KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

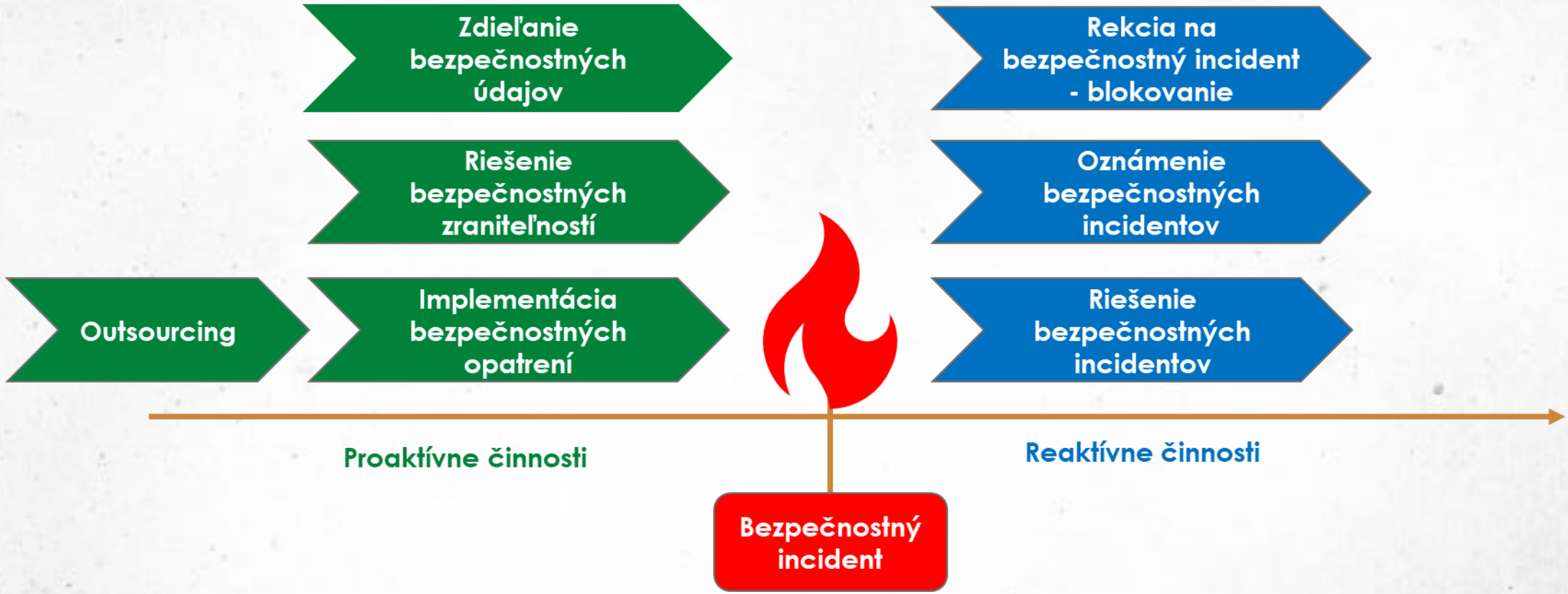
Kybernetické bezpečnostné incidenty a zraniteľnosti

Meno a priezvisko

XX.XX.XXXX

KCKB UPJS CSIRT UPJS

Preventívne a reaktívne činnosti (I.)



Preventívne a reaktívne činnosti (II.)

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

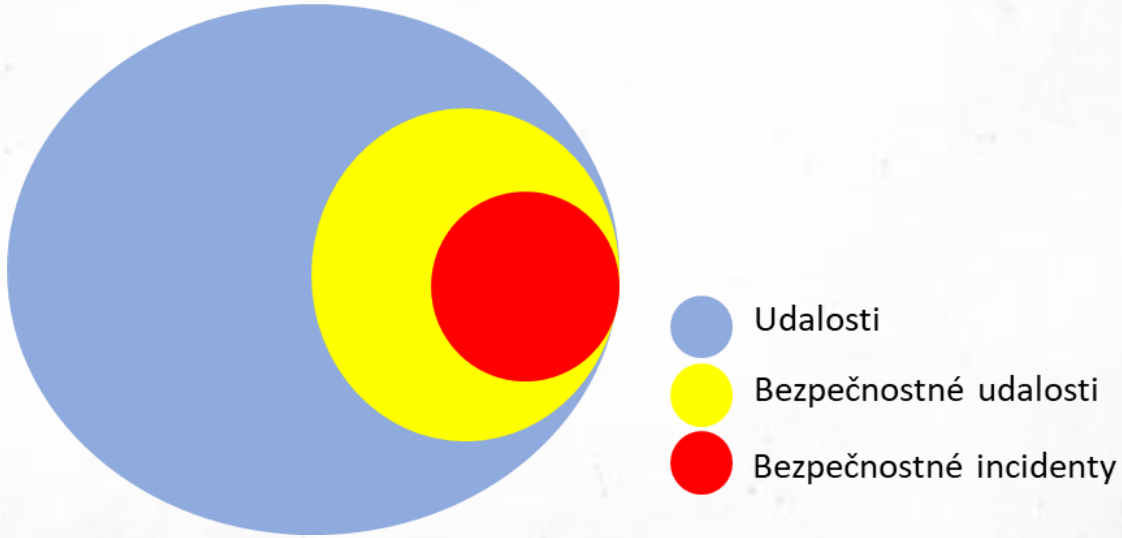
Preventívne a reaktívne činnosti (III.)

