Sme malá firma, nás sa to netýka

Andrej Eliáš
andrej.elias@nbu.gov.sk

Firma a jej

SecureMail

Andrej Dzizi

- aktuálna
- vo štvrtok
  - zrani
  - v piat
- v piatok p
- sobota - a
- nedeľa - u
- pondelok

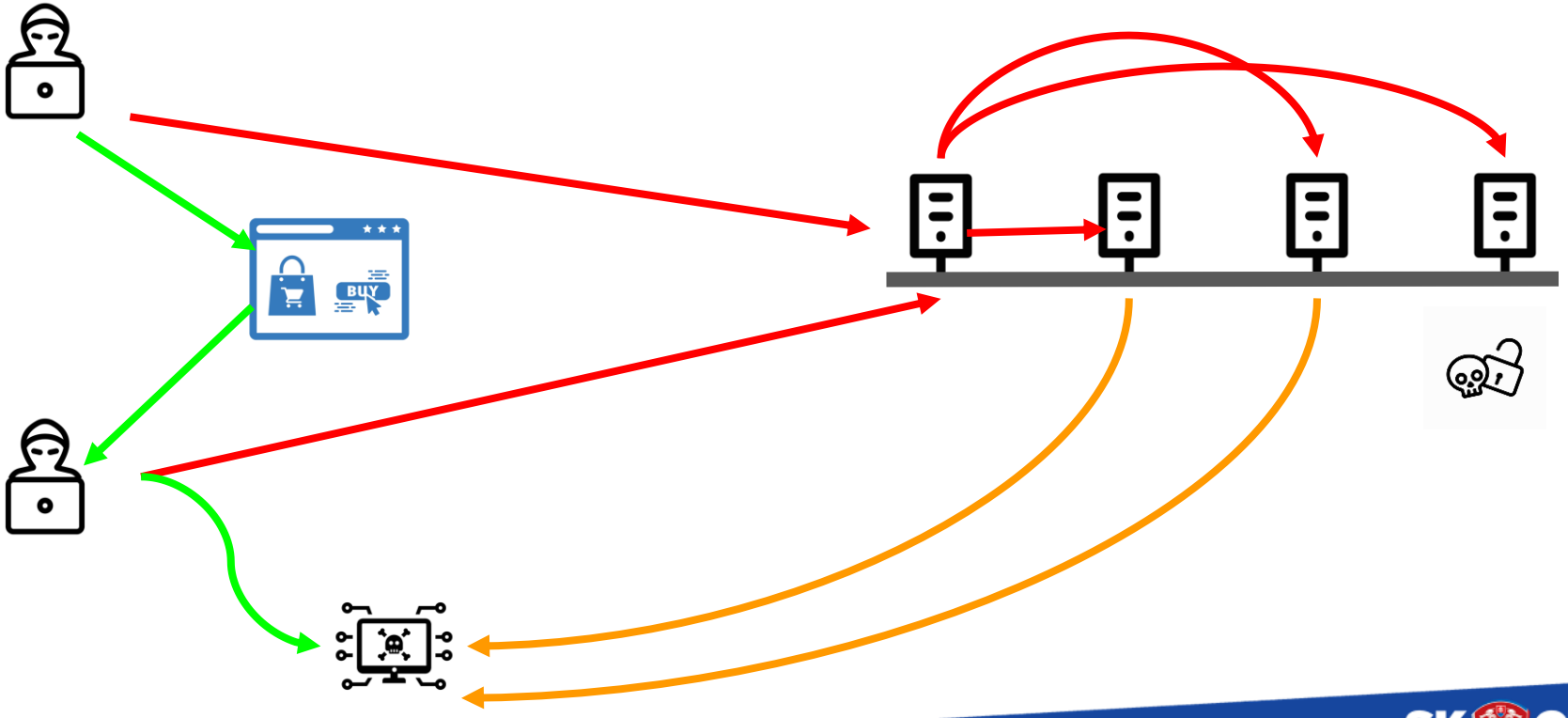
.12

ntifikácie

eniami



Čo sa stalo?



Čo sa ešte môže stať?

Nemusia šifrovať
Perzistencia
Spear-phishing voči firme
Spear-phishing voči klientom
Supply Chain Attack
Proxy
Admin nainštaluje aktualizáciu na Webmail 3.12

Stále si myslíte že nemáte nič zaujímavé a práve vás sa to netýka?

Čo môžem urobiť už teraz?

Hope for the best, but prepare for the worst...

