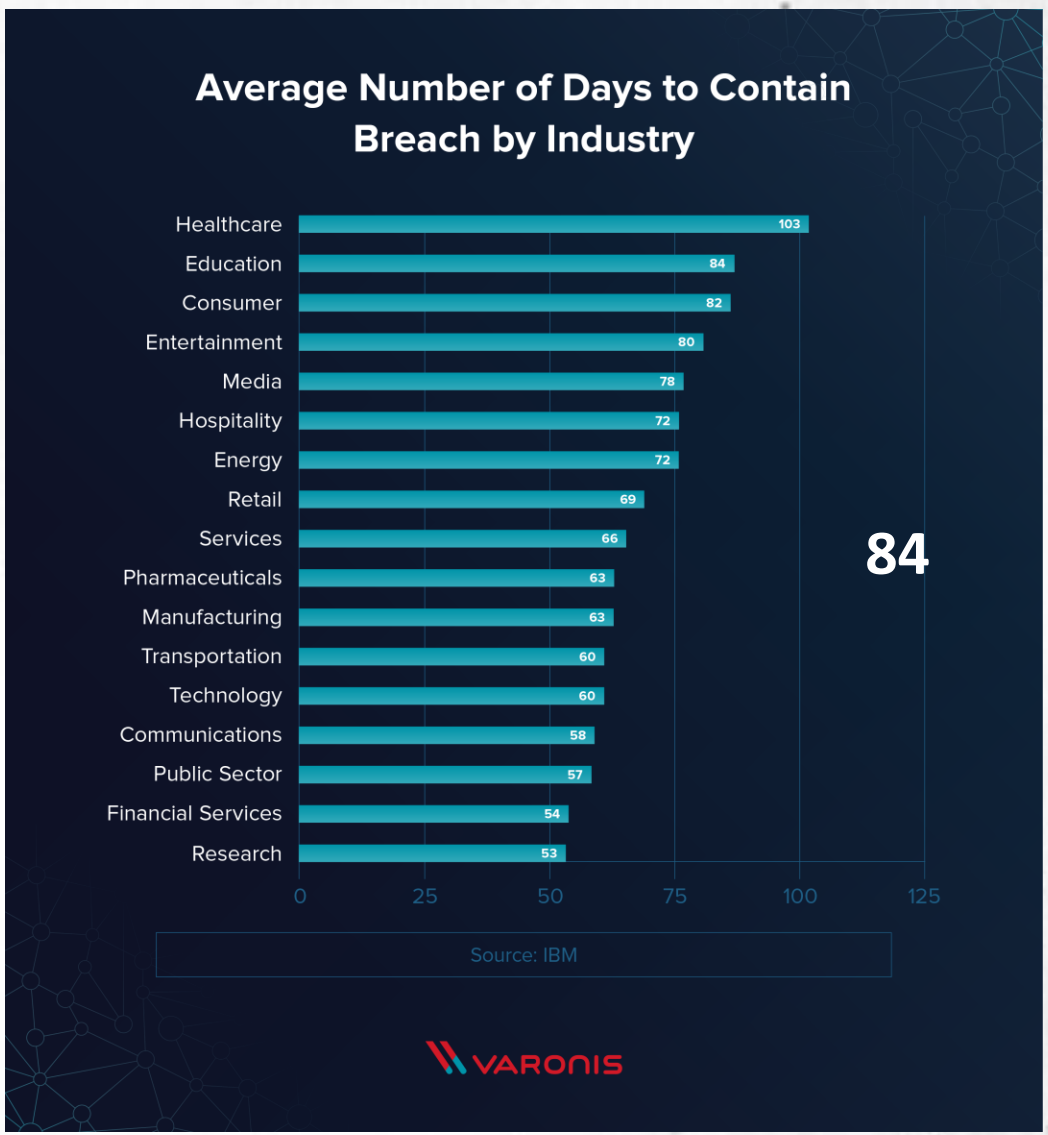
Odpoveď

Proaktívne činnosti

Reaktívne činnosti

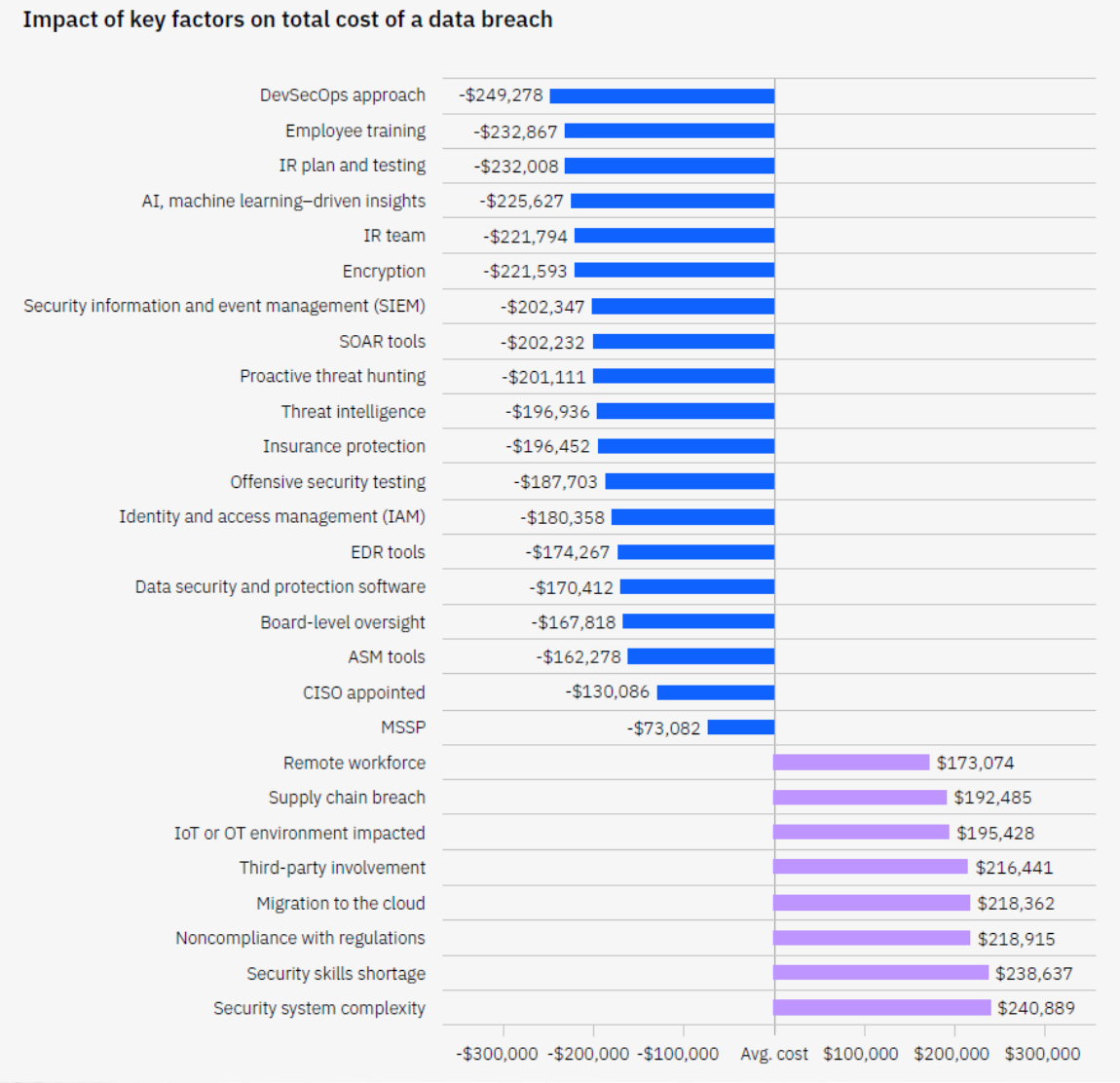
Kontinuita činností (IV.)





Zdroj: https://www.varonis.com/blog/data-breach-response-times/

Kontinuita činností (V.)

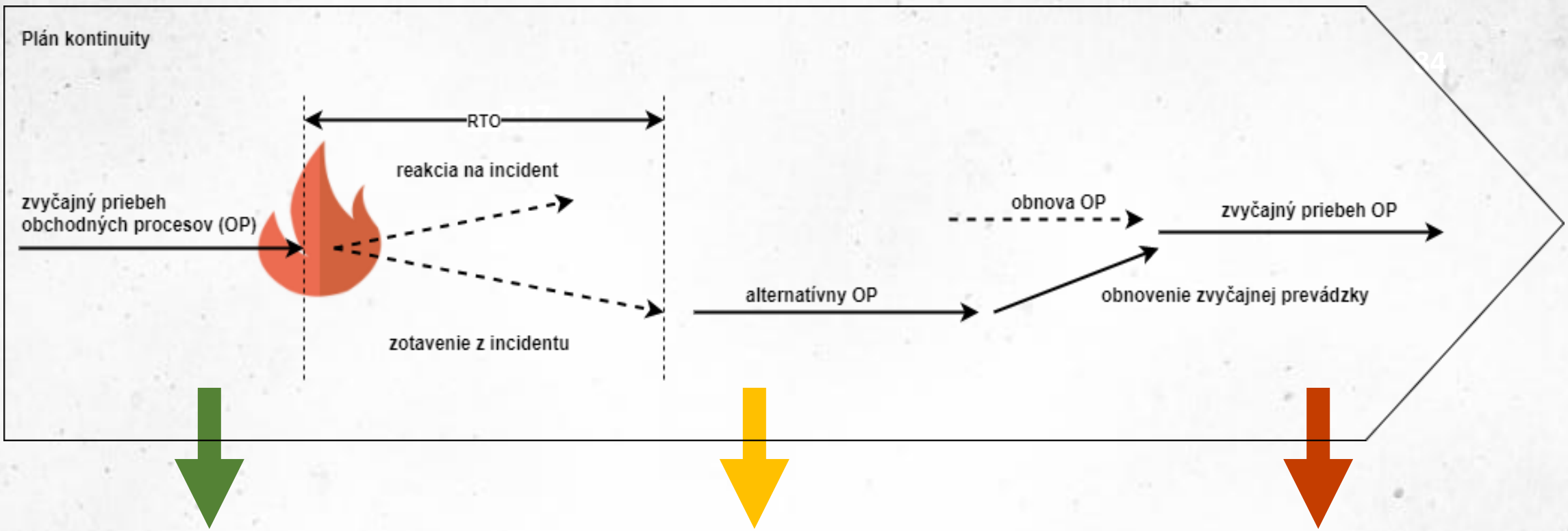


Zdroj: IBM Security - Cost of a Data Breach Report 2023

Faktory:

- Vzdelávanie zamestnancov
- Plány na riešenie incidentov a ich testovanie
- Tím na riešenie incidentov
- Šifrovanie
- Použitie monitorovanie
- ..

Kontinuita činností (VI.)



Reakcia na incident

(IR)

Kontinuita činností

(BC)

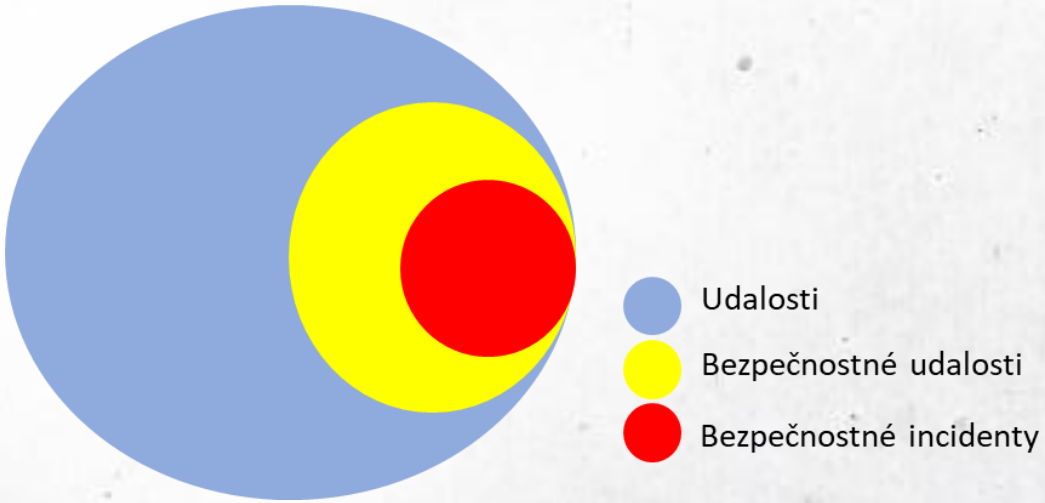
Obnova činností

(BR)

Zdroj: IBM Security - Cost of a Data Breach Report 2023

Bezpečnostný incident

- **Udalosť** – akúkoľvek pozorovateľnú udalosť, ku ktorej došlo v určitom časovom bode v systéme alebo sieti, najmä ak je dôležitá
- **Bezpečnostná udalosť** – pozorovateľná udalosť v prostredí informačných a komunikačných technológií, ktorá je relevantná pre bezpečnosť
- **Bezpečnostný incident** – porušenie alebo bezprostrednú hrozbu porušenia pravidiel počítačovej bezpečnosti, prijateľných zásad používania alebo štandardných bezpečnostných postupov



Cieľ riešenia bezpečnostného incidentu

Zastaviť útok

Zistiť vektor útoku

Zistiť dopad pre organizáciu

Návrh bezpečnostných opatrení

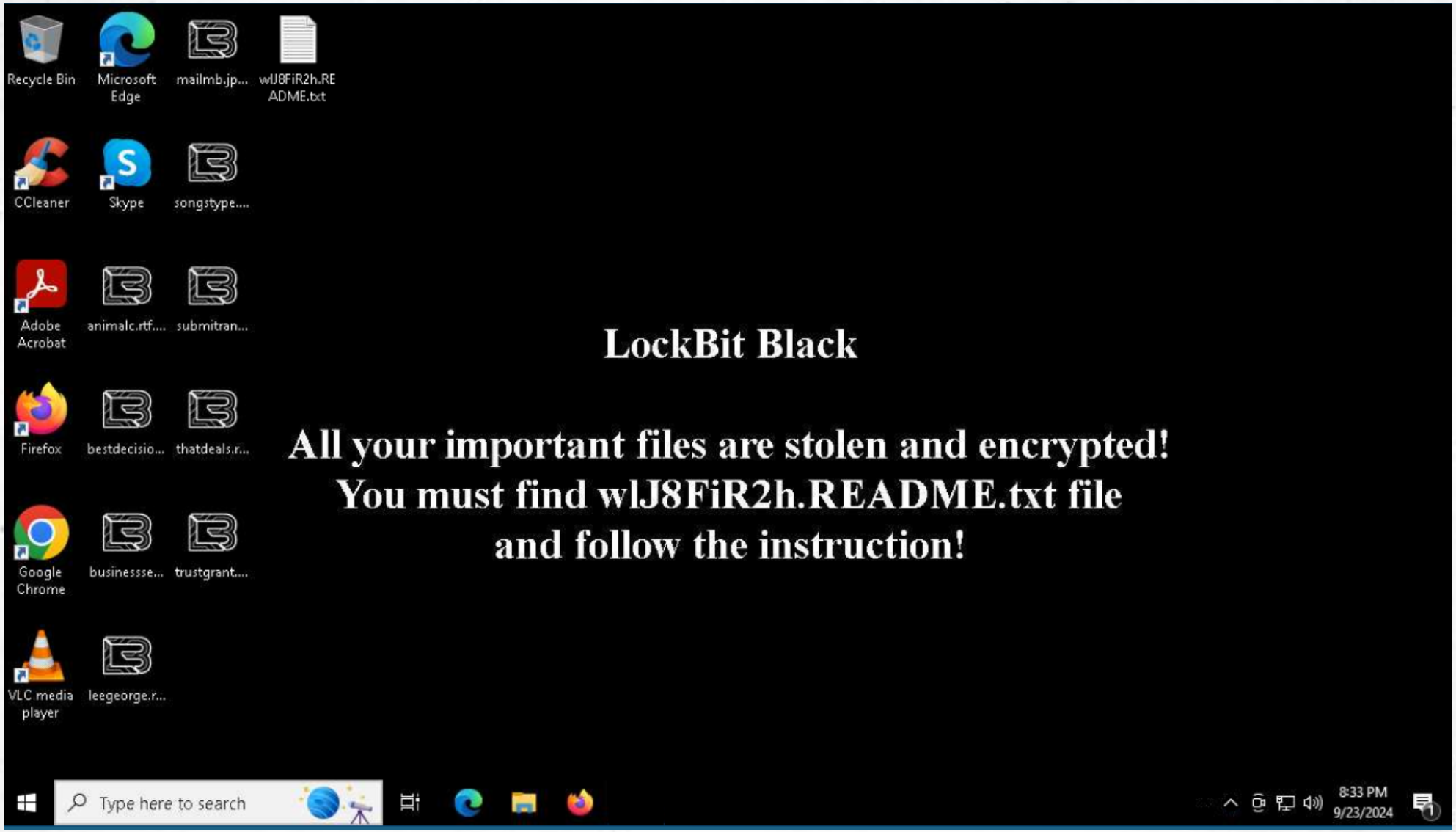
Právny rámec

- 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)
- Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti
- Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe

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

TEST

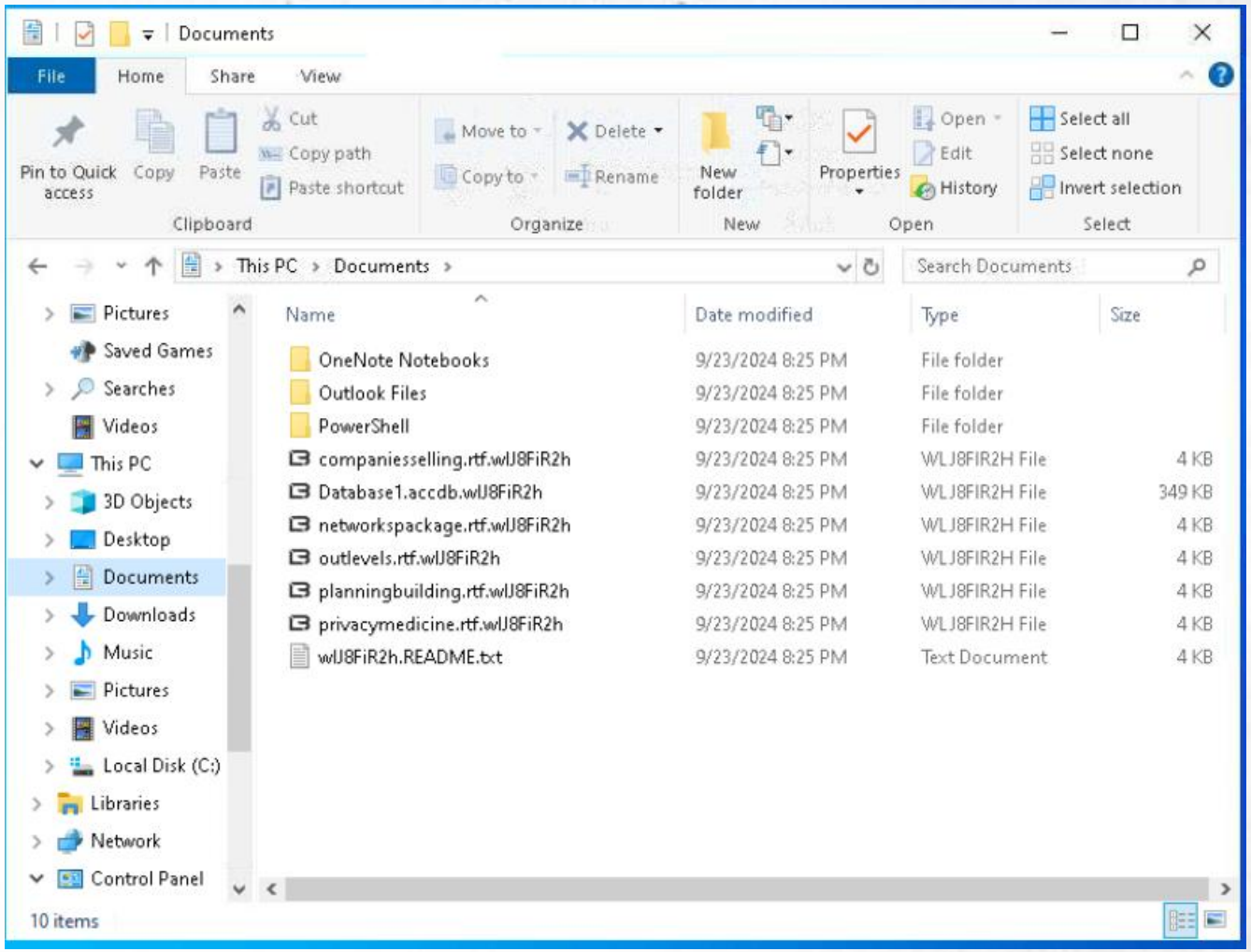
Scenár (I.)



TEST

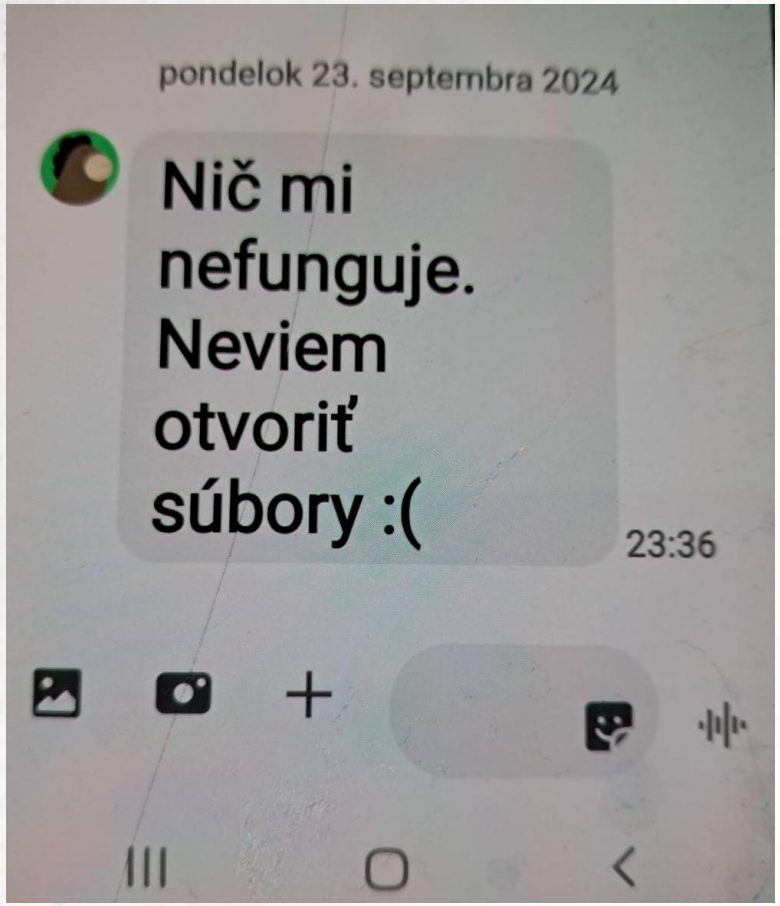
Scenár (II.)

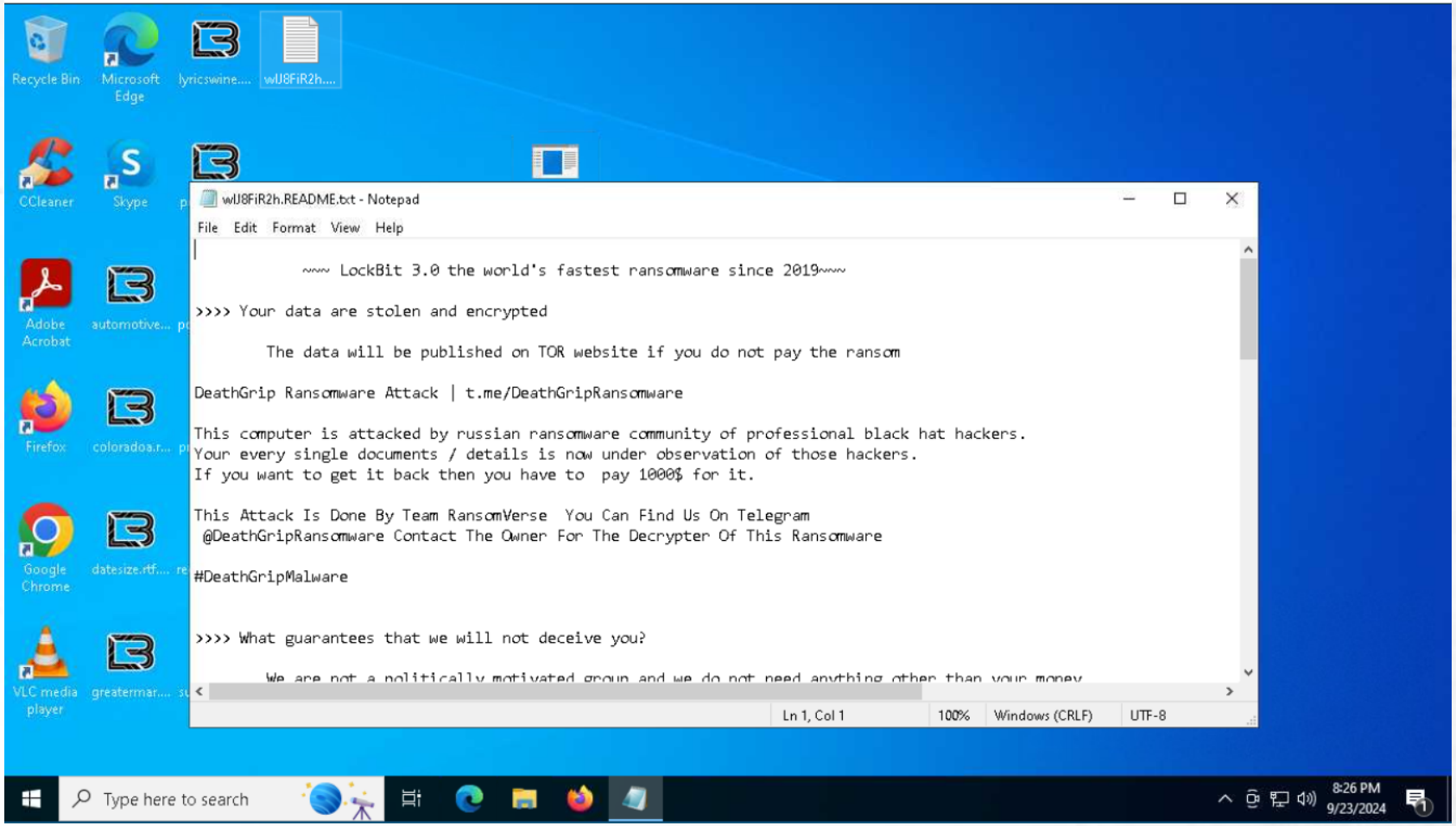
- Nejde otvoriť žiadne súbory
- Dokonca ani na úložisku organizácie
- IT podpora je nedostupná
- Kolegovia volajú/píšu SMS správy



TEST

Scenár (III.)





Aké budú Vaše prvé kroky?

TEST

Scenár (IV.)

- Ransom note – informácia o výkupnom

“ ~~~ LockBit 3.0 the world's fastest and most stable ransomware from 2019~~~

>>>>> Your data is stolen and encrypted.

If you don't pay the ransom, the data will be published on our TOR darknet sites. Keep in mind that once your data appears on our leak site, it could be bought by your competitors at any second, so don't hesitate for a long time. The sooner you pay the ransom, the sooner your company will be safe.

Tor Browser Links:

-

Links for normal browser:

-

>>>>> What guarantee is there that we won't cheat you?

We are the oldest ransomware affiliate program on the planet, nothing is more important than our reputation. We are not a politically motivated group and we want nothing more than money. If you pay, we will provide you with decryption software and destroy the stolen data. After you pay the ransom, you will quickly make even more money. Treat this situation simply as a paid training for your system administrators, because it is due to your corporate network not being properly configured that we were able to attack you. Our pentest services should be paid just like you pay the salaries of your system administrators. Get over it and pay for it. If we don't give you a decryptor or delete your data after you pay, no one will pay us in the future. You can get more information about us on Ilon Musk's Twitter hxxps://twitter.com/hashtag/lockbit?f=live

>>>>> You need to contact us and decrypt one file for free on TOR darknet sites with your personal ID

Download and install Tor Browser hxxps://www.torproject.org/

Write to the chat room and wait for an answer, we'll guarantee a response from you. If you need a unique ID for correspondence with us that no one will know about, tell it in the chat, we will generate a secret chat for you and give you his ID via private one-time memos service, no one can find out this ID but you. Sometimes you will have to wait some time for our reply, this is because we have a lot of work and we attack hundreds of companies around the world.

Tor Browser Links for chat:

Tor Browser Links for chat:

-

>>>

>>>>> Your personal ID: - <<<<<

>>>

>>>>> Warning! Do not delete or modify encrypted files, it will lead to problems with decryption of files!

>>>>> Don't go to the police or the FBI for help and don't tell anyone that we attacked you.

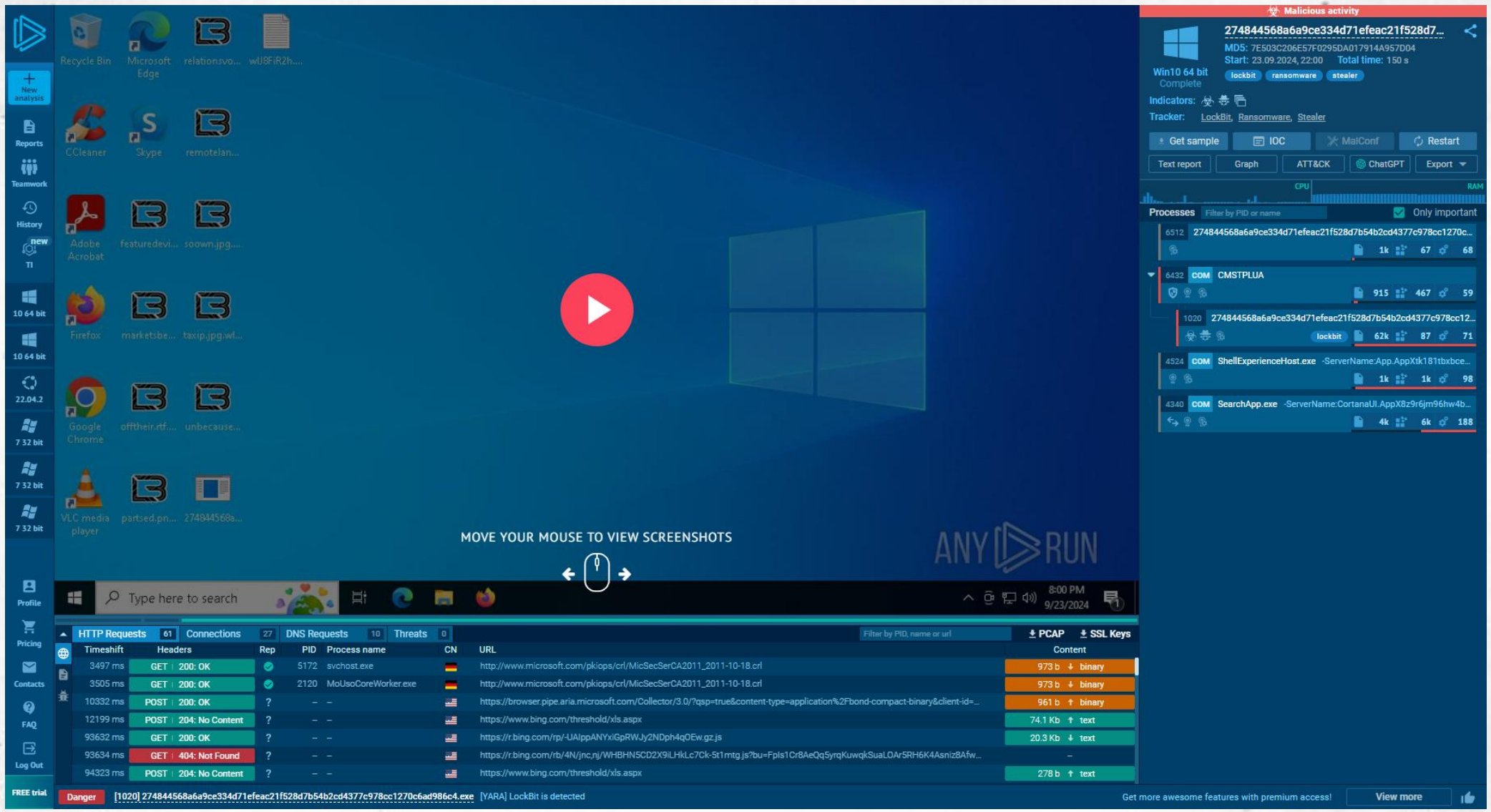
They won't help and will only make things worse for you. In 3 years not a single member of our group has been caught by the police, we are top notch hackers and we never leave a trail of crime. The police will try to prohibit you from paying the ransom in any way. The first thing they will tell you is that there is no guarantee to decrypt your files and remove stolen files, this is not true, we can do a test decryption before paying and your data will be guaranteed to be removed because it is a matter of our reputation, we make hundreds of millions of dollars and are not going to lose our revenue because of your files. It is very beneficial for the police and FBI to let everyone on the planet know about your data leak because then your state will get the fines budgeted for you due to GDPR and other similar laws. The fines will be used to fund the police and the FBI, they will eat more sweet coffee donuts and get fatter and fatter. The police and the FBI don't care what losses you suffer as a result of our attack, and we will help you get rid of all your problems for a modest sum of money. Along with this you should know that it is not necessarily your company that has to pay the ransom and not necessarily from your bank account, it can be done by an unidentified person, such as any philanthropist who loves your company, for example, Elon Musk, so the police will not do anything to you if someone pays the ransom for you. If you're worried that someone will trace your bank transfers, you can easily buy cryptocurrency for cash, thus leaving no digital trail that someone from your company paid our ransom. The police and FBI will not be able to stop lawsuits from your customers for leaking personal and private information. The police and FBI will not protect you from repeated attacks. Paying the ransom to us is much cheaper and more profitable than paying fines and legal fees.

>>>>> What are the dangers of leaking your company's data.

First of all, you will receive fines from the government such as the GDRP and many others, you can be sued by customers of your firm for leaking information that was confidential. Your leaked data will be used by all the hackers on the planet for various unpleasant things. For example, social engineering, your employees' personal data can be used to re-infiltrate your company. Bank details and passports can be used to create bank accounts and online wallets through which criminal money will be laundered. On another vacation trip, you will have to explain to the FBI where you got millions of dollars worth of stolen cryptocurrency transferred through your accounts on cryptocurrency exchanges. Your personal information could be used to make loans or buy appliances. You would later have to prove in court that it wasn't you who took out the loan and pay off someone else's loan. Your competitors may use the stolen information to steal technology or to improve their processes, your working methods, suppliers, investors, sponsors, employees, it will all be in the public domain. You

Ako postupovať ďalej?

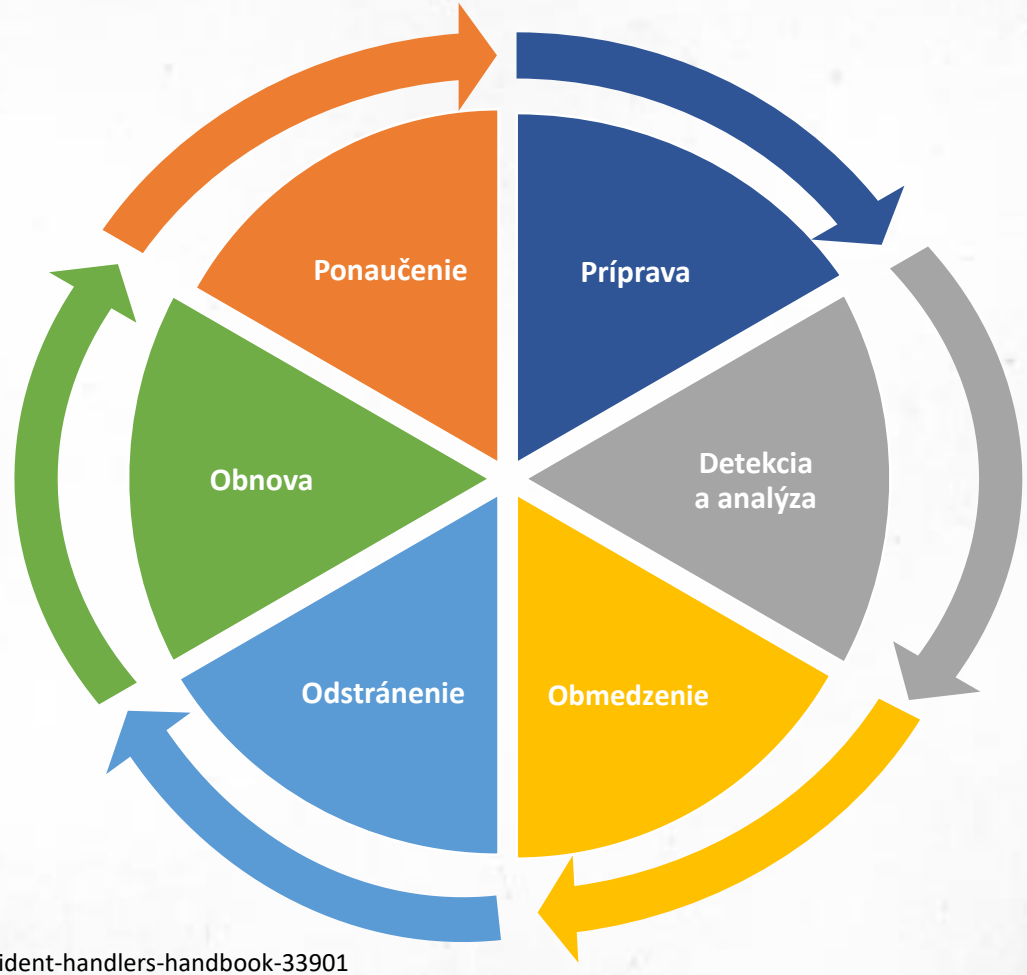
Ukážka ransomvér útoku



Zdroj: https://app.any.run/tasks/7c048de1-ccdc-47df-9f0f-985cf31dea76

Postup riešenia bezpečnostného incidentu

- Fázy riešenia bezpečnostných incidentov podľa **SANS**



Zdroj: https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

Identifikácia bezpečnostných incidentov

- Incidentom sa vždy nedá zabrániť, musia sa však vždy identifikovať
- **Externé zdroje**
  - Iné organizácie – hlásenia (SK-CERT,...)
  - Automatizované systémy (napr. have I been pwned?)
- **Interné zdroje**
  - Nahlasovanie cez kontaktné miesto (email/telefón)
  - Monitorovanie (SIEM)
  - Vlastná dohľadávacia činnosť
- ***Ako identifikujete bezpečnostné incidenty?***

Nahlásenie incidentu

Ak chcete nahlásiť incident, zavolajte na niektoré z týchto telefónnych čísel alebo nám pošlite email. Všetky potrebné detaily si od Vás počas rozhovoru vypýtame.

+421 55 234 1111

incident@upjs.sk

Pracovné hodiny: 8:00-16:00

Všeobecný email

csirt@upjs.sk

Facebook

CSIRT-UPJS

Adresa

CSIRT
Univerzita Pavla Jozefa Šafárika
Šrobárova 2
041 80 Košice

PGP kľúč

```
User ID: CSIRT team UPJS <csirt@upjs.sk>
Key ID: 0x0C62E396</csirt@upjs.sk>
Exp: n/a
Fingerprint: BBD5 D706 CBA1 FD9D 3A3B 0B9E 2AF6 8D10 0C62 E396
```

Zdroj: https://csirt.upjs.sk/#/kontakt

Analýza bezpečnostných incidentov

- Overiť si udalosť
- Bezpečnostný incident vs. technický incident
- Určenie typu bezpečnostného incidentu
  - Zdieľanie informácií
  - Spustenie špecifického postupu
- Predbežné určenie rozsahu
  - **určenie rozsahu** - identifikácia systémov, ľudí a informačných aktív, ktoré sú súčasťou udalosti.
  - **podozrivé udalosti** – nové účty, modifikácia súborov, zmeny vo výkone a pod.
- ***Máte IT oddelenie? Špecifický postup?***

Taxonómia bezpečnostných incidentov (I.)

- eCSIRT.net mkIV.
- CIRCL.LU taxonómia,
- Spoločná taxonómia pre orgány činné v trestnom konaní a jednotky CSIRT (Common Taxonomy for LE and CSIRTs).

REFERENCE TAXONOMY INCIDENT CLASSIFICATION (1ST COLUMN)	INCIDENT EXAMPLES (2ND COLUMN)
Malicious Code	Virus
	Worm
	Trojan
	Spyware
	Dialler
	Rootkit

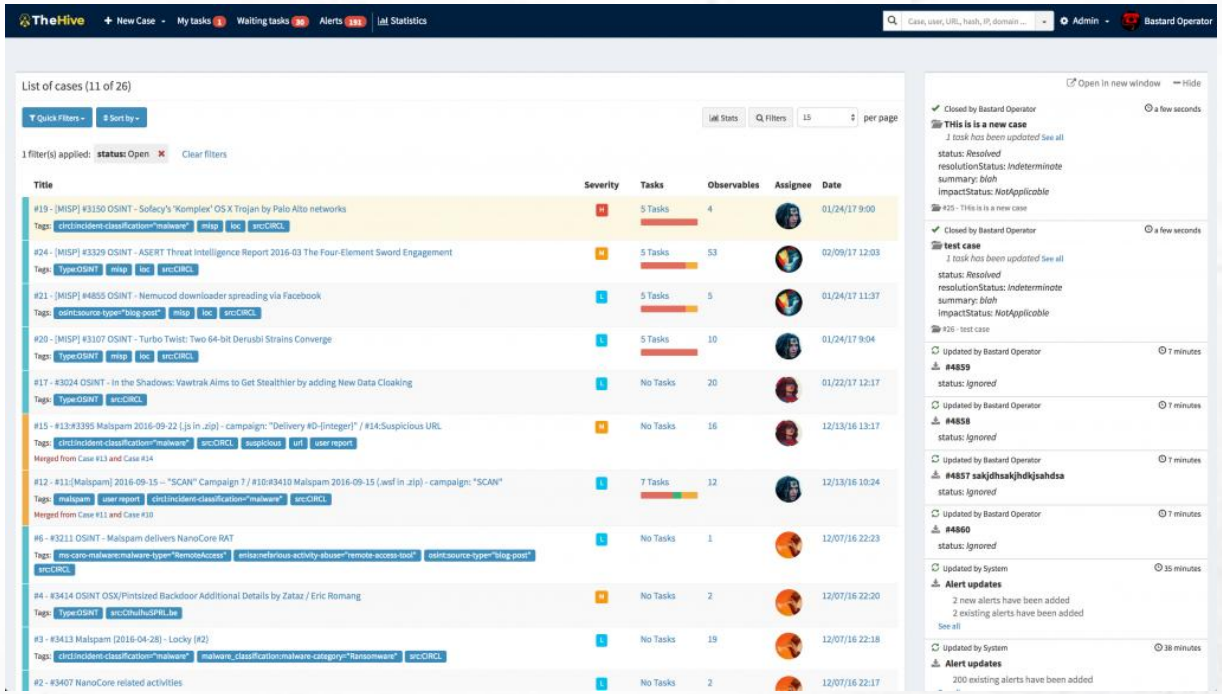
INCIDENT TYPE (2ND COLUMN)	COMMON TAXONOMY FOR LEA AND CSIRT INCIDENT CLASSIFICATION (1ST COLUMN)
Infection	Malware
Distribution	
C&C	
Undetermined	
Malicious Connection	

Zdroj: https://www.trusted-introducer.org/Incident-Classification-Taxonomy.pdf

Evidencia bezpečnostného incidentu

- **Evidencia bezpečnostných incidentov**
  - Tiketovací systém / Interná evidencia (emailové správy)
  - Zaznamenajte si postup + dôležité údaje

Ako by ste evidovali bezpečnostný incident?



