Zahrajte vítězný tah v kyber bezpečnosti s

FORESIGHT®
CYBER

Co se děje za obrazovkou a co nám přinese budoucnost

Jakub Šafařík, Foresight Cyber s.r.o.

21.11.2024

Situace ve světě - 2023

2200 útoků denně!

Každých 39s,
800 000 útoků ročně.

$ 8 000 000 000 000

© Foresight Cyber Ltd, Page 2

FORESIGHT® CYBER

Situace ve světě - 2023

TOP 5

- Prolomeno a ukradeno nejméně **60 000 emailových adres** (US State Department – Ministerstvo zahraničí)
- DarkBeam – zcizeno **3 800 000 000** osobních údajů.
- Ransomware v UK Royal Mail – výkupné **$80 000 000** nedostupnost 11 500 poboček.
- MOVEit data theft – postiženo **2 000 organizací**, ohroženy údaje více než **60 000 000 uživatelů**.
- Indonésie – zcizeno **34 000 000 osobních údajů** občanů.

https://www.weforum.org/agenda/2024/01/cybersecurity-cybercrime-system-safety/
https://www.theguardian.com/business/2023/feb/21/royal-mail-international-deliveries-cyber-attack-ransom-strikes
https://techreport.com/news/darkbeams-alarming-data-breach-exposes-3-8-billion-records/
https://www.bleepingcomputer.com/news/security/microsoft-breach-led-to-theft-of-60-000-us-state-dept-emails/
https://www.bcs.org/articles-opinion-and-research/the-biggest-cyber-attacks-of-2023/

FORESIGHT® CYBER

© Foresight Cyber Ltd, Page 3

Situace ve světě – 2024

- Smazání **2 Petabytů** dat Russian space research center
- CrowdStrike incident – **$ 10 000 000 000** ?
- National Public Data breach – USA, **2 900 000 000 záznamů**
- CDK Global – ransomware útok, škoda **$1 000 000 000**
- AT&T data breach, 2 případy, únik **110** a **73 milionů** klientských záznamů
- Synnovis ransomware – výpadek nemocnic v UK
- Snowflake – série krádeží dat, ovlivněny **stovky milionů** zákazníků? (Ticketmaster 560 000 000, …)

https://insights.integrity360.com/biggest-cyber-attacks-of-the-year-so-far
https://insights.integrity360.com/biggest-cyber-attacks-of-the-year-so-far
https://techcrunch.com/2024/10/14/2024-in-data-breaches-1-billion-stolen-records-and-rising/
https://support.microsoft.com/en-us/topic/national-public-data-breach-what-you-need-to-know-843686f7-06e2-4e91-8a3f-ae30b7213535
https://www.wired.com/story/snowflake-breach-advanced-auto-parts-lendingtree/

FORESIGHT® CYBER

© Foresight Cyber Ltd, Page 4

Situace ve světě - 2023

Zdroj: 1 Password

10x

útoků na uživatelská hesla

95%

průniků díky lidské chybě

70%

společností napadeno přes neaktualizovaná zařízení.