Stať sa môže čokoľvek:

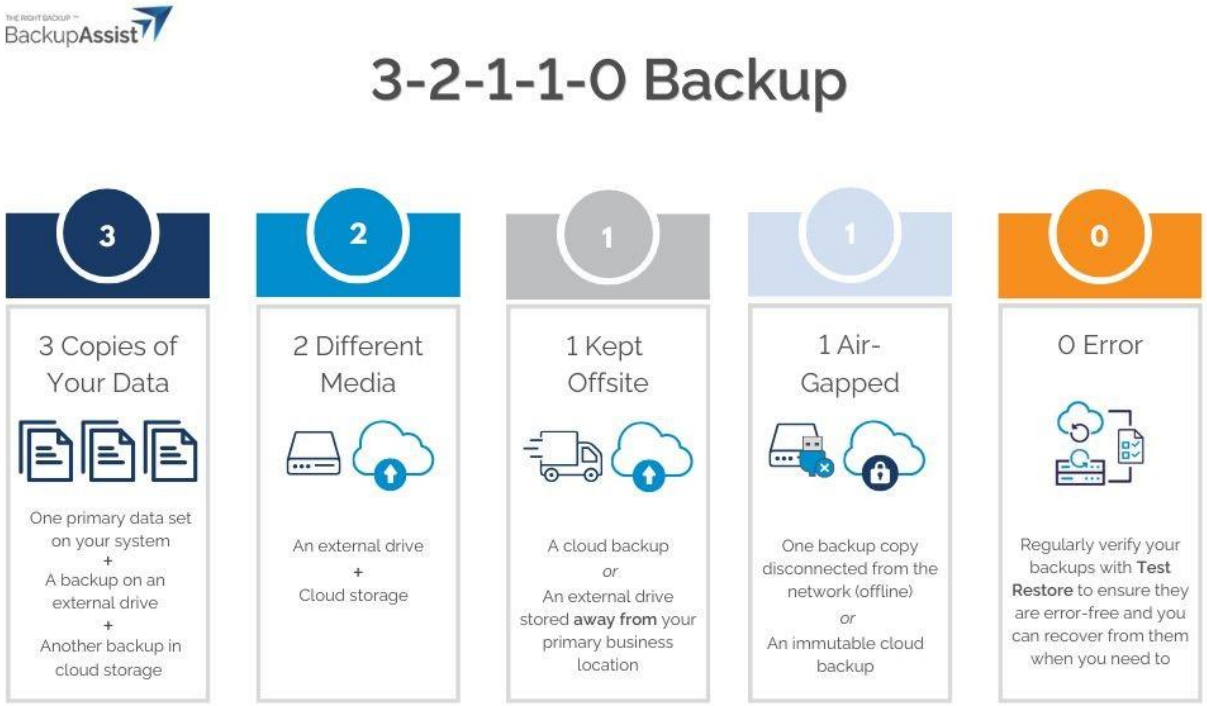
- hack,
- malvér,
- ransomvér,
- zlyhanie hardvéru,
- poškodenie súborového systému.

Buďte pripravení.

Zálohovanie

Mám zálohovanie v takom stave že viem kedykoľvek obnoviť svoju infraštruktúru?
Mám zálohy dostatočne zabezpečené pred poškodením/vymazaním? 3-2-1
Zálohovací softvér sa optimálne pripája na servery, ktoré zálohuje, kontroluje zmeny a zálohuje potrebné súbory.
Dôležitosť systému sa prejaví najčastejšie vtedy keď zlyhá

Zálohovacia stratégia 32110



Zdroj: https://d1pxskmyx0hart.cloudfront.net/app/uploads/sites/3/2024/10/3-2-1-1-0-Backup.jpg?x99680