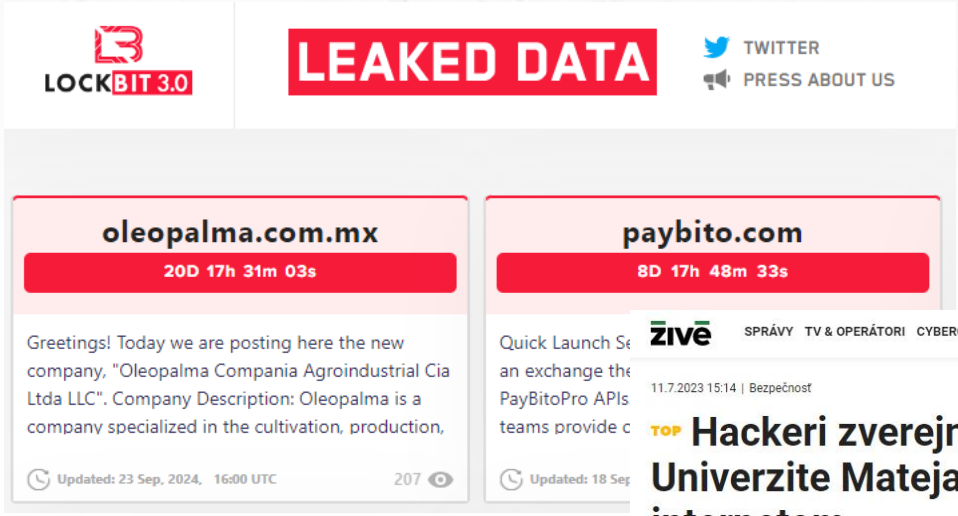
Zdroj: https://strangebee.com/thehive/

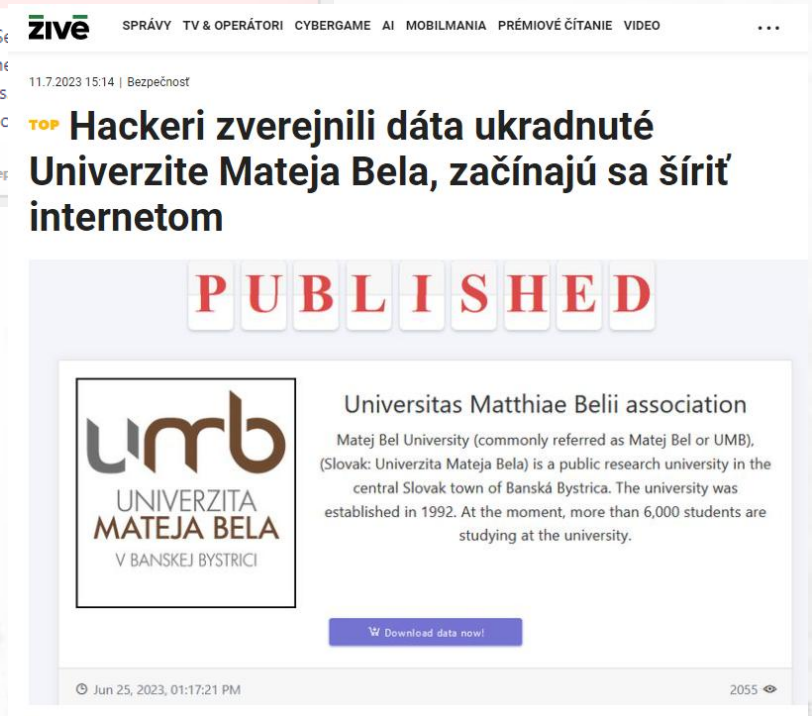
Komunikácia bezpečnostného incidentu (I.)

Zdroj: https://docs.opencti.io/latest/administration/segregation/

Komunikácia bezpečnostného incidentu (II.)

- Partneri/klienti
- Média
  - Nahlásiť
  - Zamestnanci / útočník
- OČTK
- Povinné / dobrovoľné hlásenia
  - Úrad na ochranu osobných údajov
  - NBÚ, Telekomunikačný úrad
- ***Komu by ste hlásili/komunikovali bezpečnostný incident a aký spôsobom?***





Zdroj: https://zive.aktuality.sk/clanok/cfRr3Xq/hackeri-zverejnili-data-ukradnute-univerzite-mateja-bela-zacinaju-sa-sirit-internetom/

Komunikácia bezpečnostného incidentu (III.)

Bezpečnostný pohľad

- Bezpečnostný incident
- CSIRT / Dohľadový orgán
- Zastaviť incident, zistiť dopad incidentu, zamedziť rovnakému incidentu

Trestnoprávny pohľad

- Skutok
- Orgány činné v trestnom konaní
- Nájsť páchateľa

Pohľad ochrany osobných údajov

- Bezpečnostný incident
- ÚOOÚ
- Identifikovať dopad na OOÚ a urobiť opatrenia

Komunikácia bezpečnostného incidentu (IV.)

Čl. 33 GDPR

Ktoré incidenty je potrebné oznámiť podľa GDPR?

- Porušenie ochrany osobných údajov
- Porušenie bezpečnosti

Kto musí oznamovať?

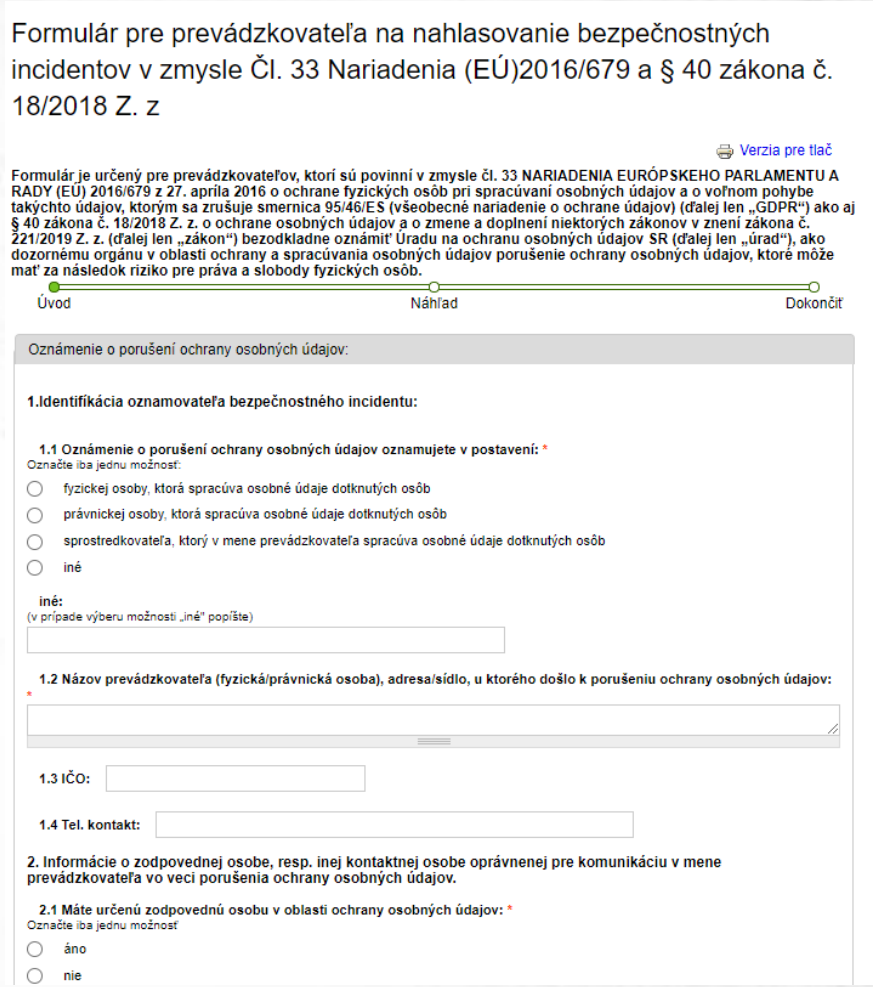
- Každý prevádzkovateľ a sprostredkovateľ

Komu je potrebné incident oznámiť?

- Úradu na ochranu osobných údajov
- Dotknutým osobám (niektoré prípady)

Do kedy je potrebné incident oznámiť?

- **Bez zbytočného odkladu**, resp. **do 72 hodín**



Formulár pre prevádzkovateľa na nahlasovanie bezpečnostných incidentov v zmysle Čl. 33 Nariadenia (EÚ)2016/679 a § 40 zákona č. 18/2018 Z. z

Verzia pre tlač

Formulár je určený pre prevádzkovateľov, ktorí sú povinní v zmysle čl. 33 NARIADENIA 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) (ďalej len „GDPR") ako aj § 40 zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení zákona č. 221/2019 Z. z. (ďalej len „zákon") bezodkladne oznámiť Úradu na ochranu osobných údajov SR (ďalej len „úrad"), ako dozornému orgánu v oblasti ochrany a spracúvania osobných údajov porušenie ochrany osobných údajov, ktoré môže mať za následok riziko pre práva a slobody fyzických osôb.

Úvod — Náhľad — Dokončiť

Oznámenie o porušení ochrany osobných údajov:

1.Identifikácia oznamovateľa bezpečnostného incidentu:

1.1 Oznámenie o porušení ochrany osobných údajov oznamujete v postavení: *
Označte iba jednu možnosť:
- fyzickej osoby, ktorá spracúva osobné údaje dotknutých osôb
- právnickej osoby, ktorá spracúva osobné údaje dotknutých osôb
- sprostredkovateľa, ktorý v mene prevádzkovateľa spracúva osobné údaje dotknutých osôb
- iné

iné:
(v prípade výberu možnosti „iné" popíšte)

1.2 Názov prevádzkovateľa (fyzická/právnická osoba), adresa/sídlo, u ktorého došlo k porušeniu ochrany osobných údajov: *

1.3 IČO:

1.4 Tel. kontakt:

2. Informácie o zodpovednej osobe, resp. inej kontaktnej osobe oprávnenej pre komunikáciu v mene prevádzkovateľa vo veci porušenia ochrany osobných údajov.

2.1 Máte určenú zodpovednú osobu v oblasti ochrany osobných údajov: *
Označte iba jednu možnosť
- áno
- nie

https://dataprotection.gov.sk/sk/prevadzkovatelia/oznamenie-poruseni-ochrany-osobnych-udajov/

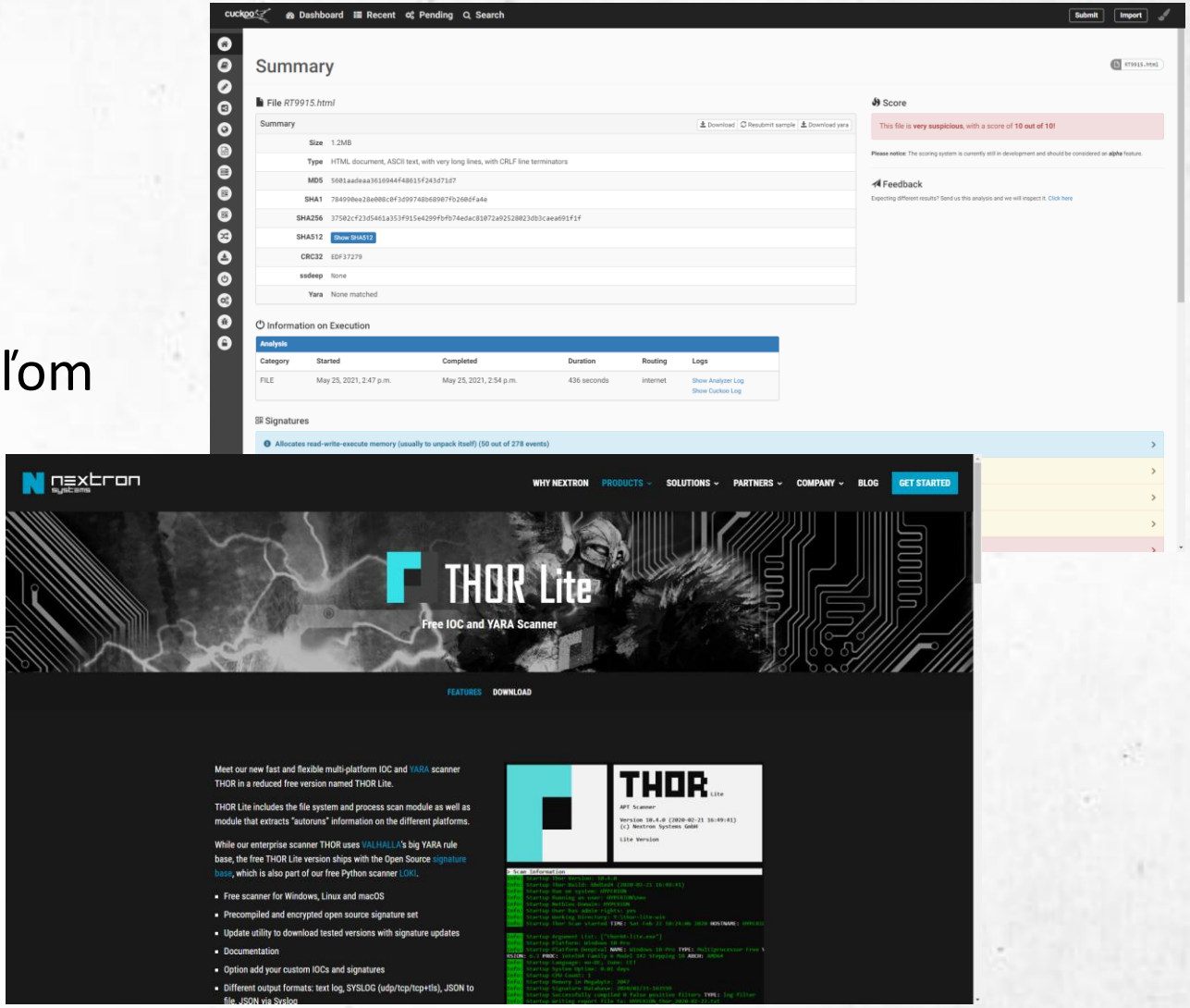
Zastavenie/Obmedzenie bezpečnostného incidentu

- **Blokovanie ďalšieho prístupu** alebo poškodenia systémov
  - Vypnutie systému, odpojenie od siete, zmena pravidiel,
  - Zvýšenie úrovne monitorovania
  - Malvér -> **izolácia** kompromitivaných systémov
  - Phishing -> **deaktivácia** odkazu

- ***Čo by ste robili v prípade ransomvér útoku?***

Analýza bezpečnostného incidentu

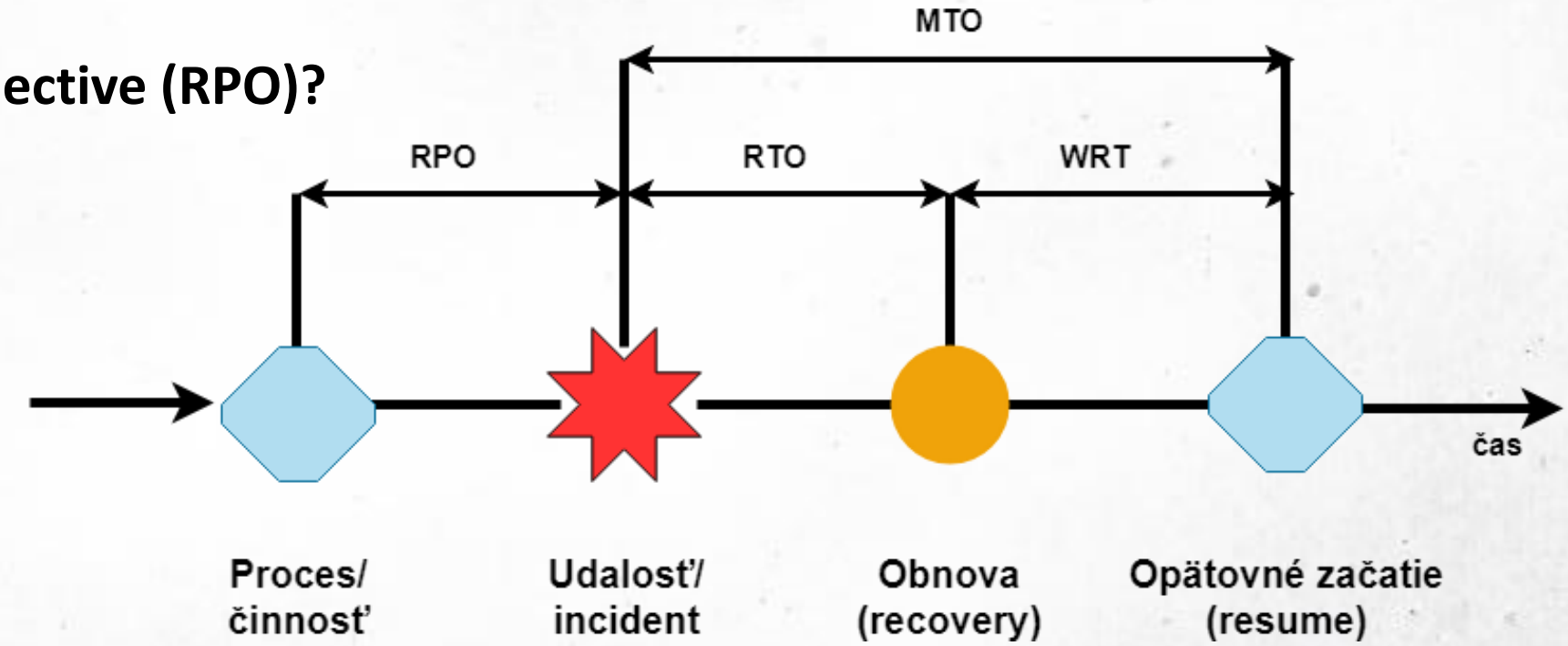
- **Zhromažďovanie digitálnych stôp** – zaisťovanie
- Zhromaždenie podrobností o vektore útoku a o krokoch podniknutých s cieľom umožniť účinné odstránenie
- Výrazne technická časť
- Viacero free/open-source nástroj



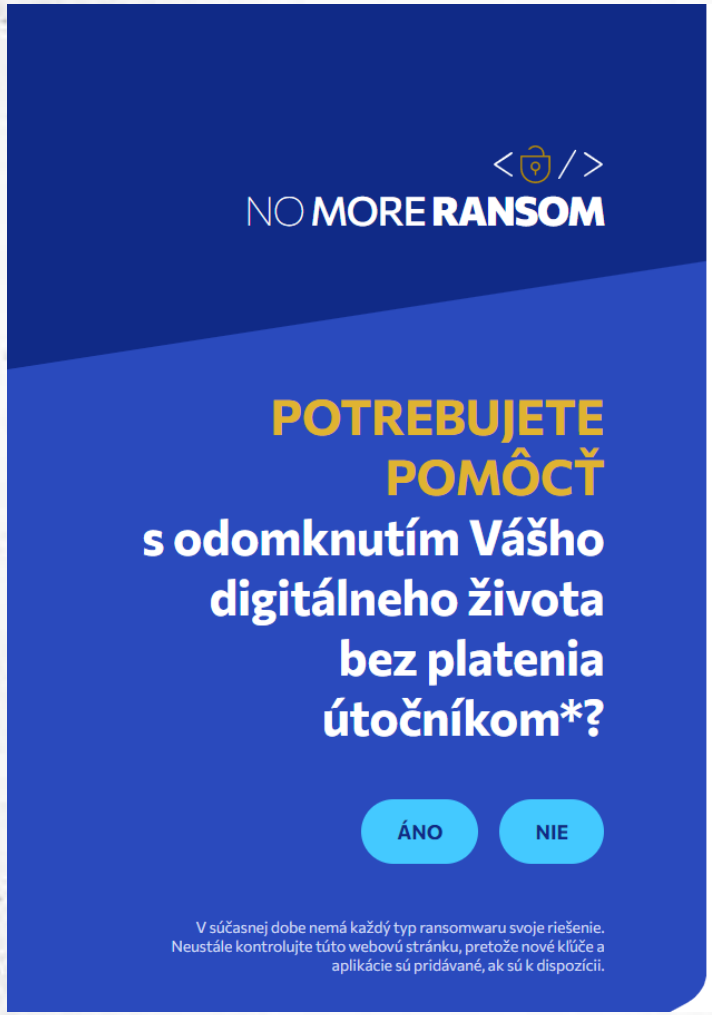
https://cuckoo.cert.ee/analysis/2232081/summary/ https://www.nextron-systems.com/thor-lite/

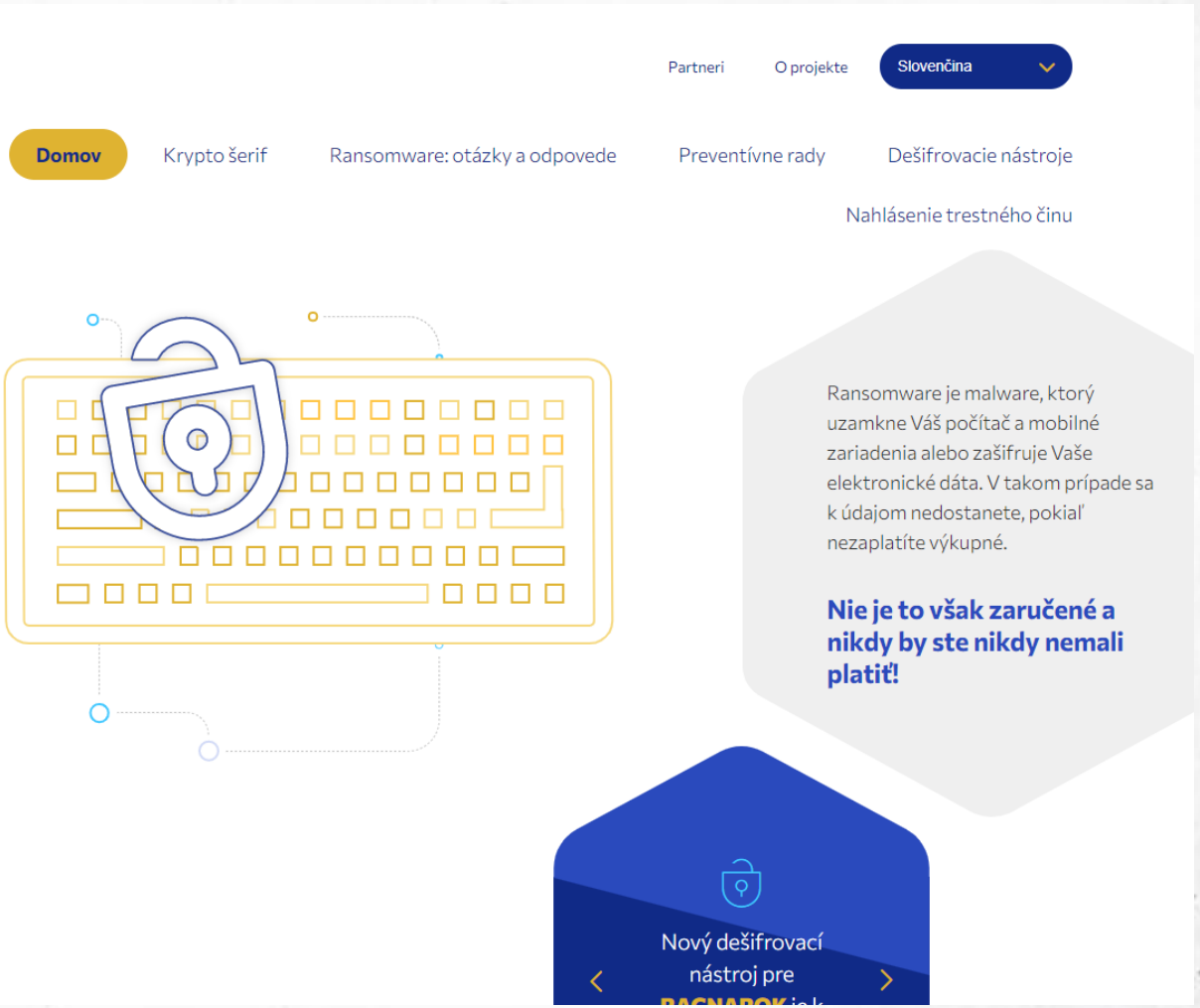
Odstránenie príčiny a obnova dát / systémov (I.)

- Identifikácia bezpečnostných zraniteľností
- Zálohy / zálohovacie systémy – 1 z cieľov útočníkov
- **Recovery point objective (RPO)?**



Odstránenie príčiny a obnova dát / systémov (II.)





https://www.nomoreransom.org/sk/index.html

Uzavretie a príprava na bezpečnostný incident

- **Uzavretie bezpečnostného incidentu**
  - Aký by bol dopad u Vás?
  - Aké systémy boli zasiahnuté?
  - Bezpečnostné opatrenia?
- **Lessons learned**
  - Ako to robiť inak?
  - **Štruktúra** siete, **inventarizácia** zariadení
  - **Prístupy** k zariadeniam (najmä sieťovým prvkom)
  - **Postupy**
    - Aké kroky vykonať
    - Koho informovať
  - **Nástroje**
    - Množstvo open-source nástrojov

KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Manažment zraniteľností

10.3.2023 10:40 | Bezpečnosť

Bezpečnosť stámiliónov zariadení je ohrozená: Zraniteľný čip nájdeme aj v moderných počítačoch

Hardvérový komponent T
môžu získať dešifrovacie

Lucia Kobzová

- Nové zraniteľnosti umožň

15.12.2022 06:08 | Bezpečnosť

Produkty od Fortinet obsahujú kritickú zraniteľnosť. Treba inštalovať aktualizáciu aj preveriť logy

Zdroj: istock

Lukáš Kosno

Útočník mohol získať neoprávnený prístup k citlivým údajom a vykonať neoprávnené zmeny.

V operačnom systéme FortiOS a produkte FortiProxy sa našla nová kritická zraniteľnosť,
upozorňuje Národné centrum kybernetickej bezpečnosti SK-CERT. Stalo sa tak opätovne po

COMPUTERWORLD

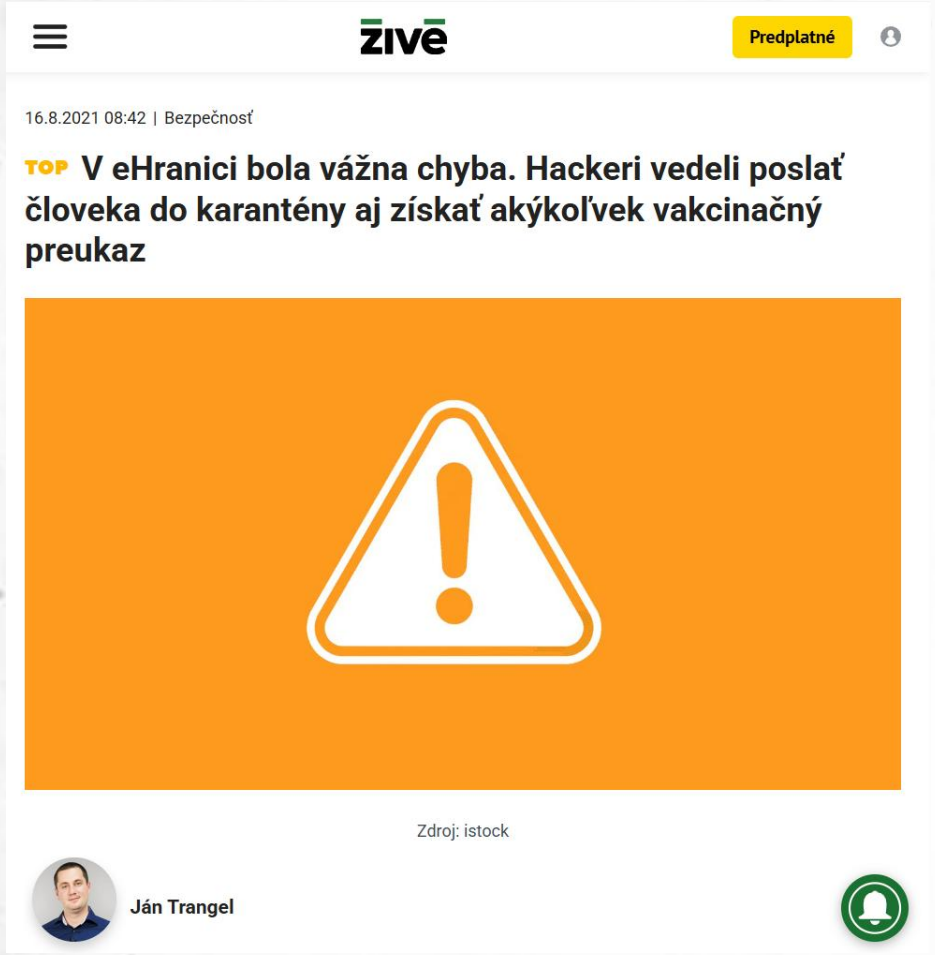
Computerworld » Security World »

Open source je prolezlý zranitelnostmi

Autor: Depositphotos

oftware obsahuje nějakou část open source kódu.
ých kódů klíčová pro zabezpečení celého programu.
společnosti Synopsys, existují v tomto směru vážné

Zdroj: https://zive.aktuality.sk/clanok/PEXrsVn/produkty-od-fortinet-obsahuju-kriticku-zranitelnost-treba-instalovat-aktualizaciu-aj-preverit-logy/, https://www.computerworld.cz/clanky/open-source-je-prolezly-zranitelnostmi/, https://zive.aktuality.sk/clanok/kTGyEfc/bezpecnost-stamilionov-zariadeni-je-ohrozena-zranitelny-cip-najdeme-aj-v-modernych-pocitacoch/x



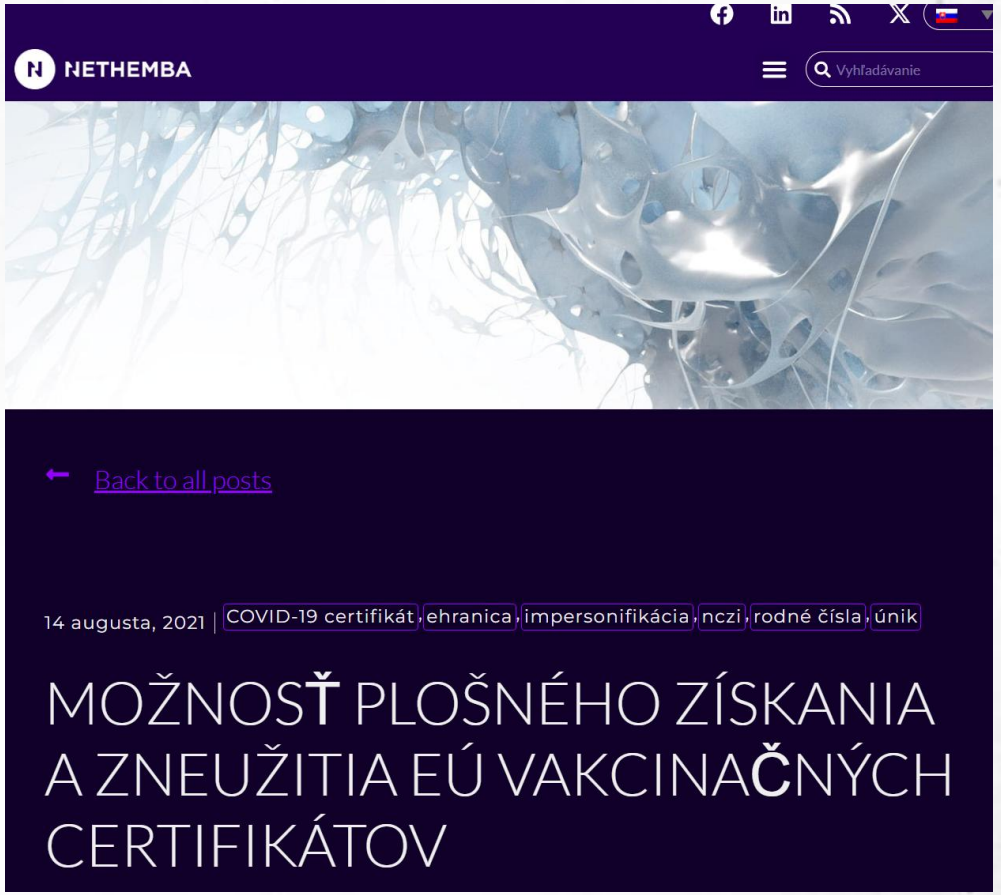
Predplatné

16.8.2021 08:42 | Bezpečnosť

TOP **V eHranici bola vážna chyba. Hackeri vedeli poslať človeka do karantény aj získať akýkoľvek vakcinačný preukaz**

Zdroj: istock

Ján Trangel



NETHEMBA

Vyhľadávanie

Back to all posts

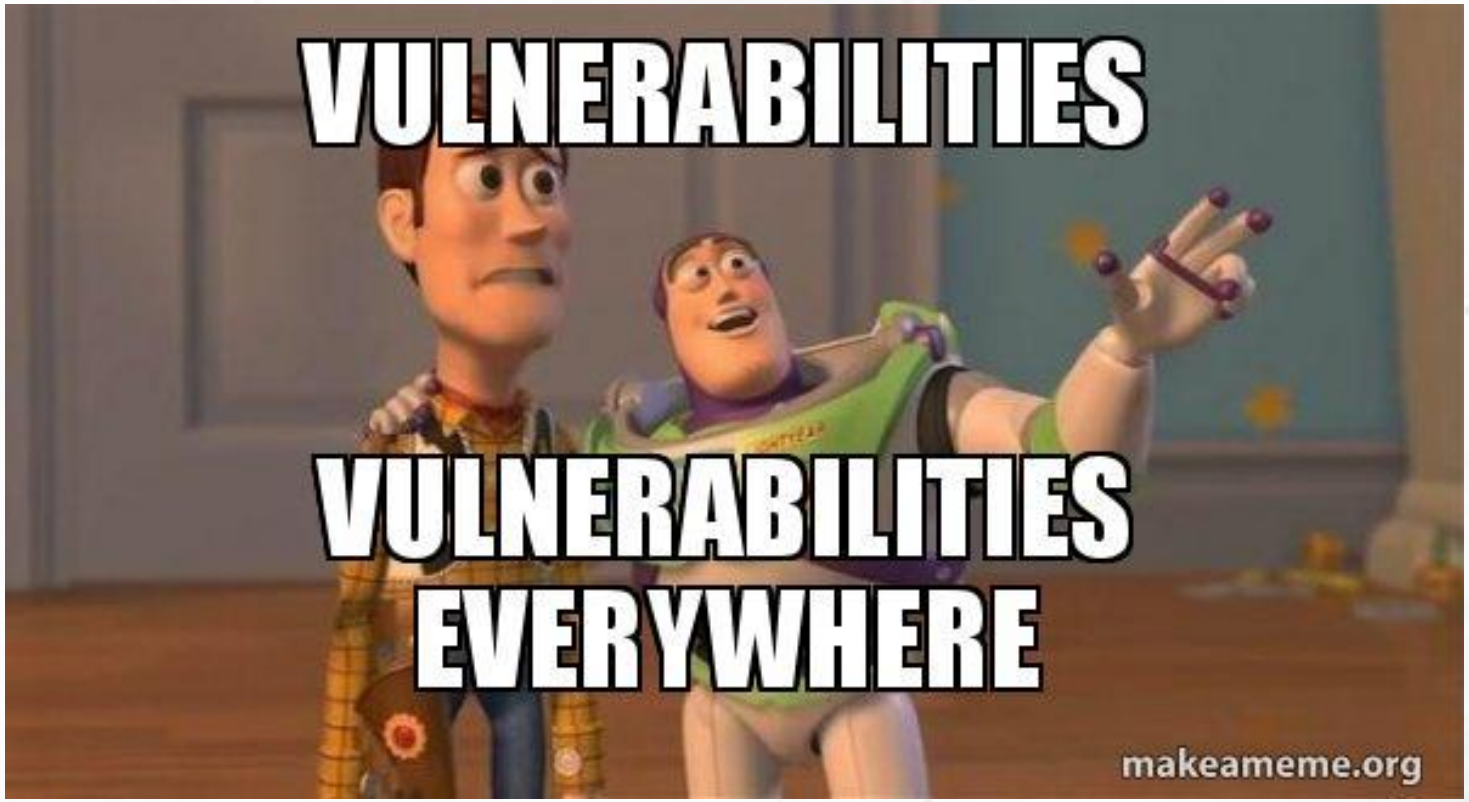
14 augusta, 2021 | COVID-19 certifikát, ehranica, impersonifikácia, nczi, rodné čísla, únik

MOŽNOSŤ PLOŠNÉHO ZÍSKANIA A ZNEUŽITIA EÚ VAKCINAČNÝCH CERTIFIKÁTOV

Zdroj: https://zive.aktuality.sk/clanok/5w4np4g/v-ehranici-bola-vazna-chyba-hackeri-vedeli-poslat-cloveka-do-karanteny-aj-ziskat-akykolvek-vakcinacny-preukaz/
https://nethemba.com/sk/moznost-plosneho-ziskania-a-zneuzitia-eu-vakcinacnych-certifikatov/

Bezpečnostné zraniteľnosti (I.)

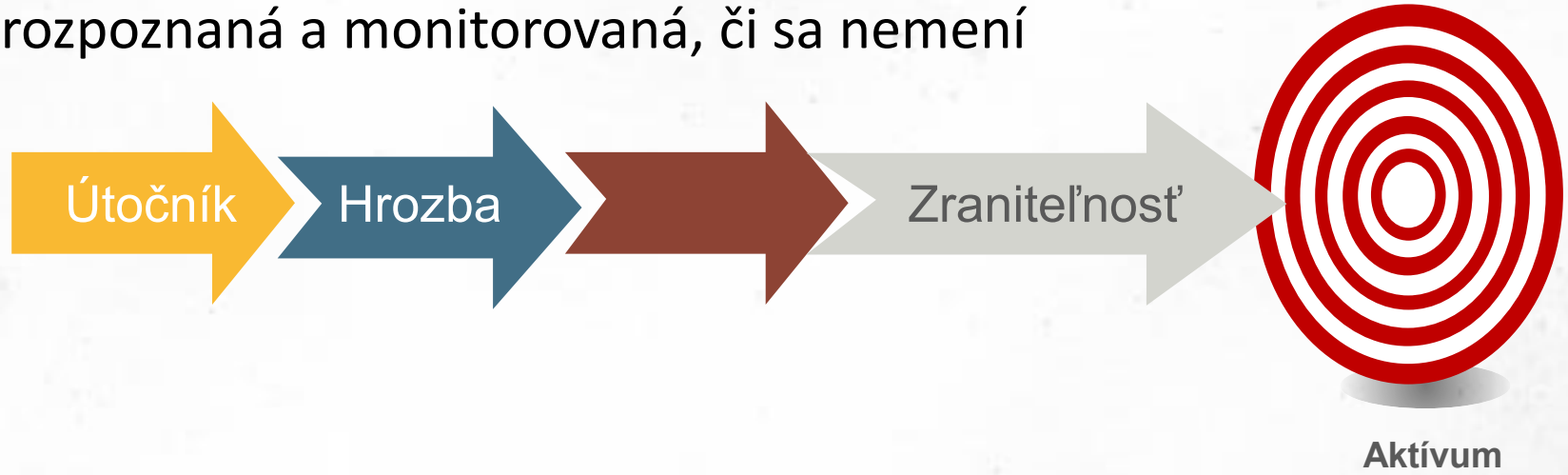
- Chyba v softvéri, firmvéri, hardvéri alebo komponente služby vyplývajúca zo slabosti, ktorú je možné zneužiť, a ktorá má negatívny vplyv na dôvernosť, integritu alebo dostupnosť ovplyvneného komponentu alebo komponentov (CVE – MITRE)



Zdroj: https://makeameme.org/meme/vulnerabilities-vulnerabilities-everywhere

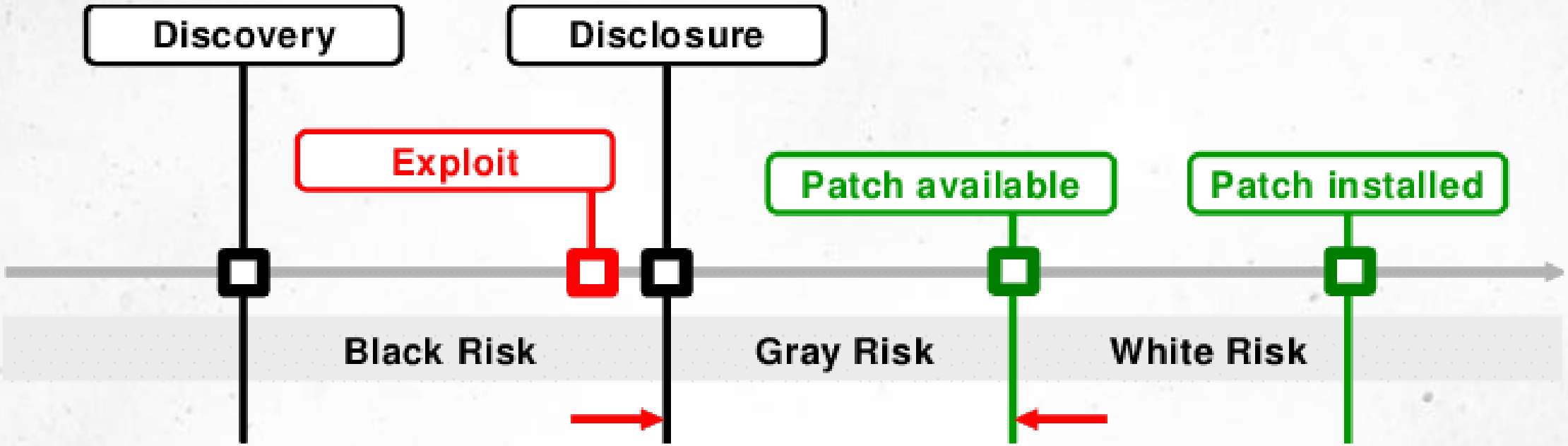
Bezpečnostné zraniteľnosti (II.)

- výskyt zraniteľnosti ako taký nespôsobuje škodu, pretože musí existovať hrozba, ktorá ho využije
- zraniteľnosť, ktorá nemá odpovedajúcu hrozbu, nemusí vyžadovať prijatie opatrení, ale mala by byť rozpoznaná a monitorovaná, či sa nemení



Zdroj: FIRST: Incident Response for Policymakers

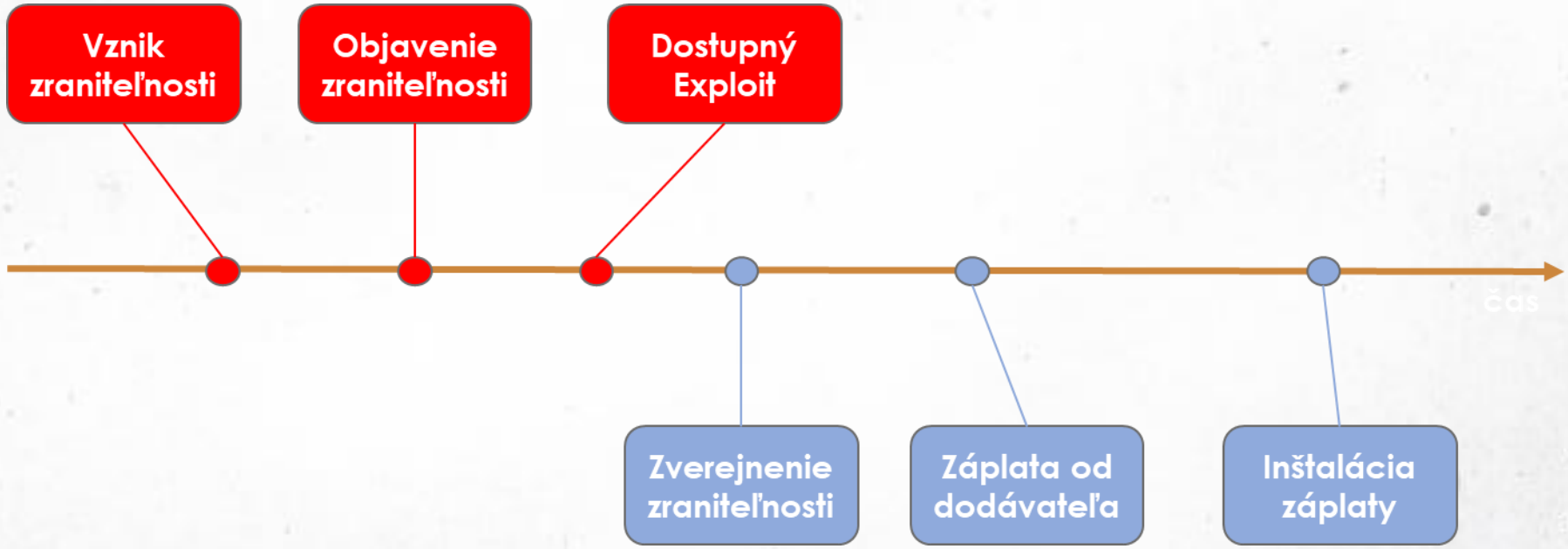
Životný cyklus zraniteľnosti



Zdroj: https://www.researchgate.net/publication/321807370/figure/fig1/AS:571534638096384@1513275884045/Lifecycle-of-a-vulnerability-Distinctive-points-in-time-divide-the-lifecycle-of-a.png

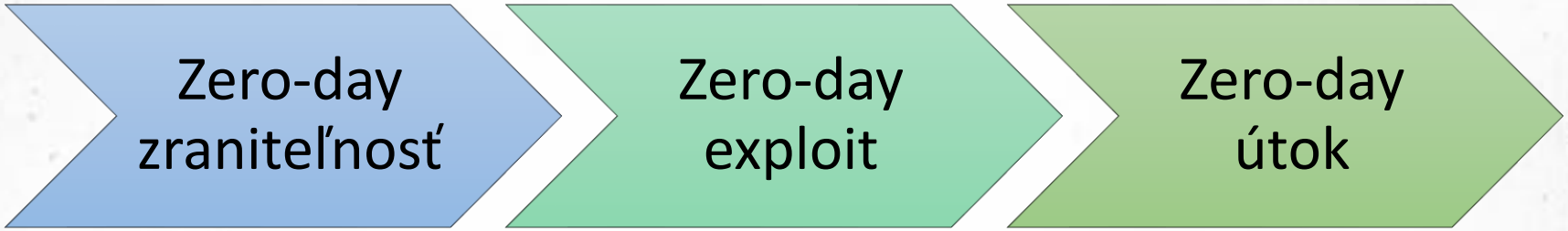
Životný cyklus (II.)