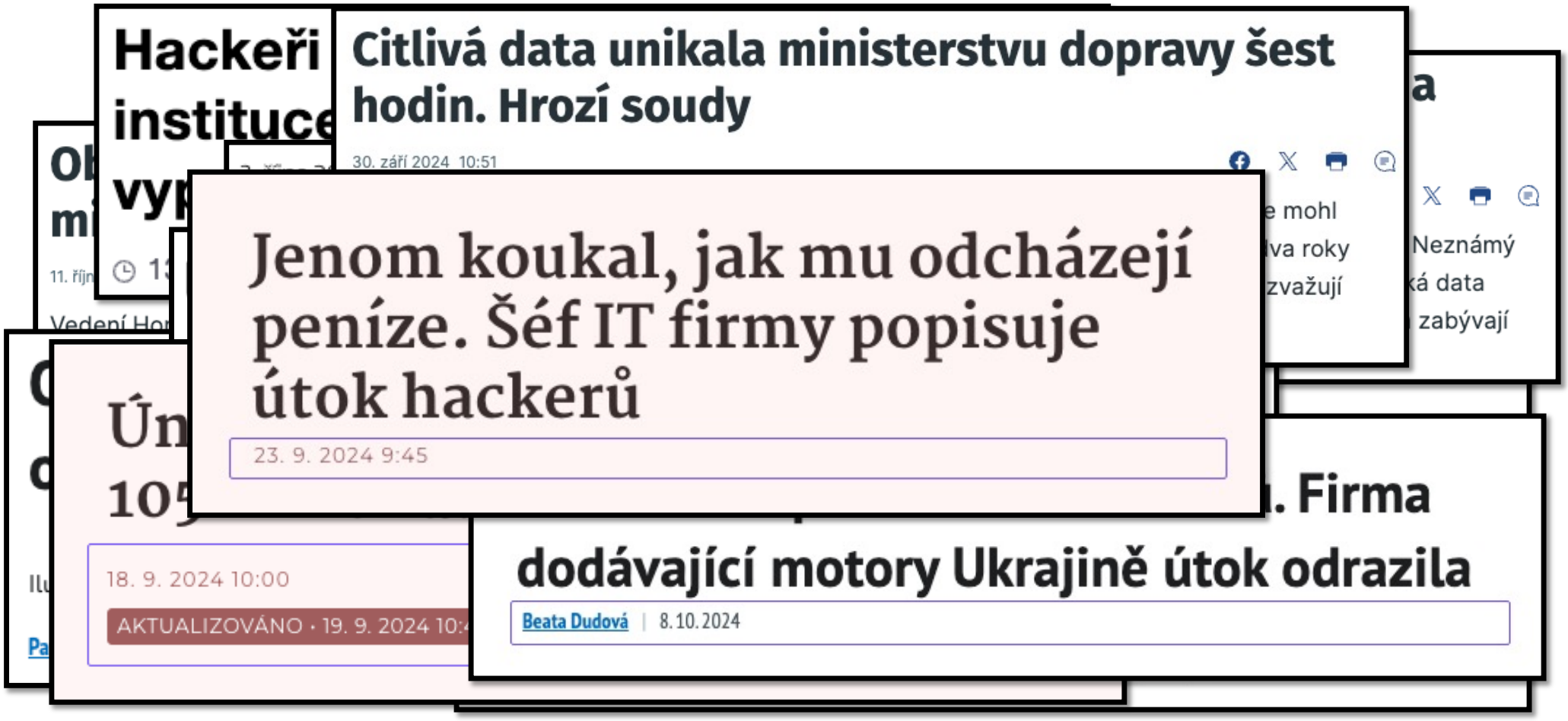
31%

útok přes neznámá zařízení

FORESIGHT® CYBER

© Foresight Cyber Ltd, Page 5

Situace v Česku



© Foresight Cyber Ltd, Page 6

FORESIGHT® CYBER

Situace v Česku 2023

Zdroj: NÚKIB – 262 útoků = 79 % nárůst oproti 2022

2 velmi významné útoky na státní subjekt a obranný sektor

Povinnost **hlásit kybernetické bezpečnostní incidenty** se vás týká, pokud jste … správcem nebo provozovatelem informačního nebo komunikačního systému **kritické informační infrastruktury**, správcem nebo provozovatelem významného informačního systému, správcem nebo provozovatelem informačního systému základní služby nebo provozovatelem základní služby, případně osobou neuvedenou **v zákoně o kybernetické bezpečnosti**.