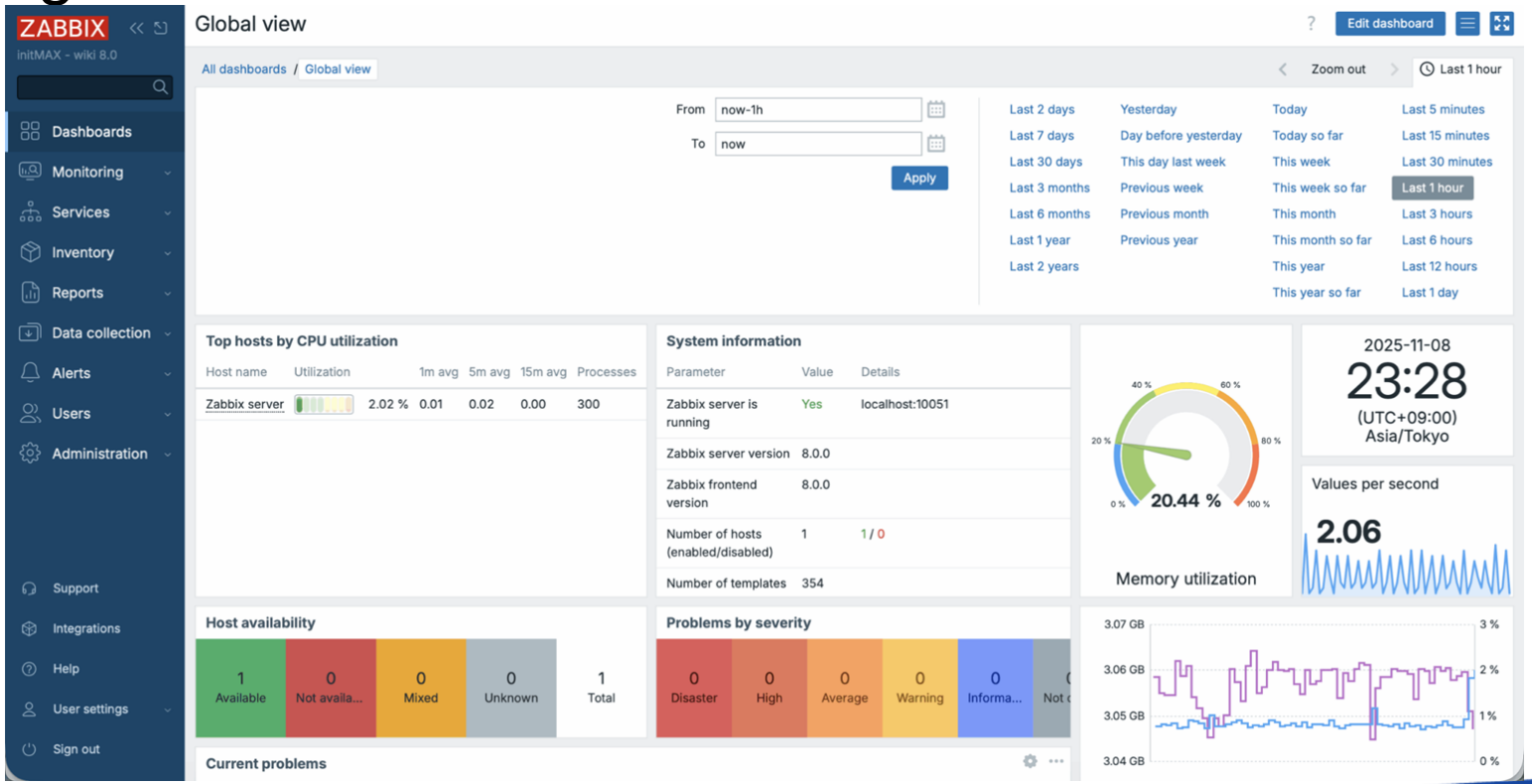
Logovanie

Logovanie by malo byť presmerované na externý, samostatný logovací server, nezaradený do domény (AD) s unikátnymi prihlasovacími údajmi.

Presmerujte aj logovanie z aktívnych prvkov - routre, switche, NAS, a pod.

Monitoring

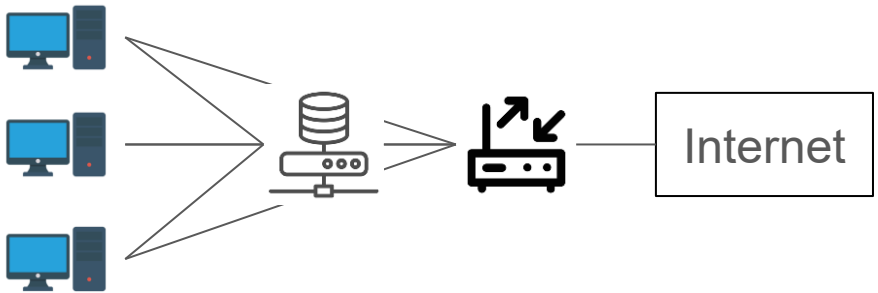
Prehľad
Varovania
Alarmy



Zdroj: https://www.initmax.com/wp-content/uploads/2025/11/setup-8.0lts8-scaled.png

Proxy a DNS

Úžasná vec na získanie viditeľnosti toho čo sa deje vo vašej sieti.
Pri bežnej office práci vás webové proxy nijako neobmedzuje.
Skvelé tiež na blokovanie prístupov na škodlivé webstránky (aspoň tie známe).
SSL/TLS inšpekcia.
Lokálne DNS.