§ 15 ods. 3 ZoKB - reaktívne služby:

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

Bezpečnostné incidenty (I.)

- **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



Bezpečnostné incidenty (II.)

Kybernetický bezpečnostný incident (ZoKB)

- akákoľvek udalosť, ktorá má z dôvodu narušenia bezpečnosti siete a informačného systému, alebo porušenia bezpečnostnej politiky alebo záväznej metodiky negatívny vplyv na kybernetickú bezpečnosť alebo ktorej následkom je:
- 1. **strata dôvernosti** údajov, zničenie údajov alebo narušenie **integrity** systému,
- 2. obmedzenie alebo odmietnutie **dostupnosti** základnej služby alebo digitálnej služby,
- 3. vysoká pravdepodobnosť kompromitácie činností základnej služby alebo digitálnej služby alebo
- 4. ohrozenie bezpečnosti informácií,

Zdroj: https://i.pinimg.com/originals/8d/d5/5c/8dd55c6295785663d6005eb76798d4cf.jpg

Bezpečnostné incidenty (III.)

REFERENCE TAXONOMY (ECSIRT.NET)[10]	COMMON TAXONOMY FOR LE AND CSIRTS	NOTE
Abusive Content	Abusive Content	
Malicious Code	Malware	
Information Gathering	Information Gathering	
Intrusion Attempts	Intrusion Attempts	
Intrusion	Intrusion	
Availability	Availability	
Information Content Security	Information Security	
Fraud	Fraud	
Vulnerable		Not relevant to LEA
Other	Other	
Test		Not relevant to LEA

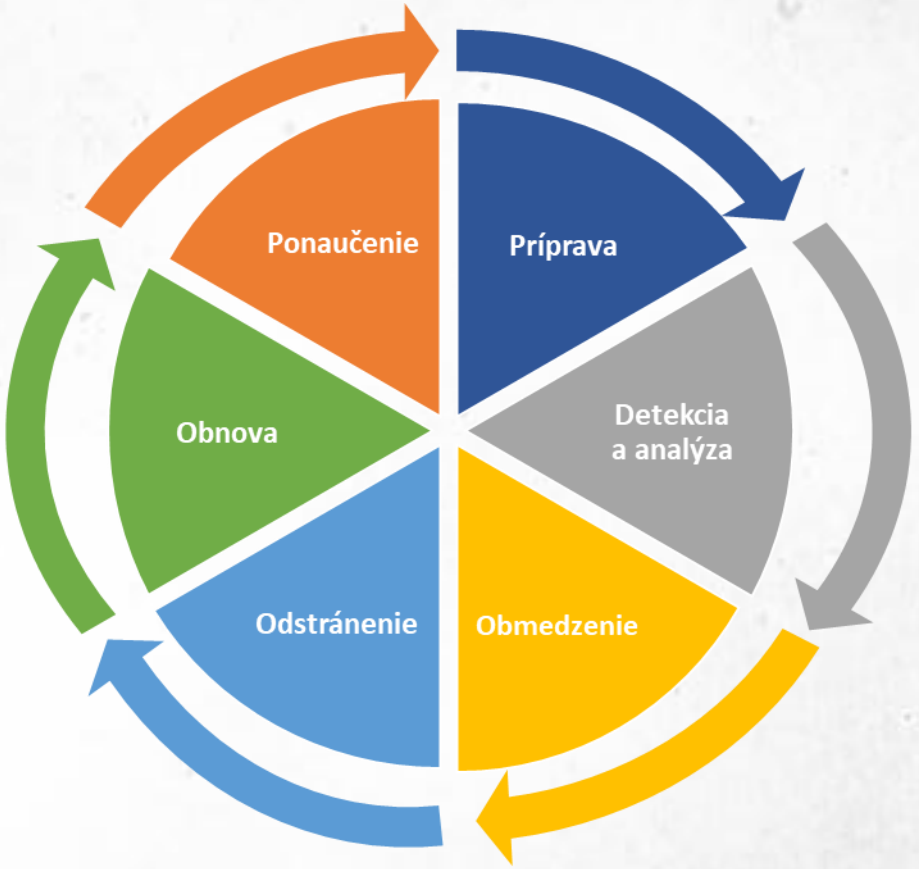
Table 2: Reference taxonomy vs Common Taxonomy for LE and CSIRTs