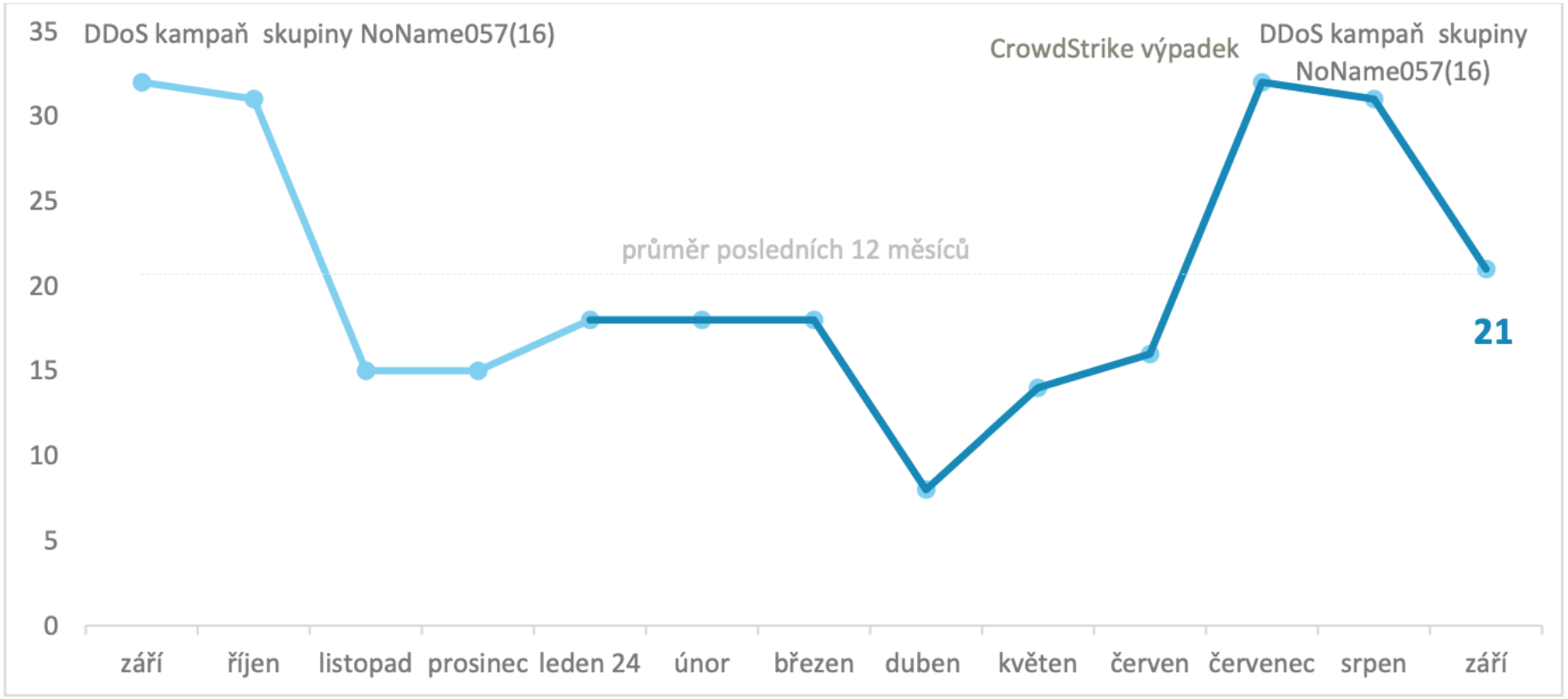
© Foresight Cyber Ltd, Page 7

FORESIGHT® CYBER

https://nukib.gov.cz/cs/infoservis/aktuality/2073-nukib-v-roce-2023-zaznamenal-rekordni-pocet-kybernetickych-incidentu/

