VNITŘNÍ BEZPEČNOST A ODOLNOST STÁTU II

Bezpečnostní incidenty: Jsme připraveni na moderní hrozby?

brig. gen. v.v. Mgr. David Dlouhý, Ph.D.
Policejní akademie České republiky v Praze

Praha 27. květen 2024

Demokratická republika

Tento příběh je smyšlený, avšak události jsou reálné.

Všechny tyto útoky se staly, avšak zatím ne všechny koordinovaně v jeden čas a na jednom místě.

- Jednoho chladného jarního rána v roce 2024 se Demokratická republika probudila do technologického chaosu.
- Klíčové vládní systémy byly paralyzovány rozsáhlým kybernetickým útokem.
- Veřejné služby byly nefunkční, nemocnice nemohly přistupovat ke zdravotním záznamům, finanční systémy byly ochromeny a vládní webové stránky byly vyřazeny z provozu. Ty, které fungovaly zobrazovaly narativ o erupci na slunci.
- Panika se rychle šířila mezi obyvateli, kteří zjistili, že nemohou používat bankomaty ani platit kreditními kartami. Mobilní telefony, IoT a další elektronická zařízení nefungovala, jak by si lidé přáli.

Útoky na: SolarWinds celosvětově (2020), NotPetya Ukrajina-celosvětově (2017), úřad pro řízení personálu USA (2015), Fakultní nemocnice Brno (2020), zdravotnické systémy v USA (2020), televize LRT Litva(2019), novinářské účty Litva (2021), zpravodajský web DELFI Litva (2017)…

Útok

- Útok začal ve 3:00 ráno, kdy tým elitních útočníků z autoritářské země zahájil koordinovaný útok.
- Informace o útoku byla obratem rozeslána všem kybernetickým bezpečnostním manažerům, avšak jen k pár z nich se zpráva skutečně dostala.
- Útočníci získali seznam všech bezpečnostních manažerů v zemi již několik měsíců zpátky, a to díky úniku z napadeného účtu managera v úřadu pro kontrolu kyber-bezpečnosti.
- Útok byl pečlivě naplánován a zahrnoval několik fází.

Útoky na: Bangladesh Bank Indie (2016), Seimas Litva (2017), novinářské účty Litva (2021), únik informací o bezpečnostních správcích IT Litva (2019), Pegasus Spyware Izrael-celosvětově (2016), Simjacker Attack Irsko-celosvětově (2019), BlueBorne Attack USA-celosvětově (2017), HummingBad USA-celosvětově (2016), Triada Malware (Android) USA-celosvětově (2016), WireLurker (iOS), XcodeGhost (iOS) Čína-celosvětově (2015), Stagefright Vulnerability (Android) USA-celosvětově (2015)…

Fáze 1

- Zaměřena na proniknutí do nejcitlivějších vládních systémů. Útočníci využili sofistikovaných phishingových kampaní a zero-day exploitů, aby získali přístup k interním sítím. Jakmile se dostali dovnitř, začali šířit ransomware, který šifroval data na klíčových serverech.
- Útočníci se zaměřili na získání vzdáleného ovládání všech zařízení, ke kterým mají manageři KB přístup.
  - Část jich přestala dostávat upozornění a všechna jejich technika přestala reagovat, avšak tak, aby to co možná nejvíce nebylo poznat.
  - Část jich byla zamčena ve elektro vozidlech nebo jiným způsobem zneškodněna, aby se nedostali k funkční technologii a nemohli zajistit svou povinnost.

Útok na: Tesla Model S (2016), Nissan Leaf (2016), nabíjecí stanice (2020), flotilu elektrických vozidel - Pen Test Partners (2021), Kia a Hyundai (2022), Tencent Keen Security Lab - BMW, Audi a další (2018), Jeep Cherokee (2015), Renault Zoe (2021), VW Golf GTE (2020), Positive Technologies – útok na elektromobily prostřednictvím aplikací pro chytré telefony (2019), Subaru (2020), Volkswagen (2020), Mercedes-Benz (2020), automatické myčky aut (2017), systém MTA (New York, 2020), San Francisco MUNI (2016), letiště v Bristolu (2018), British Airways (2018), systém železniční dopravy Deutsche Bahn (2017), semafory v Los Angeles (2006), Maersk (2017), FedEx (2017)…

Fáze 2

- Druhá fáze útoku byla zaměřena na narušení komunikace. Útočníci použil DDoS útoky (Distributed Denial of Service) k přetížení vládních a mediálních webových stránek, což způsobilo, že se staly nedostupnými.
- Útočníci infiltrovali sociální média a šířili dezinformace, které vyvolávaly strach a zmatek mezi obyvatelstvem.