LEGEND	
	The same
	Not mentioned in the other taxonomy
	Not present

Zdroj: ENISA: Reference Incident Classification Taxonomy Task Force Status and Way Forward, 2018.

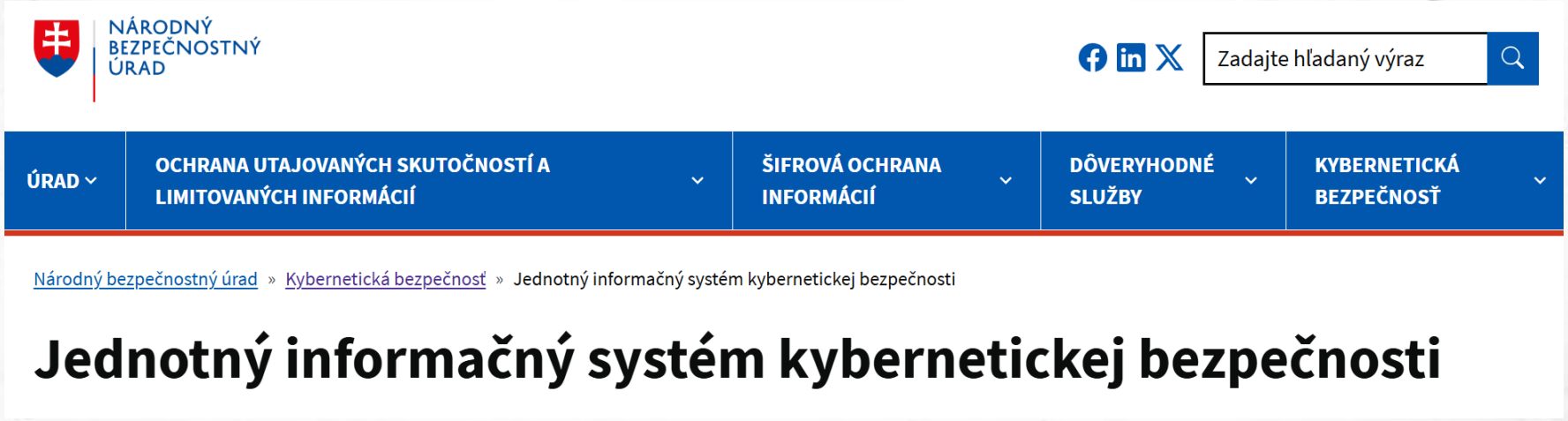
Bezpečnostné incidenty (IV.)

- SANS metodológia
- zodpovednosť v jednotlivých fázach
- paradox detekcie úniku údajov (the Breach Detection Paradox)
- obmedzenie šírenia bezpečnostného incidentu
- reakcia na bezpečnostný incident
- obnova dát



Mýtus – Incidenty nie je potrebné hlásiť

- notifikačná povinnosť – dôležitý nástroj na riešenie a predchádzanie bezpečnostných incidentov
- § 24 ods. 1 zákona o KB - Prevádzkovateľ základnej služby je povinný hlásiť každý závažný kybernetický bezpečnostný incident.
- § 23 ods. 3 písm. a) ZoITVS - Orgán riadenia je povinný, ak je zaradený do registra prevádzkovateľov základných služieb [...] nahlasovať [...] aj kybernetický bezpečnostný incident, na ktorý sa nevzťahuje povinnosť nahlasovania podľa osobitného predpisu.