- životný cyklus a manažment bezpečnostných zraniteľností
- zverejňovanie zraniteľností – úplné/obmedzené/nezverejnenie
- koordinované zverejňovanie zraniteľností

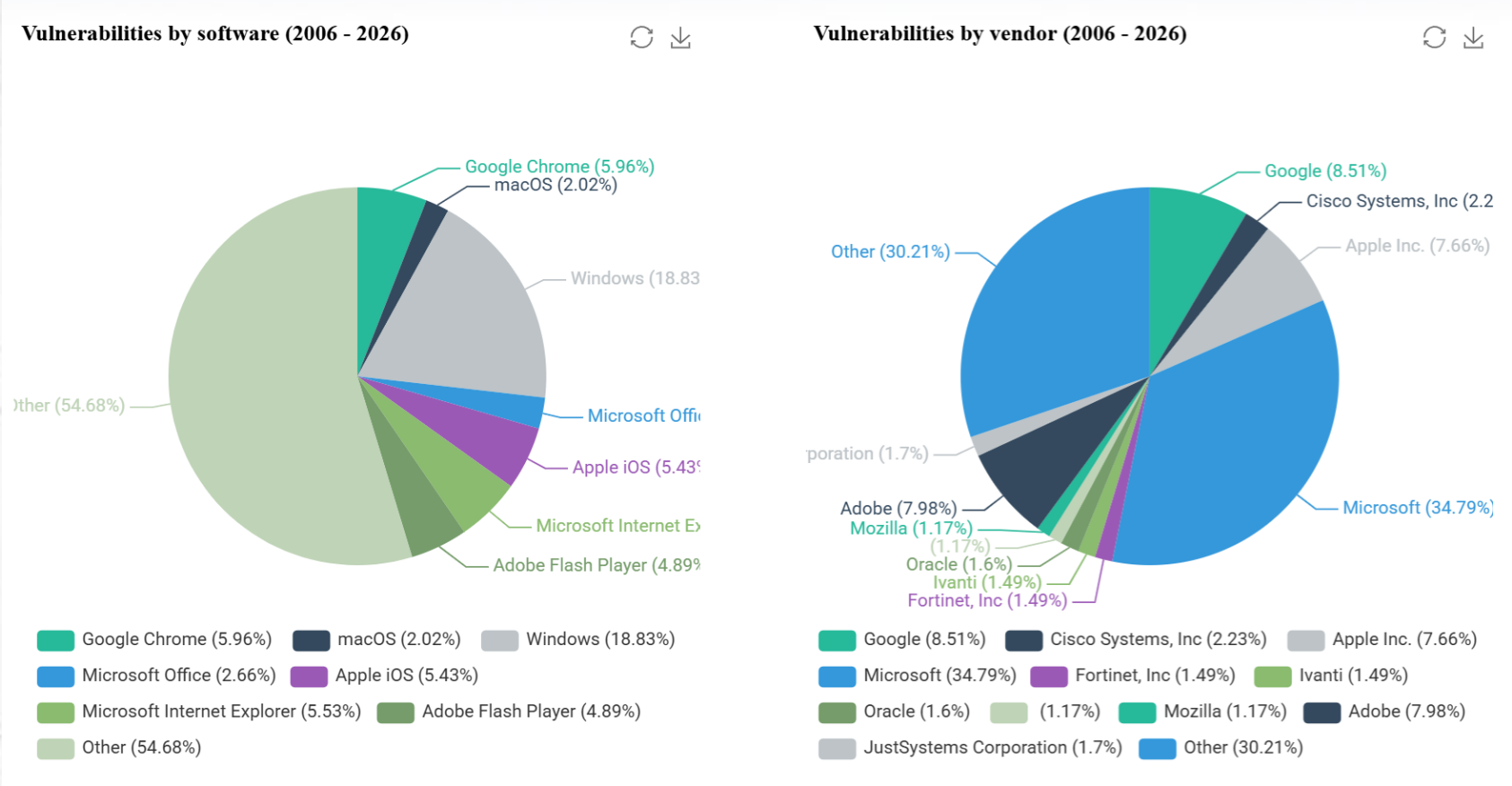


0-days zraniteľnosti (I.)

- zraniteľnosť v systéme alebo zariadení, ktorá bola odhalená, ale ešte nie je opravená
- exploit, ktorý útočí na zero-day zraniteľnosť, sa nazýva zero-day exploit
- predstavujú vyššie riziko



0-days zraniteľnosti (II.)



Zdroj: https://www.zero-day.cz/database/

0-days zraniteľnosti (III.)

Google Chrome Zero-Day Bug Under Attack, Allows Code Injection

The first Chrome zero-day bug of 2024 adds to a growing list of actively exploited vulnerabilities found in Chromium and other browser technologies.

Jai Vijayan, Contributing Writer

January 17, 2024

4 Min Read

Zdroj: https://www.darkreading.com/cloud-security/google-chrome-zero-day-bug-attack-code-injection

Indikátor zraniteľnosti

- CVE = Common Vulnerabilities and Exposure
- CVE ID
  - unikátny identifikátor referencujúci špecifickú zraniteľnosť
  - umožňuje korelovanie a zdieľanie informácií o konkrétnych zraniteľnostiach

CVE-2020-0796

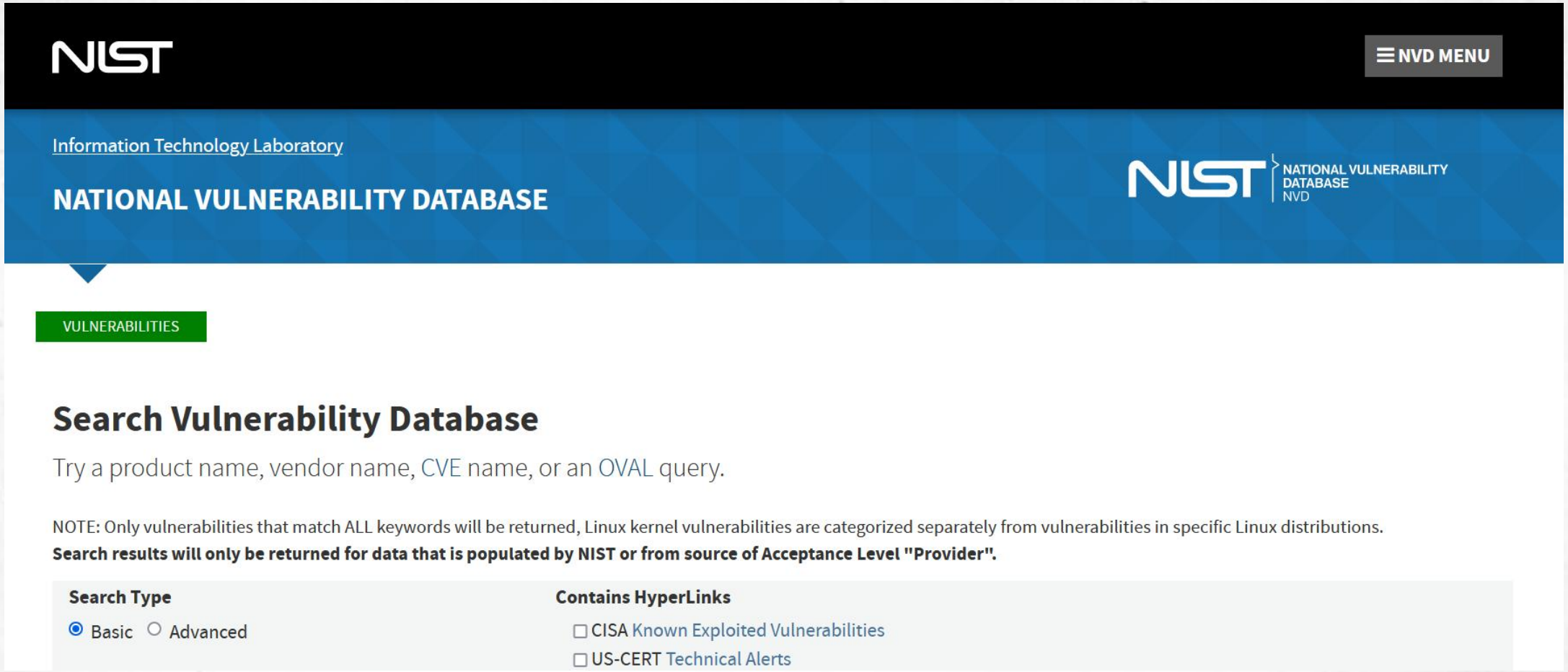
A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 3.1.1 (SMBv3) protocol handles certain requests, aka 'Windows SMBv3 Client/Server Remote Code Execution Vulnerability'.

CVE-2022-23284

Windows Print Spooler Elevation of Privilege Vulnerability.

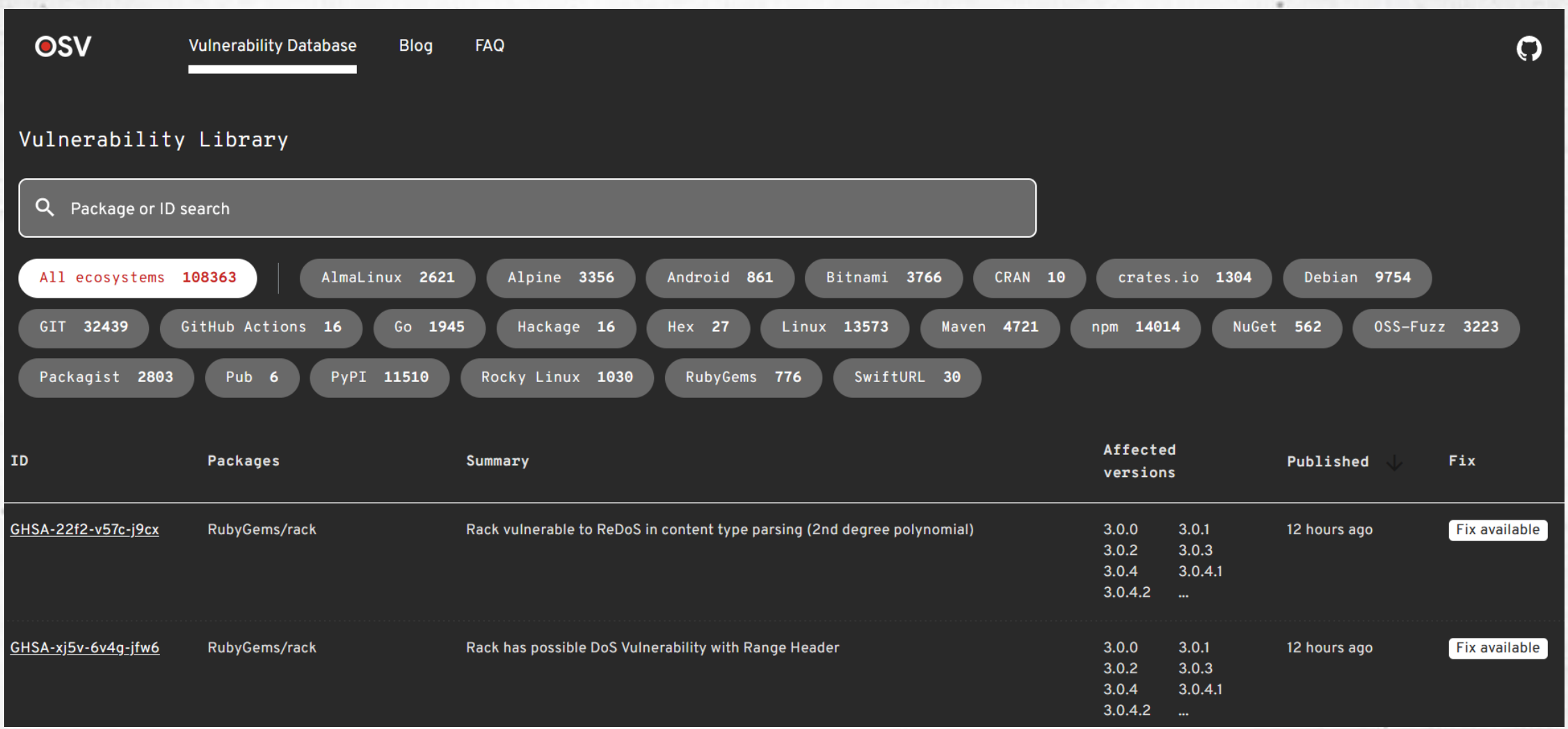
Zdroj: https://www.cvedetails.com/cve/CVE-2020-0796/, https://www.cvedetails.com/cve/CVE-2022-23284/

Databázy zraniteľností (I.)



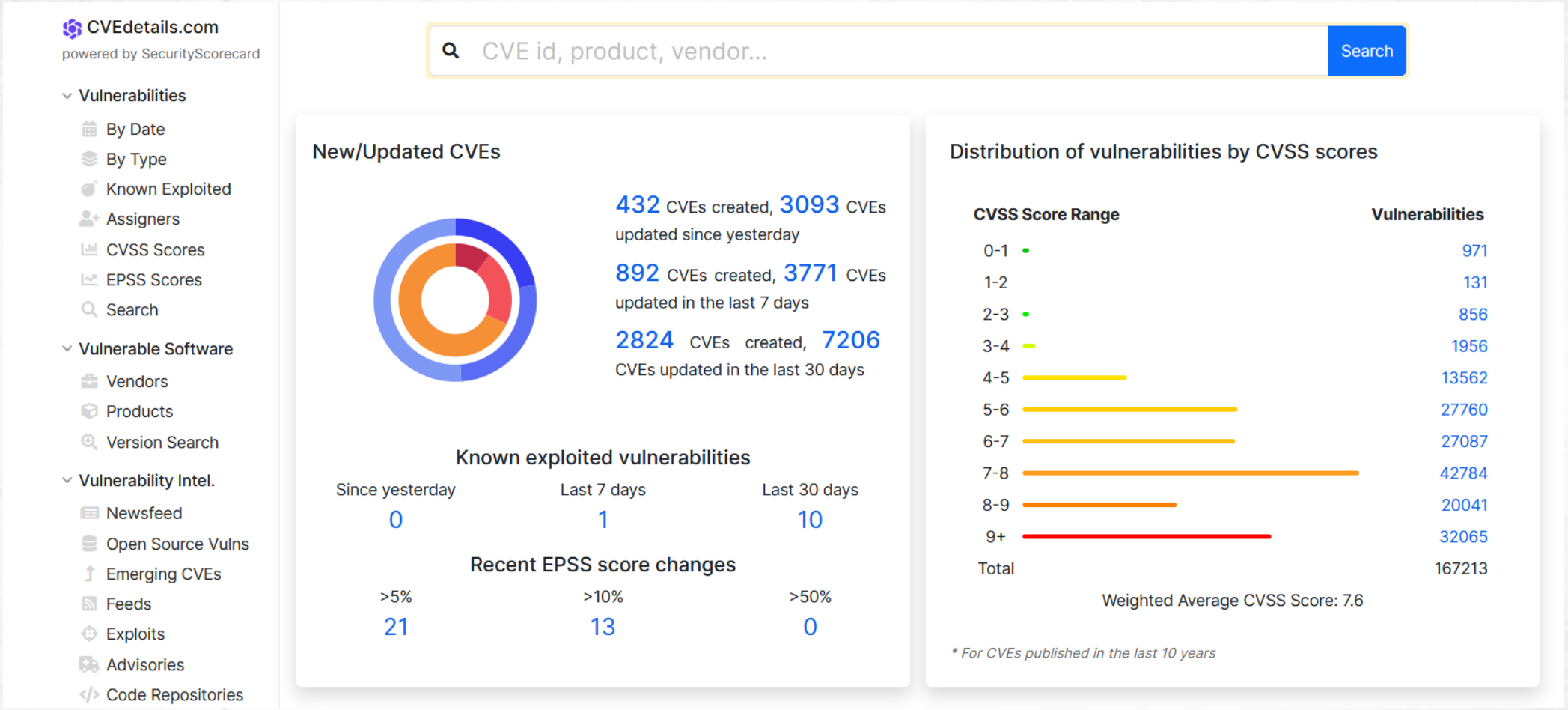
Zdroj: https://nvd.nist.gov/vuln

Databázy zraniteľností (II.)



Zdroj: https://osv.dev/

Databázy zraniteľností (III.)



Zdroj: https://www.cvedetails.com/

Popis zraniteľnosti (I.)

Vulnerability Details : CVE-2019-0708

Public exploit exists!

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

Published 2019-05-16 19:29:00 Updated 2021-06-03 18:15:08 Source Microsoft Corporation

View at NVD, CVE.org

Vulnerability category: Execute code

CVE-2019-0708 is in the CISA Known Exploited Vulnerabilities Catalog

CISA vulnerability name:
Microsoft Remote Desktop Services Remote Code Execution Vulnerability

CISA required action:
Apply updates per vendor instructions.

CISA description:
Microsoft Remote Desktop Services, formerly known as Terminal Service, contains an unspecified vulnerability that allows an unauthenticated attacker to connect to the target system using RDP and send specially crafted requests. Successful exploitation allows for remote code execution. The vulnerabil

Added on 2021-11-03 Action due date 2022-05-03

Exploit prediction scoring system (EPSS) score for CVE-2019-0708

Probability of exploitation activity in the next 30 days: 97.53%

Percentile, the proportion of vulnerabilities that are scored at or less: ~ 100 % EPSS Score History EPSS FAQ

Metasploit modules for CVE-2019-0708

CVE-2019-0708 BlueKeep Microsoft Remote Desktop RCE Check Disclosure Date: 2019-05-14 First seen: 2020-04-26

auxiliary/scanner/rdp/cve_2019_0708_bluekeep

This module checks a range of hosts for the CVE-2019-0708 vulnerability by binding the MS_T120 channel outside of its normal slot and sending non-DoS packets which respond differently on patched and vulnerable hosts. It can optionally trigger the DoS vulnerab

More information

Zdroj: https://www.cvedetails.com/cve/CVE-2019-0708/?q=cve-2019-0708

Popis zraniteľnosti (II.)

Vulnerability Details : CVE-2021-28480

Microsoft Exchange Server Remote Code Execution Vulnerability

Published 2021-04-13 20:15:21 Updated 2023-12-29 01:15:43 Source Microsoft Corporation

View at NVD, CVE.org

Vulnerability category: Execute code

Exploit prediction scoring system (EPSS) score for CVE-2021-28480

Probability of exploitation activity in the next 30 days: 4.22%

Percentile, the proportion of vulnerabilities that are scored at or less: ~ 91 % EPSS Score History EPSS FAQ

CVSS scores for CVE-2021-28480

Base Score	Base Severity	CVSS Vector	Exploitability Score	Impact Score	Score Source
10.0	HIGH	AV:N/AC:L/Au:N/C:C/I:C/A:C	10.0	10.0	NIST
9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	3.9	5.9	NIST
9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	3.9	5.9	Microsoft Corporation

References for CVE-2021-28480

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28480

CVE-2021-28480 - Security Update Guide - Microsoft - Microsoft Exchange Server Remote Code Execution Vulnerability

Patch;Vendor Advisory

Products affected by CVE-2021-28480

Microsoft » Exchange Server » Version: 2013 Update Cumulative Update 23

cpe:2.3:a:microsoft:exchange_server:2013:cumulative_update_23:*:*:*:*:*:* Matching versions

Microsoft » Exchange Server » Version: 2016 Update Cumulative Update 19

cpe:2.3:a:microsoft:exchange_server:2016:cumulative_update_19:*:*:*:*:*:* Matching versions

Zdroj: https://www.cvedetails.com/cve/CVE-2021-28480/?q=CVE-2021-28480

Zoznam zraniteľností (I.)

Security Vulnerabilities, CVEs, Published In January 2024

Published in: 2024 January February

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9 In CISA KEV Catalog

Sort Results By : Publish Date Update Date CVE Number CVE Number CVSS Score EPSS Score

2608 vulnerabilities found

1 2 3 4 5 ..... 102 103 104 105 Copy

CVE-2024-24573

facileManager is a modular suite of web apps built with the sysadmin in mind. In versions 4.5.0 and earlier, when a user updates their profile, a POST request containing user information is sent to the endpoint server/fm-modules/facileManager/ajax/processPost.php. It was found that non-admins can arbitrarily set their permissions and grant their non-admin accounts with super user privileges.

Max CVSS 8.8
EPSS Score 0.05%
Published 2024-01-31
Updated 2024-02-07

CVE-2024-24572

facileManager is a modular suite of web apps built with the sysadmin in mind. In versions 4.5.0 and earlier, the $_REQUEST global array was unsafely called inside an extract() function in admin-logs.php. The PHP file fm-init.php prevents arbitrary manipulation of $_SESSION via the GET/POST parameters. However, it does not prevent manipulation of any other sensitive variables such as $search_sql. Knowing this, an authenticated user with privileges to view site logs can manipulate the search_sql variable by appending a GET parameter search_sql in the URL. The information above

Max CVSS 6.5
EPSS Score 0.05%
Published 2024-01-31
Updated 2024-02-07

CVE-2024-24571

facileManager is a modular suite of web apps built with the sysadmin in mind. For the facileManager web application versions 4.5.0 and earlier, we have found that XSS was present in almost all of the input fields as there is insufficient input validation.

Max CVSS 5.4
EPSS Score 0.05%
Published 2024-01-31
Updated 2024-02-07

Zdroj: https://www.cvedetails.com/vulnerability-list/year-2024/month-1/January.html?page=1&order=7&trc=2608&sha=c99dbf2a36e5e59c9027922650ebf2d162a3f69e

Zoznam zraniteľností (II.)

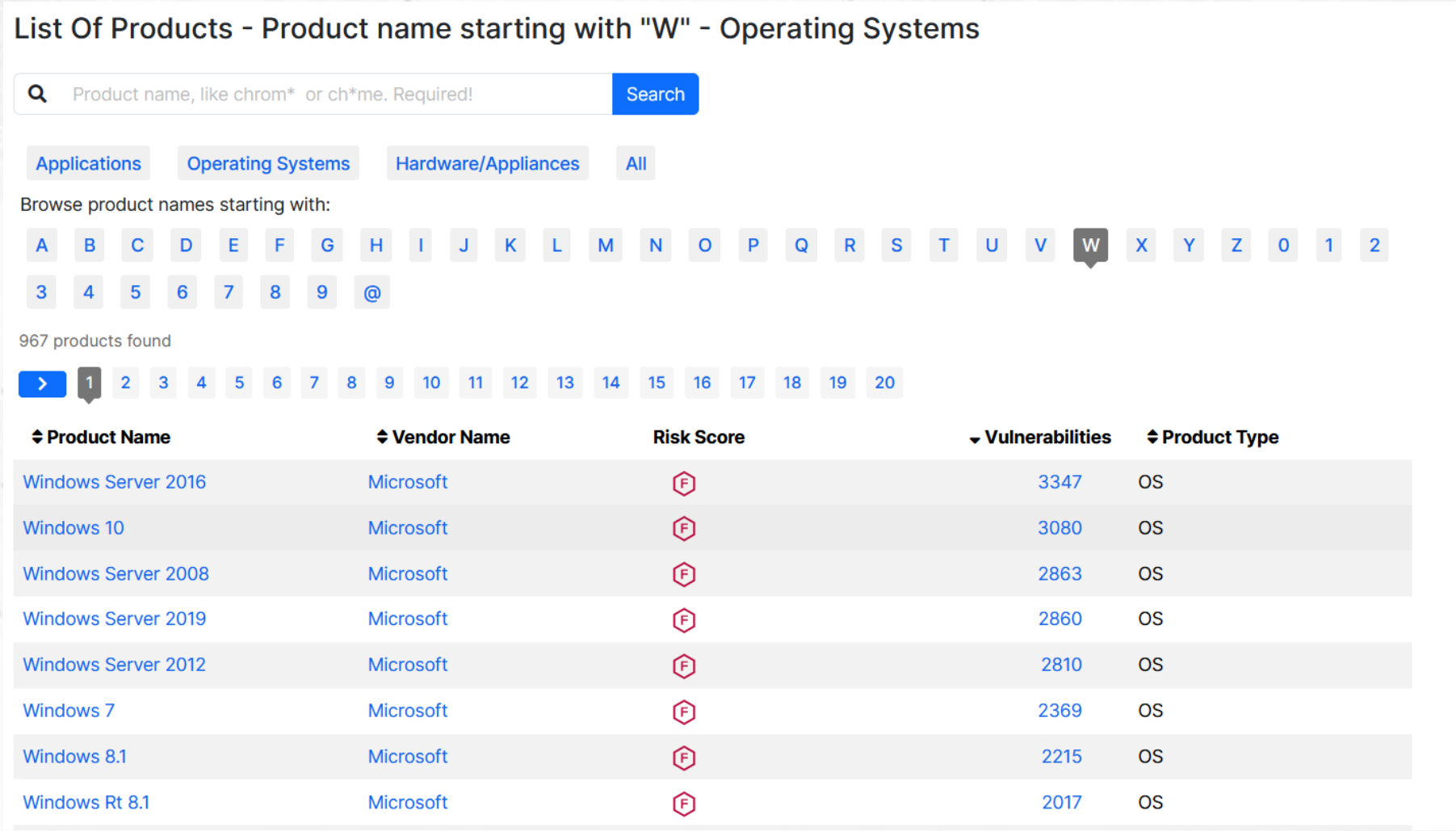
https://www.cvedetails.com/top-50-vendor-cvssscore-distribution.php

CVSS Score Distribution For Top 50 Vendors By Total Number Of "Distinct" Vulnerabilities

This page is archived and preserved for historical purposes only. This page is no longer updated.

	Vendor Name	Number of Total Vulnerabilities	# Of Vulnerabilities										Weighted Average	% Of Total									
			0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9+		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9+
1	Microsoft	2305	2	4	135	12	219	591	121	622	16	583	7.30	0	0	6	1	10	26	5	27	1	25
2	Apple	1171	2	13	78	7	184	220	172	264	5	226	7.00	0	1	7	1	16	19	15	23	0	19
3	SUN	1155	1	17	76	14	224	191	81	369	2	180	6.90	0	1	7	1	19	17	7	32	0	16
4	IBM	970	2	13	47	14	163	175	74	288	5	189	7.10	0	1	5	1	17	18	8	30	1	19
5	Oracle	798		12	28	21	138	156	86	132	5	220	7.20	0	2	4	3	17	20	11	17	1	28
6	Cisco	716	1	1	24	9	48	189	46	292	7	99	7.30	0	0	3	1	7	26	6	41	1	14
7	Mozilla	697		1	54	5	123	172	55	134		153	6.90	0	0	8	1	18	25	8	19	0	22
8	Linux	654	1	22	142	16	186	60	39	168	1	19	5.60	0	3	22	2	28	9	6	26	0	3
9	HP	611	1	4	36	3	106	92	32	204	2	131	7.20	0	1	6	0	17	15	5	33	0	21
10	Redhat	485		17	65	6	70	82	28	152	2	63	6.50	0	4	13	1	14	17	6	31	0	13

Zoznam zraniteľností (III.)



List Of Products - Product name starting with "W" - Operating Systems

Product name, like chrom* or ch*me. Required! Search

Applications | Operating Systems | Hardware/Appliances | All

Browse product names starting with:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z 0 1 2 3 4 5 6 7 8 9 @

967 products found

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20

Product Name	Vendor Name	Risk Score	Vulnerabilities	Product Type
Windows Server 2016	Microsoft		3347	OS
Windows 10	Microsoft		3080	OS
Windows Server 2008	Microsoft		2863	OS
Windows Server 2019	Microsoft		2860	OS
Windows Server 2012	Microsoft		2810	OS
Windows 7	Microsoft		2369	OS
Windows 8.1	Microsoft		2215	OS
Windows Rt 8.1	Microsoft		2017	OS

Zdroj: https://www.cvedetails.com/product-list/product_type-o/firstchar-W/vendor_id-0/page-1/products-by-name.html?sha=8986cd589448a0a76c56581cb089fab948a94935&order=3&trc=967

Zoznam zraniteľností (IV.)

Microsoft : Vulnerability Statistics

Products (1254) Vulnerabilities (13792) Search products CVSS Report Metasploit Modules

Vulnerability Trends Over Time

Year	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	File Inclusion	CSRF	XXE	SSRF	Open Redirect	Input Validation
2016	1	177	0	15	0	0	0	1	0	1	0
2017	252	191	0	20	0	0	2	3	0	2	60
2018	16	184	0	53	1	9	2	7	3	1	37
2019	8	119	0	47	3	4	3	8	0	3	39
2020	4	77	0	81	1	1	1	0	0	3	24
2021	9	36	3	10	1	0	1	0	1	0	3
2022	3	7	1	2	1	0	0	0	0	0	0
2023	3	7	0	24	1	0	0	1	0	0	1
2024	2	6	0	11	2	0	1	0	2	0	2
2025	126	199	9	9	7	0	0	0	7	0	0
2026	24	41	2	5	2	0	0	0	4	0	0
Total	448	1044	15	277	19	14	10	20	17	10	166

Zdroj: https://www.cvedetails.com/vendor/26/Microsoft.html

Zoznam zraniteľností (V.)

Vulnerabilities By Types/Categories

CVEdetails.com assigns types/categories to vulnerabilities using CWE ids and keywords.

Year	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	File Inclusion	CSRF	XXE	SSRF	Open Redirect	Input Validation
2016	418	1096	85	476	90	4	85	39	15	28	0
2017	2469	1537	505	1499	281	154	334	109	57	97	929
2018	2056	1722	503	2039	569	111	479	187	118	85	1208
2019	1196	1998	544	2387	485	125	559	136	103	121	892
2020	1216	1831	464	2198	435	107	414	119	130	100	799
2021	1654	2498	740	2723	546	89	520	126	187	133	665
2022	1754	2815	1761	3368	685	85	766	123	229	137	656
2023	1594	1992	2115	5100	741	108	1392	124	238	168	511
2024	1722	2355	2646	7434	919	243	1433	110	372	113	86
2025	2250	2894	3944	8736	1053	669	1949	115	558	166	0
2026	694	570	779	1630	335	348	258	22	207	45	0
Total	17023	21308	14086	37590	6139	2043	8189	1210	2214	1193	5746

Zdroj: https://www.cvedetails.com/vulnerabilities-by-types.php

Zoznam zraniteľností (VI.)

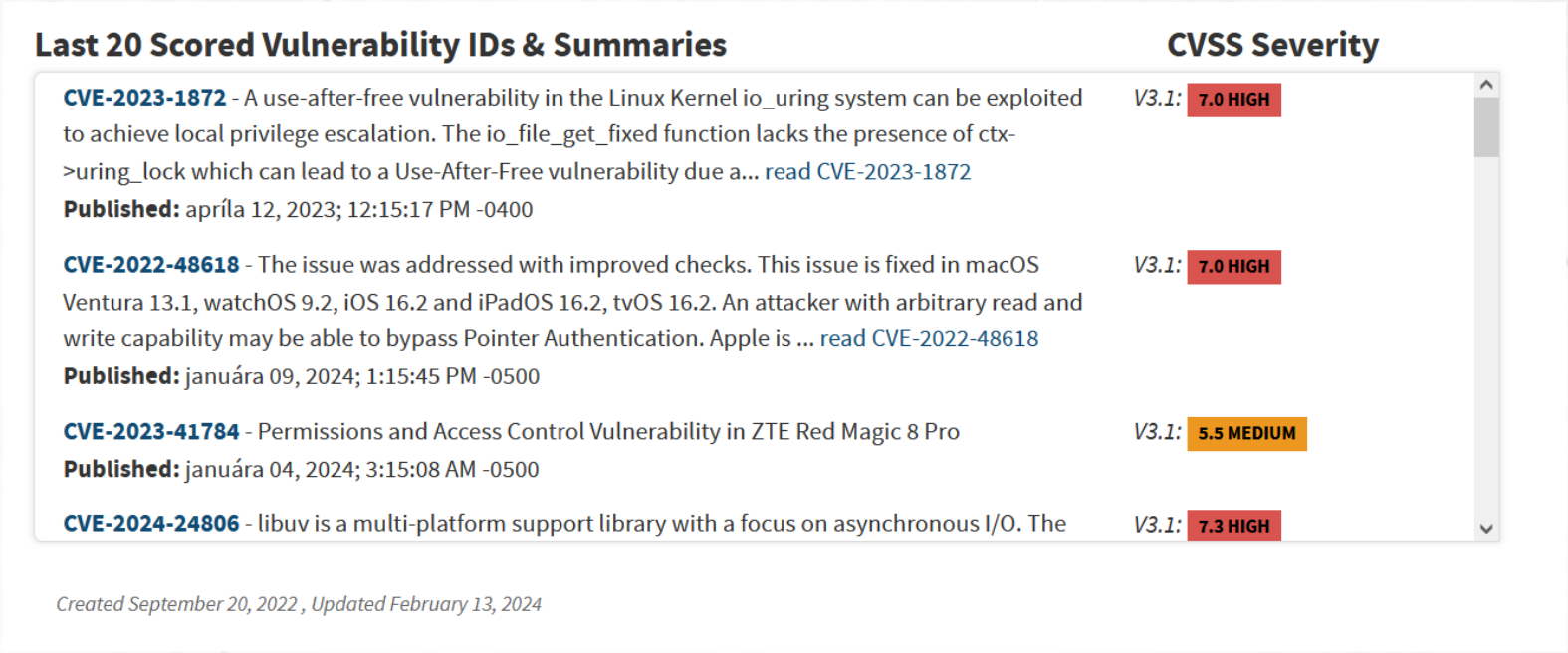
Vulnerabilities by impact types

Year	Code Execution	Bypass	Privilege Escalation	Denial of Service	Information Leak
2016	1239	1	149	2050	102
2017	1870	842	1011	3372	1378
2018	1728	643	827	2207	1395
2019	1556	654	898	1697	1313
2020	1691	794	1365	1677	1089
2021	2087	774	1087	2297	911
2022	2067	820	1404	2437	1108
2023	2580	858	1324	2560	1426
2024	3966	633	1063	2470	932
2025	3036	635	1017	2527	741
2026	913	203	273	978	199
Total	22733	6857	10418	24272	10594

Zdroj: https://www.cvedetails.com/vulnerabilities-by-types.php

Zverejnené zraniteľnosti (I.)

nvd.nist.gov



Last 20 Scored Vulnerability IDs & Summaries | **CVSS Severity**

CVE-2023-1872 - A use-after-free vulnerability in the Linux Kernel io_uring system can be exploited to achieve local privilege escalation. The io_file_get_fixed function lacks the presence of ctx->uring_lock which can lead to a Use-After-Free vulnerability due a... read CVE-2023-1872
Published: apríla 12, 2023; 12:15:17 PM -0400 — *V3.1:* **7.0 HIGH**

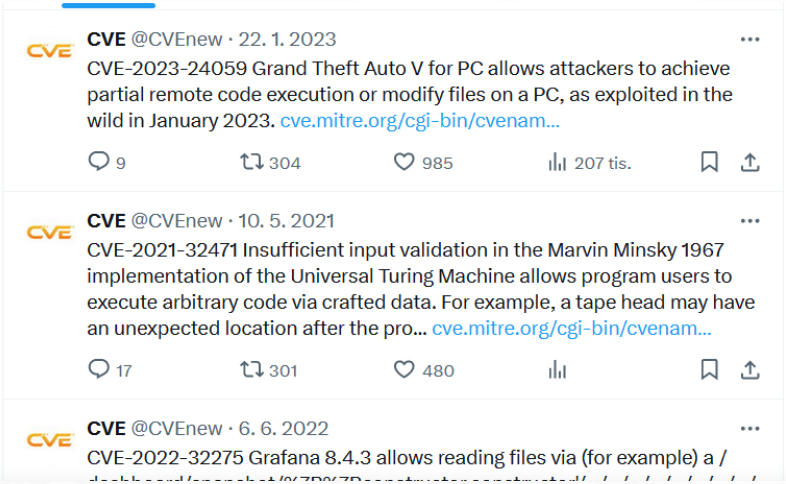
CVE-2022-48618 - The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.1, watchOS 9.2, iOS 16.2 and iPadOS 16.2, tvOS 16.2. An attacker with arbitrary read and write capability may be able to bypass Pointer Authentication. Apple is ... read CVE-2022-48618
Published: januára 09, 2024; 1:15:45 PM -0500 — *V3.1:* **7.0 HIGH**

CVE-2023-41784 - Permissions and Access Control Vulnerability in ZTE Red Magic 8 Pro
Published: januára 04, 2024; 3:15:08 AM -0500 — *V3.1:* **5.5 MEDIUM**

CVE-2024-24806 - libuv is a multi-platform support library with a focus on asynchronous I/O. The — *V3.1:* **7.3 HIGH**

Created September 20, 2022 , Updated February 13, 2024

cve.mitre.org

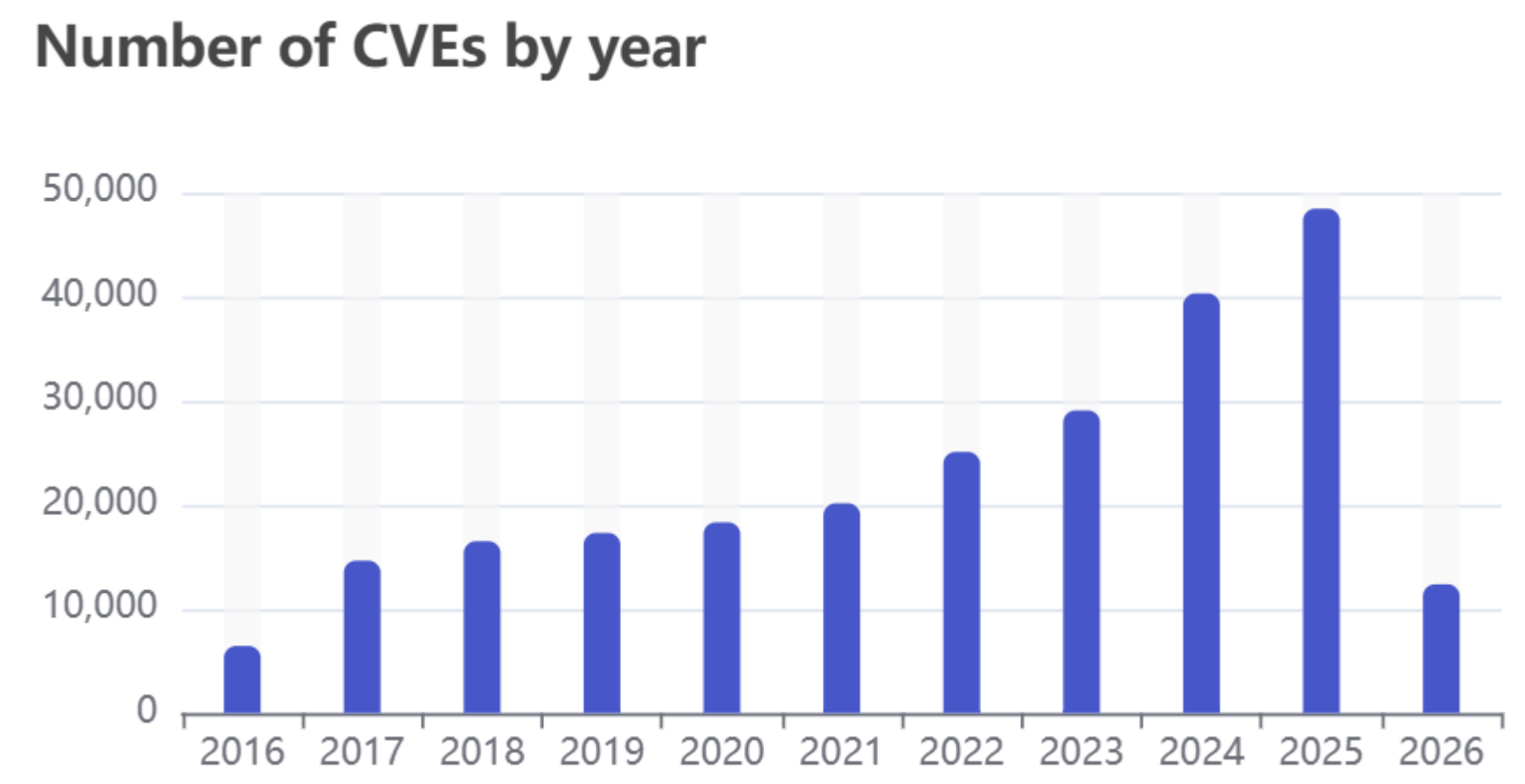


CVE @CVEnew · 22. 1. 2023
CVE-2023-24059 Grand Theft Auto V for PC allows attackers to achieve partial remote code execution or modify files on a PC, as exploited in the wild in January 2023. cve.mitre.org/cgi-bin/cvenam...
9 304 985 207 tis.

CVE @CVEnew · 10. 5. 2021
CVE-2021-32471 Insufficient input validation in the Marvin Minsky 1967 implementation of the Universal Turing Machine allows program users to execute arbitrary code via crafted data. For example, a tape head may have an unexpected location after the pro... cve.mitre.org/cgi-bin/cvenam...
17 301 480

CVE @CVEnew · 6. 6. 2022
CVE-2022-32275 Grafana 8.4.3 allows reading files via (for example) a /

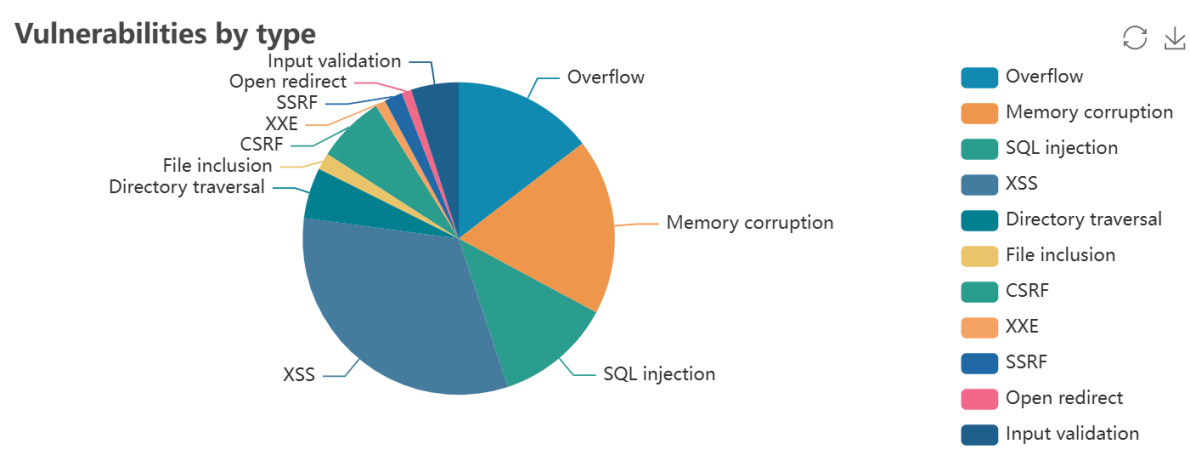
Zverejnené zraniteľnosti (II.)