Situace v Česku

NÚKIB – report září 2024

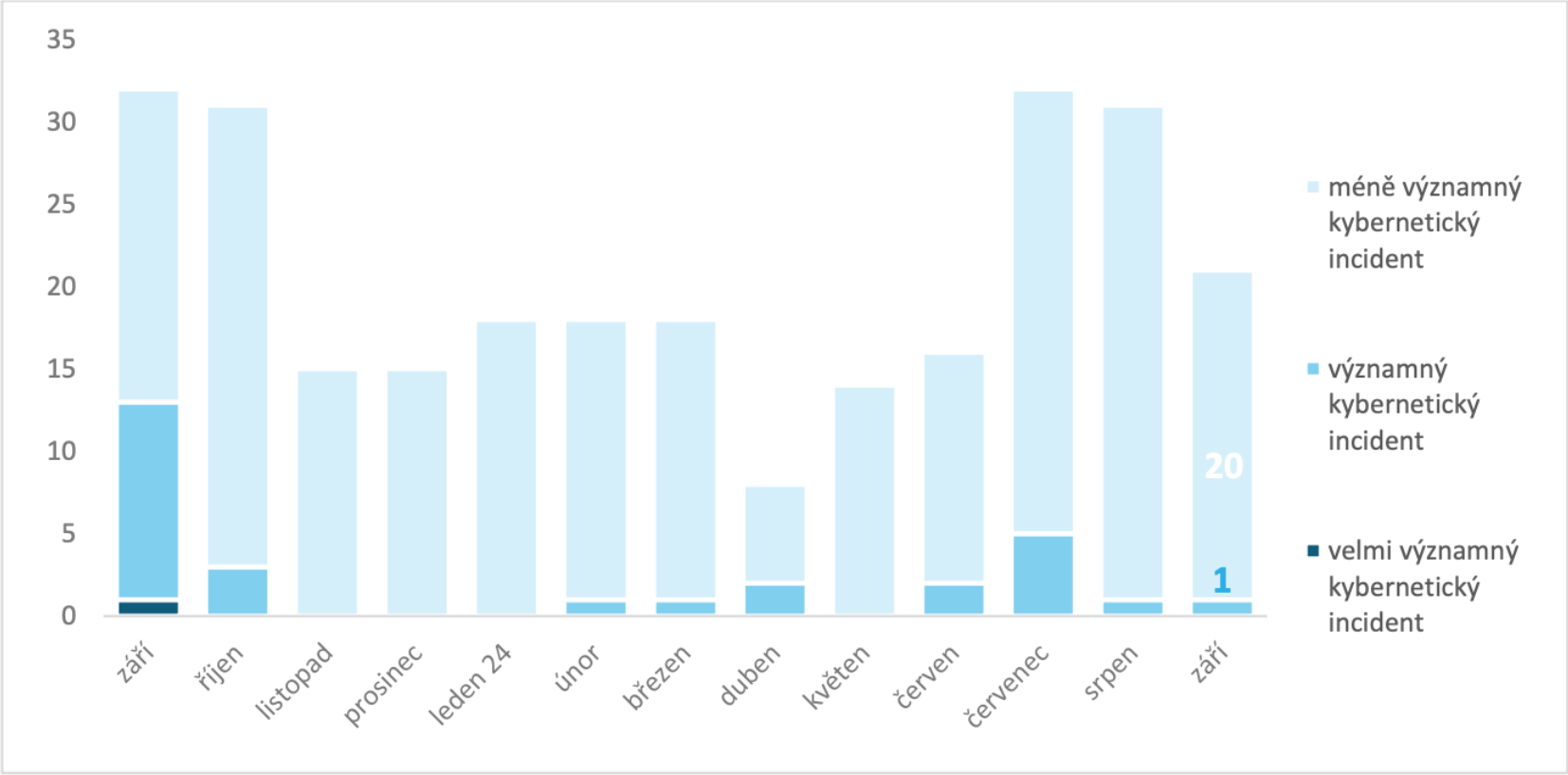


https://nukib.gov.cz/download/publikace/vyzkum/Kybernetticke-incidenty-pohledem-NUKIB-zari-2024.pdf