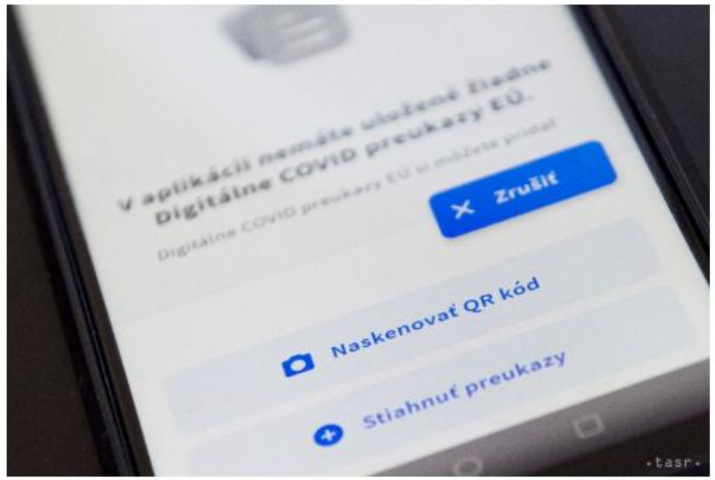
Zdroj: https://www.nbu.gov.sk/jednotny-informacny-system-kybernetickej-bezpecnosti/

Bezpečnostné zraniteľnosti (I.)

< sekcia Slovensko

NCZI nesúhlasí s tým, že by nebolo schopné ochrániť dáta občanov

Zdieľaj na Facebooku



Slovenská bezpečnostná IT spoločnosť Nethemba špecializujúca sa primárne na bezpečnosť webových aplikácií a penetračné testy tvrdí, že NCZI nebolo opäť schopné ochrániť osobné dáta miliónov ľudí.

Autor TASR
16. augusta 2021 17:06

ŽIVĒ SPRÁVY TV & OPERÁTORI BEZPEČNOSŤ AI MOBILMANIA PRÉMIOVÉ ČÍTANIE VIDEO

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

Ako tiež ukázali etickí hackeri z Nethemba, pomocou jednoduchého útoku vedeli získať rodné číslo akéhokoľvek občana Slovenska.

Zdroj: https://zive.aktuality.sk/clanok/5w4np4g/v-ehranici-bola-vazna-chyba-hackeri-vedeli-poslat-cloveka-do-karanteny-aj-ziskat-akykolvek-vakcinacny-preukaz/, https://www.teraz.sk/slovensko/nczi-nesuhlasi-s-tym-ze-by-opat-n/570328-clanok.html

Bezpečnostné zraniteľnosti (II.)

NETHEMBA

O NÁS REFERENCIE BLOG KONTAKT SLUŽBY

MOŽNOSŤ PLOŠNÉHO ZÍSKANIA A ZNEUŽITIA EÚ VAKCINAČNÝCH CERTIFIKÁTOV

2021-08-14 10:49
Pavol Lupták

TAGY:

COVID-19 CERTIFIKÁT
EHRANICA
IMPERSONIFIKÁCIA
NCZI
RODNÉ ČÍSLA
ÚNIK

AKO NA ZÁKLADE MENA A DÁTUMU NARODENIA ZÍSKAŤ EÚ VAKCINAČNÝ PREUKAZ ĽUBOVOĽNÉHO OBČANA SR

1 HISTÓRIA ZRANITEĽNOSTÍ

Podobne ako pri poslednej zraniteľnosti NCZI, kedy sme boli schopní stiahnuť všetky PCR/antigen testy a osobné informácie všetkých testovaných občanov, aj túto zraniteľnosť sme objavili čistou náhodou (**čo znamená, že sme nerealizovali žiadny cielený scan, nehľadali konkrétne zraniteľnosti, ale identifikovali sme ju pri bežnom používaní aplikácie**).