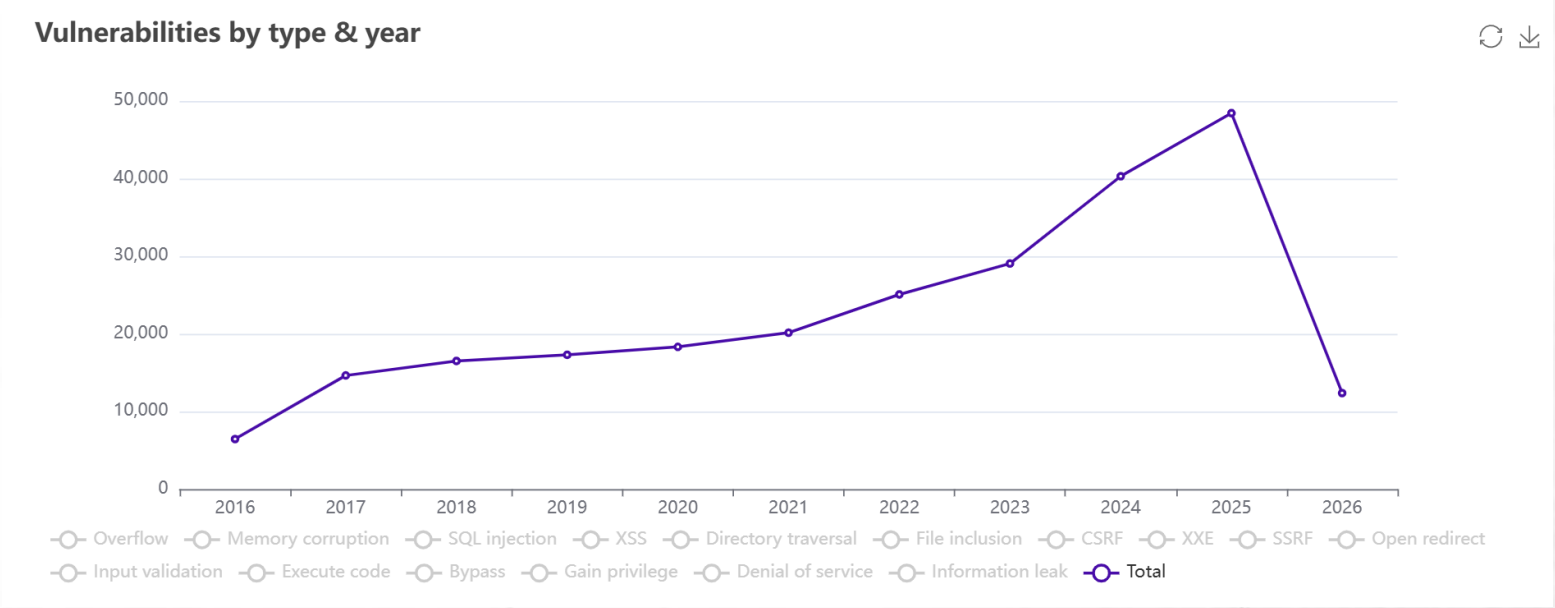


2026	12375
2025	48448
2024	40308
2023	29066
2022	25084
2021	20153
2020	18323
2019	17305
2018	16510
2017	14643
2016	6449

Zdroj: https://www.cvedetails.com/browse-by-date.php

Zverejnené zraniteľnosti (III.)





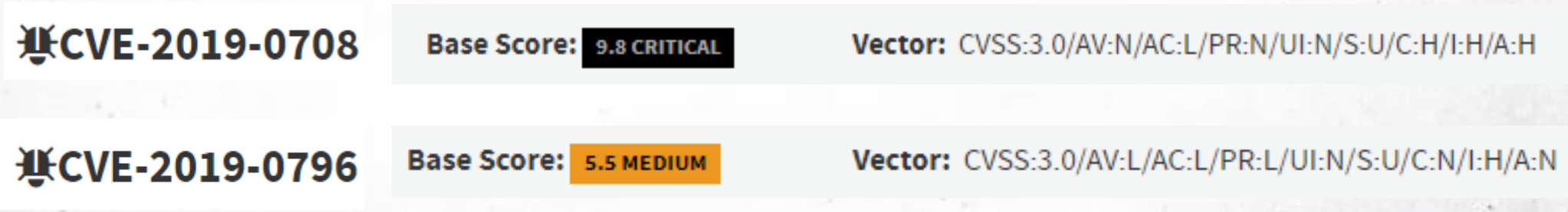
Zdroj: https://www.cvedetails.com/vulnerabilities-by-types.php

Závažnosť (skóre) zraniteľnosti (I.)

CVSS = Common Vulnerability Scoring System

CVSS skóre

- otvorený štandard pre ohodnotenie závažnosti zraniteľností
- umožňuje systematicky prioritizovať riešenie zraniteľností
- CVSS v3.1 Specification Document (first.org)
- CVSS v4.0 Specification Document (first.org)



Zdroj: https://www.cvedetails.com/

Závažnosť (skóre) zraniteľnosti (II.)

Qualitative Severity Ratings

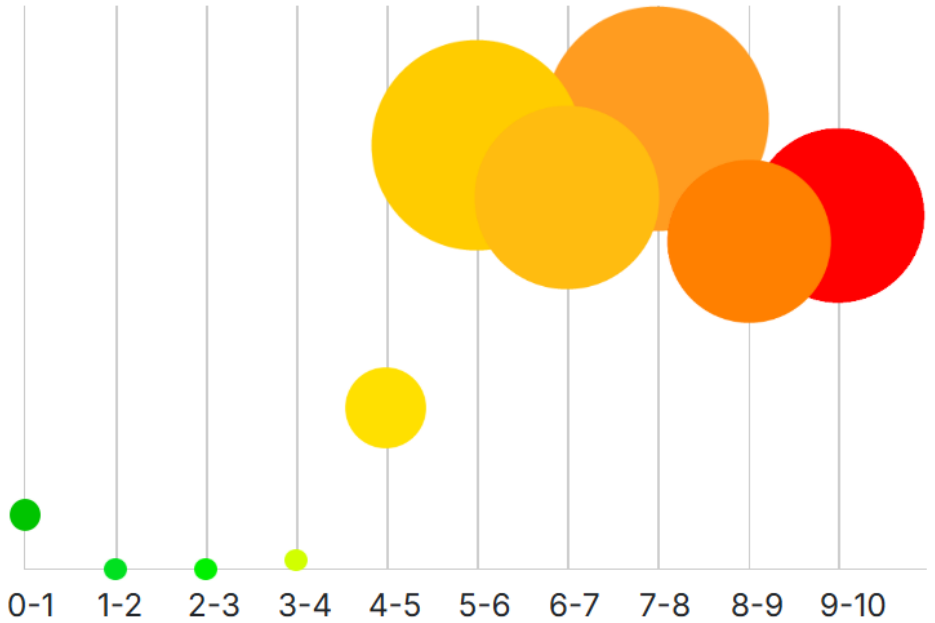
CVSS v2.0 Ratings		CVSS v3.x Ratings		CVSS v4.0 Ratings	
Severity	**Severity Score Range**	**Severity**	**Severity Score Range**	**Severity**	**Severity Score Range**
		None*	0.0	None*	0.0
Low	0.0-3.9	Low	0.1-3.9	Low	0.1-3.9
Medium	4.0-6.9	Medium	4.0-6.9	Medium	4.0-6.9
High	7.0-10.0	High	7.0-8.9	High	7.0-8.9
		Critical	9.0-10.0	Critical	9.0-10.0

Zdroj: https://nvd.nist.gov/vuln-metrics/cvss

Závažnosť (skóre) zraniteľnosti (III.)

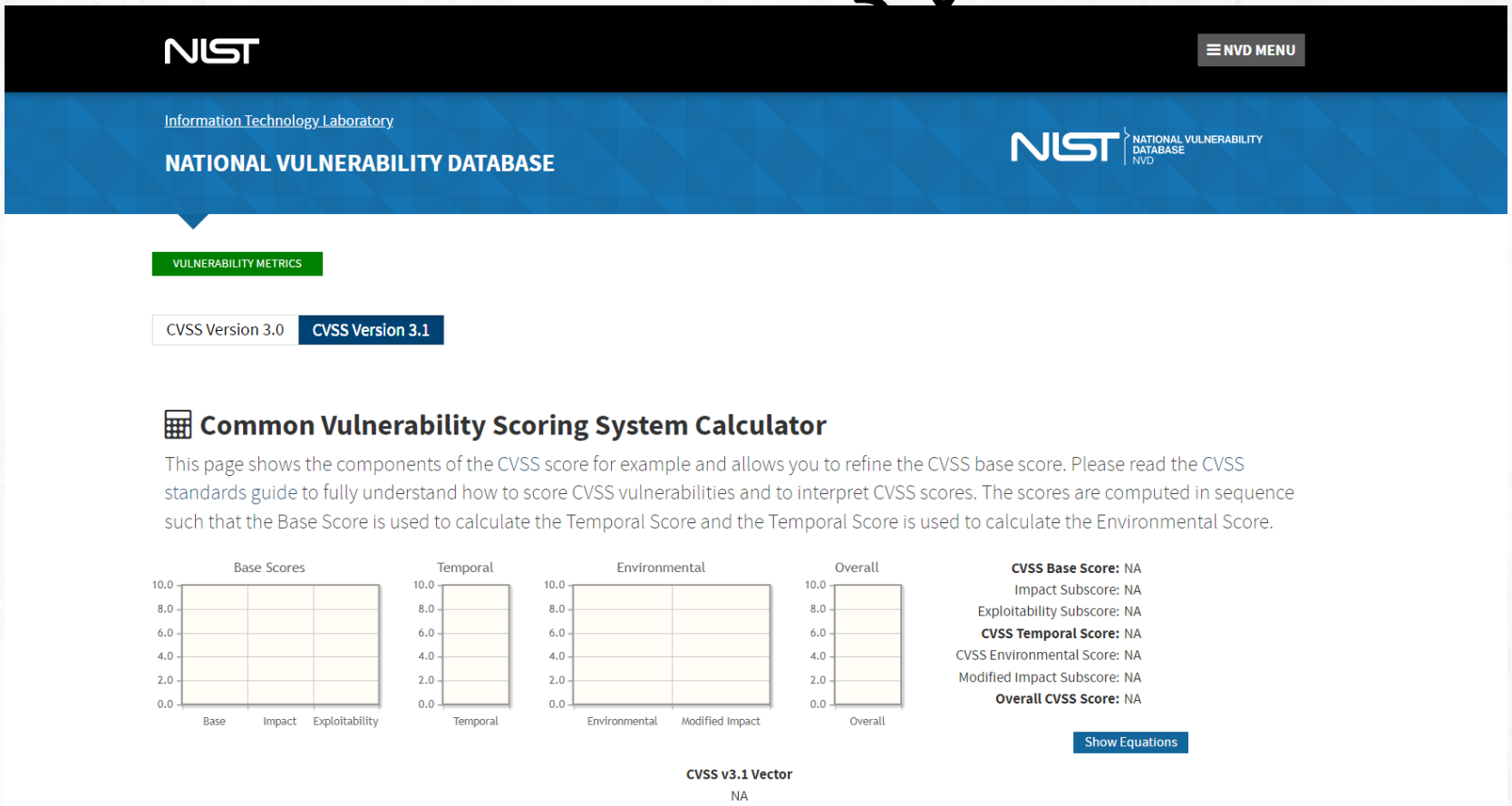
CVSS Score Range	Vulnerabilities
0-1	1507
1-2	52
2-3	348
3-4	573
4-5	3777
5-6	9793
6-7	8582
7-8	10428
8-9	7581
9+	8182
Total	50823

Weighted Average CVSS Score: 7.4



Zdroj: https://www.cvedetails.com/

Závažnosť (skóre) zraniteľnosti – CVSS 3.x



Zdroj: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

Závažnosť (skóre) zraniteľnosti – CVSS

Base Score Metrics

Exploitability Metrics

Attack Vector (AV)*

Network (AV:N) | Adjacent Network (AV:A) | Local (AV:L) | Physical (AV:P)

Attack Complexity (AC)*

Low (AC:L) | High (AC:H)

Privileges Required (PR)*

None (PR:N) | Low (PR:L) | High (PR:H)

User Interaction (UI)*

None (UI:N) | Required (UI:R)

Scope (S)*

Unchanged (S:U) | Changed (S:C)

Impact Metrics

Confidentiality Impact (C)*

None (C:N) | Low (C:L) | High (C:H)

Integrity Impact (I)*

None (I:N) | Low (I:L) | High (I:H)

Availability Impact (A)*

None (A:N) | Low (A:L) | High (A:H)

* - All base metrics are required to generate a base score.

Temporal Score Metrics

Exploit Code Maturity (E)

Not Defined (E:X) | Unproven that exploit exists (E:U) | Proof of concept code (E:P) | Functional exploit exists (E:F) | High (E:H)

Remediation Level (RL)

Not Defined (RL:X) | Official fix (RL:O) | Temporary fix (RL:T) | Workaround (RL:W) | Unavailable (RL:U)

Report Confidence (RC)

Not Defined (RC:X) | Unknown (RC:U) | Reasonable (RC:R) | Confirmed (RC:C)

Environmental Score Metrics

Exploitability Metrics

Attack Vector (MAV)

Not Defined (MAV:X) | Network (MAV:N) | Adjacent Network (MAV:A) | Local (MAV:L) | Physical (MAV:P)

Attack Complexity (MAC)

Not Defined (MAC:X) | Low (MAC:L) | High (MAC:H)

Privileges Required (MPR)

Not Defined (MPR:X) | None (MPR:N) | Low (MPR:L) | High (MPR:H)

User Interaction (MUI)

Not Defined (MUI:X) | None (MUI:N) | Required (MUI:R)

Scope (MS)

Not Defined (MS:X) | Unchanged (MS:U) | Changed (MS:C)

Impact Metrics

Confidentiality Impact (MC)

Not Defined (MC:X) | None (MC:N) | Low (MC:L) | High (MC:H)

Integrity Impact (MI)

Not Defined (MI:X) | None (MI:N) | Low (MI:L) | High (MI:H)

Availability Impact (MA)

Not Defined (MA:X) | None (MA:N) | Low (MA:L) | High (MA:H)

Impact Subscore Modifiers

Confidentiality Requirement (CR)

Not Defined (CR:X) | Low (CR:L) | Medium (CR:M) | High (CR:H)

Integrity Requirement (IR)

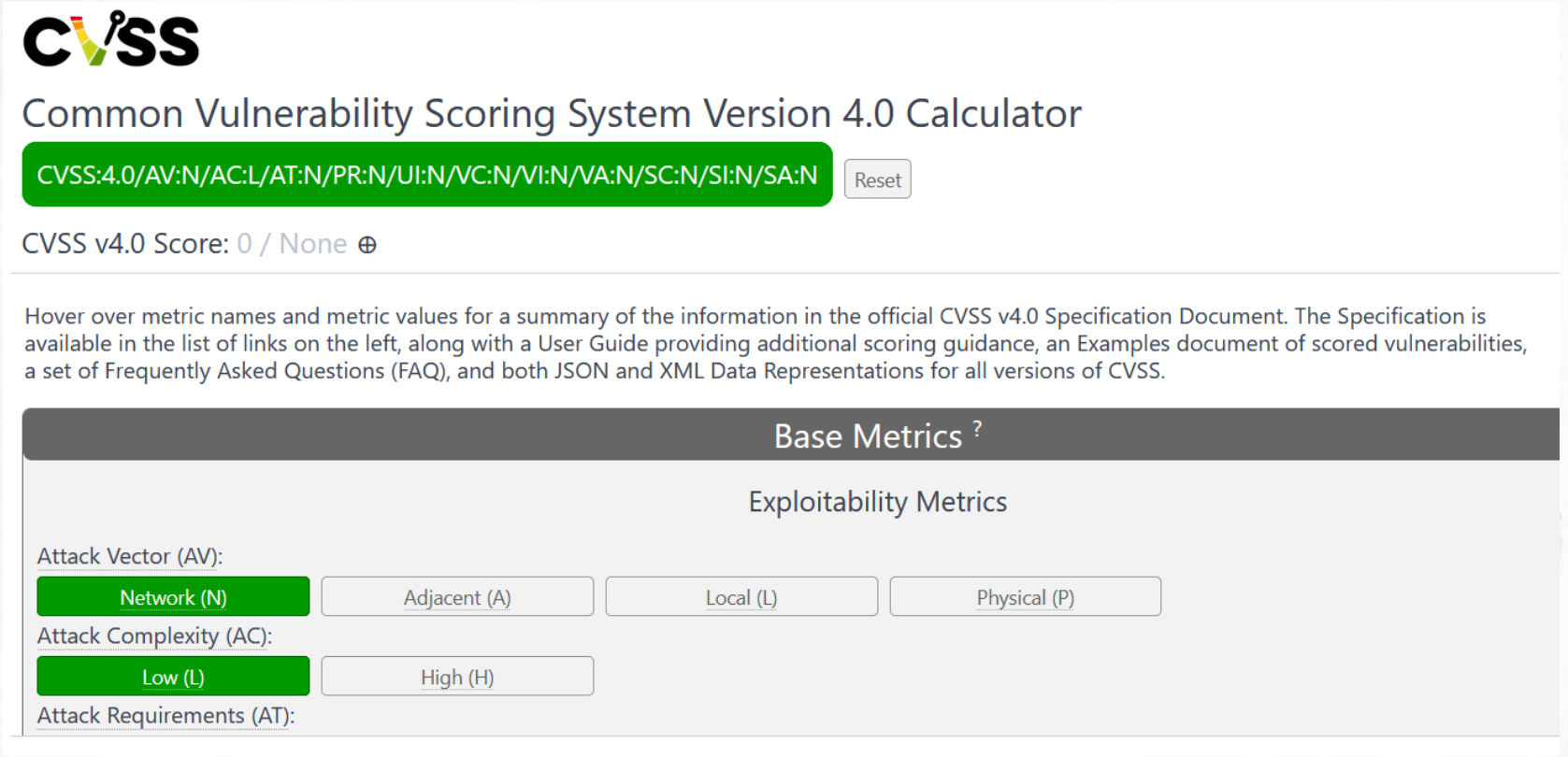
Not Defined (IR:X) | Low (IR:L) | Medium (IR:M) | High (IR:H)

Availability Requirement (AR)

Not Defined (AR:X) | Low (AR:L) | Medium (AR:M) | High (AR:H)

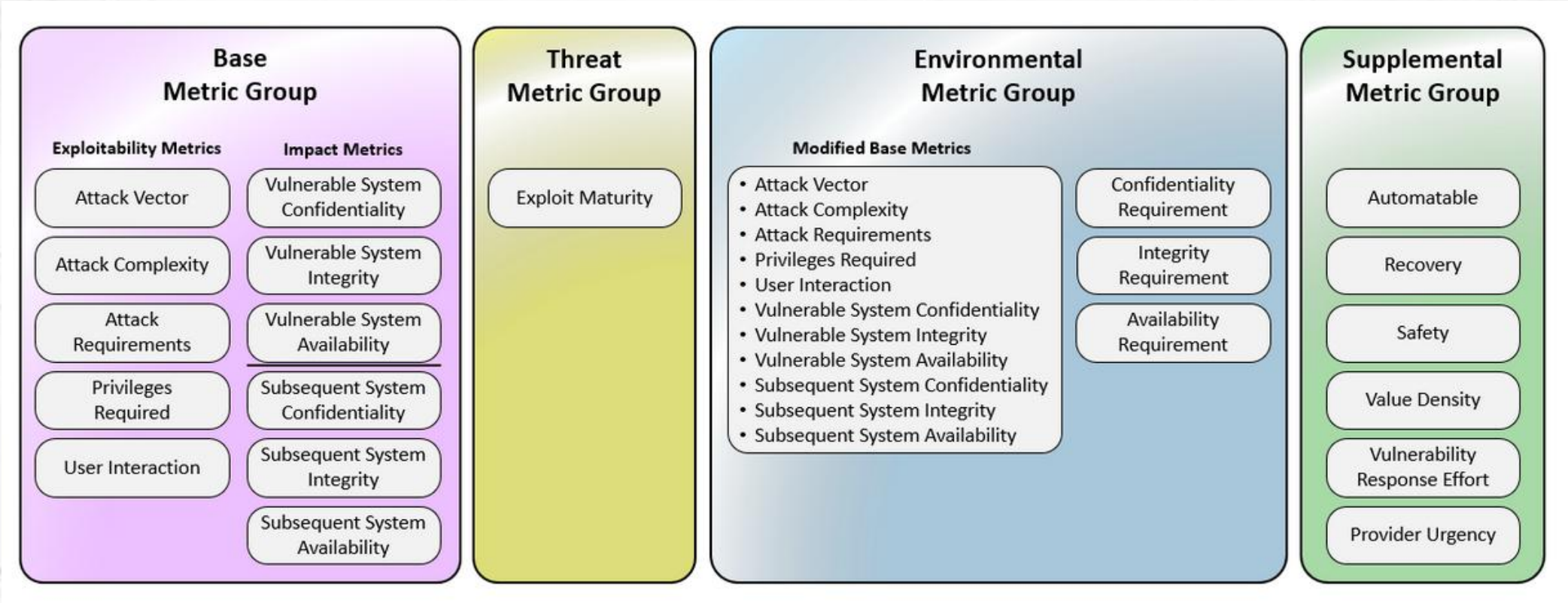
Zdroj: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

Závažnosť (skóre) zraniteľnosti – CVSS 4.0



Zdroj: https://www.first.org/cvss/calculator/4.0

Závažnosť (skóre) zraniteľnosti – CVSS 4.0



Zdroj: https://www.first.org/cvss/v4.0/specification-document

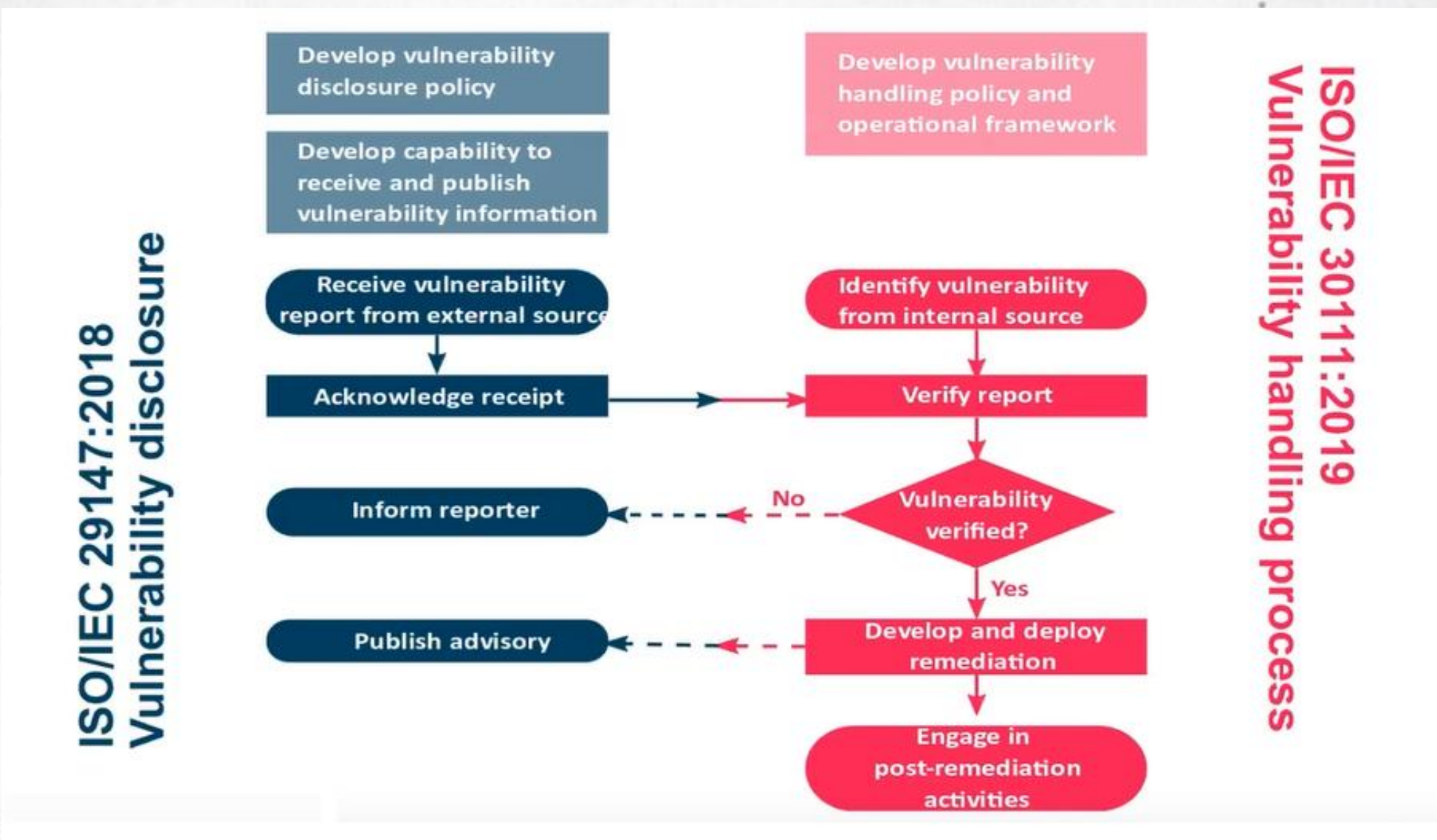
Čo je ovplyvnené zraniteľnosťou?

CPE = Common Platform Enumeration

- štruktúrovaná schéma pomenovania systémov informačných technológií, softvéru a balíkov

- cpe:/ <part>:<vendor>:<product>:<version>:<update>:<edition>:<language>

Handling a disclosure zraniteľnosti



Zdroj: ISO/IEC 29147:2018, ISO/IEC 30111:2019

Manažment zraniteľností (I.)

- Manažment hrozieb a zraniteľností využíva rôzne nástroje a riešenia na prevenciu a riešenie kybernetických hrozieb.

- Nepretržitý, proaktívny a často automatizovaný proces, ktorý chráni počítačové systémy, siete a aplikácie pred kybernetickými útokmi.

Phase 1: Discovery

Create a full asset inventory across your organization's network. Develop a baseline for your security program by identifying vulnerabilities on an automated schedule so you can stay ahead of threats to company information.

Phase 2: Prioritization of assets

Assign a value to each asset group that is reflective of its criticality. This will help you understand which groups need more attention and will help streamline your decision-making process when faced with allocating resources.

Phase 3: Assessment

The third part of the vulnerability management lifestyle is assessing your assets to understand the risk profile of each one. This allows you to determine which risks to eliminate first based on a variety of factors, including its criticality and vulnerability threat levels as well as classification.

Phase 4: Reporting

Next, determine the various levels of risk associated with each asset based on your assessment results. Then, document your security plan and report known vulnerabilities.

Phase 5: Remediation

Now that you know which vulnerabilities are the most pressing for your business, it's time to fix them, starting with those that pose the highest risks.

Phase 6: Verification and monitoring

The final phase of the vulnerability management process includes using regular audits and process follow-up to ensure that threats have been eliminated.

Zdroj: https://www.microsoft.com/en-us/security/business/security-101/what-is-vulnerability-management

Manažment zraniteľností (II.)

- **Zisťovanie aktív a inventarizácia (Asset discovery and inventory)**
- IT je zodpovedné za sledovanie a udržiavanie záznamov o všetkých zariadeniach, softvéri a serveroch v digitálnom prostredí spoločnosti, čo však môže byť mimoriadne zložité, pretože mnohé organizácie majú tisíce aktív na viacerých miestach.

- **Skenovanie zraniteľností (Vulnerability scanning)**
- Skenery zraniteľností zvyčajne fungujú tak, že vykonávajú sériu testov proti systémom a sieťam, pričom hľadajú zraniteľnosti, slabiny alebo chyby. Testy môžu zahŕňať pokusy o zneužitie známych zraniteľností, uhádnutie predvolených hesiel alebo používateľských účtov alebo iné.
-

Zdroj: https://www.microsoft.com/en-us/security/business/security-101/what-is-vulnerability-management

Manažment zraniteľností (III.)

- **Správa opráv (Patch Management)**
- Je to nástroj, ktorý pomáha organizáciám udržiavať ich počítačové systémy aktuálne pomocou najnovších bezpečnostných opráv. Väčšina riešení automaticky skontroluje aktualizácie a upozorní používateľa, keď sú k dispozícii nové. Niektoré systémy na správu opráv tiež umožňujú nasadenie opráv na viacero počítačov v organizácii.

- **Manažment bezpečnostných informácií a udalostí (SIEM)**
- SIEM koreluje bezpečnostné informácie a udalosti organizácie v reálnom čase. Riešenia SIEM sú navrhnuté tak, aby organizáciám poskytli prehľad o všetkom, čo sa deje v rámci celého ich digitálneho majetku, vrátane IT infraštruktúry. To zahŕňa monitorovanie sieťovej prevádzky, identifikáciu zariadení, ktoré sa pokúšajú pripojiť k interným systémom, sledovanie aktivity používateľov a ďalšie.

Zdroj: https://www.microsoft.com/en-us/security/business/security-101/what-is-vulnerability-management

Manažment zraniteľností (IV.)

- **Penetračné testovanie (Penetration testing)**
- Softvér na penetračné testovanie je navrhnutý tak, aby pomohol IT profesionálom nájsť a využiť zraniteľné miesta v počítačových systémoch. Niektoré produkty ponúkajú aj automatizačné funkcie, ktoré pomáhajú urýchliť proces testovania. Simuláciou útokov môžu testeri identifikovať slabé miesta v systémoch, ktoré by mohli zneužiť reálni útočníci.

- **Threat intelligence**
- Jedná sa o zhromažďovanie údajov z rôznych zdrojov – ako sú napríklad databázy exploitov a podobne – tieto riešenia pomáhajú spoločnostiam identifikovať trendy a vzory, ktoré by mohli naznačovať budúce narušenie bezpečnosti alebo útok.

Zdroj: https://www.microsoft.com/en-us/security/business/security-101/what-is-vulnerability-management

Penetračné testovanie a exploity

Penetration testing tools

From sources across the web

- Metasploit
- Wireshark
- Burp Suite
- Nmap
- Kali Linux
- Aircrack-ng
- Nessus
- Sqlmap
- Acunetix
- John the Ripper
- W3af
- Hashcat
- Nikto
- Beef
- Astra Pentest
- Ettercap

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

EXPLOIT DATABASE

Verified | Has App | Filters | Reset All

Show 15 | Search:

Date	D	A	V	Title	Type	Platform	Author
2024-02-28				WP Fastest Cache 1.2.2 - Unauthenticated SQL Injection	WebApps	PHP	Meryem Taşkın
2024-02-28				(shellcode) Linux-x64 - create a shell with execve() sending argument using XOR (/bin//sh) [55 bytes]	Local	Linux	Alexys (0x177git)
2024-02-28				Blood Bank v1.0 - Multiple SQL Injection	WebApps	PHP	Ersin Erenler
2024-02-28				Saflok - Key Derication Function Exploit	Local	Hardware	planthopper3301
2024-02-28				WordPress Plugin Admin Bar & Dashboard Access Control Version: 1.2.8 - "Dashboard Redirect" field Stored Cross-Site Scripting (XSS)	WebApps	PHP	Rachit Arora

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

Manažment zraniteľností (V.)

- **Oprava zraniteľností (Remediation vulnerabilities)**
- Oprava zahŕňa stanovenie priorít zraniteľných miest, identifikáciu vhodných ďalších krokov a generovanie tiketov na nápravu, aby ich IT tímy mohli vykonať. Sledovanie je dôležitým nástrojom na zabezpečenie toho, aby bola zraniteľnosť alebo nesprávna konfigurácia správne vyriešená.

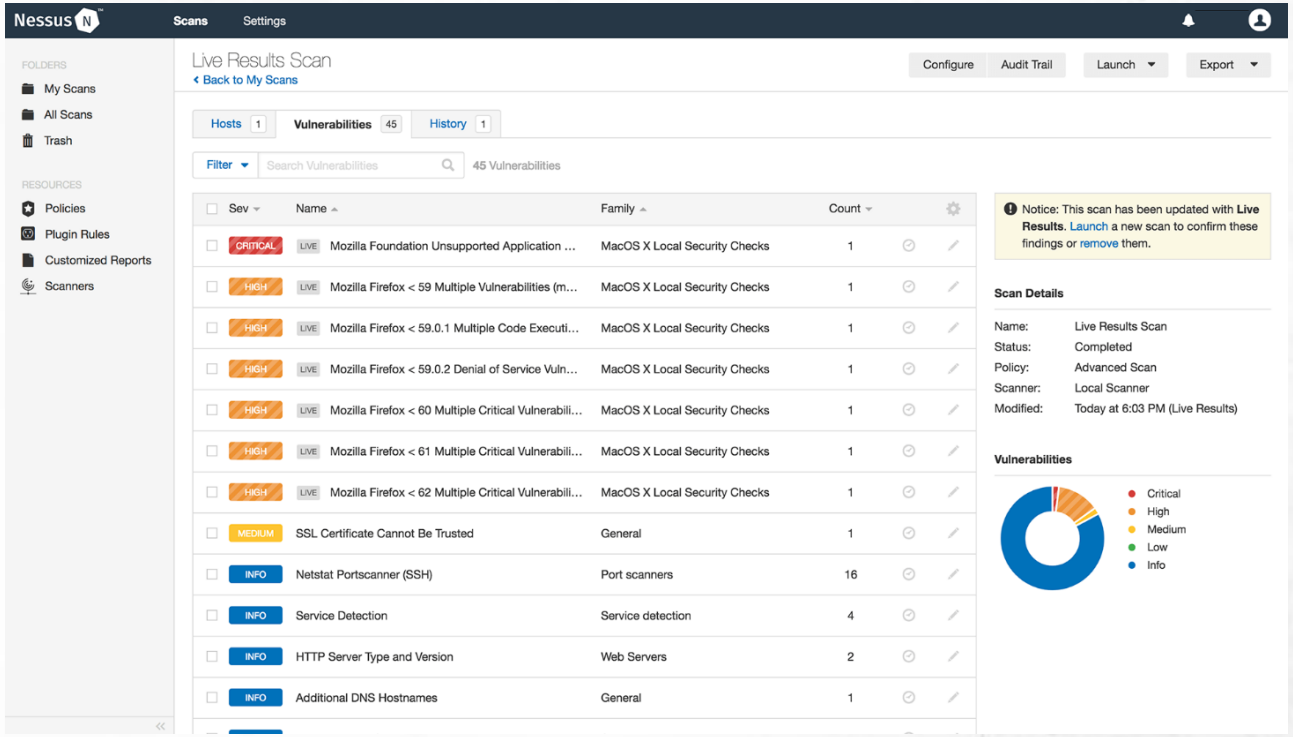
Zdroj: https://www.microsoft.com/en-us/security/business/security-101/what-is-vulnerability-management

Skenovanie zraniteľností

OpenVAS
Open Vulnerability Assessment Scanner

Nessus
vulnerability scanner

BURPSUITE 2.0



Qualys®

Zdroj: https://www.tenable.com/products/nessus, https://www.openvas.org/, https://portswigger.net/burp, https://www.qualys.com/

Príklad – Log4j (I.)

Malé internetové inferno. Objavili chybu, ktorá ohrozuje mnohé služby

Firmy sa musia zaplátať.

Renáta Zelná
Redaktorka

Ilustračná fotografia. (Zdroj: unsplash)

TOUCHIT NAVIGOVAŤ : TOUCHIT

ESET eviduje celosvetovo stovky tisícov pokusov o útoky, ktoré sa snažia zneužiť kritickú zraniteľnosť Log4Shell.

živě Prihlásenie

DOPLNENÉ **Knižnica Javy obsahuje kritickú zraniteľnosť. Môžu ju zneužiť ransomvéry**

Zdroj: Pexels

živě Viliam Kaliňák

Aktivujte si newslettre

Používateľom knižnice sa odporúča, aby ju okamžite aktualizovali.

Zdroj: https://touchit.sk/pozor-na-zranitelnost-log4shell-ohrozeni-su-aj-slovenske-firmy/387431, https://tech.sme.sk/c/22803385/chyba-v-log4j-co-je-jej-podstatou-a-koho-ohrozuje.html, https://zive.aktuality.sk/clanok/7t17zjl/kniznica-javy-obsahuje-kriticku-zranitelnost-mozu-ju-zneuzit-ransomvery/

Príklad – Log4j (II.)

https://www.cvedetails.com/cve/CVE-2021-44228/

263	Application	Cisco	Workload Optimization Manager
264	OS	Debian	Debian Linux
265	OS	Debian	Debian Linux
266	OS	Debian	Debian Linux
267	OS	Fedoraproject	Fedora
268	OS	Fedoraproject	Fedora
269	Application	Intel	Audio Development Kit
270	Application	Intel	Computer Vision Annotation Tool
271	Application	Intel	Data Center Manager
272	Application	Intel	Genomics Kernel Library
273	Application	Intel	Oneapi Sample Browser
274	Application	Intel	Secure Device Onboard
275	Application	Intel	Sensor Solution Firmware Development Kit
276	Application	Intel	System Debugger
277	Application	Intel	System Studio
278	Application	Netapp	Active Iq Unified Manager
279	Application	Netapp	Active Iq Unified Manager
280	Application	Netapp	Active Iq Unified Manager
281	Application	Netapp	Cloud Insights
282	Application	Netapp	Cloud Manager

Zdroj: https://zive.aktuality.sk/clanok/x2p2pxj/hacknu-vrtulnik-na-marse-tiez-vyuziva-zranitelnu-kniznicu-log4j/ https://jncie.eu/log4j-juniper-sirt-page/

Príklad – Log4j (III.)

CVE-2021-44228

CVSS 3.x Severity and Metrics:

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

Base Score Metrics

Exploitability Metrics

Attack Vector (AV)*

Network (AV:N)	Adjacent Network (AV:A)	Local (AV:L)	Physical (AV:P)

Attack Complexity (AC)*

Low (AC:L)	High (AC:H)

Privileges Required (PR)*

None (PR:N)	Low (PR:L)	High (PR:H)

User Interaction (UI)*

None (UI:N)	Required (UI:R)

Scope (S)*

Unchanged (S:U)	Changed (S:C)

Impact Metrics

Confidentiality Impact (C)*

None (C:N)	Low (C:L)	High (C:H)

Integrity Impact (I)*

None (I:N)	Low (I:L)	High (I:H)

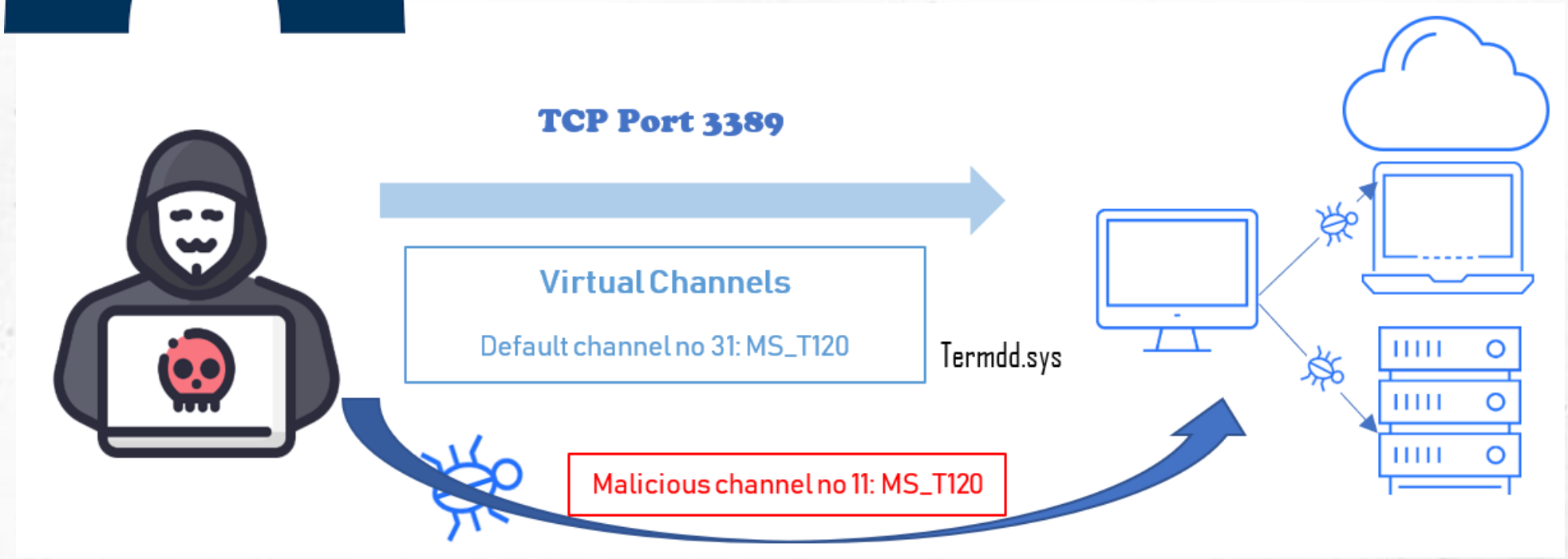
Availability Impact (A)*

None (A:N)	Low (A:L)	High (A:H)

Zdroj: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?name=CVE-2021-44228&vector=AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H&version=3.1&source=NIST

Príklad – bluekeep (I.)

- CVE-2019-0708
- Microsoft's Remote Desktop Protocol (RDP) implementácia
- remote code execution.



Zdroj: https://en.wikipedia.org/wiki/BlueKeep, https://www.opswat.com/blog/bluekeep-detecting-and-remediating-a-critical-and-wormable-remote-code-execution-vulnerability

Príklad – bluekeep (II.)