Útoky na: Dyn DNS (2016), společnost Cloudflare (2020), Estonsko (2007), GitHub (2018), Spamhaus (2013), BBC (2015), Bank of America (2012), The New York Times a Twitter (2013), KrebsOnSecurity (2016), Telegram (2019)…

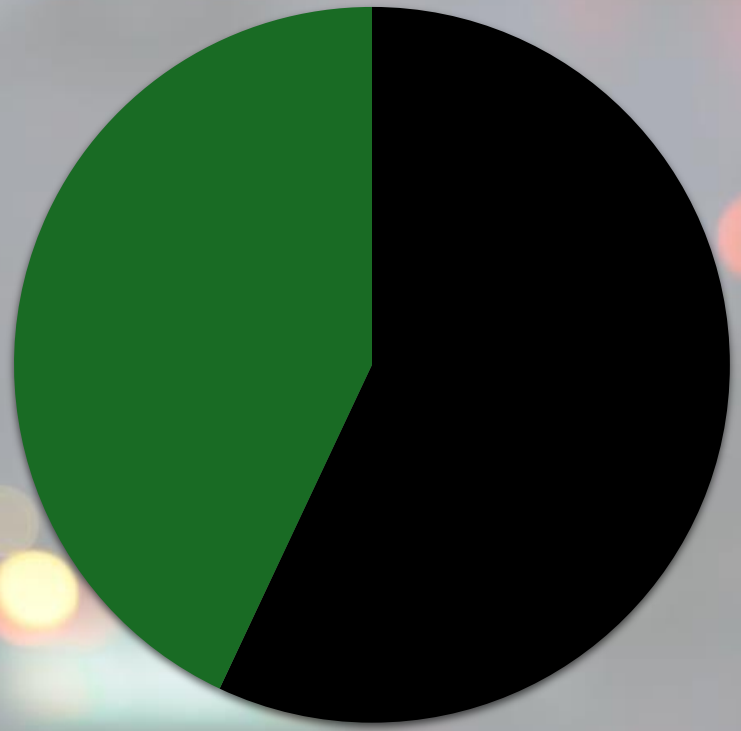
Fáze 3

- Třetí a závěrečná fáze útoku se soustředila na kritickou infrastrukturu.
- Útočníci napadli energetickou síť a způsobili výpadky elektřiny v hlavních městech Demokratické republiky.
- Byli schopni infiltrovat i vodárenské systémy a ohrozit dodávky pitné vody.
- Proběhl i úspěšný útok na společnost zajišťující dopravu pohonných hmot.

Útoky na: Stuxnet (2010), Colonial Pipeline (2021), vodní zdroje v USA (2021), Ukrajinskou elektrickou síť (2015), Saudi Aramco (2012), vodárnu ve Floridě (2021), hydroelektrárnu v New Yorku (2020), Irskou zdravotní službu HSE (2021), elektrárnu v Indii (2020), elektrárnu v Íránu (2020), Ukrajinskou telekomunikační síť (2015)...