© Foresight Cyber Ltd, Page 8

Situace v Česku

NÚKIB – report září 2024

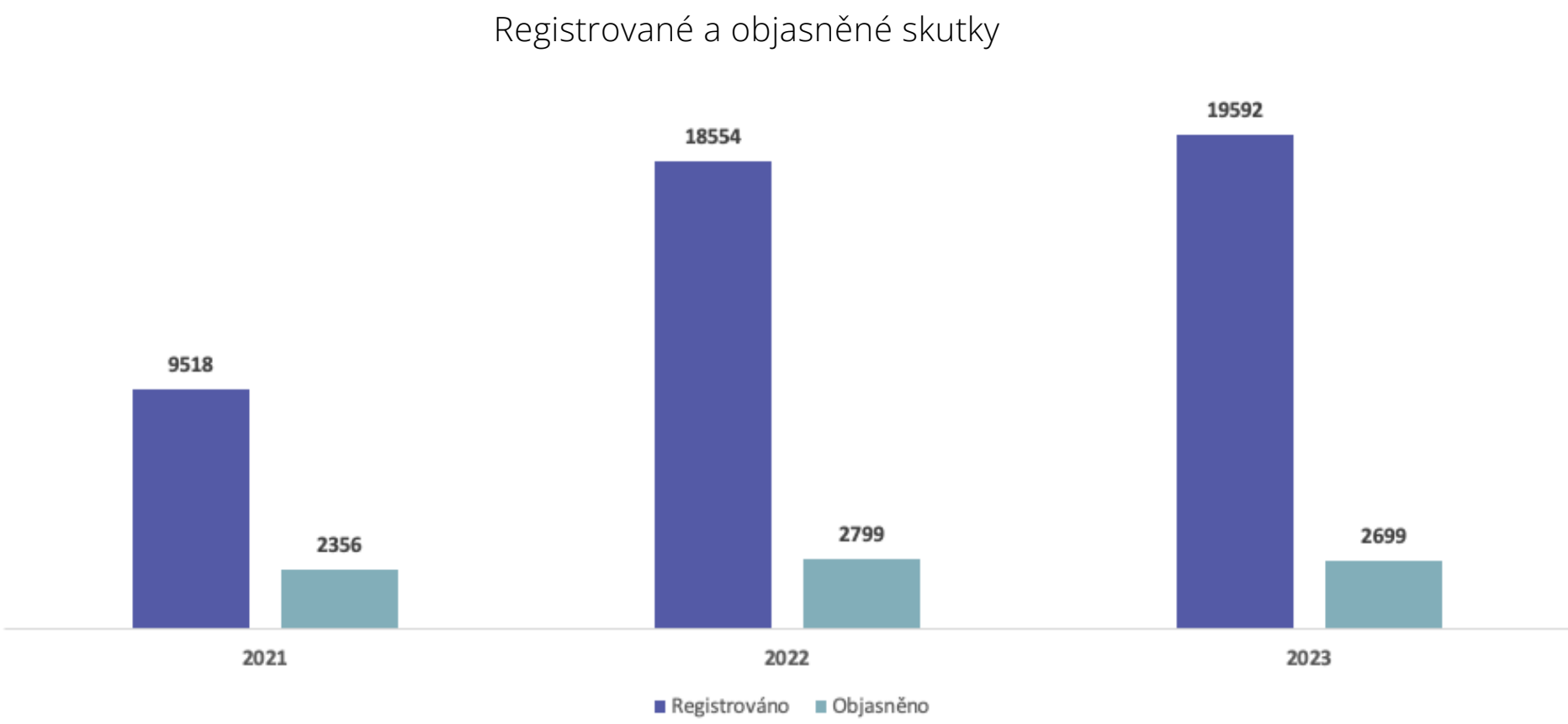


https://nukib.gov.cz/download/publikace/vyzkum/Kybernetticke-incidenty-pohledem-NUKIB-zari-2024.pdf