CVE-2019-0708 Detail

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** 9.8 CRITICAL **Vector:** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Base Score Metrics

Exploitability Metrics

Attack Vector (AV)*

Network (AV:N)	Adjacent Network (AV:A)	Local (AV:L)	Physical (AV:P)

Attack Complexity (AC)*

Low (AC:L)	High (AC:H)

Privileges Required (PR)*

None (PR:N)	Low (PR:L)	High (PR:H)

User Interaction (UI)*

None (UI:N)	Required (UI:R)

Scope (S)*

Unchanged (S:U)	Changed (S:C)

Impact Metrics

Confidentiality Impact (C)*

None (C:N)	Low (C:L)	**High (C:H)**

Integrity Impact (I)*

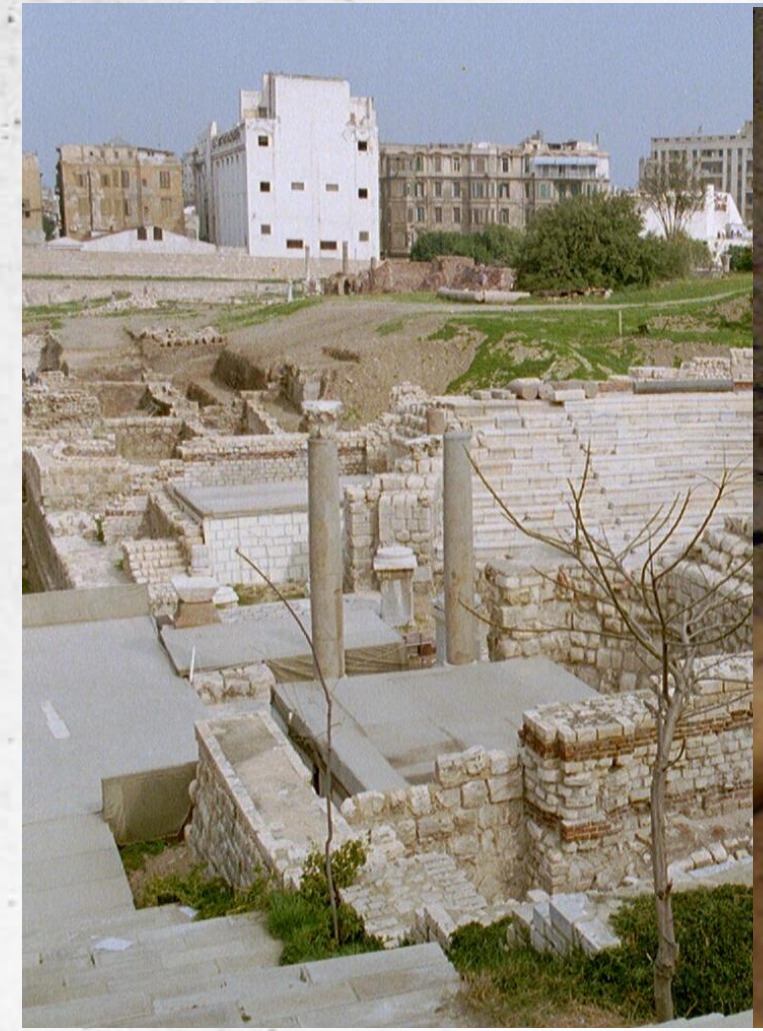
None (I:N)	Low (I:L)	**High (I:H)**

Availability Impact (A)*

None (A:N)	Low (A:L)	**High (A:H)**

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

Archeológia

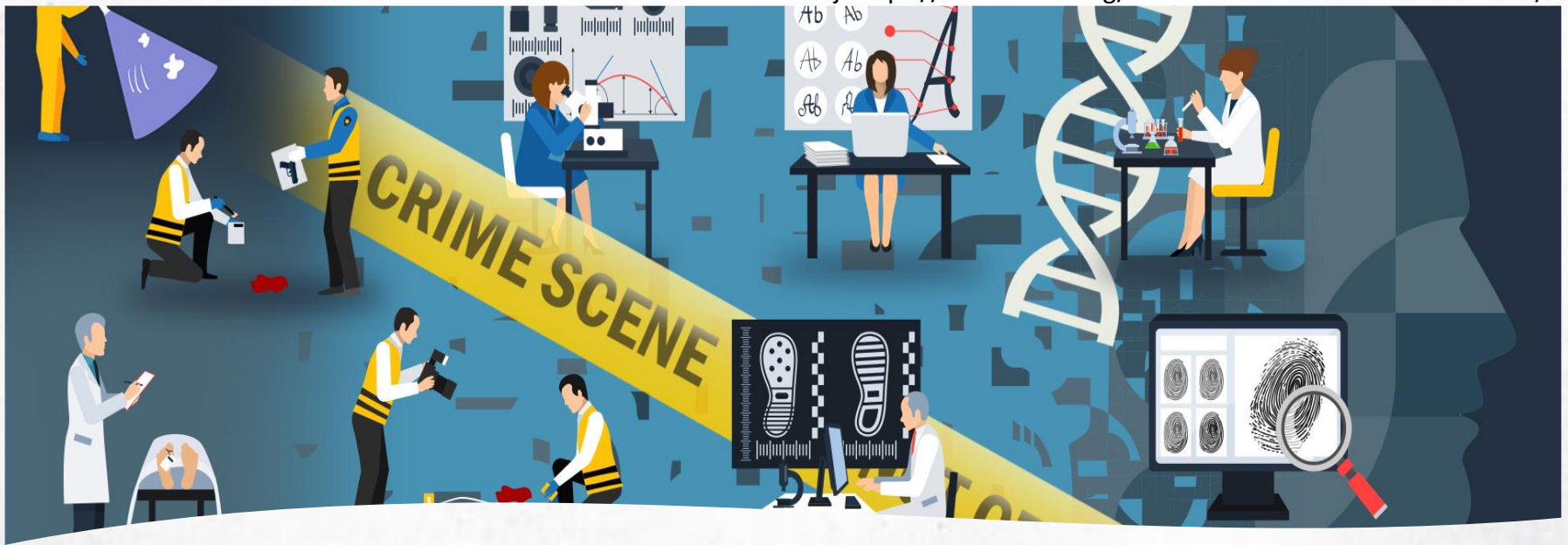


Zdroj: https://sk.wikipedia.org/wiki/Archeol%C3%B3gia, https://www.literama.sk/sk/knihy-kategoria/81/archeologia?_p_p=10, https://vedanadosah.cvtisr.sk/ludia/historia-a-archeologia/archeologovia-objavili-desiatky-vynimocne-zachovanych-vikinskych-kostier/

Forezná veda

- praktická aplikácia rôznych druhov vedy pre zodpovedanie otázok súvisiacich s právnym systémom
- "forenzná„ - v latinčine znamená "z fóra alebo pred ním".
- vzťahuje sa na proces získavania stôp, ktoré môžu byť prijaté ako dôkazy na súde
- forenzní vedci zhromažďujú, uchovávajú a analyzujú vedecké stopy

Zdroj: https://forensiccoe.org/webinar-human-factors-sourcebook/



Digitálna forezná analýza

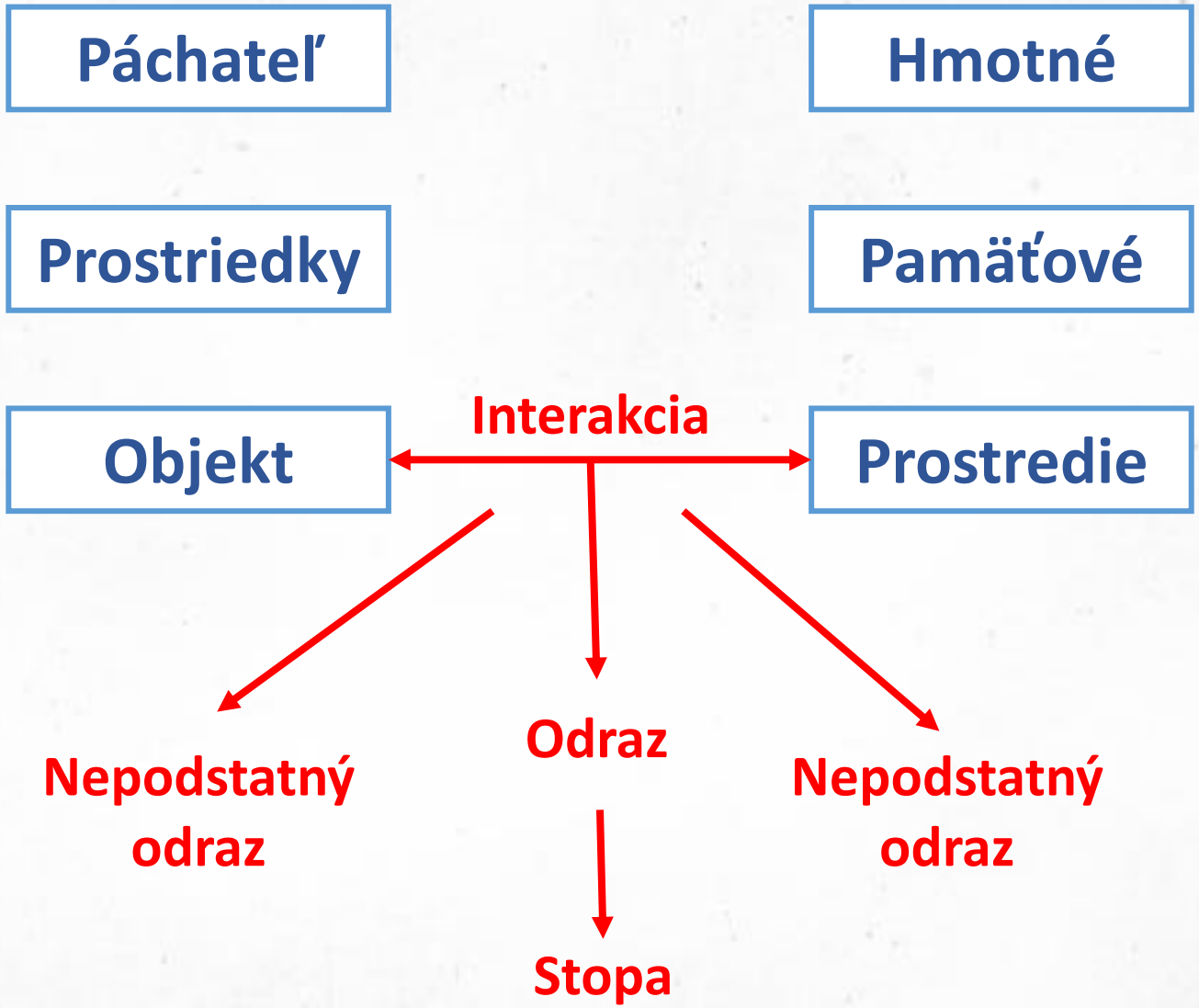
- je **viacstupňový proces** začínajúci identifikáciou digitálnych médií zo scény (možného trestného činu) ako potenciálneho dôkazu do fázy, v ktorej je predložený ako dôkaz odborným svedkom na súde (RAGHAVAN, 2013)

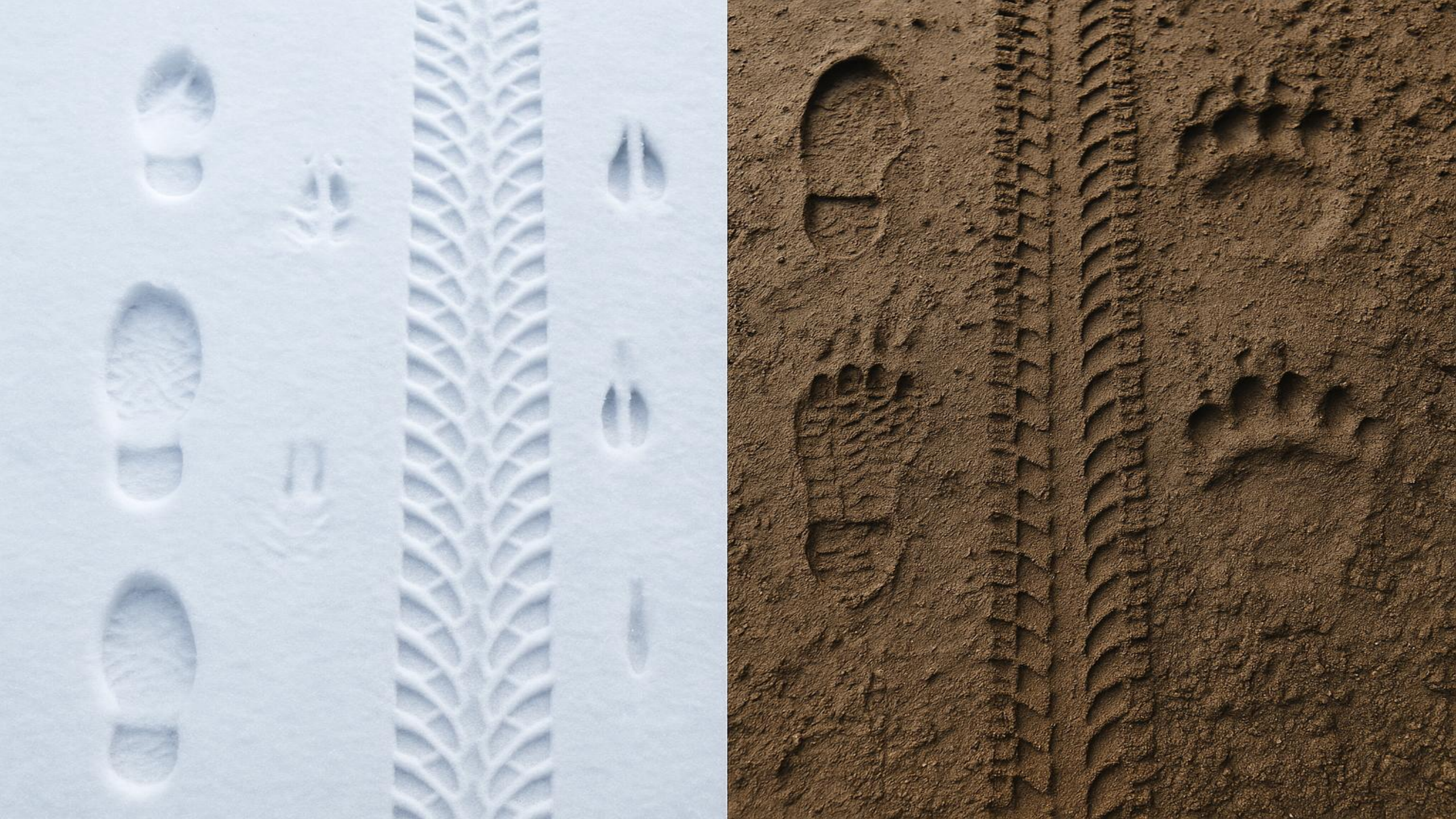
Locardov princíp výmeny

- **Locardov princíp výmeny**
  - „s kontaktom medzi dvoma body bude prebiehať výmena“
  - páchateľ priniesol niečo na miesto činu a odniesol niečo so sebou
  - napr. odtlačky, krv, vlasy a pod.

Zdroj: https://simplyforensic.com/edmond-locard/

Digitálna stopa (I.)





Digitálna stopa (III.)

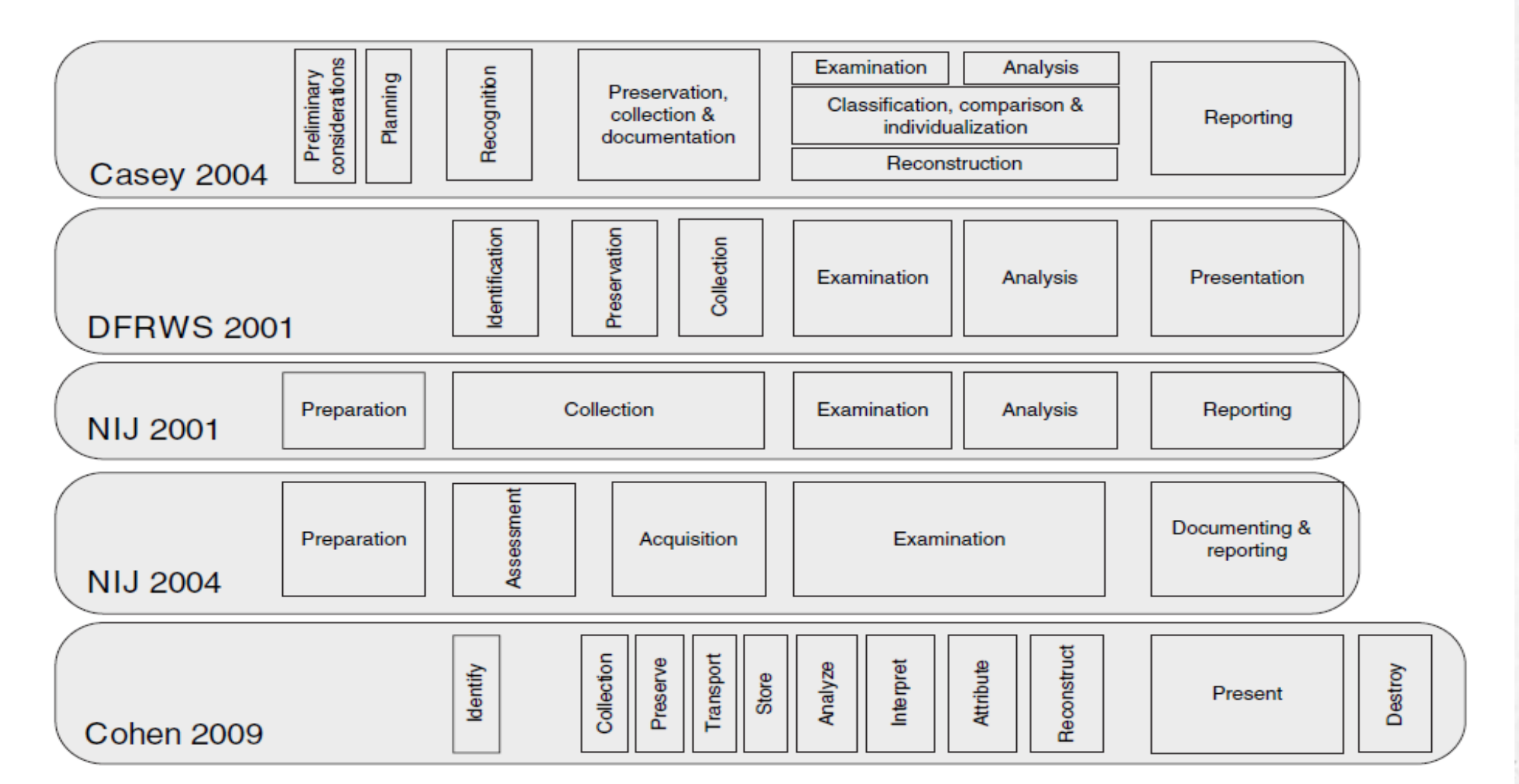
- je akákoľvek informácia s vypovedajúcou hodnotou uloženou alebo prenášanou v digitálnej podobe. **(Whitcomb, 2002)**

- je akákoľvek informácia uložená alebo prenášaná v binárnej forme, ktorá môže byť predložená súdu ako vecný dôkaz (**International Organization of Computer Evidence**)

- je akákoľvek informácia s vypovedacou hodnotou uložená alebo prenášaná v digitálnej binárnej forme, ktorá môže byť predložená súdu ako vecný dôkaz s vypovedacou hodnotou (**Scientific Working Group on Digital Evidence**)

Digitálna stopa (IV.)

Proces forenznej analýzy (I.)



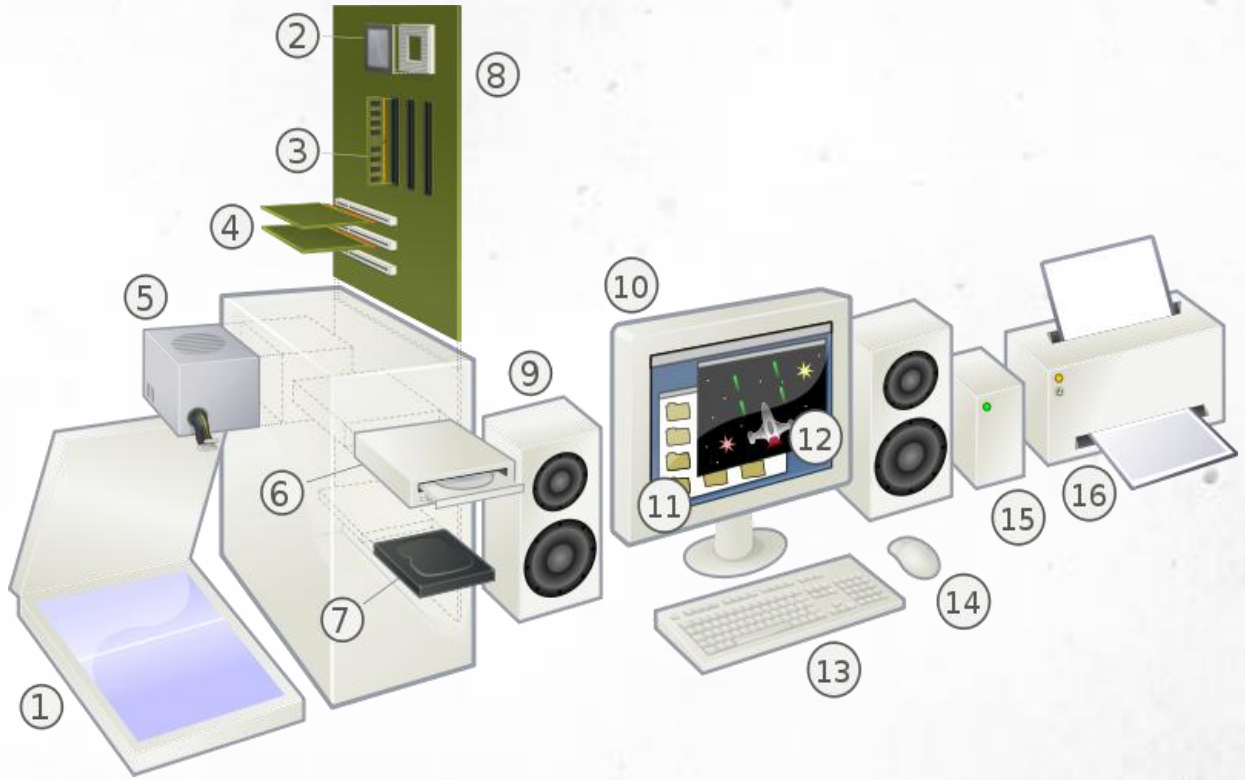
Zdroj: CASEY, Eoghan. Digital evidence and computer crime: Forensic science, computers, and the internet. 3. vydanie. Academic press, 2011. ISBN: 978-0123742681.

Proces forenznej analýzy (II.)

Fáza	Popis činností	Výstup fázy
Identifikácia (Identification)	▪ identifikácia účelu vyšetrovania a potrebných zdrojov ▪ vyhľadávanie, rozpoznávanie a dokumentáciu potenciálnych digitálnych stôp	▪ identifikované zariadenia
Zaisťovanie (Acquisition) a zber (Collection)	▪ zhromažďovanie údajov z digitálnych zariadení ▪ zhromažďovania zariadení, ktoré obsahujú potenciálne digitálne stopy	▪ forenzný image ▪ iné digitálne stopy
Uchovanie (Preservation)	▪ uloženie digitálnych stôp na vhodnom médií ▪ zaistenie integrity zaistených digitálnych stôp	▪ kryptografický haš
Vyťažovanie (Examination)	▪ extrakciu údajov (artefaktov) z digitálnych stôp ▪ redukcia a filtrovanie údajov (artefaktov) ▪ obnova súborov a získavanie (carving) údajov	▪ Výber relevantných digitálnych stôp (artefaktov)
Analýza (Analysis)	▪ Identifikujú sa nástroje a techniky, ktoré sa majú použiť ▪ prioritizácia, filtrácia, korelácia digitálnych stôp ▪ Interpretujú sa výsledky analýzy a potvrdzujú/vyvracajú hypotézy	▪ Potvrdenie/vyvrátenie hypotéz
Prezentácia (Presentation)	▪ sumarizácia a vysvetlenie výsledkov ▪ predloženie výsledkov zadávateľovi	▪ forenzná správa ▪ prezentácia

Identifikácia (I.)

- identifikácia účelu vyšetrovania a potrebných zdrojov
- vyhľadávanie, rozpoznávanie a dokumentáciu potenciálnych digitálnych stôp
- výstup: identifikované zariadenia



Identifikácia (II.)

- Dátové nosiče

Identifikácia (III.)

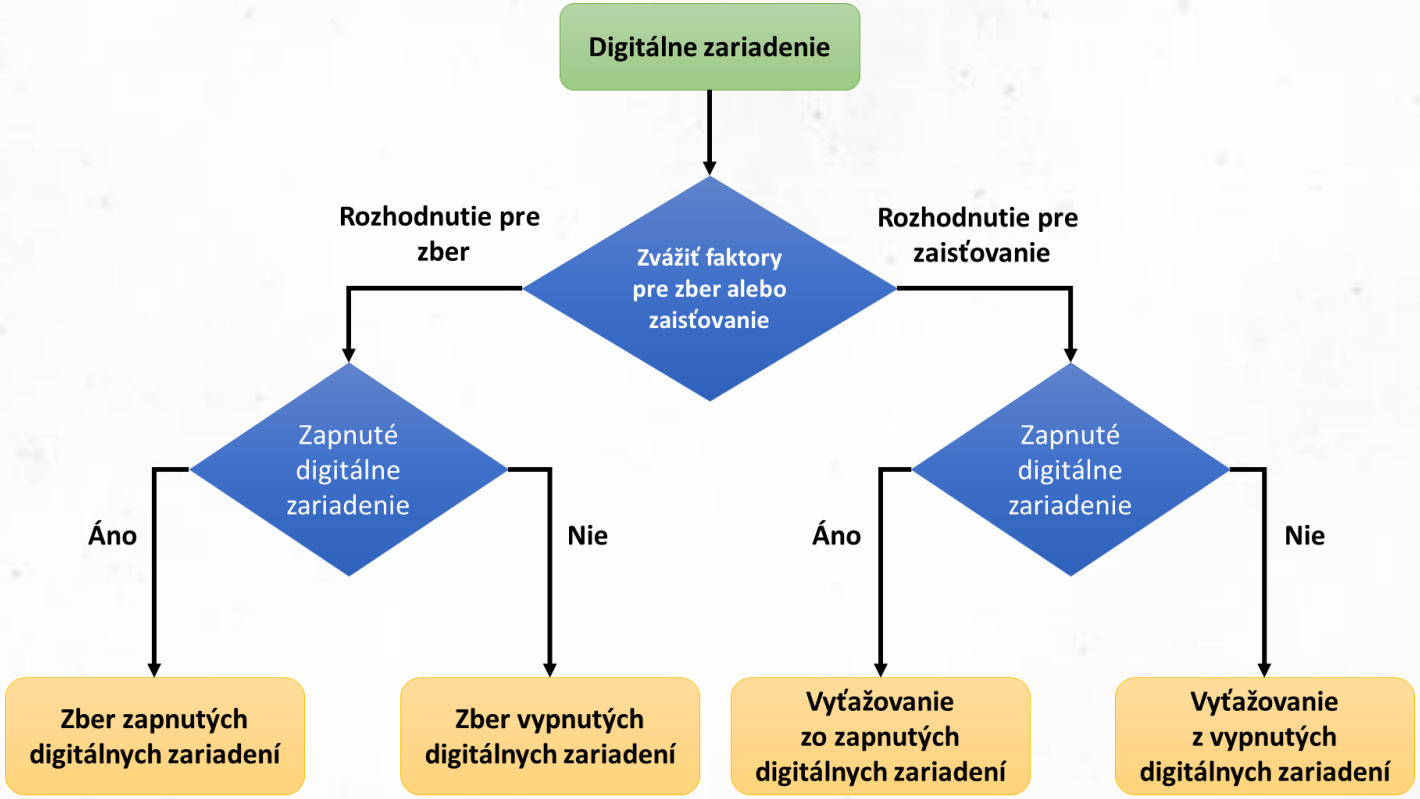
- Kde hľadať stopy?

Zdroj: http://web-cyb.org/hardware-info/elvn-desktop-progression.htm

Zdroj: https://www.flickr.com/photos/68800167@N07/6256946041

Zber a zaisťovanie (I.)

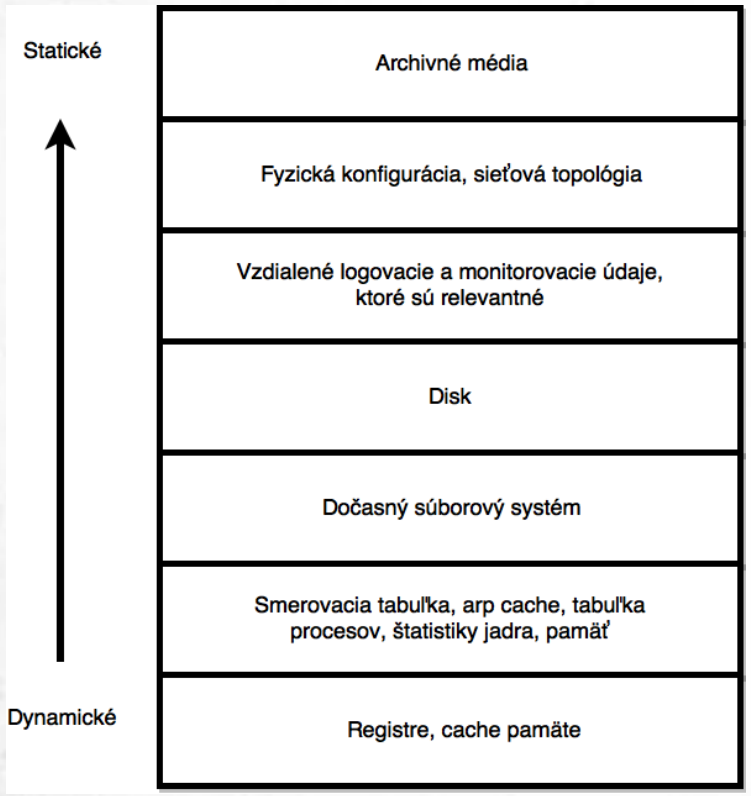
- cieľom tejto fázy je zhromažďovanie údajov z digitálnych zariadení za účelom vytvorenia digitálnej kópie s použitím riadnych forenzných metód a techník (Palmer, 2001).



ISO/IEC 27037:2012

Zber a zaisťovanie (II.)

- **Guidelines for Evidence Collection and Archiving** (RFC 3227), ktoré sa týkajú **poradia volatility** digitálnych stôp



Typ úložného média a údaje	Typická životnosť údajov
Registre, cache pamäte	nanosekundy
RAM	desiatky nanosekúnd
Stav siete	milisekundy
Procesy	sekundy
Údaje na disku (cache)	minúty
Cloudové úložisko	mesiace až roky
HDD úložisko	roky
Magnetické pásky	roky až dekády
CD-ROM, DVD, vytlačené údaje	dekády
Read-only pamäte, flash, SSD	dekády až storočia

Zber a zaisťovanie (III.)

Chain of Custody (reťazec uchovávania dôkazov)

- proces zabezpečujúci autentickosť, integritu
- dokumentácia zaisťovania stôp
- dokumentácia manipulácie s médiom s digitálnymi stopami

Číslo prípadu:			Číslo oddelenia:	
Vyšetrovateľ:				
Popis prípadu:				
Miesto získania dôkazu:				
Popis dôkazu		Výrobca	Výrobné číslo	Poznámky
Odtlačok dát	MD5			
	SHA2-256			
Dôkaz získaný:			Dátum a čas:	
Dôkaz zaznačovaný:			Dátum a čas:	
Dôkaz zabezpečený:			Dátum a čas:	
Dátum a čas	Akcia vykonaná s dôkazovým materiálom			Osoba + podpis
Strana:		Celkový počet strán:		Podpis:

Zber a zaisťovanie (IV.)

- používať **writeblocker**
  - špecializované zariadenia na zabránenie zápisu na zaistené médium počas kopírovania
  - pevné disky, USB kľúče, USB disky

Zdroj: https://amazon.com

Zber a zaisťovanie (V.)

Chyby pri zaisťovaní:

- **zlé zaistenie stôp** -> **znehodnotenie pre účely trestného konania**
- vypnutie zapnutého zariadenia bez zaistenia volatilných stôp
- **zle zapečatený hardvér** (napr. USB porty na na bokoch a vzadu na notebooku)
- **nepresné označenie** stôp (napr. obraz disku bieleho notebooku)
- **chaotické označenie** stôp (ak zaisťuje stopy viacero ľudí)
- **nezaistenie potrebného príslušenstva** (napr. dokumentácia, špecifické napájacie adaptéry)
- **nezaistenie ďalšieho príslušenstva** (napr. usb flash, CD/DVD)

Spôsob zaisťovania (I.)

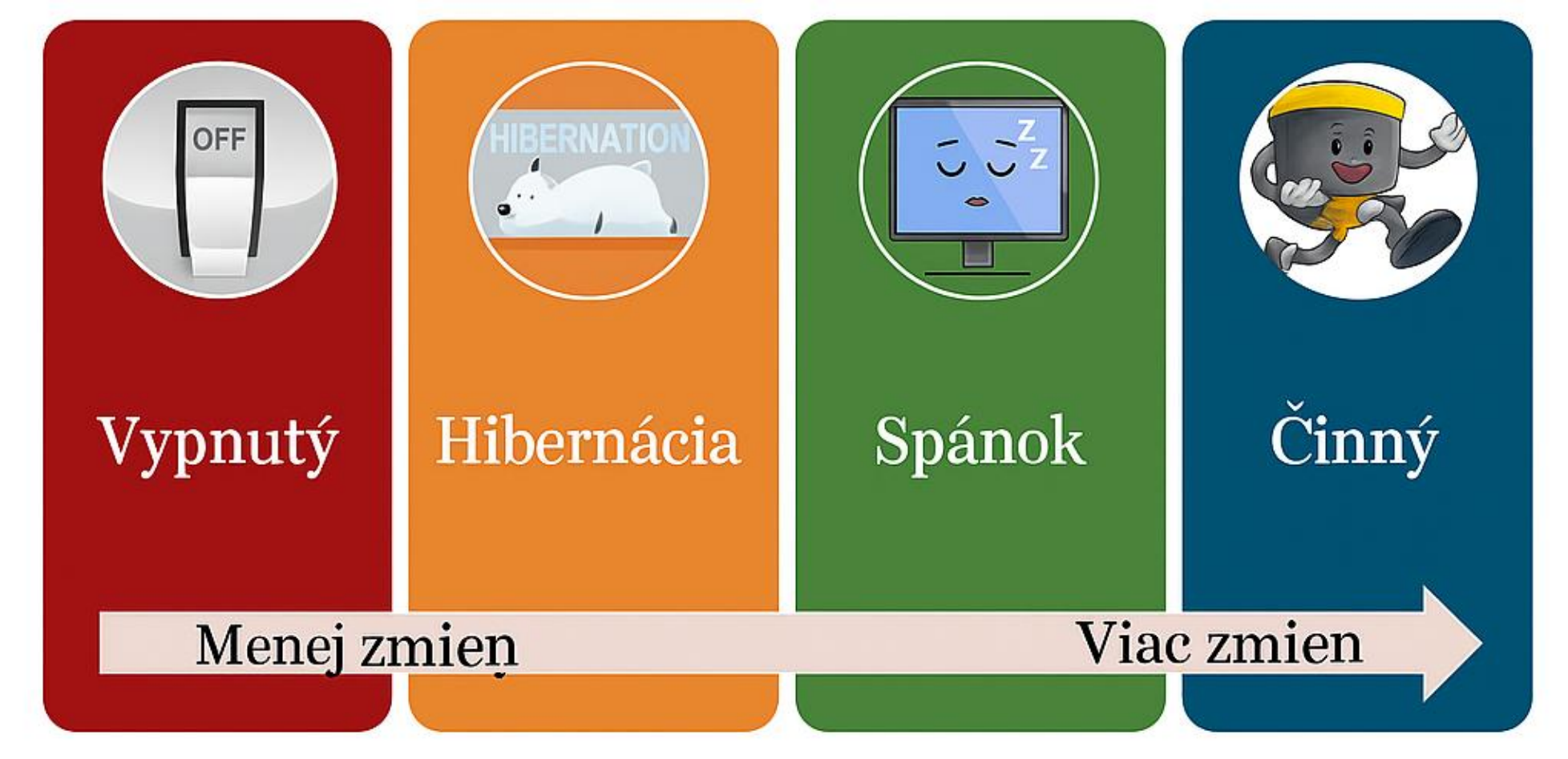
Live

- zariadenie je zapnuté
- dáta sa menia vplyvom zaisťovania aj bežnej činnosti systému
- RAM, swap, pripojené disky a pamäťové média, hardvérové
- kľúče, sieťová komunikácia

Post Mortem

- zariadenie je vypnuté
- bitové kópie zaistených médií cez writeblockery
- disky, pamäťové médiá

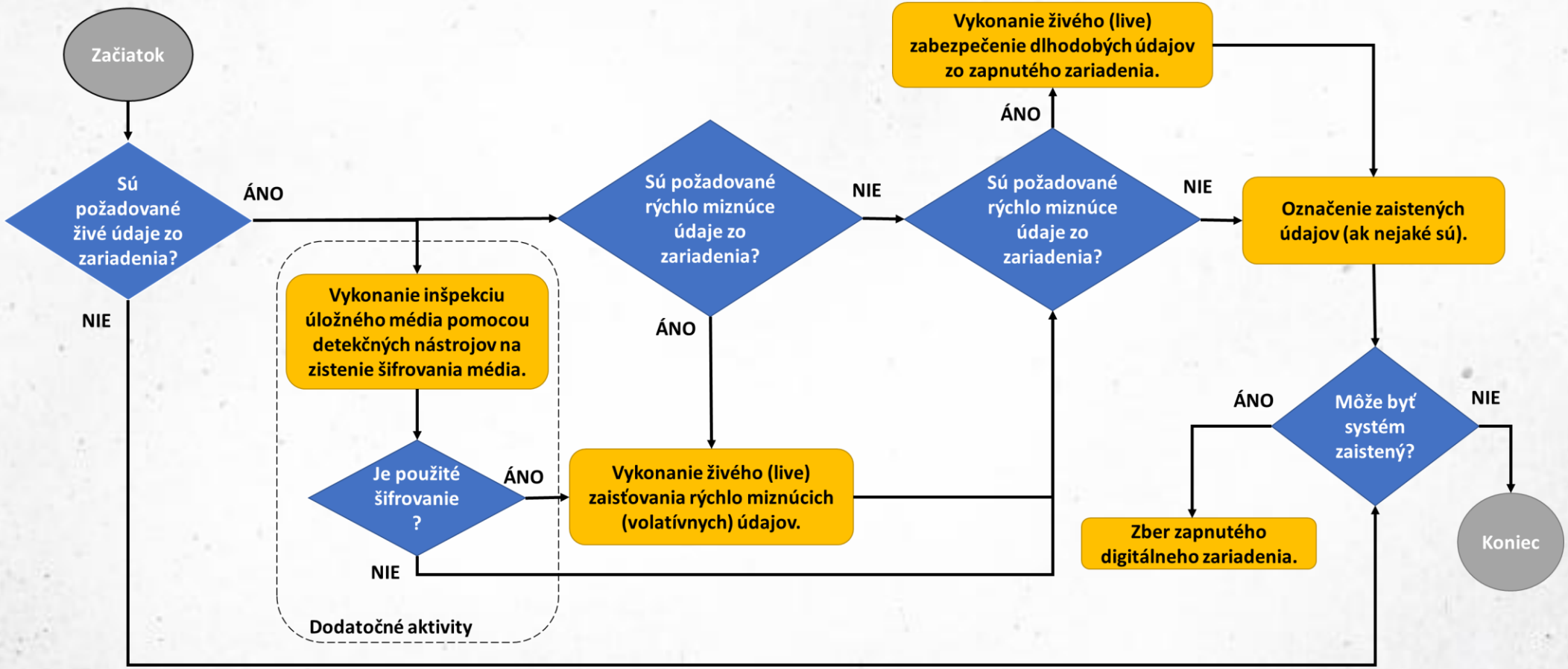
Spôsob zaisťovania (II.)



Zdroj: SANS materiál, FOR500

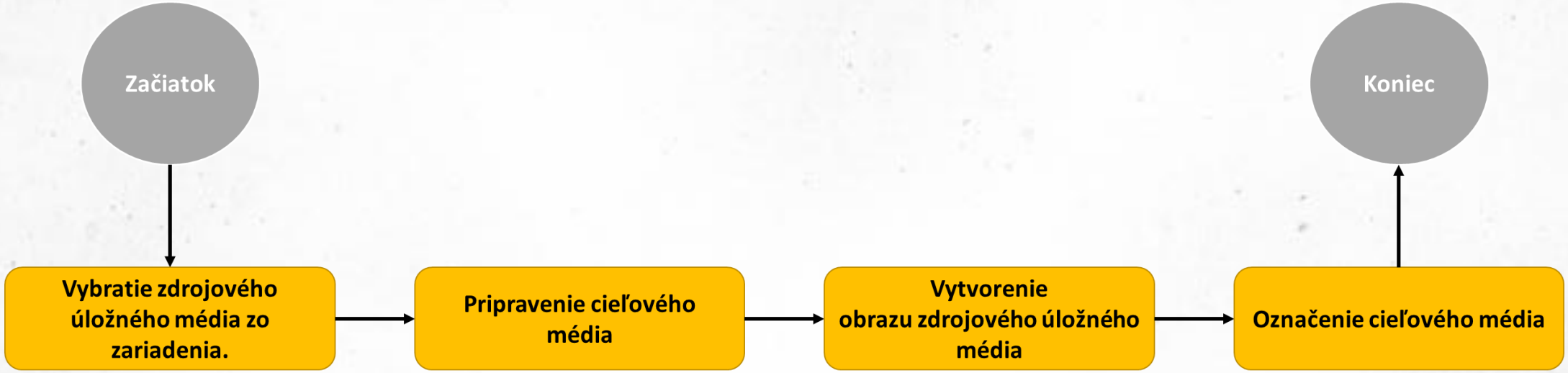
Spôsob zaisťovania (III.)

- **Zaisťovanie zo zapnutého zariadenia** (ISO/IEC 27037)



Spôsob zaisťovania (IV.)

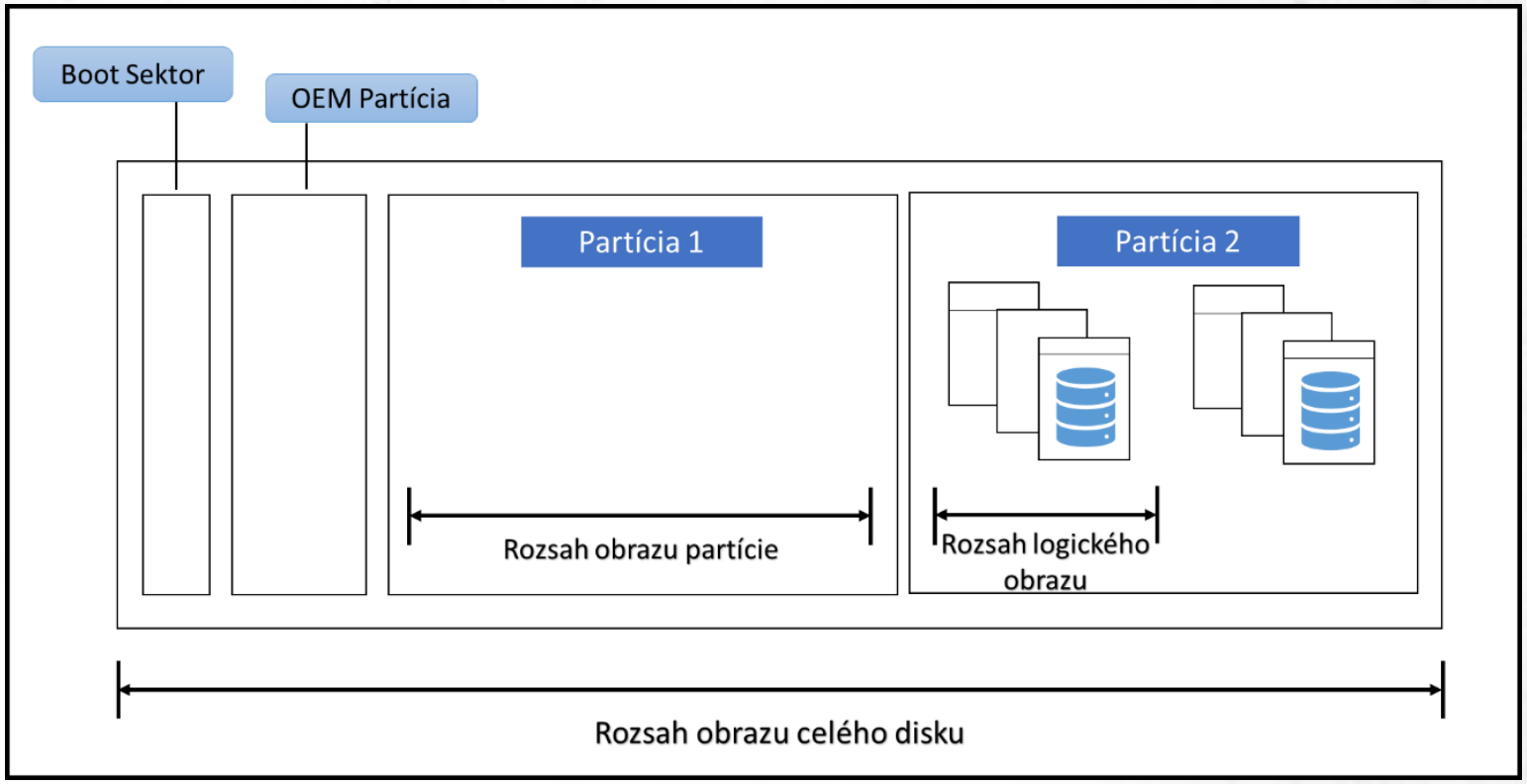
- **Zaisťovanie z vypnutého zariadenia** (ISO/IEC 27037)



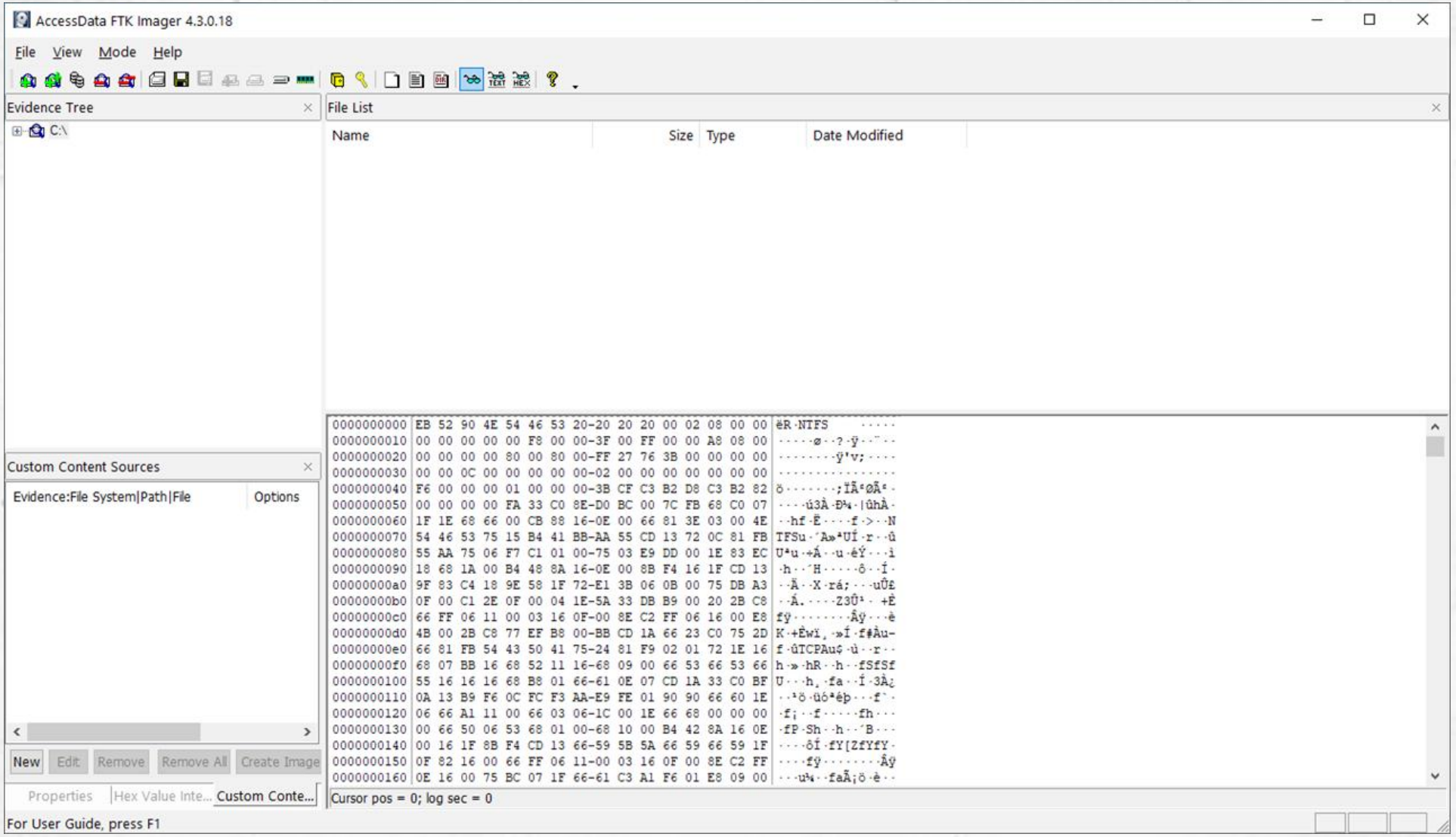
Zaisťovanie (I.)