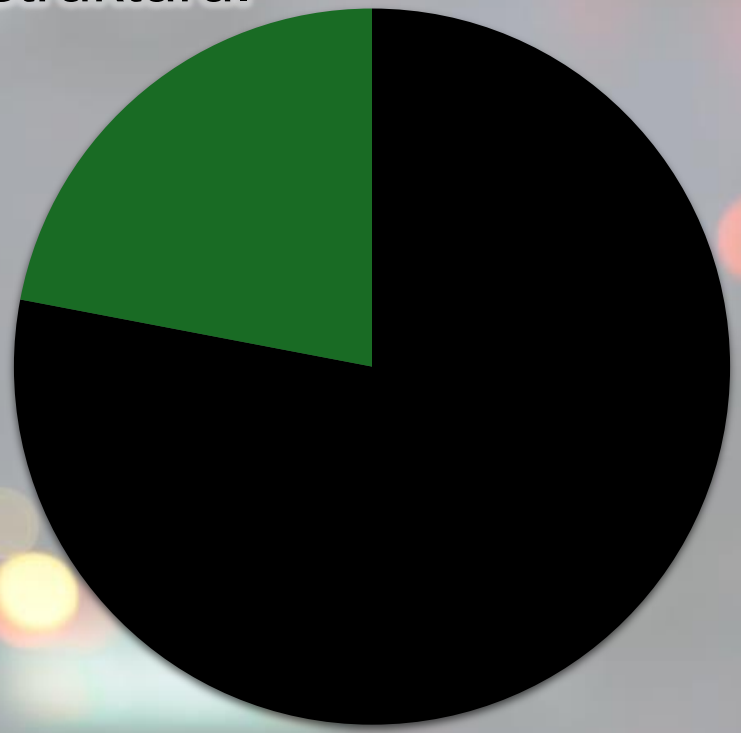
57% zařízení na světě je zneužitelných více než 10 známými zranitelnostmi dle CVE

CVE (Common Vulnerabilities and Exposures) je seznam veřejně známých kybernetických zranitelností obsahuje jich přes 233 tis.



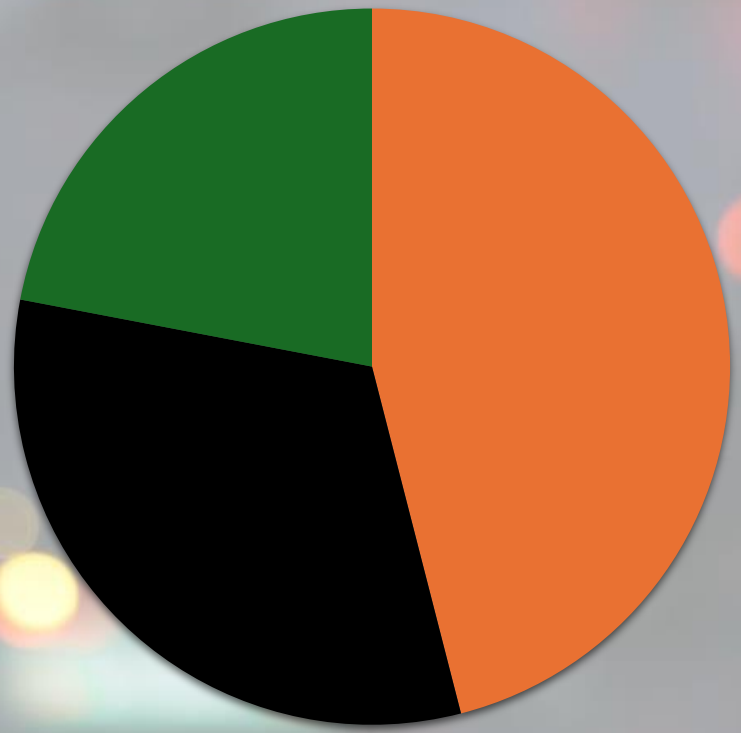
78% IoT zařízení mají známé zranitelnosti

Internet věcí (Internet of Things, IoT) je koncept, který označuje propojení běžných fyzických zařízení k internetu, což jim umožňuje komunikovat, sbírat data a provádět určité úkony autonomně. IoT zahrnuje širokou škálu zařízení, od chytrých domácích spotřebičů a nositelných technologií po průmyslové stroje a infrastrukturu.



46% z nich nelze opravit

Firmware zařízení nelze změnit je již nepodporovaný.
Zdroj: Microsoft Defender for IoT and aDolus Technology



Závěr

- **Nelze vyloučit okamžik, kdy všechny útoky proběhnou organizovaně v jeden čas a na jednom místě.**
- Všechny tyto útoky spojuje skutečný dopad na každého člověka v místě a času působení.
- **Je důležité uplatňovat přístup „secure by design“, od nejmenších IoT zařízení až po velké SCADA systémy.**
  - **Secure by design je koncept, který se zaměřuje na zajištění bezpečnosti IT již v době návrhu a vývoje.**
- V minulosti incident Stuxnet ukázal, že odpojení softwaru a hardwaru od společného kybernetického prostoru nelze považovat za zaručené řešení pro dosažení 100% bezpečnosti neaktuálních a nepromyšlených systémů již od jejich prvotního návrhu.
- **V soukromém sektoru jsou využívány technologie, které nejsou moderovány nařízeními a které budou mít dopad na kritickou infrastrukturu, neboť nelze oddělit pracovní nástroje od soukromých ve chvíli, kdy sdílejí společný kybernetický prostor.**