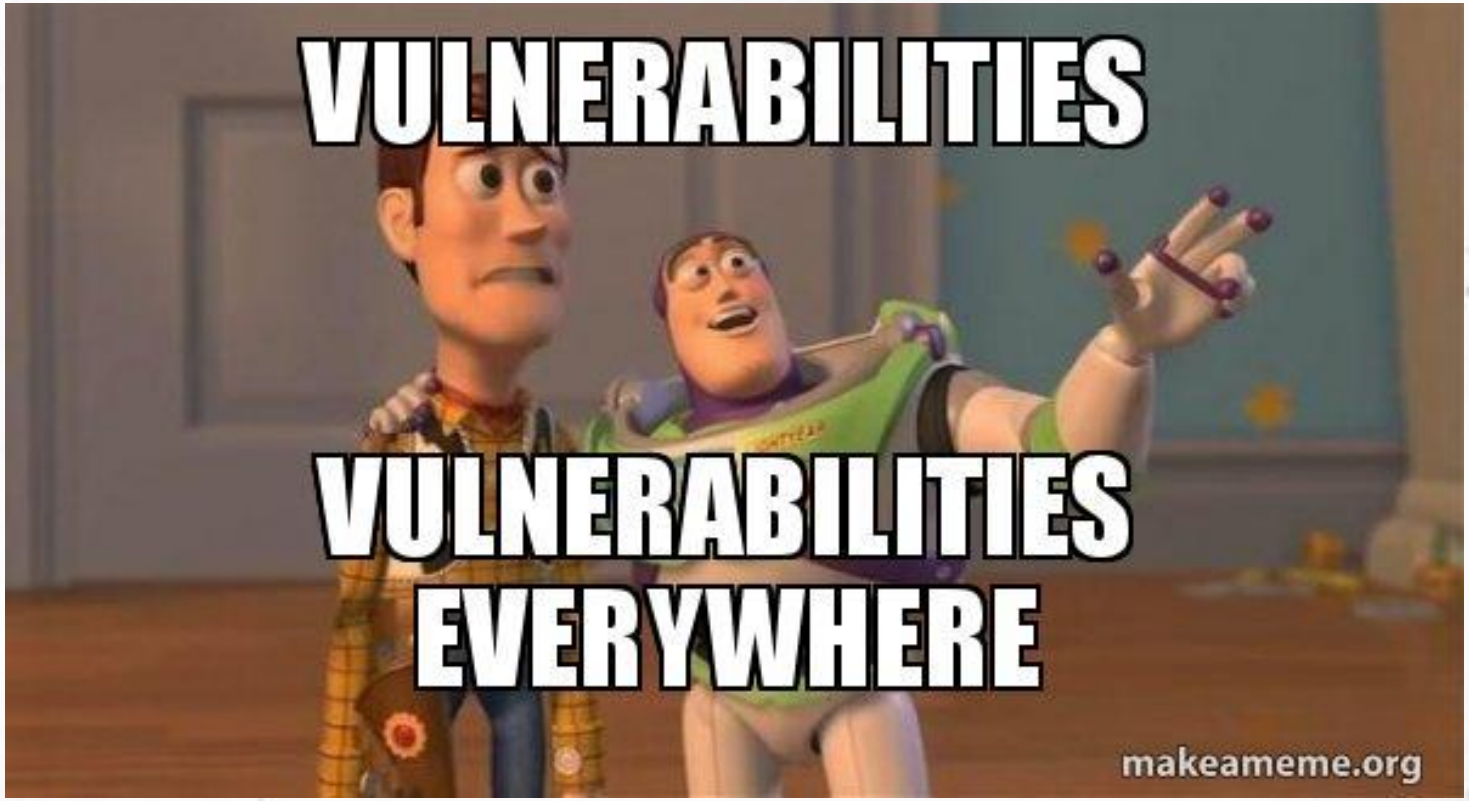
"Cestoval som z Kyjeva do Bratislavy a pri vypĺňaní eHranica formulára som zadal iné kontaktné údaje (iný email, iné mobilné číslo) ako som zadal pri samotnej vakcinácii. Prekvapilo ma, že deň na to, som si nedokázal stiahnuť svoj EÚ COVID-19 certifikát a musel som kontaktovať NCZI supportné centrum. To mi síce nikdy neodpovedalo, ale prišiel som na to, že keď ako kontaktné údaje na získanie COVID-19-PASS zadám tie, ktoré som naposledy zadával pri vypĺňaní eHranica formulára, tak mi to COVID-19-PASS normálne prepošle a súčasne si dokážem stiahnuť svoj EÚ COVID-19 certifikát. Vtedy som si uvedomil, že týmto trikom dokážem získať COVID-19-PASS / EÚ vakcinačný preukaz prakticky akéhokoľvek človeka, ktorého rodné číslo poznám. Behom pár minút som našiel iný štátny web, ktorý mi dokázal pre konkrétne rodné číslo a meno overiť, či jeho rodné číslo je platné alebo nie. Jednoduchou enumeráciou som následne dokázal získať rodné číslo pre ľubovoľného človeka, ktorého dátum narodenia poznám. A potom som si všimol, že väčšina politikov a celebrít má svoj dátum narodenia uvedený na wikipedii a všetci ostatní na socialných sieťach..."