3 typy forenzných imagov (obrazov):

- **Obraz kompletného disku**
- **Obraz partície**
- **súbory/adresáre – logický obraz**



Zaisťovanie (II.)



Uchovanie (I.)

- **dostatok úložnej kapacity**
  - disky
  - sieťové úložisko
- **zaistenie integrity dát**
  - napr. hash

Zdroj: http://www.vcfed.org/forum/showthread.php?24476-Sorting-floppy-disks-LOTS-of-floppy-disks

Integrita údajov

- Zabezpečenie integrity – Hash (digitálny odtlačok)

- **hašovacia funkcia** vytvára pre rovnaký vstup rovnaký výstup konštantnej dĺžky.
- checksum

- Známe hašovanie funkcie:
  - MD5 (Message-digest 5)
  - SHA-1 (Secure hash algorithm 1)
  - SHA-2 (256/384/512)
  - SHA-3 (256/384/512)
  - CRC32

Triáž

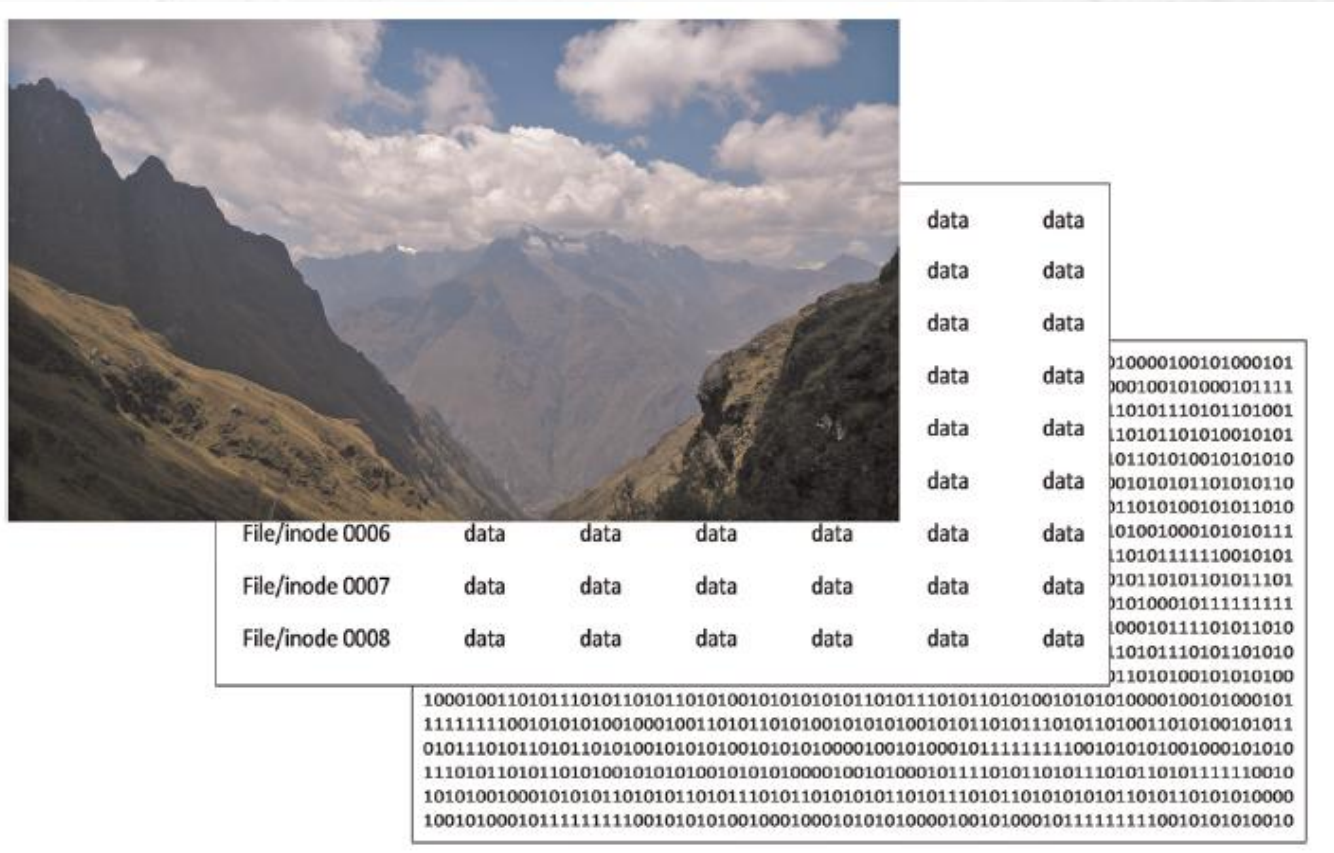
- Triáž (triedenie)

- Máme priestor na uloženie forenzného obrazu (imagu)?
- Máme čas na vytváranie forenzného obrazu (imagu)?
- Je nutné zaistiť celý disk?

- 99% forenzného vyšetrovania sa zameriava na 1% zaistených dát

Vyťaženie

- extrakciu údajov (artefaktov) z digitálnych stôp
- redukcia a filtrovanie údajov (artefaktov)
- obnova súborov a získavanie (carving) údajov
- Výstup: Výber relevantných digitálnych stôp (artefaktov)



Analýza (I.)

A	B	C	D	E	F	G	J	
date	time	timezon	MAC	source	sourcetype	type	short	desc
6/18/2009	22:30:26	EST5EDT	MACB	LOG	WMIprov Log file	Time Written	C:/Windows/system32/DRIVERS/msiscsi.sys[MofResource](Thu Jun 18 22:30:26 2009.29992	Entry in log file: C:/Windows/
6/18/2009	22:30:26	EST5EDT	MACB	LOG	WMIprov Log file	Time Written	C:/Windows/system32/drivers/ndis.sys[MofResourceName](Thu Jun 18 22:30:26 2009.2998	Entry in log file: C:/Windows/
6/18/2009	22:36:15	EST5EDT	MACB	PRE	Vista/Win7 Prefetch	Last run	LOGON.SCR-7C80CA1C.pf: LOGON.SCR was executed	LOGON.SCR-7C80CA1C.pf - [L
6/18/2009	22:41:26	EST5EDT	MACB	REG	Deleted Registry	Last Written	[DELETED] SYSTEM	[DELETED] SYSTEM
6/18/2009	22:41:54	EST5EDT	MACB	PRE	Vista/Win7 Prefetch	Last run	DEFRAG.EXE-738093E8.pf: DEFRAG.EXE was executed	DEFRAG.EXE-738093E8.pf - [D
6/18/2009	22:41:54	EST5EDT	MACB	PRE	Vista/Win7 Prefetch	Last run	DFRGNTFS.EXE-4F838A89.pf: DFRGNTFS.EXE was executed	DFRGNTFS.EXE-4F838A89.pf -
6/18/2009	22:41:59	EST5EDT	MACB	REG	Deleted Registry	Last Written	[DELETED] emRoot/System32/Config/SOFTWARE	[DELETED] emRoot/System32/
6/18/2009	23:33:57	EST5EDT	MACB	REG	Deleted Registry	Last Written	[DELETED] ???/0000000E/00000000/	[DELETED] ???/0000000E/000
6/18/2009	23:33:57	EST5EDT	MACB	REG	Deleted Registry	Last Written	[DELETED] ???/{83da6326-97a6-4088-9453-a1923f573b29}/00000003/00000000/	[DELETED] ???/{83da6326-97a
6/18/2009	23:33:57	EST5EDT	MACB	REG	Deleted Registry	Last Written	[DELETED] ???/00000003/00000000/	[DELETED] ???/00000003/000
6/18/2009	23:33:57	EST5EDT	MACB	REG	Deleted Registry	Last Written	[DELETED] ???/00000008/00000000/	[DELETED] ???/00000008/000
6/18/2009	23:34:09	EST5EDT	MACB	PRE	Vista/Win7 Prefetch	Last run	PKMAILER.EXE-83FAD500.pf: PKMAILER.EXE was executed	PKMAILER.EXE-83FAD500.pf -
6/18/2009	23:34:35	EST5EDT	MACB	REG	NTUSER key	Last Written	Software/Google/GoogleToolbarNotifier/Stats	Key name: HKEY_USER/Softwa
6/18/2009	23:34:36	EST5EDT	MACB	REG	NTUSER key	Last Written	Software/Google/GoogleToolbarNotifier/Temp	Key name: HKEY_USER/Softwa
6/18/2009	23:34:50	EST5EDT	MACB	PRE	Vista/Win7 Prefetch	Last run	IPODSERVICE.EXE-FE1A6FF7.pf: IPODSERVICE.EXE was executed	IPODSERVICE.EXE-FE1A6FF7.p
6/18/2009	23:34:59	EST5EDT	MACB	PRE	Vista/Win7 Prefetch	Last run	RUNDLL32.EXE-2E65B341.pf: RUNDLL32.EXE was executed	RUNDLL32.EXE-2E65B341.pf -
6/18/2009	23:34:59	EST5EDT	MACB	REG	UserAssist key	Time of Launch	UEME_RUNPATH:C:/Windows/system32/rundll32.exe	UEME_RUNPATH:C:/Windows
6/18/2009	23:35:05	EST5EDT	MACB	LSO	Flash Cookie	LSO created	Flash Cookie: site ui/preferences	LSO created -> File: C://mnt/v
6/18/2009	23:35:07	EST5EDT	MACB	REG	NTUSER key	Last Written	Software/Microsoft/InternetExplorer/LowRegistry/Audio/PolicyConfig/PropertyStore/5447cc	Key name: HKEY_USER/Softwa
6/18/2009	23:35:38	EST5EDT	MACB	REG	UserAssist key	Time of Launch	UEME_RUNPATH:Mozilla Firefox.lnk	UEME_RUNPATH:Mozilla Firef
6/18/2009	23:35:39	EST5EDT	MACB	REG	UserAssist key	Time of Launch	UEME_RUNPATH:C:/Program Files/Mozilla Firefox/firefox.exe	UEME_RUNPATH:C:/Program
6/18/2009	23:35:39	EST5EDT	MACB	PRE	Vista/Win7 Prefetch	Last run	FIREFOX.EXE-E60C0AA7.pf: FIREFOX.EXE was executed	FIREFOX.EXE-E60C0AA7.pf - [
6/18/2009	23:41:36	EST5EDT	MACB	REG	Deleted Registry	Last Written	[DELETED] ???/00000003/	[DELETED] ???/00000003/
6/18/2009	23:41:36	EST5EDT	MACB	REG	Deleted Registry	Last Written	[DELETED] ???/{83da6326-97a6-4088-9453-a1923f573b29}/	[DELETED] ???/{83da6326-97a
6/18/2009	23:41:36	EST5EDT	MACB	REG	Deleted Registry	Last Written	[DELETED] ???/0000000E/	[DELETED] ???/0000000E/
6/18/2009	23:41:36	EST5EDT	MACB	REG	Deleted Registry	Last Written	[DELETED] ???/00000008/	[DELETED] ???/00000008/
6/18/2009	23:41:36	EST5EDT	MACB	REG	Deleted Registry	Last Written	[DELETED] ???/{83da6326-97a6-4088-9453-a1923f573b29}/00000003/	[DELETED] ???/{83da6326-97a

Analýza (II.)

Analýza (III.)

Postup analýzy:

- **pozorovanie** - digitálne dátové objekty čitateľné (alebo viditeľné) človekom majú obsah
- **hypotéza** - vypracovanie teórie na vysvetlenie digitálnych stôp.
- **predikcia** - na základe forenznej hypotézy forenzní vyšetrovatelia predpovedajú, kde by sa mohli nachádzať zaujímavé forenzné artefakty.
- **experiment/testovanie**
- **závery** - rekonštrukcia udalostí založenú na spojení a korelácii informácií.

Analýza (IV.)

- Koľko stoličiek je na obrázku?
- Koľko kresieb je na obrázku?

Zdroj: https://www.sans.org/security-resources/posters/windows-forensic-analysis/170/download

Analýza (V.)


User Comms
Web Based E-mail
E-mail
Calendar
Chat / Webmail Memory Artifacts
Chat and IM
File Download
Open / Save MRU
E-mail
Skype History
Index.dat/ Places.sqlite
Downloads.sqlite
Program Execution
UserAssist
LastVisited MRU
RunMRU Start->Run
MUI Cache
Win7 Jump Lists
Prefetch
Services (EVT)
File Opening/ Creation
Recent Files
Office Recent Files
Shell bags
Link Files
Jump Lists
Prefetch
Index.dat file://
Deleted File or File Knowledge
XP Search - ACMRU
Win7 Search – WordWheelQuery
Last Visited MRU
Thumbs.db
Vista/Win7 Thumbnails
Recycle Bin
Browser Artifacts
Physical Location
Timezone
Wireless SSID
VISTA/Win7 Network History
Cookies
Browser Search Terms
USB Key Usage
Key Identification
First/ Last Times
User
Volume Name
Drive Letter
Link Files
P&P Event Log
Account Usage (SAM)
Last Login
Last Failed Login
Last Password Change
Group Membership
Account Usage (EVT)
Success / Fail Logons
Logon Types
RDP Usage
Account Logon/ Authentication
Rogue Local Accounts
Browser Usage
History
Cookies
Cache
Session Restore
Flash & Super Cookies
Suggested Sites
Memory Fragments of Private Browsing

Prezentácia (I.)

Postup 5W 1H

- **Kto (Who)** – odpoveď na otázku, kto každý bol zapojený do procesu
  - zadávateľ, zamestnanci ...

- **Kedy (When)** - zaznamenanie dátumu a času, kedy sa začalo a kedy skončilo vyšetrovanie/incident/analýza
  - pozor na jednotlivé časy a časové pásma
  - používatejte štandardné časové zóny (UTC)

- **Kde (Where)** - uvedenie podrobnostiach informácie o umiestnení
  - napríklad kancelária, serverovňa a pod.

Prezentácia (II.)

Postup 5W 1H

- **Čo (What)** – zaznamenanie činnosti, ktoré boli vykonané
  - napríklad získanie pamäte alebo získanie záznamov z firewallu , vytvorenie imagu disku

- **Prečo (Why)** - odôvodnenie, prečo bola každá činnosť vykonaná.

- **Ako (How)** – uvedenie popisu spôsobu vykonávania akcie.
  - napr. ak CSIRT tím použil nejaký operačný postup, tak sa zahrnutie do výstupu
  - akákoľvek odchýlka od štandardných prevádzkových postupov by sa mala rovnako zaznamenať

Prezentácia (III.)

Písomné správy (Written reports)

- niektoré bezpečnostné incidenty si vyžadujú rozšírený písomný výstup

- 3 hlavné typy
  - **Zhrnutie (Executive summary)**
  - **Správa o incidente (Incident report)**
  - **Správa z forenznej analýzy (Forensic report)**

Číslo prípadu: 1405222/2018
Interné číslo prípadu: 123/2018
Forenzný znalec: Ján Mrkvička

Správa z forenznej analýzy

Číslo prípadu:	1405222/2018	Interné číslo prípadu:	123/2017

Forenzný znalec:	Ján Mrkvička		Evidenčné číslo znalca:	912344		
Adresa znalca:	Mesto:	Košice	Ulica:	Neznáma	PSČ:	04001
	Štát:	Slovenská republika	Číslo domu:	71		
Adresa inštitútu:	Mesto:	Košice	Ulica:	XXXX	PSČ:	0000
	Štát:	Slovenská republika	Číslo domu:	71		

Odbor:	10 00 00	Odvetvia:	10 04 00, 10 09 00, 10 10 00

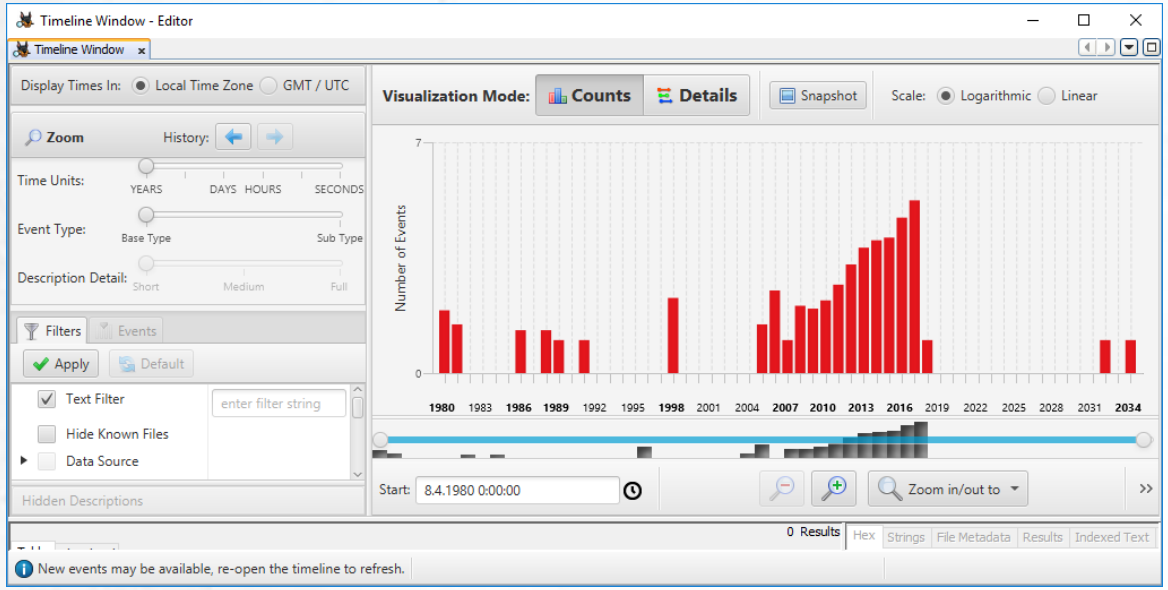
Dátum a čas nahlásenia incidentu (dd.mm.rrrr, hh:mm:ss):	24.05.2017 09:15:34	Dátum a čas vypracovania a ukončenia forenznej správy:	26.05.2017 17:30:00

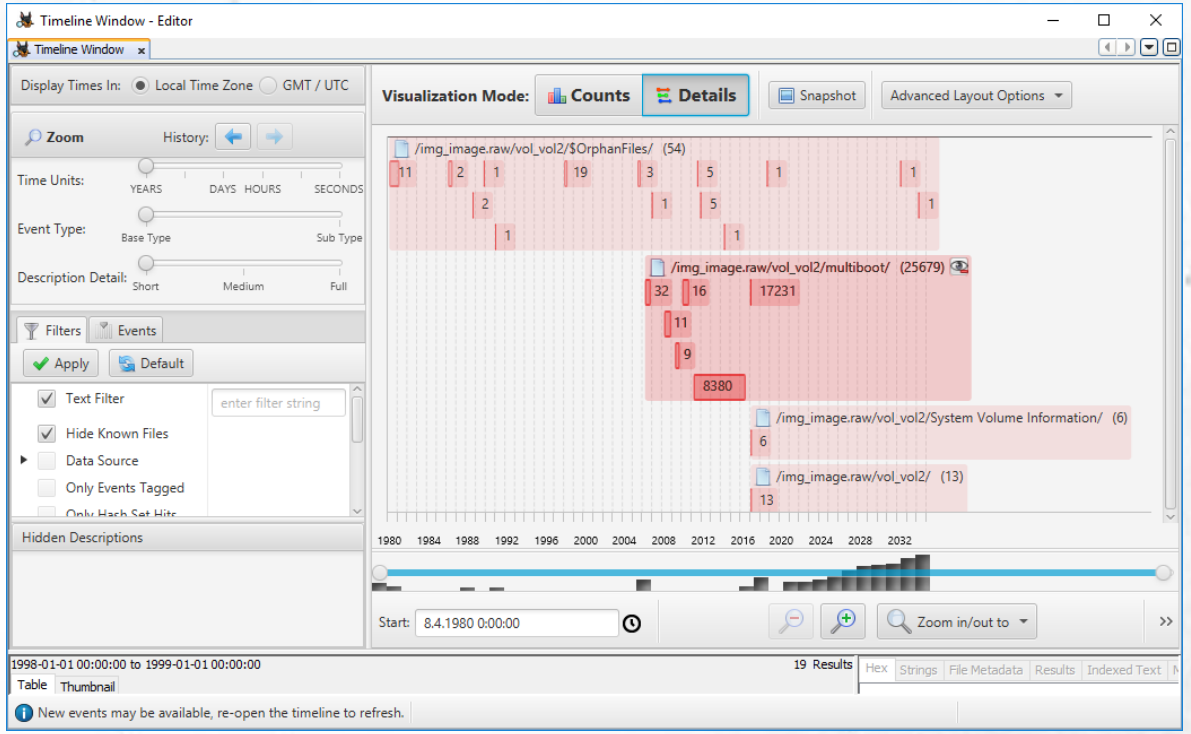
Osoby a subjekty

Číslo: 0001	☒ Svedok	☒ Zadávateľ	☐ Iné:		
Meno:	Ján	Priezvisko:	Admin	Titul:	Mgr.
Hodnosť:	----------	Národnosť:	Slovenská Republika		
Štátna príslušnosť:	Slovenská				
Identifikačné číslo:	o.p.: FA 547846989, číslo zamestnanca: 15254782				

Prezentácia (IV.)

- zostaviť zoznam všetkých udalostí, ktoré sa udiali v rámci operačného systému v chronologickom poradí bez ohľadu na jeho typ, umiestnenie alebo dokonca aplikáciu.





Právne aspekty (I.)

Právne aspekty vzťahujúca sa na oblasť digitálnej forenznej analýzy:

- Trestné právo
  - Trestné právo hmotné
  - Trestné právo procesné
- Ochrana súkromia a osobných údajov
- Kybernetická bezpečnosť
- Znalecká činnosť

Právne aspekty (II.)

- **Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti**
  - §19 ods. 6 písm. d) v čase kybernetického bezpečnostného incidentu zabezpečiť dôkaz alebo dôkazný prostriedok tak, aby mohol byť použitý v trestnom konaní

- **Zákon č. 18/2018 Z. z. o ochrane osobných údajov / GDPR**
  - informácie o **dátumoch, volaných telefónnych číslach alebo prijatých hovoroch**, ako aj informácie o **dĺžke hovoru**, treba považovať za osobné údaje dotknutej osoby
  - IP adresa
  - Právny základ spracovania – GDPR čl.6 ods. 1 písm. f) - spracúvanie je nevyhnutné na účely oprávnených záujmov, ktoré sleduje prevádzkovateľ alebo tretia strana, s výnimkou prípadov, keď nad takýmito záujmami prevažujú záujmy alebo základné práva a slobody dotknutej osoby, ktoré si vyžadujú ochranu osobných údajov, najmä ak je dotknutou osobu dieťa.

Právne aspekty (III.)

- **Dohovor** Rady Európy **o počítačovej kriminalite**
- **Zákon č. 300/2005 Z. z. trestný zákon**
- **Zákon č. 301/2005 Z. z. trestný poriadok**

- **Zákon č. 382/2004 Z. z. o znalcoch, tlmočníkoch a prekladateľoch a** o zmene a doplnení niektorých zákonov

Štádia trestného konania (I.)

- **Predsúdne konanie**
  1) postup pred začatím trestného stíhania
  2) prípravné konanie

- **Konanie pred súdom**
  1) preskúmanie a predbežné prejednanie obžaloby
  2) hlavné pojednávanie
  3) opravné konanie
  4) vykonávacie konanie

Dokazovanie v trestnom konaní (I.)

- **Dokazovanie v trestnom konaní**
  - je zákonom upravený postup OČTK a súdu, ktorého úlohou je poznanie všetkých podstatných skutočností dôležitých pre ďalší postup konania a v konečnej fáze aj pre rozhodnutie.
  - **účel** - rekonštruovať skutočnosti tak, aby poznanie bolo jej správnym odrazom a mohlo byť základom spravodlivého rozhodnutia.
  - vykonáva vo všetkých štádiách konania

  - za **dôkaz** možno použiť všetko, čo môže prispieť k náležitému objasneniu veci a čo bolo získané zákonným spôsobom (§ 119 ods. 2 TP)

Dokazovanie v trestnom konaní(II.)

Trestný poriadok (§ 119 - 161) demonštratívne vypočítava jednotlivé dôkazné prostriedky:

- výsluch obvineného a obžalovaného (§ 121 - 124,258 - 260)
- výsluch svedka (§ 131 - 139, 261 - 267)
- výsluch znalca (§ 145, § 268)
- znalecký posudok (§ 145 - 150)
- odborné vyjadrenie a písomné potvrdenie (§ 141)
- ...

Dôkaz	Dôkazný prostriedok	Prameň dôkazu
Obsah výpovede	Výsluch svedka	Svedok
Obsah výpovede	Výsluch znalca	Znalec
Obsah posudku	Znalecký posudok	Digitálna stopa

Znalec (I.)

- **Znalec**
  - je osoba rozdielna od procesných strán, ktorú orgán činný v trestnom konaní a súd priberá s tým účelom,
  - účel – na základe svojich odborných znalostí objasnila určitú skutočnosť, dôležitú pre trestné konanie, na objasnenie ktorej sa takéto odborné znalosti vyžadujú.

Znalec (II.)

a) **znalecká organizácia**

- ústavy špecializované na znaleckú činnosť podľa § 143 ods. 1 Trestného poriadku

b) **fyzická osoba zapísaná do zoznamu znalcov pre určitý odbor**

- podľa zákona č. 382/2004 Z. z. o znalcoch, tlmočníkoch a prekladateľoch.

c) **fyzická osoba nezapísaná do zoznamu znalcov**

- vo výnimočných prípadoch - tzv. "**znalci ad hoc**",
- po zložení sľubu znalca (§ 143 ods. 2 TP).

d) **znalecký ústav** (§ 147 TP)

Znalec (III.)

Zoznam znaleckých odborov (Príloha č. 1 vyhlášky MS SR č. 228/2018 Z. z.)

- relevantných z hľadiska kybernetickej bezpečnosti

10 00 00 Elektrotechnika

10 01 00 Elektro-energetické stroje a zariadenia
10 02 00 Elektronika
10 04 00 Riadiaca technika, výpočtová technika (hardvér)
10 06 00 Elektronické komunikácie
10 07 00 Odhad hodnoty elektrotechnických zariadení a elektroniky
10 08 00 Nosiče zvukových a zvukovoobrazových záznamov
10 09 00 Počítačové programy (softvér)
10 10 00 Bezpečnosť a ochrana informačných systémov
10 11 00 Kybernetická bezpečnosť

49 00 00 Kriminalistika

49 20 00 Kriminalistická informatika

Znalecká činnosť (I.)

Zadávatelia znaleckých úkonov

- Fyzická osoba,
- Právnická osoba,
- OČTK
- Predseda senátu
- Súd
- Správny orgán

Znalecká činnosť (II.)

Právny základ pre zadanie znaleckého úkonu

- súkromný znalecký posudok, predložený stranou bez toho, aby znalecké dokazovanie nariadil súd, v zmysle § 209 ods. 1 zákona č. 160/2015 Z. z. CSP,
- znalecké dokazovanie, nariadené súdom, ktorý ustanoví znalca, v zmysle § 207 ods. 1 zákona č. 160/2015 Z. z. CSP,
- znalecký posudok, na základe ustanovenie znalca zo strany správneho orgánu, v zmysle § 36 ods. 1 zákona č. 71/167 Zb. o správnom konaní (správny poriadok),
- znalecký posudok, na základe pribratia znalca orgánom činným v trestnom konaní alebo predsedom senátu, v zmysle § 142 ods. 1 zákona č. 301/2005 Z. z. TP

Znalecká činnosť (III.)

Trestný poriadok

- **§142, ods. 1 – Znalecká činnosť**
  - Ak pre zložitosť objasňovanej skutočnosti nie je postup podľa § 141 (odborná činnosť) postačujúci, priberie orgán činný v trestnom konaní a v konaní pred súdom predseda senátu znalca na podanie znaleckého posudku. Ak ide o objasnenie skutočnosti obzvlášť zložitej, priberú sa **dvaja znalci**.

Podmienky výkonu znaleckej činnosti (I.)

§ 11 Vylúčenie znalca

- (1) Znalec, tlmočník alebo prekladateľ je vylúčený, ak možno mať pre jeho pomer k veci, k zadávateľovi alebo k inej osobe, ktorej sa úkon týka, pochybnosť o jeho nezaujatosti.
- (3) Znalec, tlmočník alebo prekladateľ zapísaný v zozname nesmie vykonať úkon v odbore alebo odvetví, v ktorom nie je zapísaný; to sa nevzťahuje na znalca, tlmočníka alebo prekladateľa ustanoveného na účely súdneho alebo iného konania súdom alebo iným orgánom verejnej moci.
- (4) To, či úkon patrí do odboru alebo odvetvia, v ktorom je znalec, tlmočník alebo prekladateľ zapísaný do zoznamu, posudzuje ministerstvo.

Podmienky výkonu znaleckej činnosti (II.)

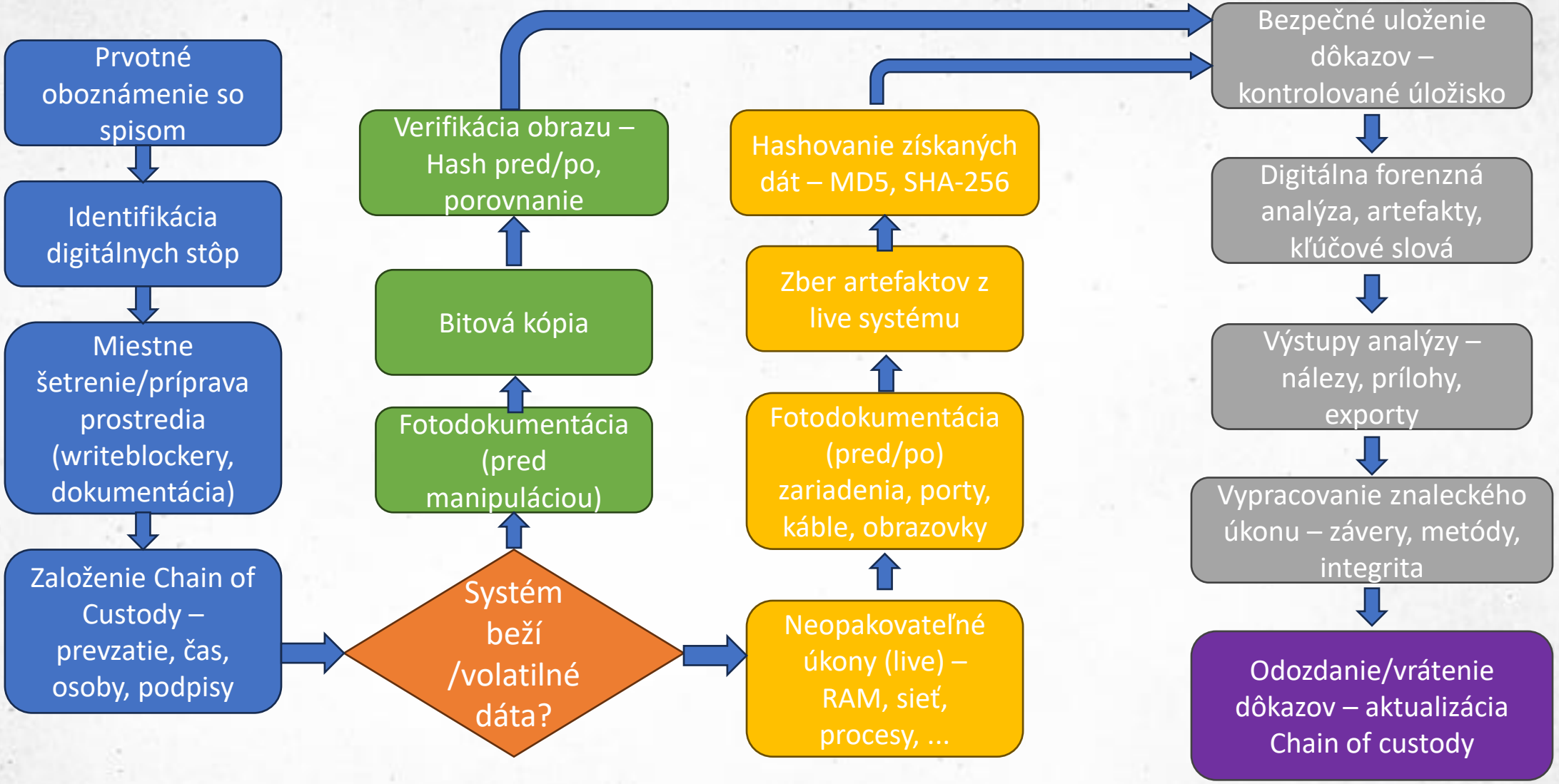
§ 12 Odmietnutie výkonu činnosti

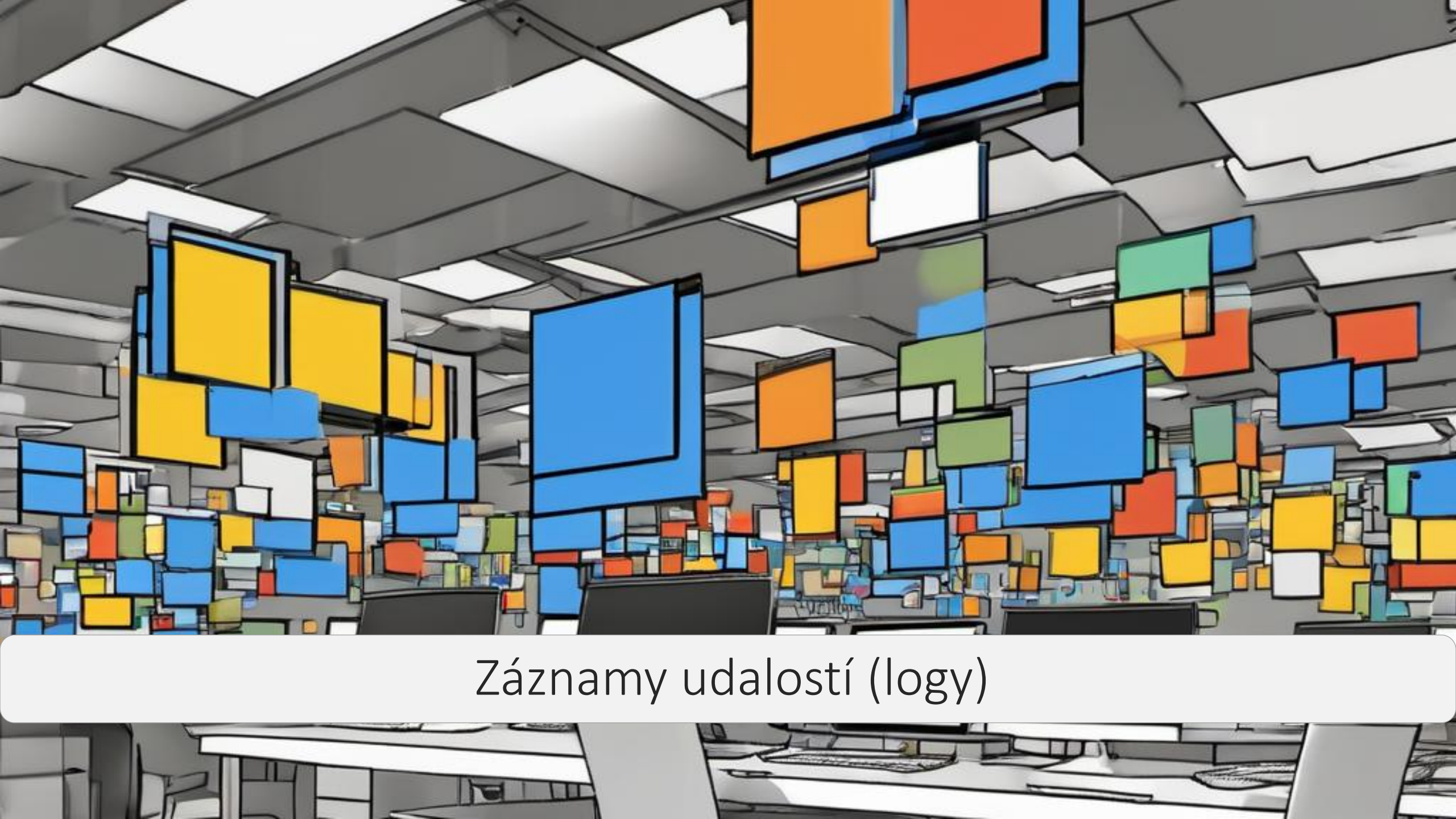
(1) Znalec, tlmočník alebo prekladateľ zapísaný v zozname nesmie bezdôvodne odmietnuť vykonať úkon, ak je ustanovený súdom alebo iným orgánom verejnej moci.

Bežné úlohy znalca v trestnom konaní

- asistencia pri vykonávaní domových prehliadok (napr. získavanie a vyťažovanie dát priamo na mieste),
- účasť na výsluchoch v prípade potreby technickej konzultácie,
- zabezpečenie prístupu do počítačov alebo iných technických zariadení,
- dokumentovanie softvérového a hardvérového vybavenia,
- zisťovanie licenčných informácií operačných systémov a aplikácií,
- zaistenie dát z techniky použitej pri páchaní trestnej činnosti (napr. pre potreby znalcov iných odborov),
- obsahová analýza e-mailovej komunikácie vrátane príloh,
- vyhľadávanie konkrétnych dokumentov v dátových úložiskách,
- obnova vymazaných dát z dátových nosičov (HDD, USB, pamäťové karty),
- stanovenie všeobecnej hodnoty vecí alebo výšky spôsobenej škody,
- zásahy do účtovných systémov/dát,
- tvorba fiktívnych dokumentov.

Proces znaleckého skúmania

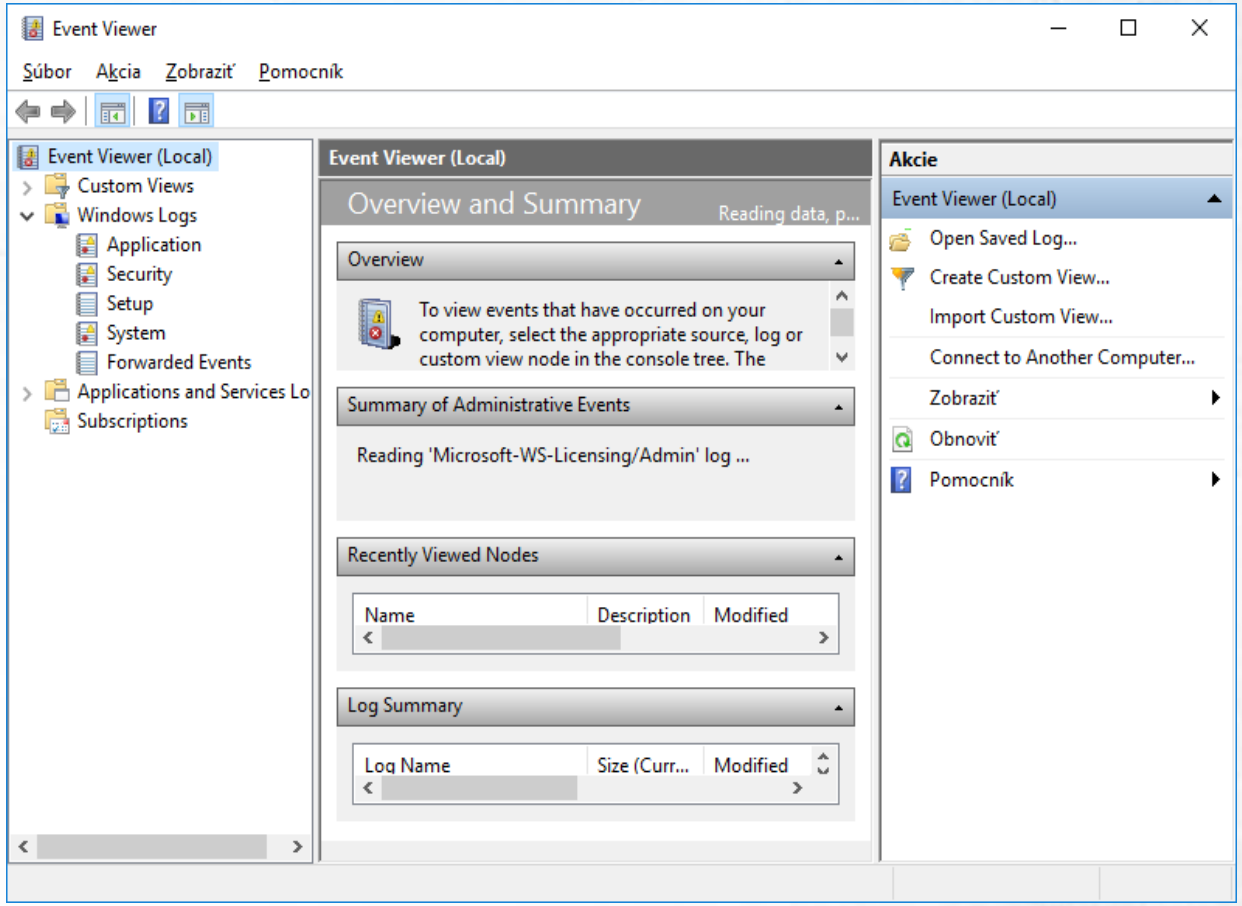




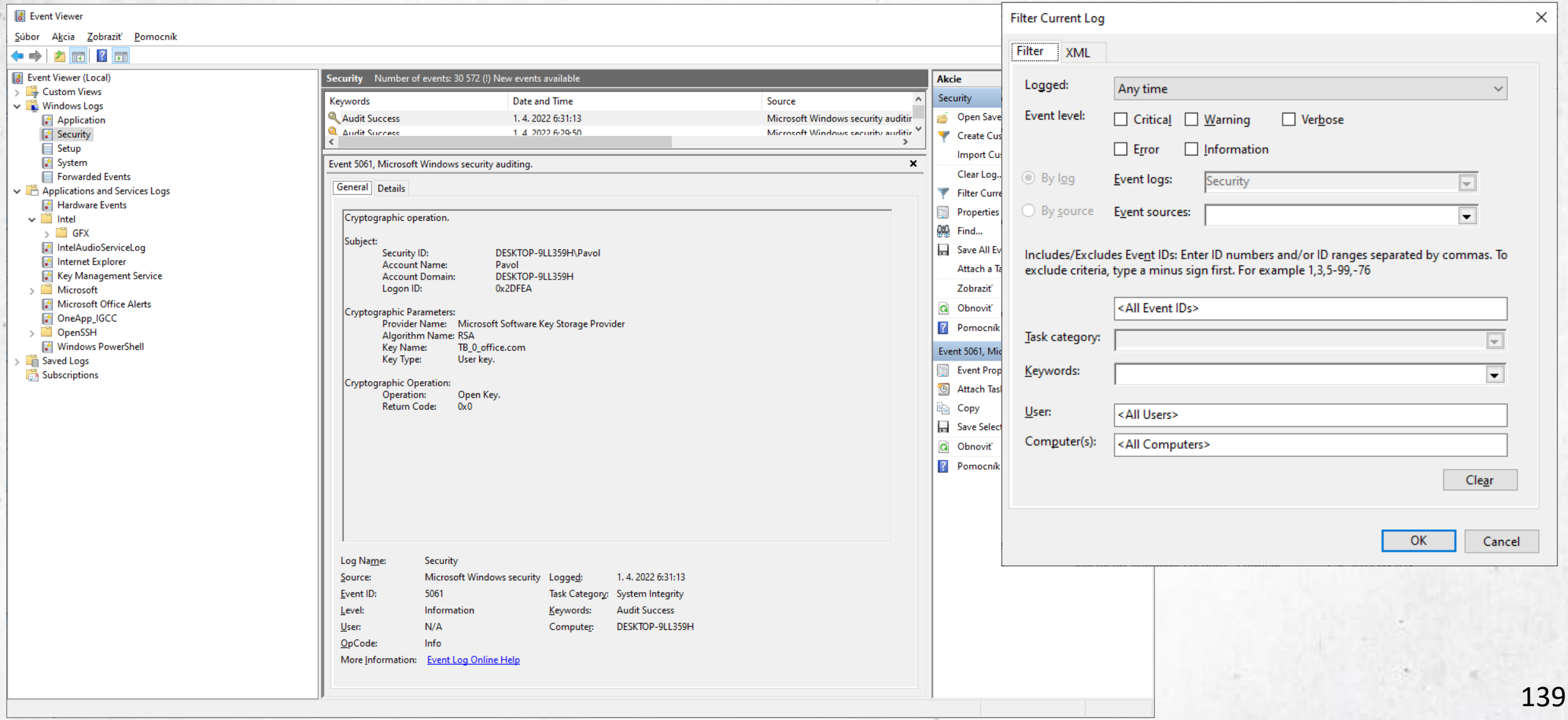
Záznamy udalostí (logy)

Záznamy udalostí (I.)