Děkuji Vám za pozornost

brig. gen. v.v. Mgr. David Dlouhý, Ph.D.
Policejní akademie České republiky v Praze

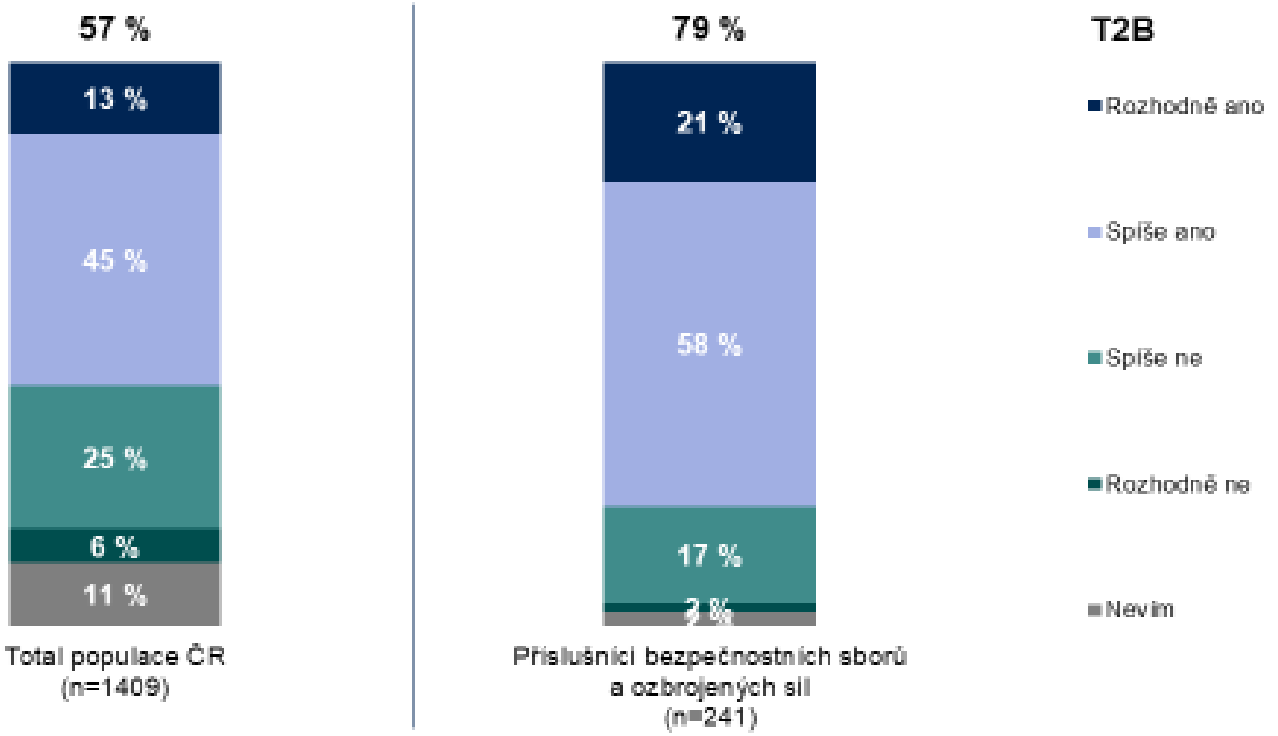
Lhotecká 559/7
Praha 4
Tel. 974 828 501

Vybrané výsledky výzkumu 2023

(porovnání dat populace ČR vs. příslušníci bezpečnostních sborů a ozbrojených sil)

PŘÍSTUP K POCHYBNÝM INFORMACÍM

Příslušníci bezpečnostních sborů a ozbrojených sil mají častěji potřebu zjistit, zda informace, která v nich vyvolává pochybnost, je pravdivá, či nikoli.