Dátum nahlásenia zraniteľnosti CSIRT: 30.7.2021 o 18:23:43

Zdroj: https://nethemba.com/sk/moznost-plosneho-ziskania-a-zneuzitia-eu-vakcinacnych-certifikatov/

Bezpečnostné zraniteľnosti (III.)

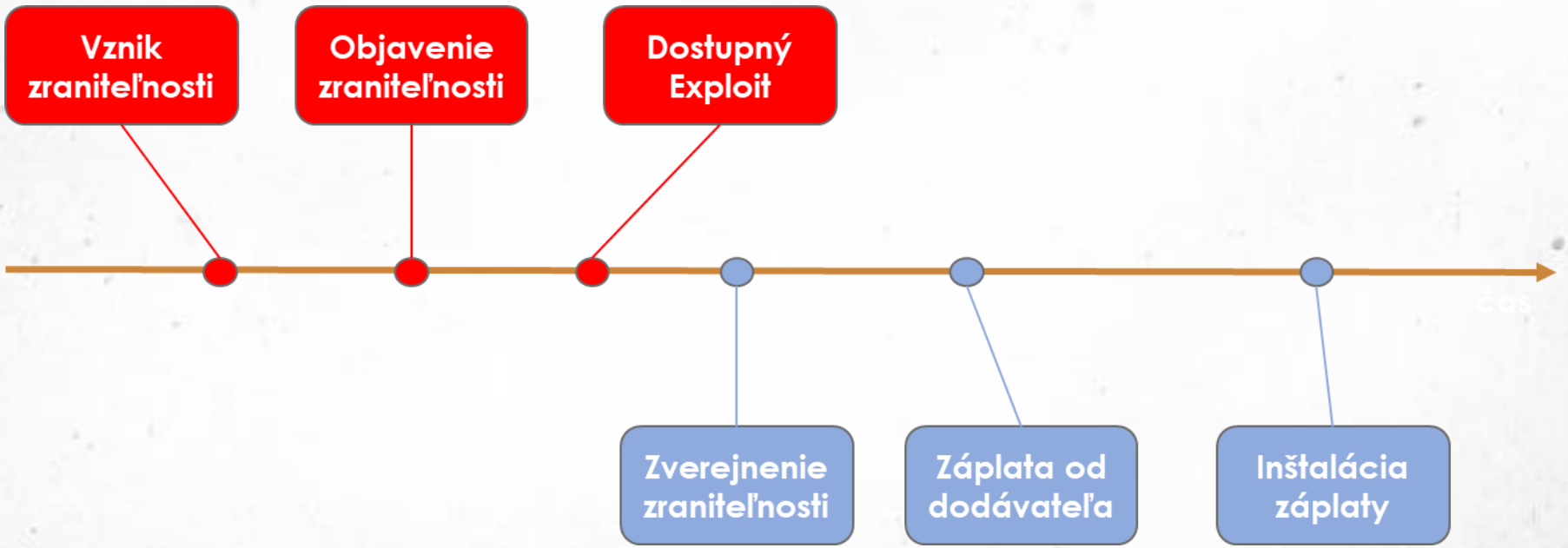
- chyba v softvéri, firmvéri, hardvéri alebo komponente služby vyplývajúca zo slabosti, ktorú je možné zneužiť, a ktorá má negatívny vplyv na dôvernosť, integritu alebo dostupnosť ovplyvneného komponentu alebo komponentov (CVE – MITRE)



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

Bezpečnostné zraniteľnosti (IV.)

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



Bezpečnostné zraniteľnosti (V.)

- recitál 60 smernice NIS 2 *„by sa členské štáty mali v rámci svojej vnútroštátnej politiky snažiť ... riešiť výzvy, ktorým čelia výskumníci zaoberajúci sa zraniteľnosťami, vrátane ich možného vystavenia sa trestnej zodpovednosti. Vzhľadom na to, že fyzické a právnické osoby, ktoré skúmajú zraniteľnosti, by v niektorých členských štátoch mohli byť vystavené trestnej a občianskoprávnej zodpovednosti, členské štáty sa nabádajú, aby prijali usmernenia týkajúce sa* ***nestíhania výskumníkov v oblasti bezpečnosti informácií a udelenia výnimky z občianskoprávnej zodpovednosti za ich činnosti.“***

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

pavol.sokol@upjs.sk

https://cyberawareness.sk