- operačný systém zaznamenáva konkrétne udalosti (napr. prihlásenie/odhlásenie používateľa)
- **udalosťou** môže byť akákoľvek udalosť, ktorú chce operačný systém alebo program sledovať alebo na ňu upozorniť používateľa
- Operačný systém Windows má centralizovanú službu zaznamenávania



Záznamy udalostí (II.)



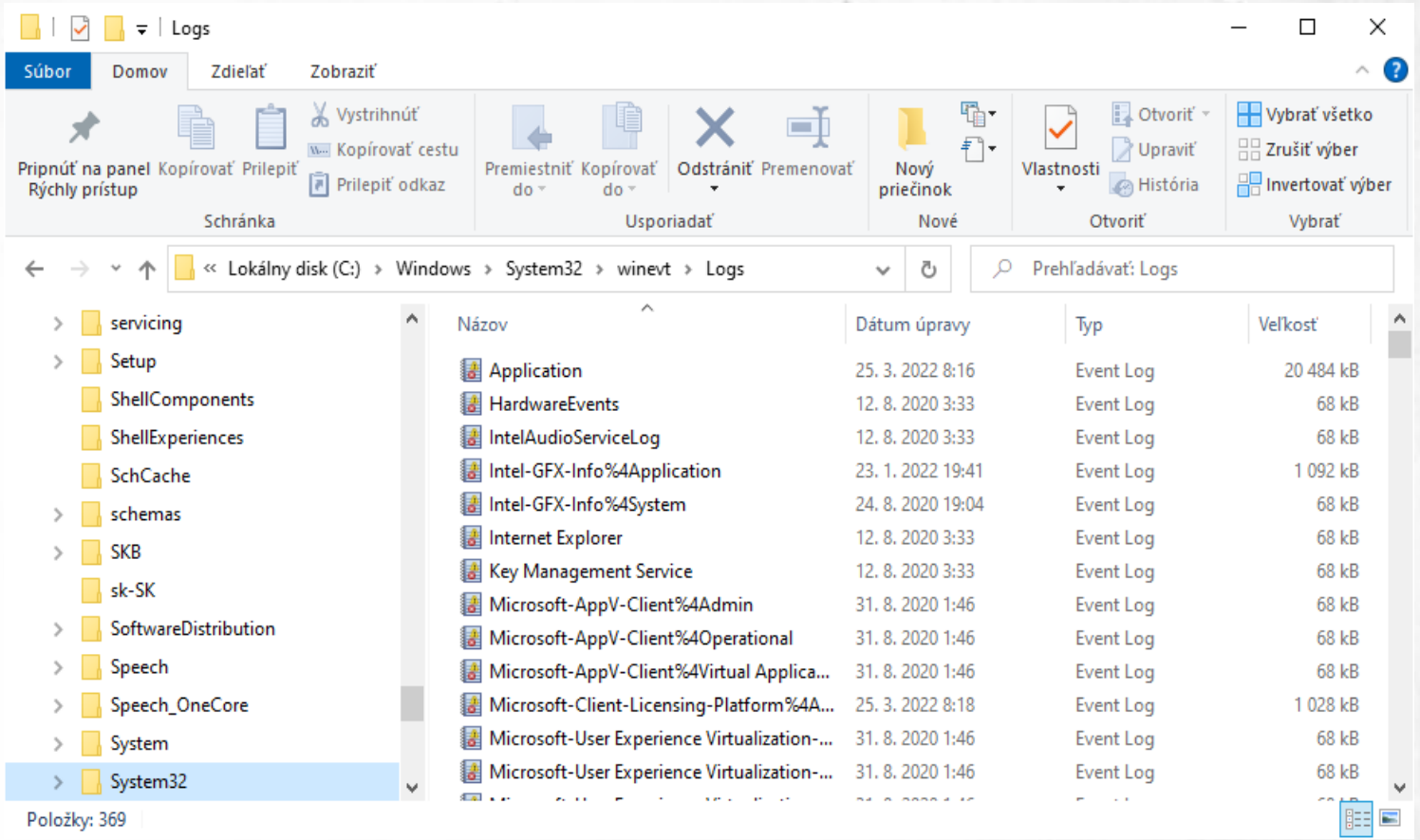
Záznamy udalostí (III.)

Formát

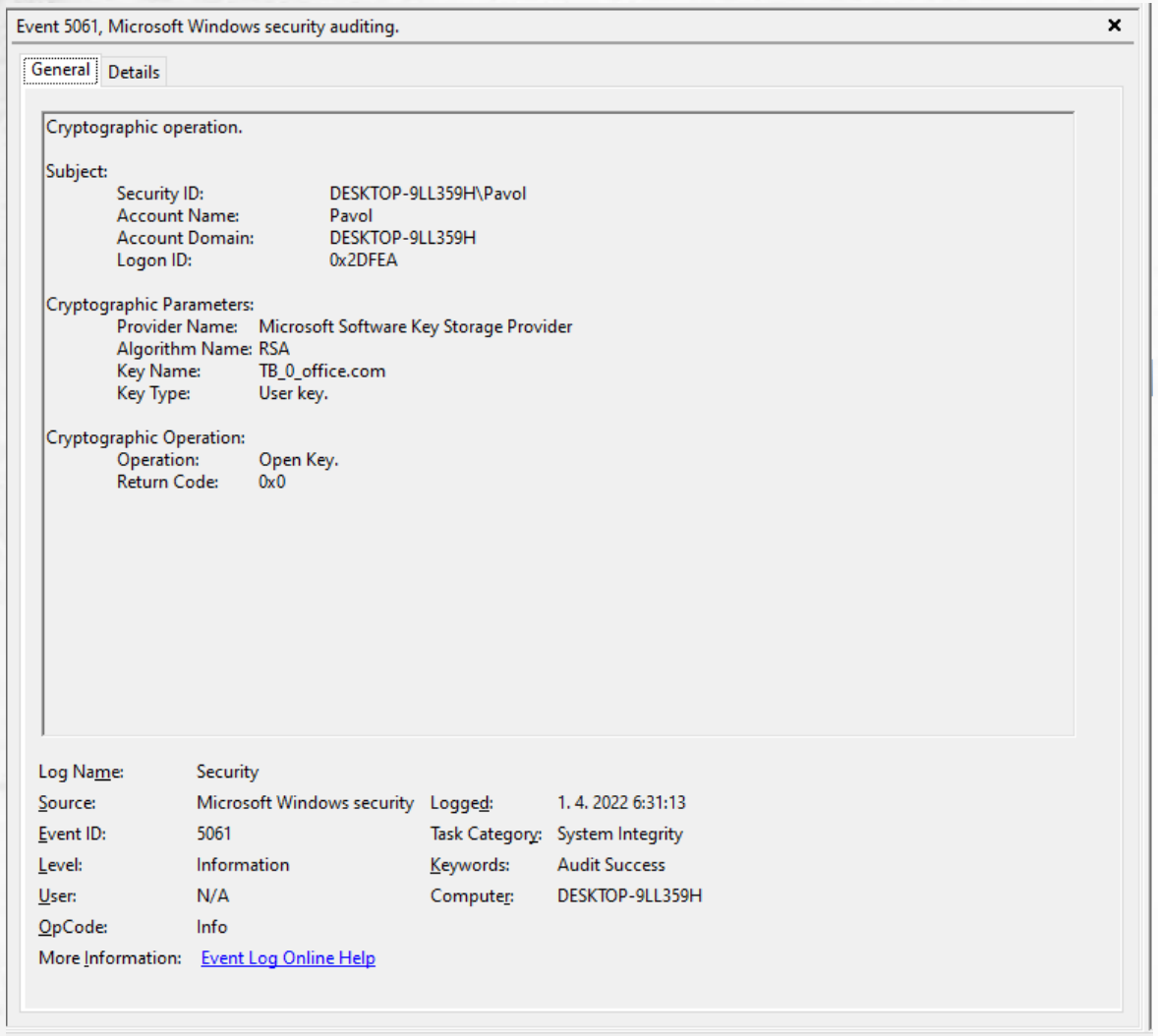
- .evt/.evtx

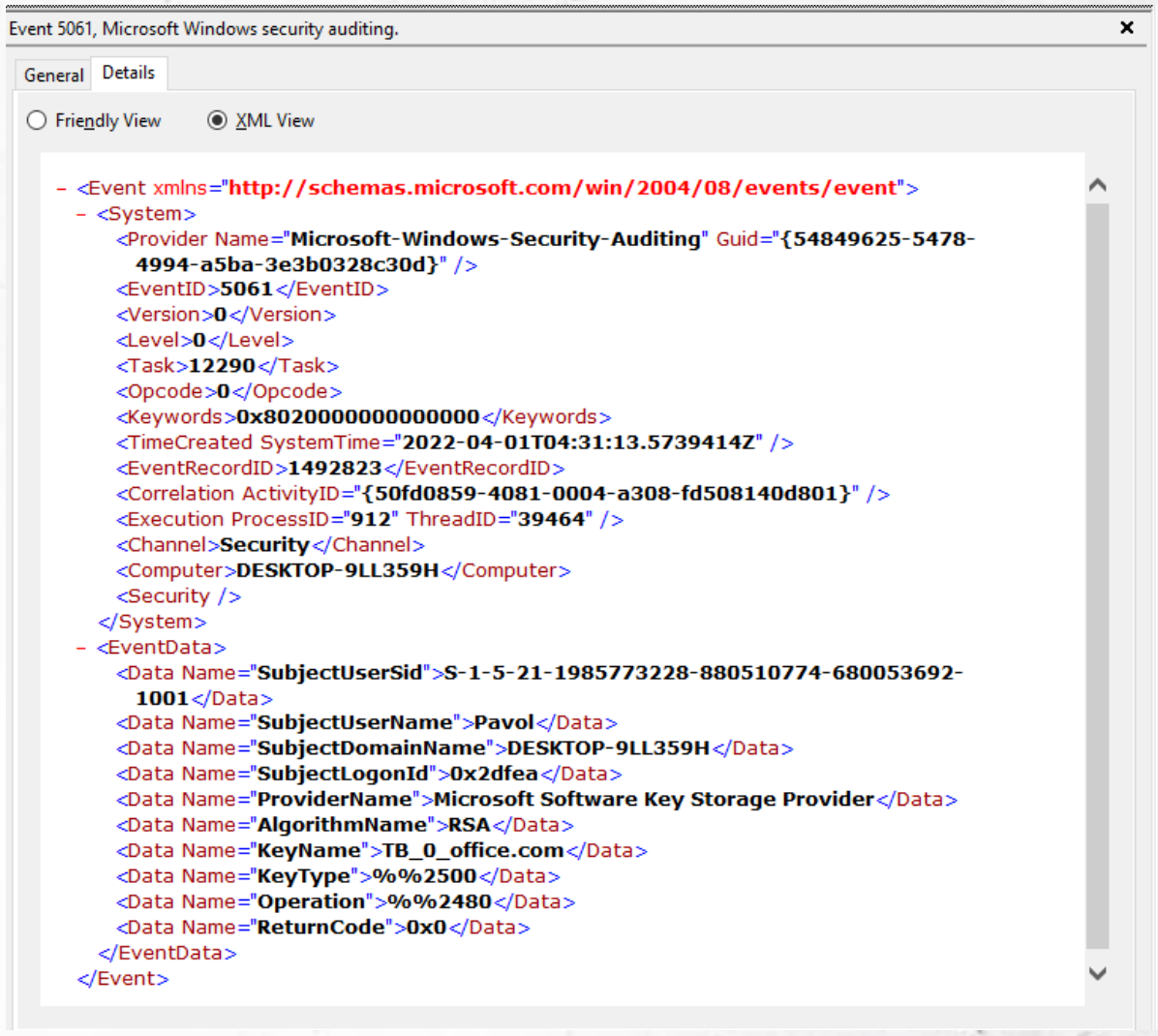
Umiestnenie

- %win_dir%\System32\config
- %win_dir%\System32\winevt\Logs



Záznamy udalostí (IV.)





Záznamy udalostí (V.)

- https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/

Register operačného systému Windows

Register OS Windows (I.)

„Srdce a duša“ operačného systému Windows

- konfigurácia systému
- zariadenia v systéme
- používateľské mená
- osobné nastavenia a nastavenia prehliadača
- aktivita prehliadania webu
- súbory otvorené
- spustené program
- nastavenia aplikácií
- heslá

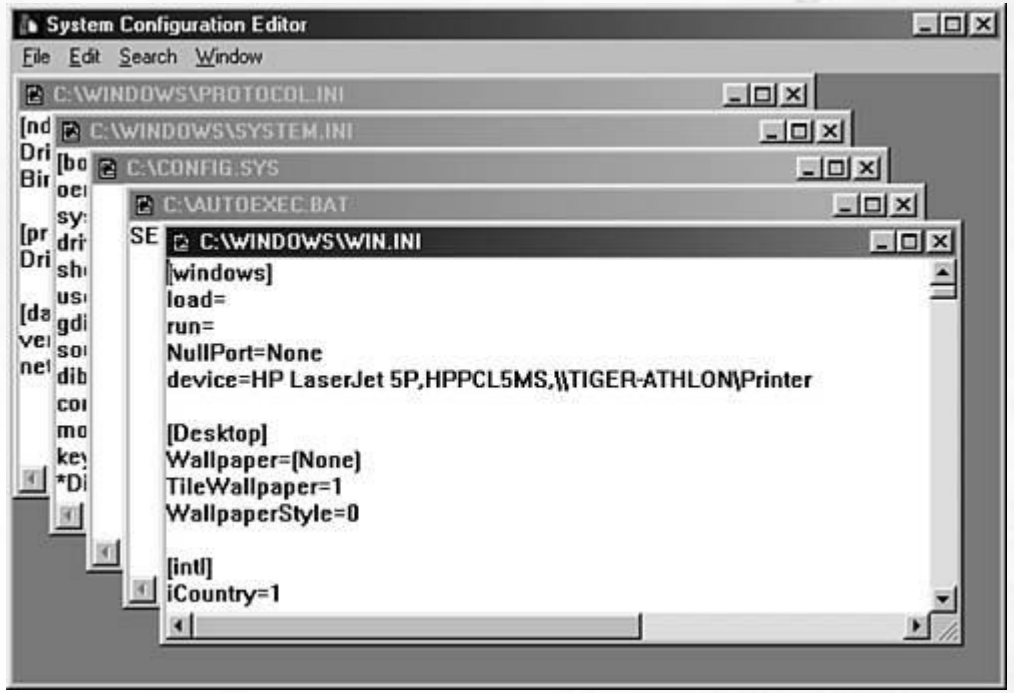
Register OS Windows (II.)

INI súbory

- predchodca registrov (DOS, Windows 3.x)
- SYSTEM.INI - Tento súbor riadil všetok hardvér v počítačovom systéme.
- WIN.INI - Tento súbor riadil všetky plochy a aplikácie
  v počítačovom systéme.

Nevýhody

- pomalý prístup
- bez štandardov
- fragmetované



Zdroj: https://flylib.com/books/en/3.171.1.163/1/

Register OS Windows (III.)

- **centrálna hierarchická databáza** používaná v skupine operačných systémov Microsoft Windows na ukladanie informácií potrebných na konfiguráciu systému pre jedného alebo viacerých používateľov, aplikácií a hardvérových zariadení.

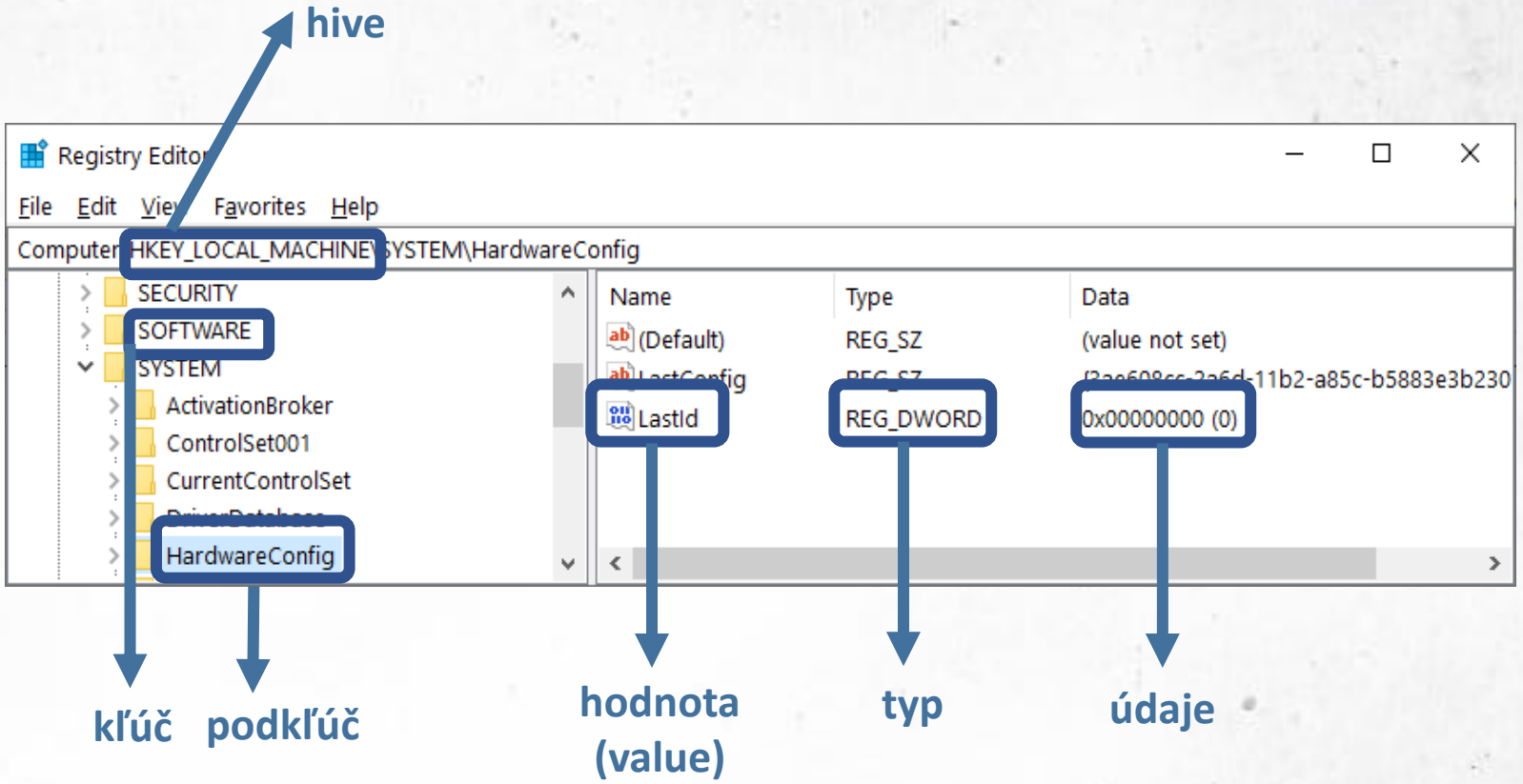
- prekonanie obmedzení INI súborov a REG.DAT súborov
- 2 typy informácií:
  - **všeobecné údaje o systéme** – údaje o nastavení softvéru a hardvéru. Tieto informácie sa zvyčajne vzťahujú na všetkých používateľov počítača.
  - **údaje špecifické pre používateľa** - údaje o individuálnej konfigurácii. Tieto informácie sú špecifické pre profil používateľa

Zdroj: A central hierarchical database used in Microsoft Windows 9x, Windows CE, Windows NT, and Windows 2000 used to store information necessary to configure the system for one or more users, applications and hardware devices.”, https://en.wikipedia.org/wiki/Windows_Registry#/media/File:Registry_Editor_icon.png

Register OS Windows (IV.)

- špecifická štruktúra
  - Key (kľúč)
  - Value (hodnota)

- ako adresárová štruktúra
  - Hlavné koreňové kľúče = koreňový adresár
  - podkľúče = podadresáre
  - hodnoty= súbory



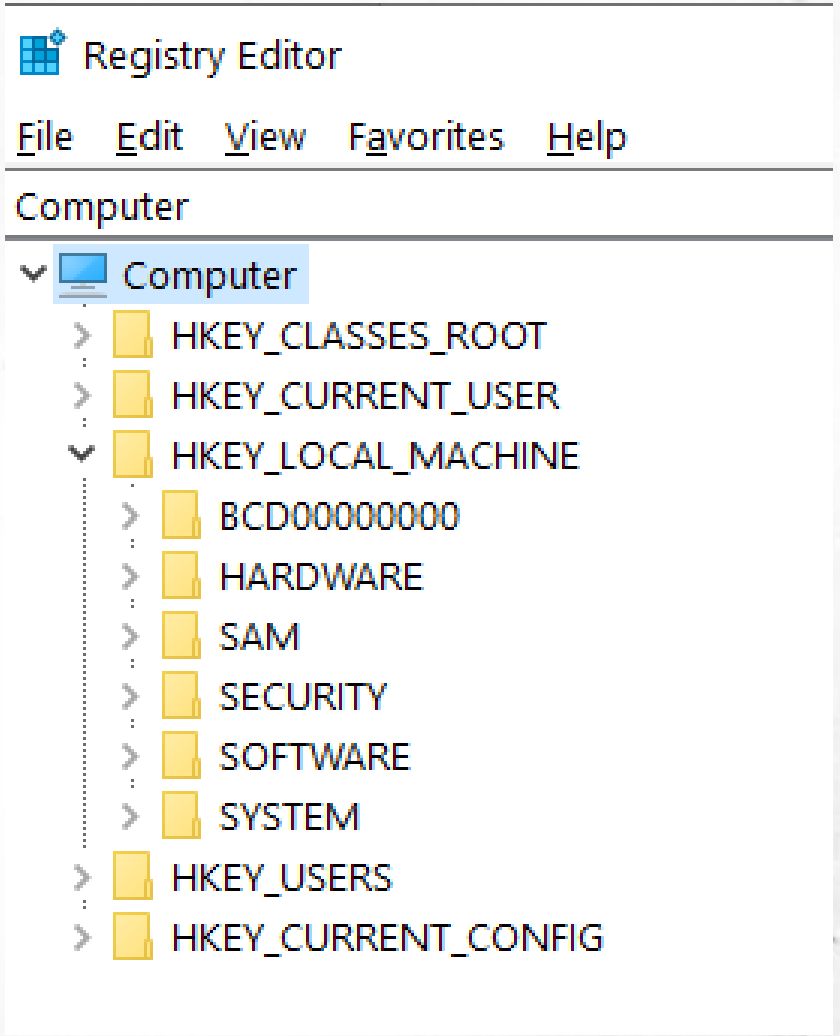
Každá **hodnota** má 3 vstupy:

- **Name**
- **Type**
- **Data**

Koreňové kľúče (I.)

Každý **koreňový kľúč (root key)** ukladá rôzne informácie a nastavenia o bežiacom systéme a jeho užívateľoch.

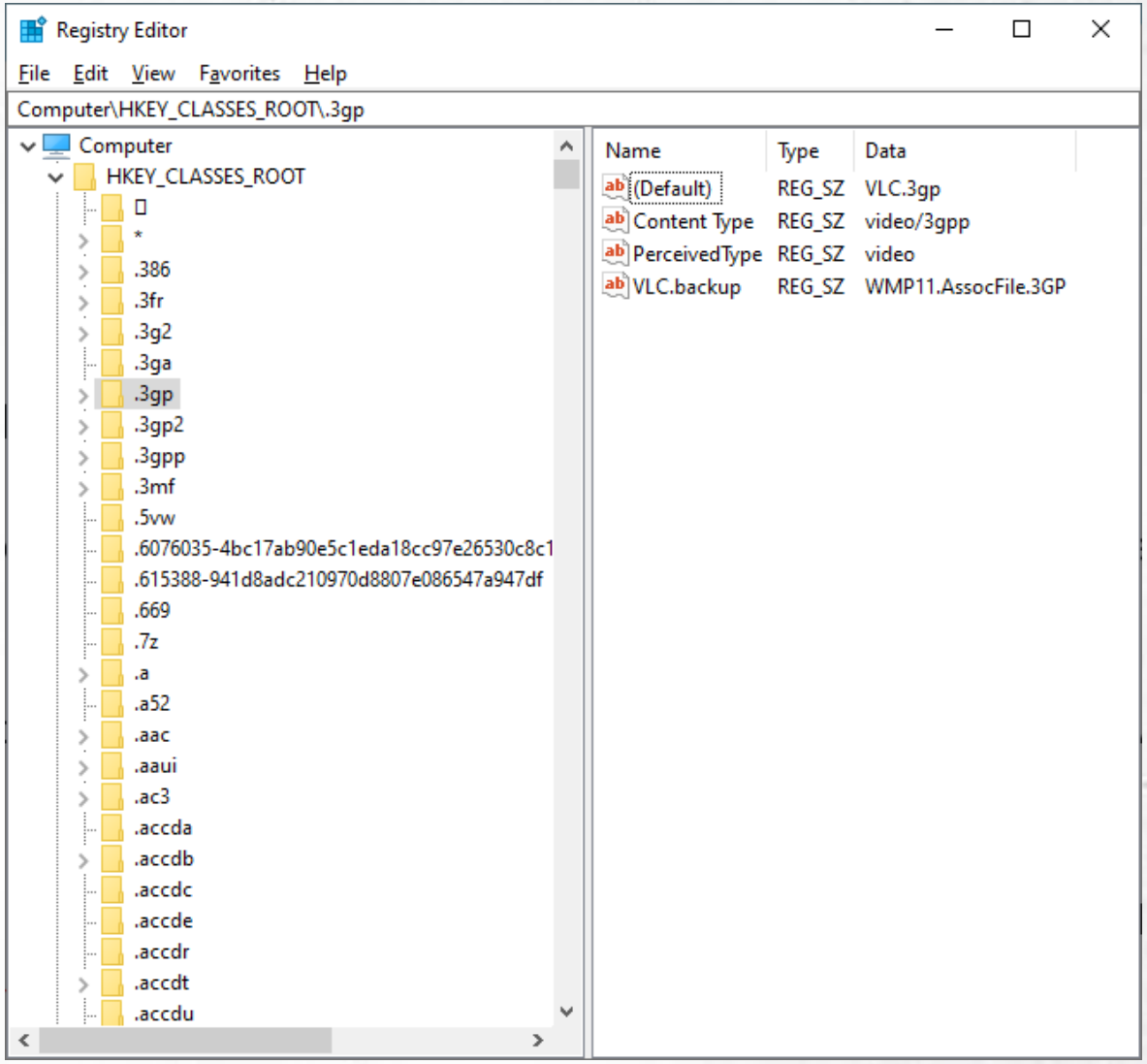
- HKEY_CLASSES_ROOT
- HKEY_LOCAL_MACHINE (HLKM)
  - **SAM**
  - **SECURITY**
  - **SYSTEM**
  - **SOFTWARE**
  - **DEFAULT**
- HKEY_USERS
- HKEY_CURRENT_USER (HKCU)
  - **NTUSER.DAT**
- HKEY_CURRENT_CONFIG



Koreňové kľúče (II.)

HKEY_CLASSES_ROOT (HKCR)

- popisuje predvolený program, ktorý sa musí použiť na otvorenie tohto rozšírenia v systéme.
- Uchováva informácie, aby sa zabezpečilo, že program sa otvorí po spustení v Prieskumníkovi systému Windows.



Koreňové kľúče (III.)

HKEY_LOCAL_MACHINE (HLKM)

- tento kľúč obsahuje konfiguráciu a nastavenia, ktoré systém používa pri spúšťaní.
- je nezávislý od prihlásenia používateľa
- obsahuje nasledujúcich päť podkľúčov:

  - **System**: Obsahuje konfiguráciu systému, napríklad názov počítača, systémové časové pásmo a sieťové rozhrania.
  - **Software**: Obsahuje nastavenia a konfiguráciu nainštalovaných aplikácií v systéme a služieb operačného systému.
  - **SAM**: Toto je správca bezpečnostných účtov a ukladá informácie o bezpečnosti používateľa a skupiny. Sumarizuje celkové práva používateľa, ktoré udeľuje správca v miestnom systéme a doméne.
  - **Security**: Obsahuje bezpečnostnú politiku v systéme, ak existuje. Je to rovnaké ako SAM, jeho obsah nie je možné prezerať zo živého systému.
  - **Hardware:** Obsahuje informácie o hardvérových zariadeniach pripojených k systému. Tieto informácie sa ukladajú počas zavádzania systému.

Koreňové kľúče (IV.)

HKEY_USERS (HKU)

- všetky používateľské profily v systémoch vrátane konfigurácií aplikácií a vizuálnych nastavení.

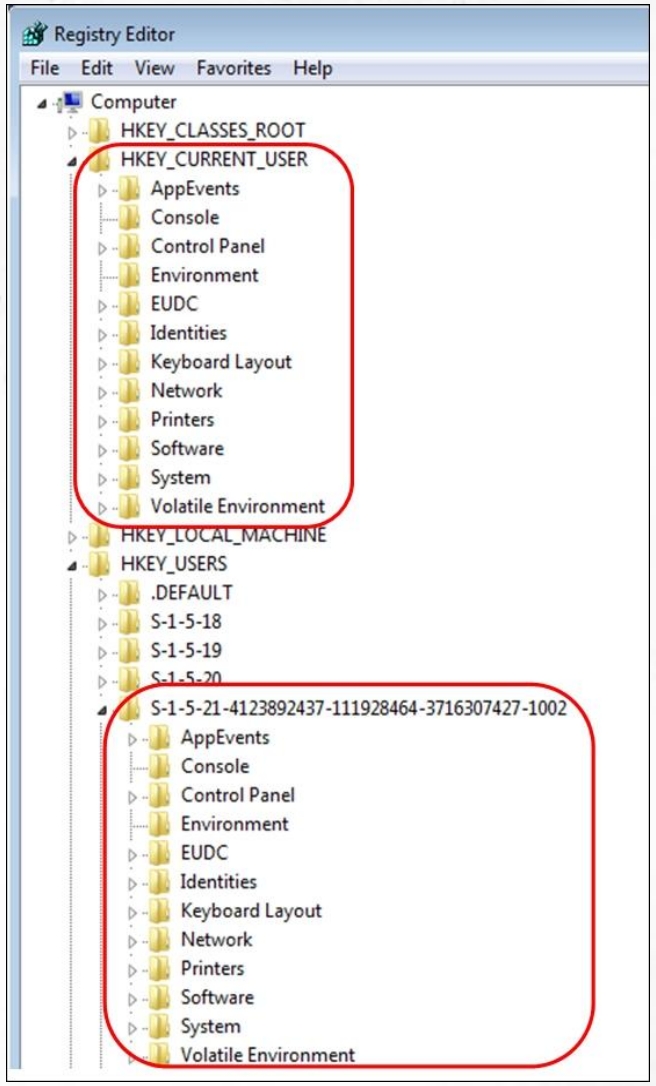
  - **S-1-5-18**: Toto je systémový profil umiestnený na% systemroot% \ system32 \ config \ systemprofile.
  - **S-1-5-19**: Súvisí to s LocalService a nachádza sa na% systemroot% \ C: \ Windows \ ServiceProfiles \ LocalService.
  - **S-1-5-20**: Súvisí to s NetworkService a nachádza sa pod% systemroot% \ C: \ Windows \ ServiceProfiles \ NetworkService.
  - **S-1-5-21-4123892437-111928464-3716307427-1002:** Toto je aktuálne prihlásený užívateľ s úplným SID. Naše sa nachádza v adresári používateľov C: \ Users \ Forensics2.
  - **Default user:** Toto je predvolený profil pre každého nového používateľa. Je umiestnený na% SystemDrive% \ Users \ Default.

Koreňové kľúče (V.)

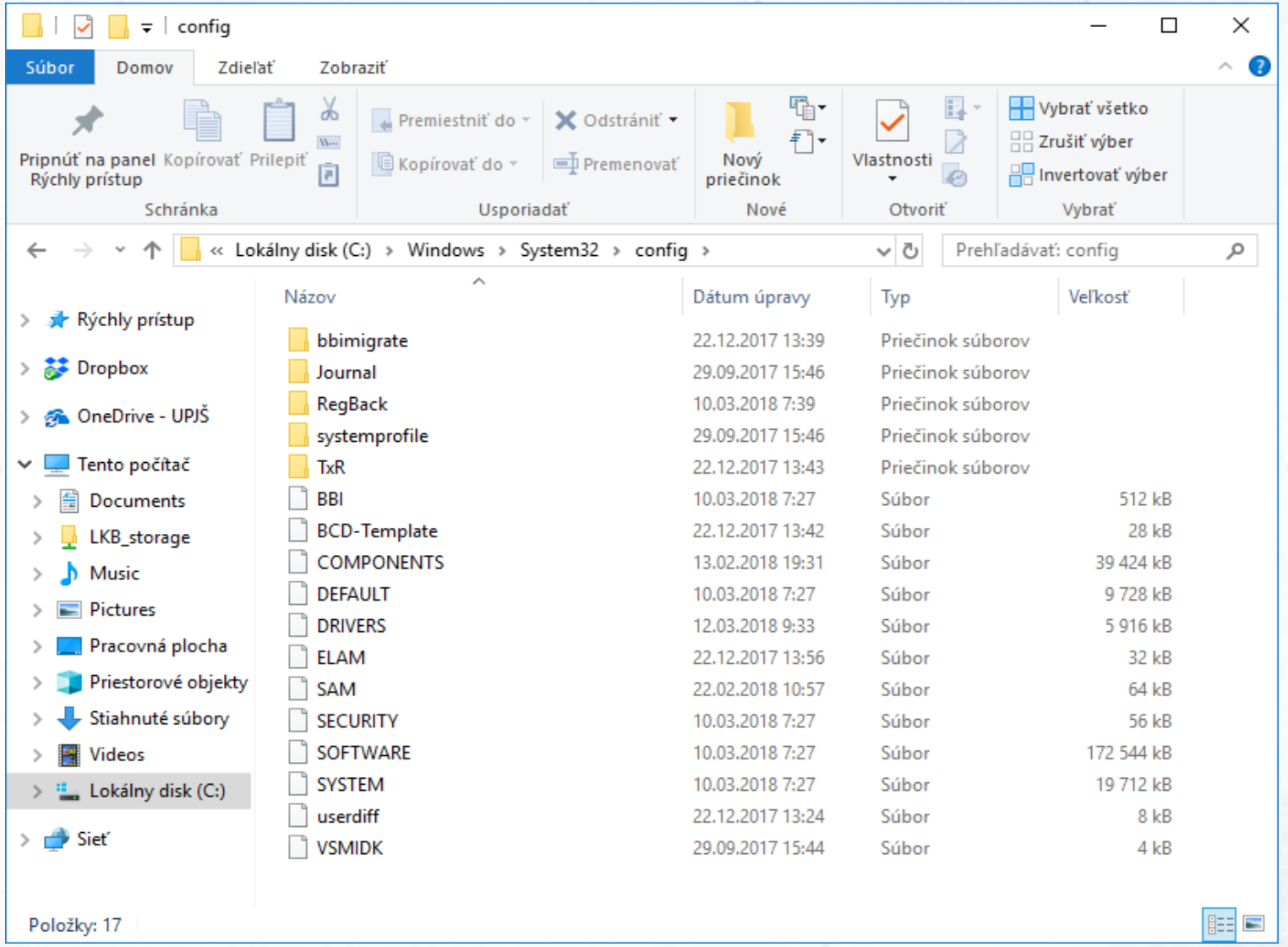
HKEY_CURRENT_USER (HKCU)

HKCU je iba **ukazovateľ** na aktuálneho používateľa v rámci HKU, s rovnakou konfiguráciou a nastaveniami:

- Obsahuje informácie o konfigurácii aktuálneho používateľa.
- Informácie ako priečinky, farby obrazovky a nastavenia ovládacieho panela.
- alias pre vetvu špecifickú pre používateľa v HKEY_USERS.
- všeobecné informácie sa zvyčajne vzťahujú na všetkých používateľov a nachádzajú sa v HKU \ .DEFAULT.



Umiestnenie registra (I.)



Umiestnenie registra (II.)

- %WINDIR%\System32\Config
- tieto súbory sa aktualizujú pri každom prihlásení používateľa

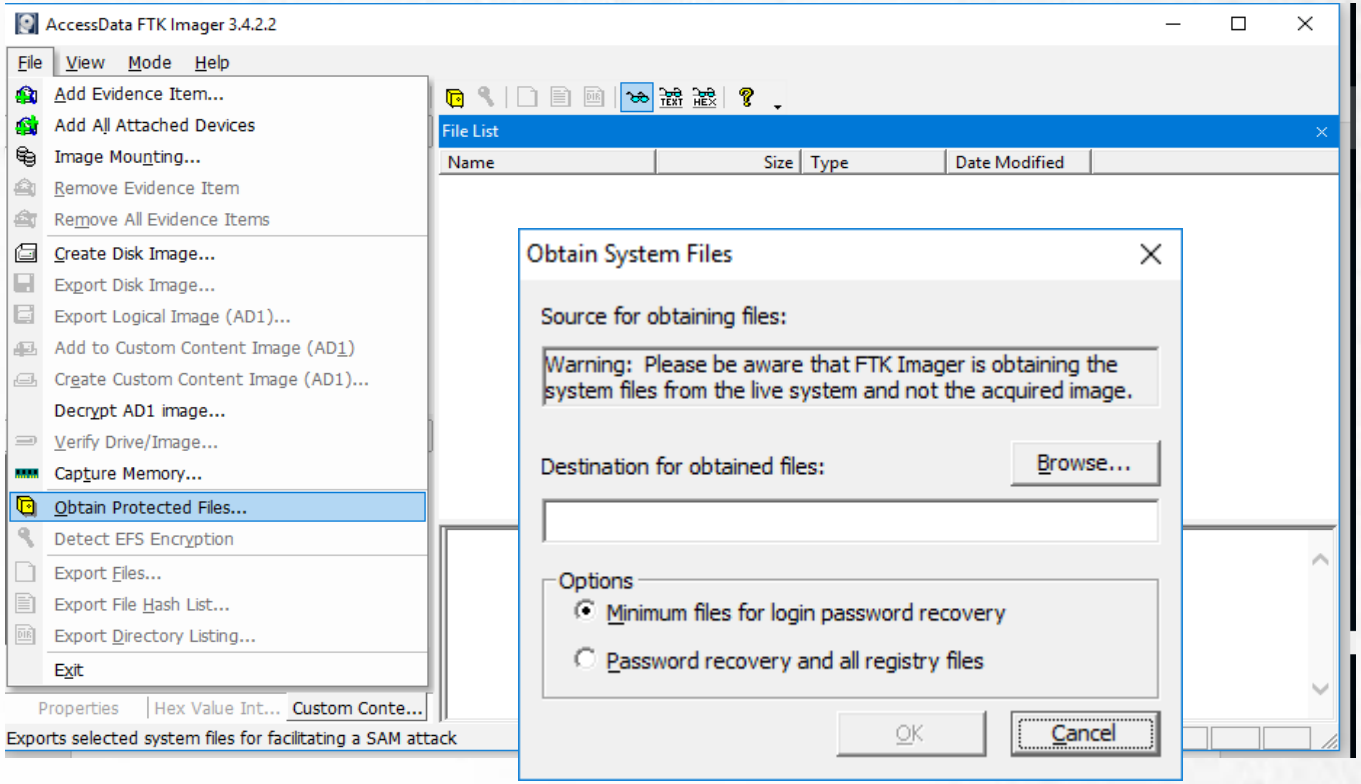
Hive name	Location in the filesystem
HKEY_LOCAL_MACHINE\System	%WINDIR%\system32\config\System
HKEY_LOCAL_MACHINE\SAM	%WINDIR%\system32\config\Sam
HKEY_LOCAL_MACHINE\Security	%WINDIR%\system32\config\Security
HKEY_LOCAL_MACHINE\Software	%WINDIR%\system32\config\Software
HKEY_USERS\User SID	Toto je užívateľský profil (NTUSER.DAT); Dokumenty a nastavenia \ Používateľ (v systéme Vista sa zmenil na Users\User). Každý profil v HKU musí byť prepojený s jedným súborom NTUSER.DAT v adresári užívateľského profilu HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList
HKEY_CURRENT_USER	len ukazovateľ na HKU aktuálne prihlásené používateľa
HKEY_USERS\.Default	%WINDIR%\system32\config\default

Zaistenie registra (II.)

- **živé systémy**
- **reg save HKLM\<hive name> <savename>**
  VSC a odtial vykopírovať (tip: robocopy)
  FTK Imager -> obtain protected files

  powershell: PowerForensics

  ```
  $r= Get-ForensicFileRecord  -Path
  C:\Windows\System32\config\SYSTE
  M
  $r.CopyFile("C:\w\exports\SYSTEM")
  ```



Forenzný obraz (image):

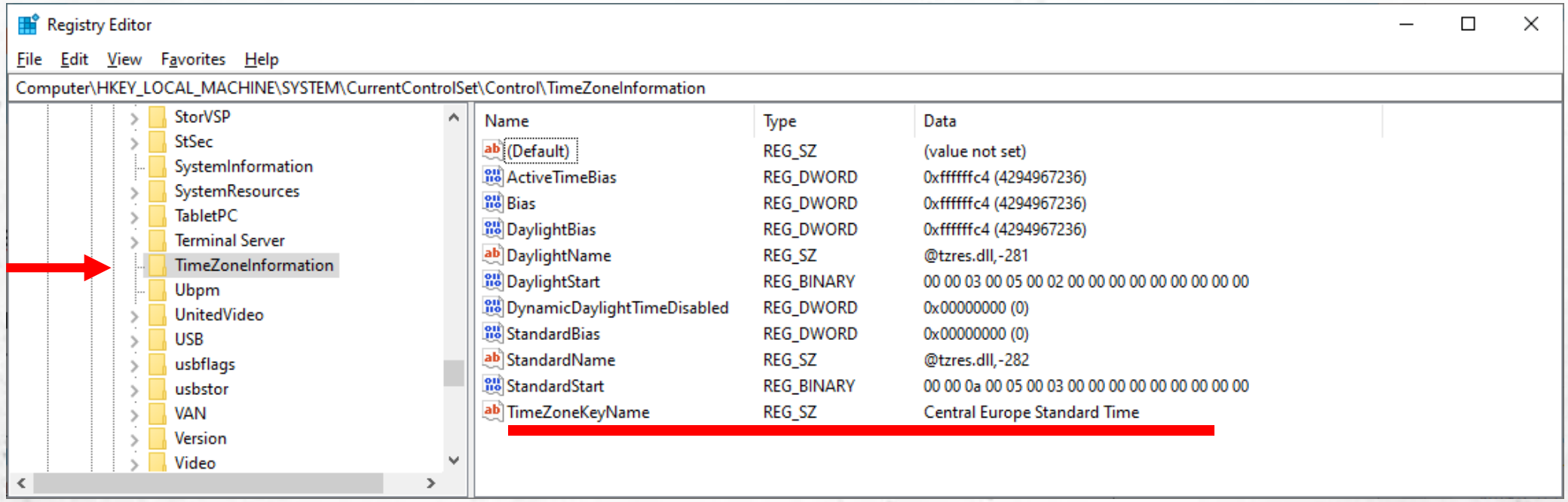
```
digforensics@forensics: /mnt/hgfs/image/registry
digforensics@forensics:/mnt/hgfs/image/registry$ cp /mnt/mountpoint/windows/system32/config/sam sam
digforensics@forensics:/mnt/hgfs/image/registry$ cp /mnt/mountpoint/windows/system32/config/system system
digforensics@forensics:/mnt/hgfs/image/registry$ cp /mnt/mountpoint/windows/system32/config/software software
digforensics@forensics:/mnt/hgfs/image/registry$ cp /mnt/mountpoint/windows/system32/config/security security
digforensics@forensics:/mnt/hgfs/image/registry$
```

Príklady kľúčov (I.)