SOCIODEMOGRAFICKÝ DETAIL

- Muži obecně častěji než ženy si u podezřelých informací zjišťují, zdali jsou pravdivé, či nikoli.

Otázka: Z4. Když se střetnete s informací, která u Vás vyvolá pochybnost, máte obvykle potřebu zjistit, zda je pravdivá či nikoli?
Pozn.: T2B = součet hodnot „Rozhodně ano" + „Spíše ano"

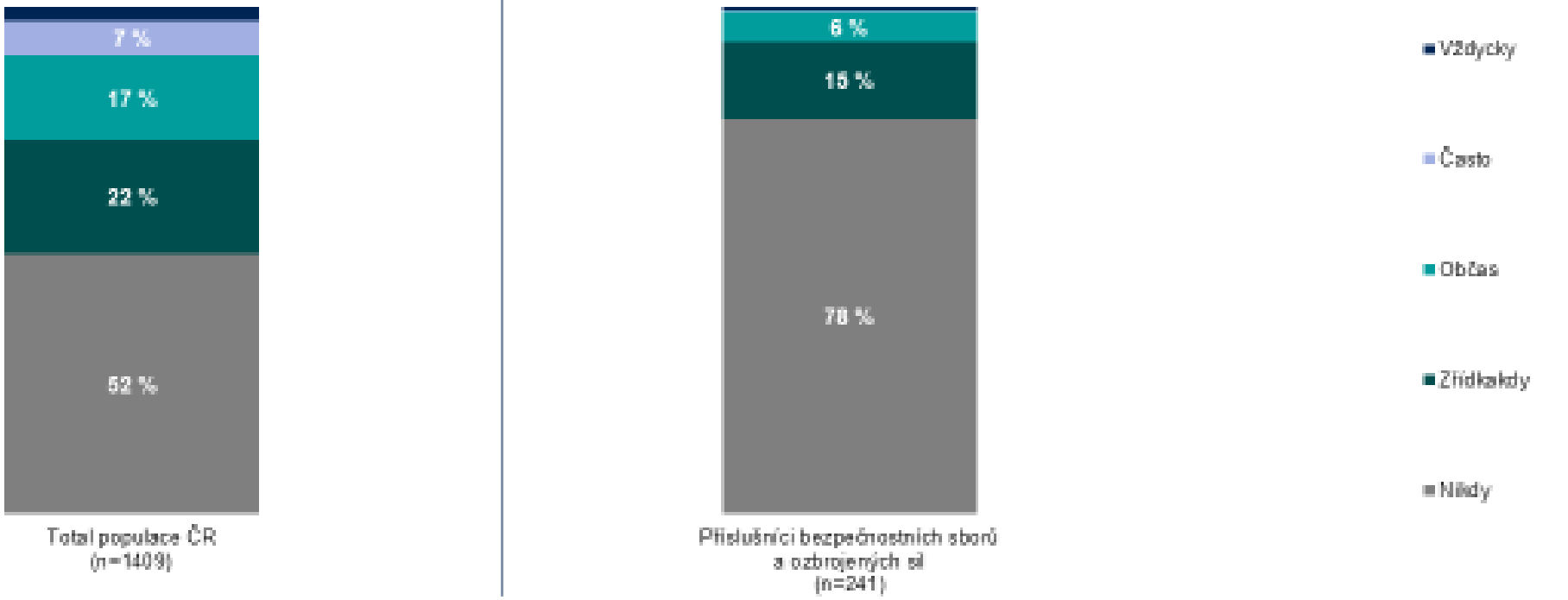
Vybrané výsledky výzkumu 2023

(porovnání dat populace ČR vs. příslušníci bezpečnostních sborů a ozbrojených sil)

PŘÍSTUP K POTENCIÁLNÍM DEZINFORMACÍM

Příslušnici bezpečnostních sborů a ozbrojených sil v porovnání s populací ČR častěji nikdy nešíří informaci, u které mají podezření, že se může jednat o dezinformaci, a to i v případech, kdy je zaujme nebo odpovídá jejich pohledu na svět.

Pokud mě zaujme nebo když odpovídá mému pohledu na svět, šířím ji dál, i když může jít o dezinformaci.



Otázka: Z3a. Co obvykle děláte s informací, u které máte podezření, že může jít o dezinformaci?