© Foresight Cyber Ltd, Page 9

Situace v Česku

Údaje Policie ČR

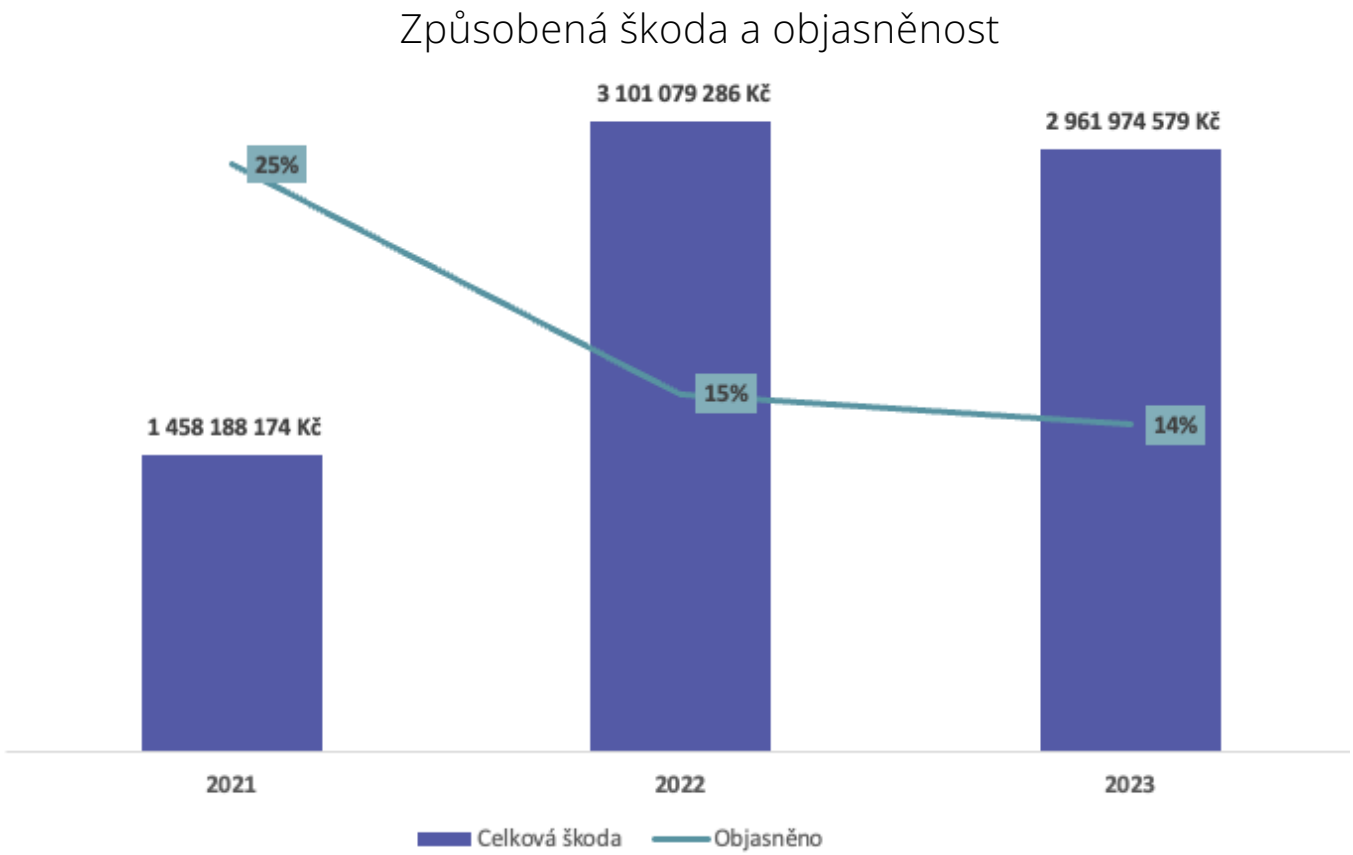


Data Policie ČR

© Foresight Cyber Ltd, Page 10

Situace v Česku

Údaje Policie ČR



Data Policie ČR

© Foresight Cyber Ltd, Page 11

Kam směřujeme

Rizika

Ztráta dat Cena za obnovu?

Nesoulad s normou Pravděpodobnost a velikost pokuty.

Ztráta reputace Ztráta klientů, poškození jména, značky.

Nedostupnost Ztráty během nedostupnosti.

Míra tolerance Správná kombinace tolerance, protiopatření a pojištění.

© Foresight Cyber Ltd, Page 12

FORESIGHT® CYBER

Kam směřujeme

Rizika – technická aktiva

© Foresight Cyber Ltd, Page 13

FORESIGHT® CYBER

Kam směřujeme

Rizika a hrozby

5 dnů
Externí

7 dnů
Interní

Doporučený interval nasazení záplat dle UK NCSC (*obdoba CZ NUKIB*)

30,6 dnů
Průměrná doba do nasazení oprav

19,5 dní
Pr. doba do aktivního zneužití

11,1
Okno pro exploit

Ohrožená aktiva

40% Bez aplikace oprav.

25% Exploitů do 24h po zveřejnění.

5% Zranitelností je rizikem.

FORESIGHT® CYBER

Data Qualys

© Foresight Cyber Ltd, Page 14

Kam směřujeme

Protiopatření – nekonečný cyklus

- Organizace nemají úplný a aktualizovaný seznam zařízení (CMDB).
- Bezpečnostní týmy se zaměřují na řešení zranitelností, které neredukují rizika.
- IT týmy nestíhají SLA pro vysoce rizikové zranitelnosti.
- Nejednotná komunikace rizik.
- Zbytečné vystavení se riziku.

© Foresight Cyber Ltd, Page 15

Foresight Cyber

Závěrečná doporučení

Protect & Identify – proaktivní přístup před bezpečnostní incidentem

- Nelze očekávat delegaci zodpovědnosti na IT oddělení.
- Každý zaměstnanec je nedílnou součástí bezpečnosti.
- Důvěra Vašich zákazníků – chráníte také jejich data.
- Odolnost vůči útokům – technická stránka, procesní a lidská.
- Kyberbezpečnost je výhodou, nikoli zátěží. Musí být základní hodnotou společnosti.

© Foresight Cyber Ltd, Page 16

FORESIGHT® CYBER

FORESIGHT®
CYBER

Kontaktujte mě

+420 603 902 414
kuba.safarik@foresightcyber.com

www.foresightcyber.cz