Časová zóna

- **Účel:** Idetifikuje časovú zónu daného systému
  - Interné záznamy (logy) a dátumové/časové pečiatky sú založené na informáciách o časovom pásme systému.

- **Umiestnenie:** HKLM\System\CurrentControlSet\Control\TimeZoneInformation

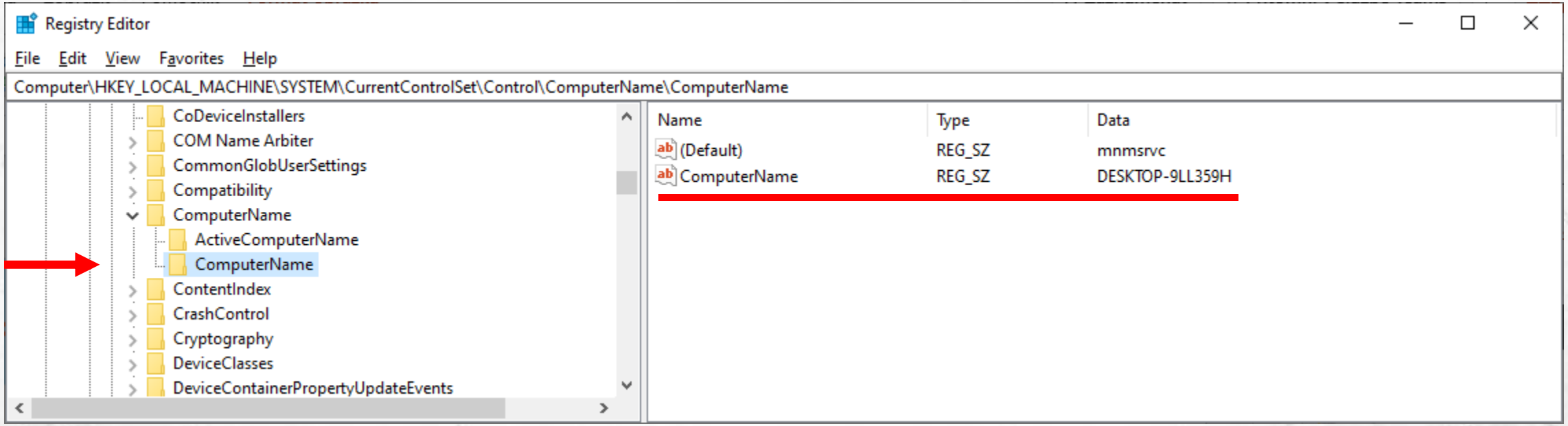


Príklady kľúčov (II.)

Názov počítača

- zapnuté zariadenie – ActiveComputerName a ComputerName.
- vypnuté zariadenie – len ComputerName.

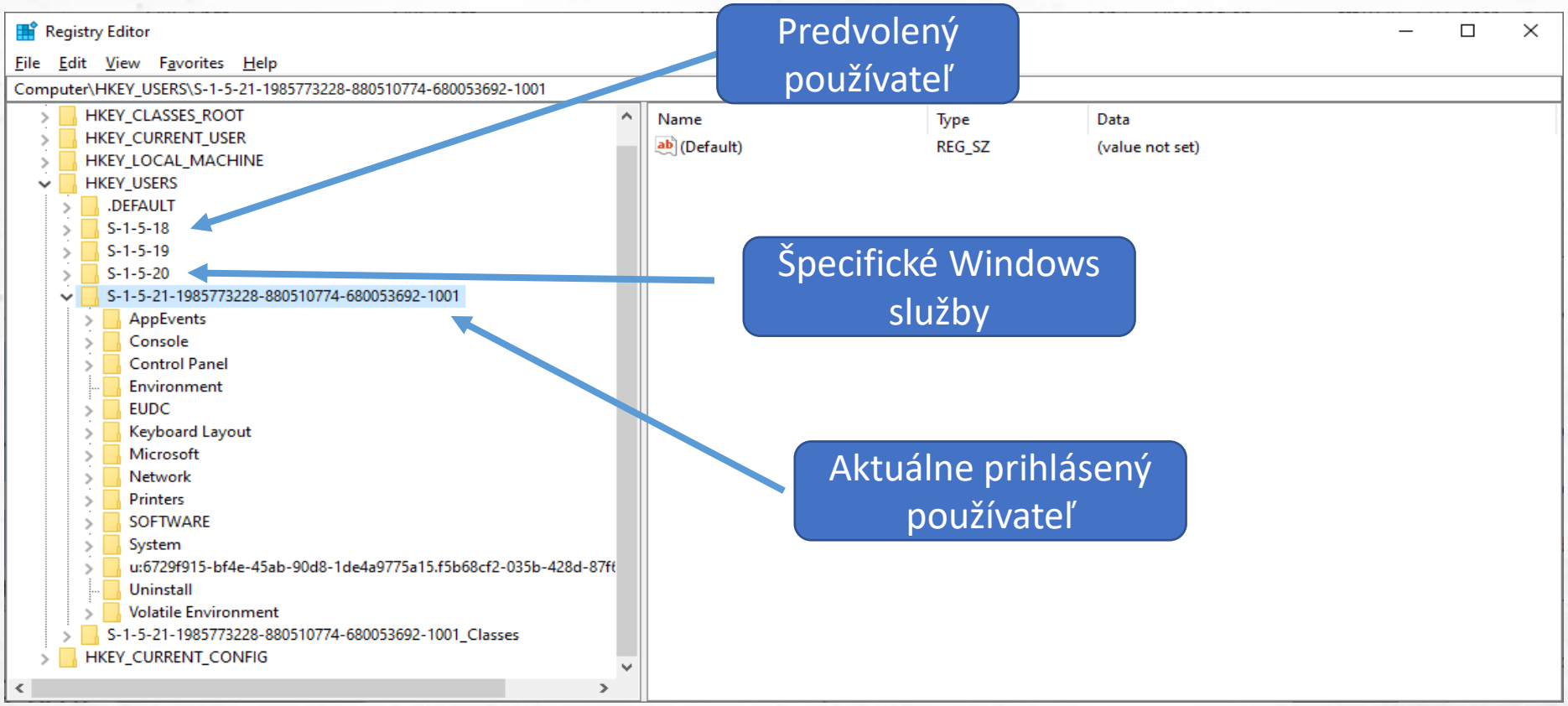
- **Umiestnenie:** HKLM\SYSTEM\{CurrentControlSet}\Control\ComputerName\ComputerName

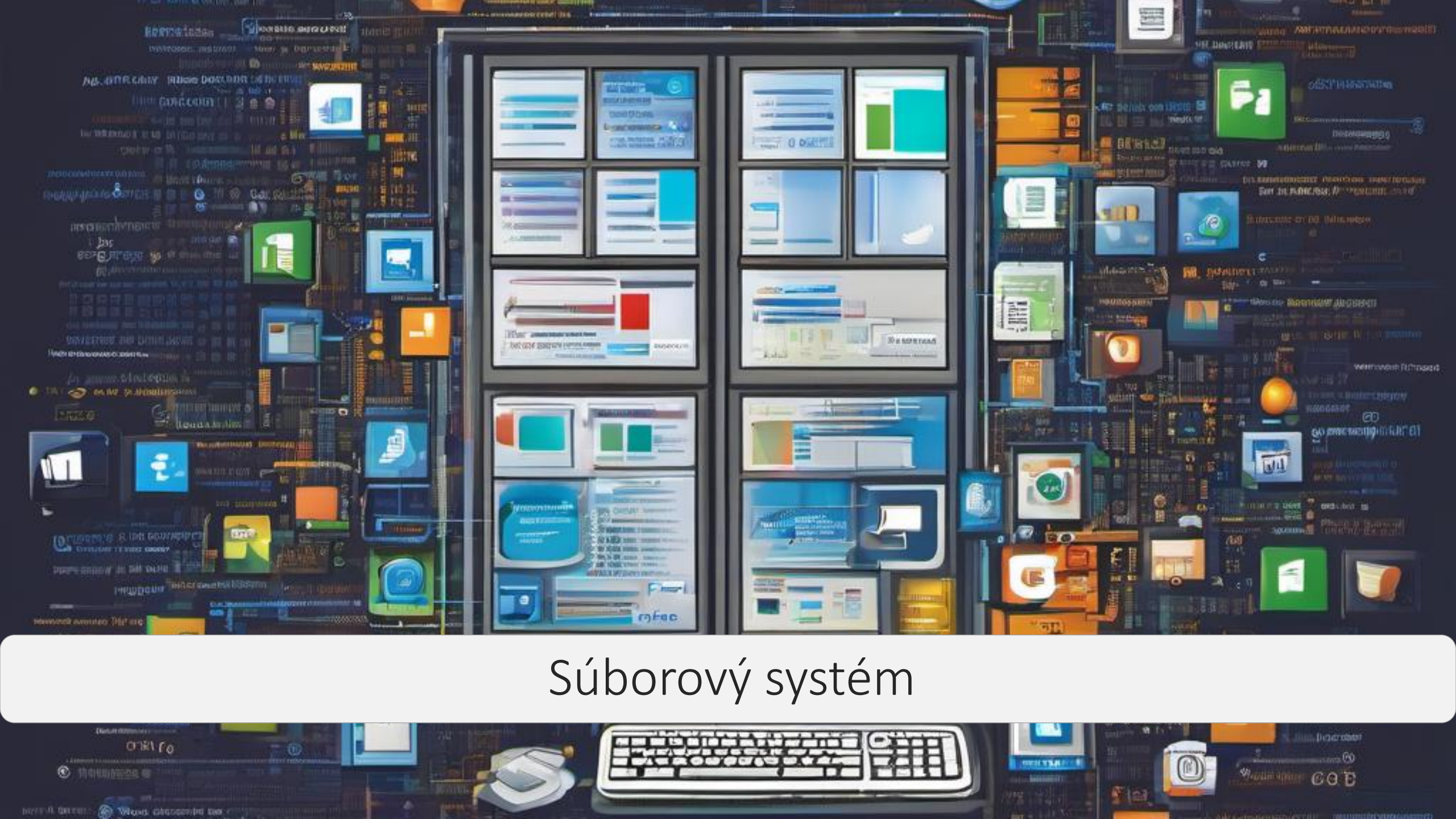


Príklady kľúčov (III.)

HKEY_USERS

- **Účel:** obsahuje informácie o špecifických konfiguráciách pre všetkých aktuálne aktívnych používateľov zariadenia

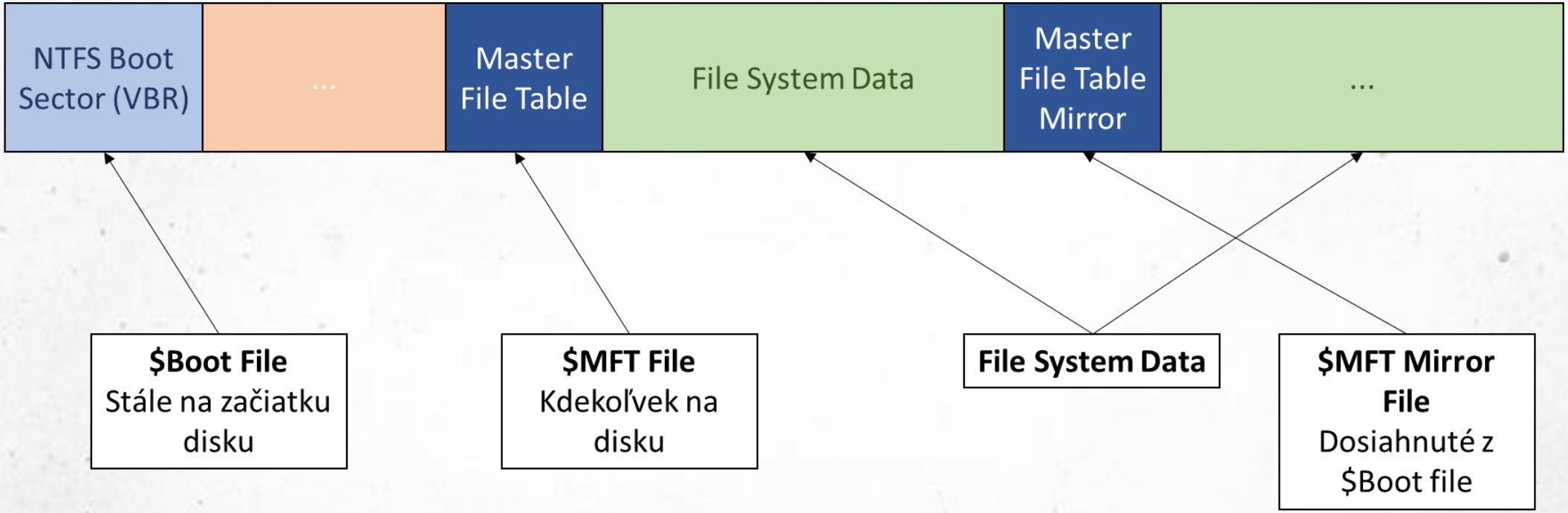




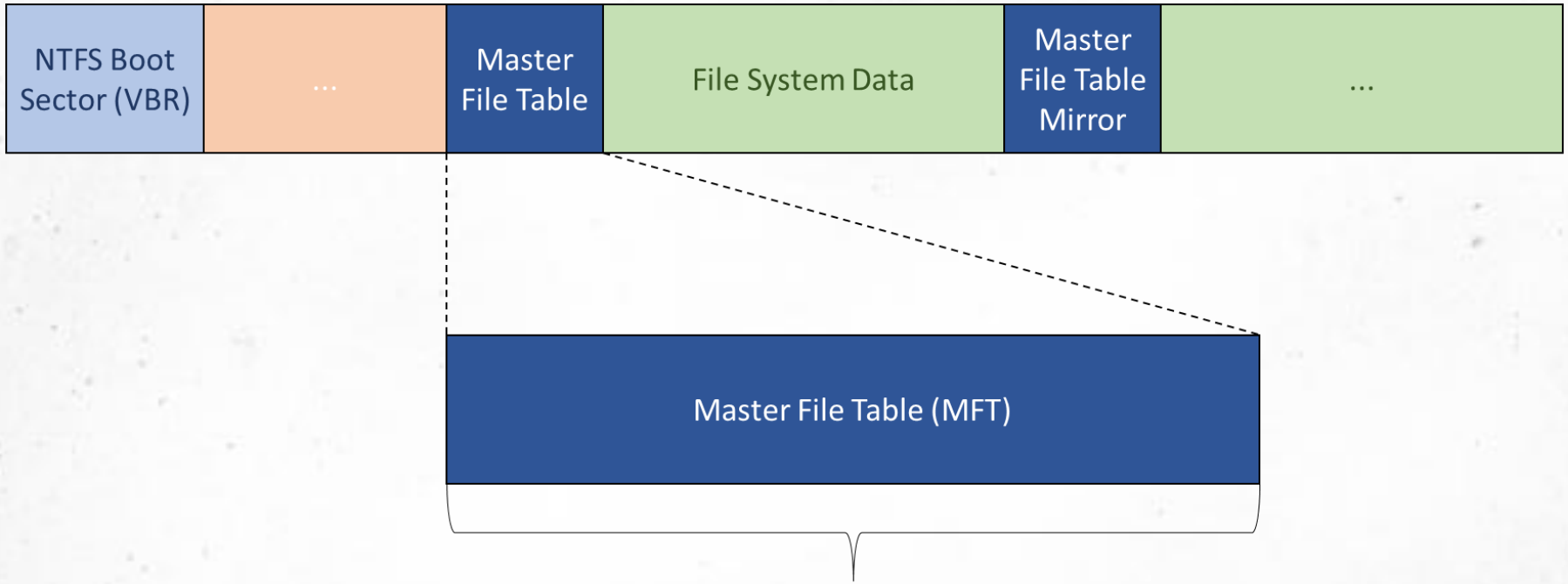
Súborový systém

NTFS (I.)

NTFS

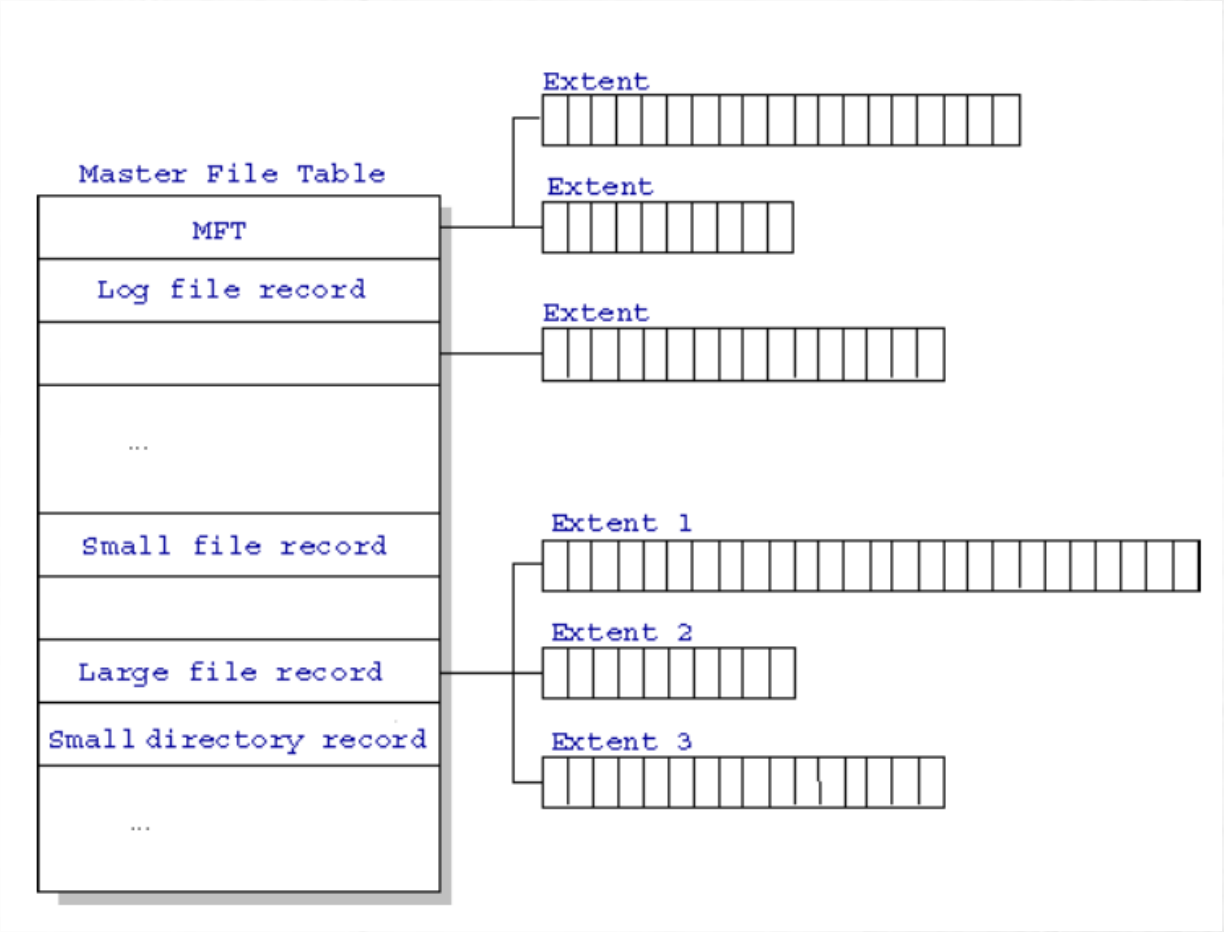

NTFS Boot Sector (VBR)
...
Master File Table
File System Data
Master File Table Mirror
...
$Boot File
Stále na začiatku disku
$MFT File
Kdekoľvek na disku
File System Data
$MFT Mirror File
Dosiahnuté z $Boot file

NTFS (II.)


NTFS Boot Sector (VBR)
...
Master File Table
File System Data
Master File Table Mirror
...
Master File Table (MFT)
Veľkosť = 12,5% diskovej kapacity

MFT (I.)

- Master file table (MFT)
- niektoré súbory sa zmestia úplne do MFT
- väčšie súbory vyžadujú pridelenie rozsahov



MFT (II.)

- NTFS ukladá metadáta v niekoľkých súboroch metadát
- Samotná MFT je súbor metadát súborového systému
- Prvých 16 položiek MFT je vyhradených pre tieto súbory
- Názvy súborov metadát začínajú znakom $ a veľkými písmenami

Názov položky	Poradie	Účel
$MFT	0	Súbor obsahujúci záznam pre každý súbor a adresár na zväzku.
$MFTMirror	1	Na obnovu v prípade zlyhania MFT.
$LogFile	2	Uchováva informácie o zmenách metadát súborového systému a pomáha pri obnove.
$Volume	3	Informácie o zväzku a jeho označení.
$AttrDef	4	Obsahuje informácie o všetkých atribútoch používaných v súborovom systéme.
. (bodka)	5	Koreňový adresár.
$Bitmap	6	Sledovanie voľných nepoužívaných klastrov v rámci zväzku.
$Boot	7	Pripojenie zväzku a ďalšieho zavádzacieho kódu, keď je zväzok spustiteľný.
$BadClus	8	Sledovanie zlých klastrov v rámci zväzku.
$Secure	9	Ukladá bezpečnostné deskriptory pre všetky súbory vo zväzku.
$Upcase	10	Prevod malých znakov na zodpovedajúce veľké znaky Unicode.
$Extended	11	Obsahuje voliteľné a rozšírené funkcie, ako sú kvóty, reparse body atď.
	12 - 15	Rezervované na budúce použitie.
	16 - 23	Nepoužité.
$ObjId	Akékoľvek	Unikátne ID pridelené každému súboru.
$Quota	Akékoľvek	Informácie o kvótach.
$Reparse	Akékoľvek	Informácie o reparse bodoch.
$UsrJrnl	Akékoľvek	Denník pre súbory a informácie o adresároch.

MFT (III.)

- záznamy v MFT sa nazývajú **atribúty**
- každý atribút sa používa na uloženie iného typu informácií.
- atribúty sa používajú na ukladanie rôznych informácií (meno, časové pečiatky, obsah atď.)
- väčšina z nich sa nachádza v samotnom zázname MFT.
- každý atribút má hlavičku

On-Disk

	VBR			
MFT záznam 0	Atribút #1	Atribút #2	....	Atribút ##
MFT záznam 1	Atribút #1	Atribút #2	....	Atribút ##
MFT záznam 2	Atribút #1	Atribút #2	....	Atribút ##
MFT záznam 3	Atribút #1	Atribút #2	....	Atribút ##
...	Atribút #1	Atribút #2	....	Atribút ##
MFT záznam 15	Atribút #1	Atribút #2	....	Atribút ##

Dátová oblasť

Hlavička MFT záznamu	Pole Fixup	Hlavička atribútu	Obsah atribútu	Hlavička atribútu	Obsah atribútu	Hlavička atribútu	Obsah atribútu	Označenie konca	Nevyužitý priestor

MFT (IV.)

Typ atribútu	Názov	Účel
Standard Information	$STANDARD_INFORMATION	Uloženie informácií týkajúcich sa časovej pečiatky režimu prístupu (read-only, read/write, atď) a počtu odkazov.
Attribute List	$ATTRIBUTE_LIST	Umiestnenie ďalších atribútov, ktoré sa nezmestili do jedného záznamu.
File Name	$FILE_NAME	Ukladá názvy súborov. Ak sa použije dlhý názov súboru alebo POSIX názov súboru, bude ich viac.
Data	$DATA	Ukladá údaje o súboroch. NTFS umožňuje, aby jeden súbor mal viac ako jeden atribút $DATA.
Object ID	$OBJECT_ID	Jedinečný identifikátor súboru v celom zväzku.
Reparse Point	$REPARSE_POINT	Mountovanie diskov.
Index Root	$INDEX_ROOT	Implementácia adresárov a iných indexov.
Index Allocation	$INDEX_ALLOCATION	Implementácia štruktúry B-stromu pre veľké adresáre a veľké indexy.
Bitmap	$BITMAP	Predstavuje stav entity.
Volume Information	$VOLUME_INFORMATION	Nachádza sa len v systémovom súbore $Volume a obsahuje verziu zväzku.
Volume Name	$VOLUME_NAME	Obsahuje názov zväzku.
Security Descriptor	$SECURITY_DESCRIPTOR	Ukladanie informácií o zabezpečení súborov (napr. zoznamy riadenia prístupu)

MFT (V.)

- Atribút **Standard Information** ($SI) – ukladá štandardné informácie o súbore, ako je veľkosť, bezpečnosť, časové pečiatky, informácie o protokolovaní atď.

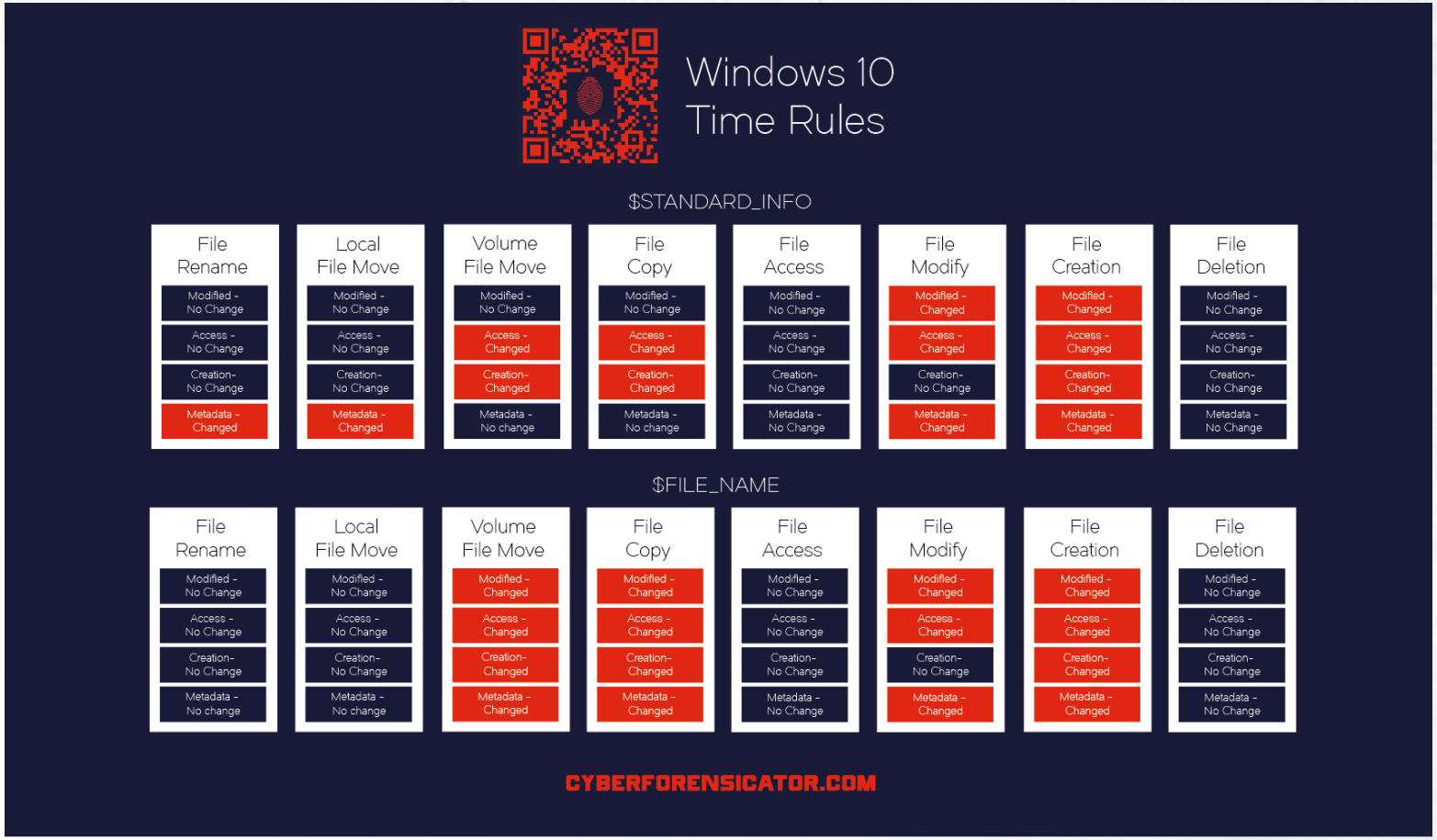
Offset	Dĺžka v bajtoch	Popis
		Štandardná hlavička atribútu
0x00	8	Čas vytvorenia súboru
0x08	8	Čas modifikácie súboru
0x10	8	Čas zmeny MFT záznamu
0x18	8	Čas prístupu k súboru
0x20	4	Súborové oprávnenia
0x24	4	Maximálny počet verzií
0x28	4	Číslo verzie
0x2C	4	ID triedy
0x30	4	ID vlastníka
0x34	4	Bezpečnostné ID
0x38	8	Quota - Množstvo bajtov, ktoré tento súbor spotreboval z kvóty používateľa.
0x40	8	Update Sequence Number (USN)

- Atribút **File Name ($FILE_NAME) -** tento atribút sa používa na uloženie názvu súboru a ďalších podrobností, ako je nadradený adresár, index adresára a časové pečiatky

Offset	Dĺžka v bajtoch	Popis
		Štandardná hlavička atribútu
0x00	8	Odkaz na súbor rodičovského adresára
0x08	8	Čas vytvorenia súboru
0x10	8	Čas modifikácie súboru
0x18	8	MFT čas modifikácie (nie je viditeľný vo vlastnostiach súboru)
0x20	8	Čas modifikácie súboru
0x24	8	Alokovaná veľkosť súboru
0x30	8	Skutočná veľkosť súboru
0x38	4	Príznaky(rovnaké ako $SIA príznaky)
0x3C	4	Reparse hodnota
0x40	1	Dĺžka názvu
0x41	1	Využitý priestor pre názov
0x42	~	Názov

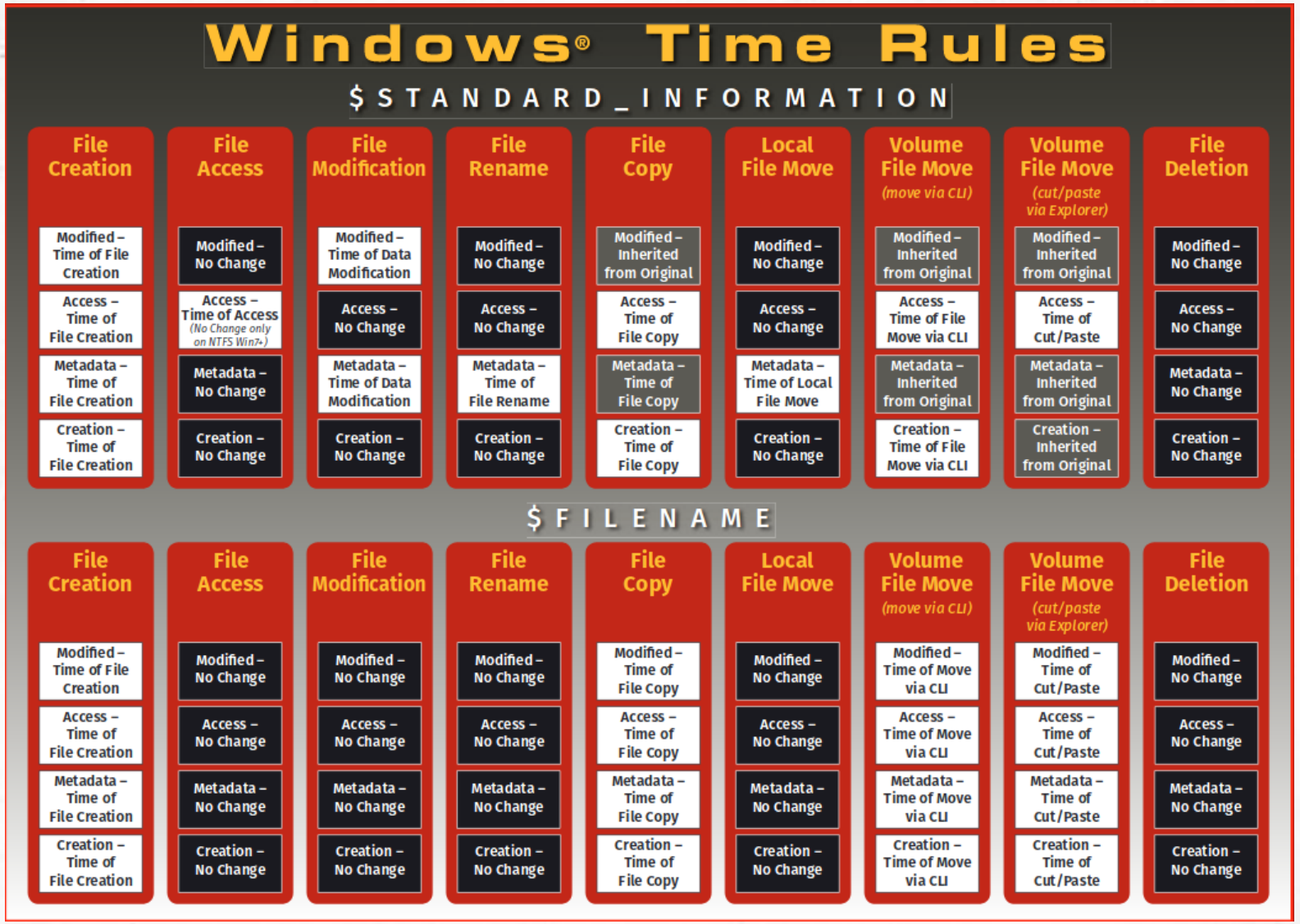
Časové pečiatky (I.)

- 2 sety časových pečiatok:
  - **$STANDARD_INFORMATION (SI)**
  - to, čo je v GUI
  - modifikovateľne používateľskými aplikáciami
  - nedôveryhodné – možnosť time Stomping-u
  - **$FILE_NAME (FN)**
  - RAW – viditeľne iba po parsovani $MFT
  - nie sú priamo modifikovateľne používateľskými aplikáciami
  - ťažšie modifikovateľné



Zdroj: https://www.sans.org/security-resources/posters/windows-forensic-analysis/170/download

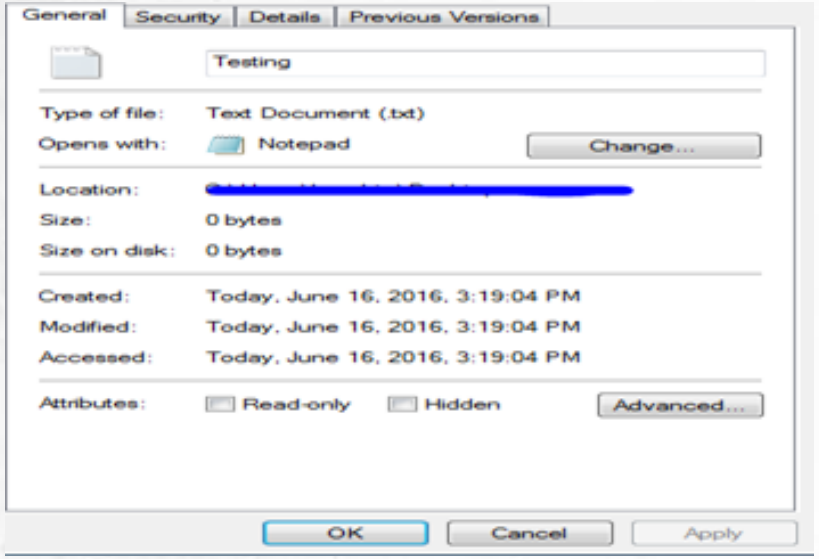
Časové pečiatky (II.)



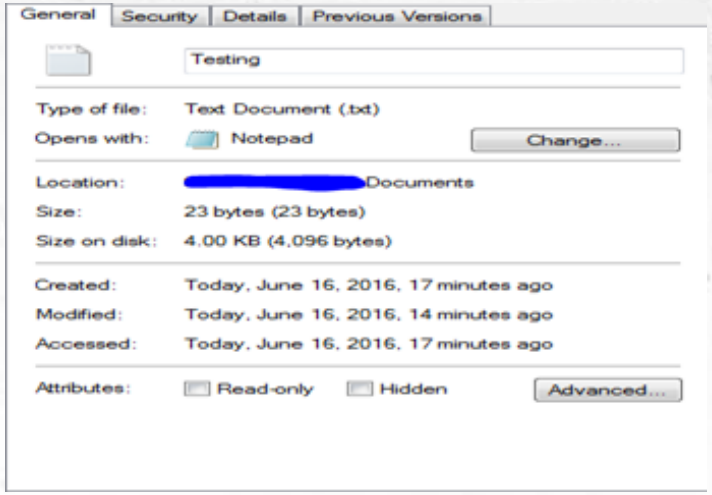
Zdroj: https://www.sans.org/security-resources/posters/windows-forensic-analysis/170/download

Časové pečiatky (III.)

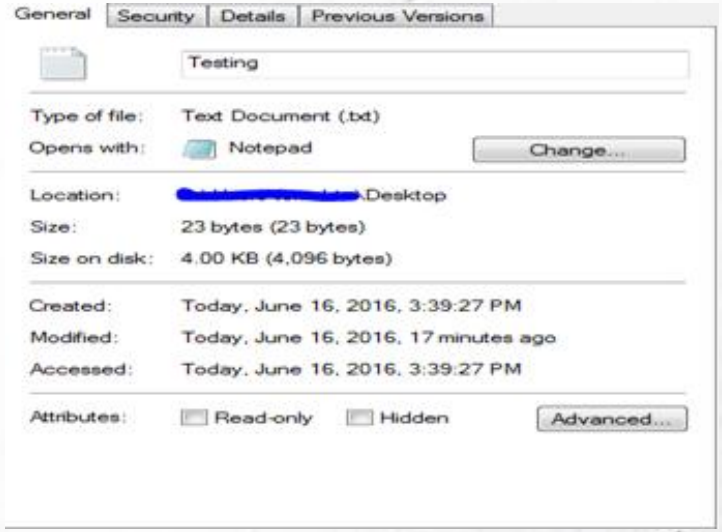
Vytvorenie súboru



Presunutie súboru

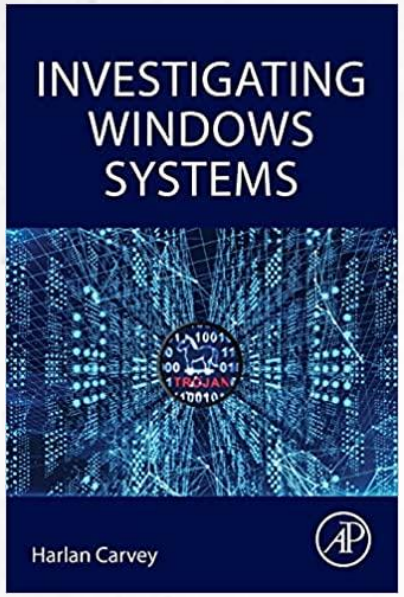


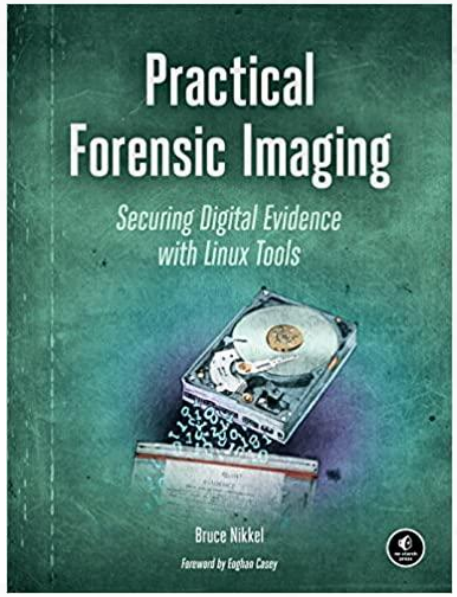
Skopírovanie súboru

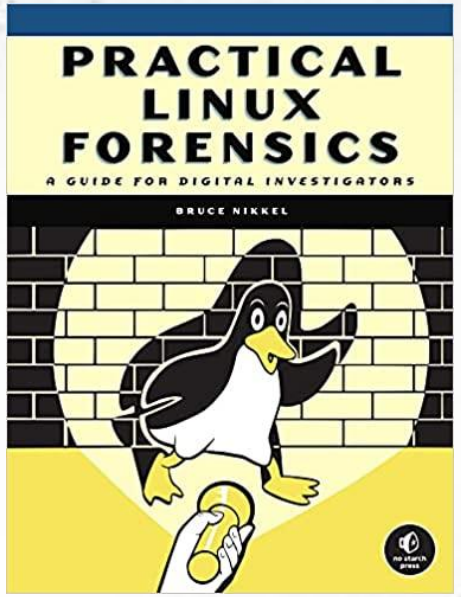


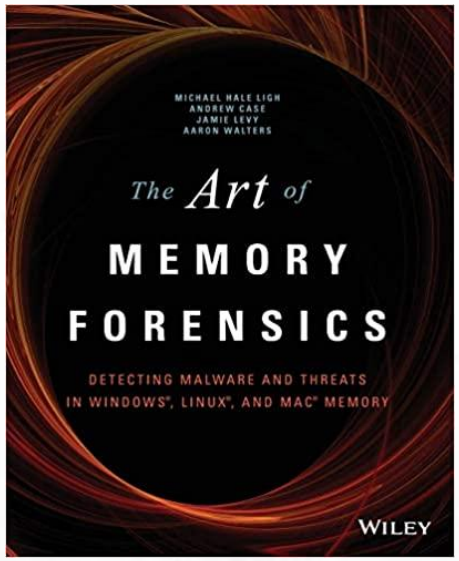
Zdroj: http://www.kazamiya.net/en/NTFS_Timestamps, https://www.forensixchange.com/posts/19_04_22_win10_ntfs_time_rules/

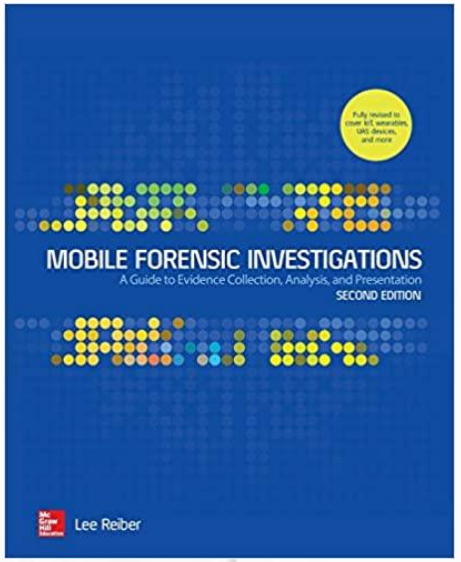
Literatúra


INVESTIGATING
WINDOWS
SYSTEMS
Harlan Carvey


Practical
Forensic Imaging
Securing Digital Evidence
with Linux Tools
Bruce Nikkel
Foreword by Eoghan Casey


PRACTICAL
LINUX
FORENSICS
A GUIDE FOR DIGITAL INVESTIGATORS
BRUCE NIKKEL


MICHAEL HALE LIGH
ANDREW CASE
JAMIE LEVY
AARON WALTERS
The Art of
MEMORY
FORENSICS
DETECTING MALWARE AND THREATS
IN WINDOWS®, LINUX®, AND MAC® MEMORY
WILEY


MOBILE FORENSIC INVESTIGATIONS
A Guide to Evidence Collection, Analysis, and Presentation
SECOND EDITION
Lee Reiber

...

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