Zdroj: https://www.techaddressed.com/wp-content/uploads/2022/04/pihole-dashboard.webp

Update, upgrade

Nezabúdať…
Všetko "vystrčené" do internetu je kritické, ale... ak je útočník už v sieti, všetko sa stáva kritickým.
Dnešné AI asistované útoky nás nútia predpokladať že útočník je už tam…

Znížiť attack surface

VPN

- Množstvo voľne dostupných VPN pre vlastnú inštaláciu.
- Opäť level bezpečnosti prakticky zadarmo…

Vyraďovanie / Decommisioning

- Ak to už nepotrebujem, odzálohovať, odpojiť, vypnúť.

Firewall

Perimeter firewall.
Buďme paranoidní aj voči spojeniam zvnútra.
Never trust, always verify! Zero trust…
Host firewall.
Pravidlá, pravidlá, pravidlá.

Procesy

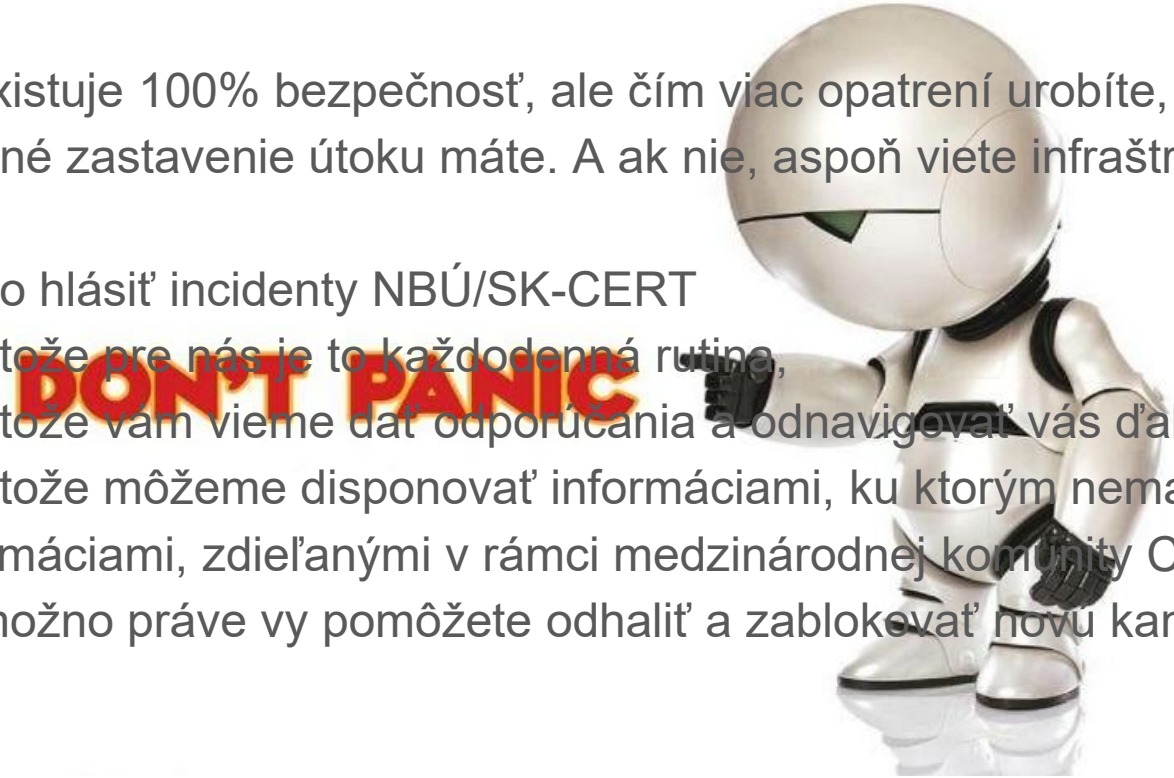
Audit prístupov
- už neexistujúci zamestnanci
- zabudnuté VPN pre dodávateľov

Disaster recovery plans
- automatizácia inštalácie serverov
- automatizovaný healthcheck

Vzdelávanie
- phishing, správa hesiel, komplexnosť hesiel,...
- cybergame

Čo môžem urobiť keď zistím že mám škodnú?

Neexistuje 100% bezpečnosť, ale čím viac opatrení urobíte, tým väčšiu šancu na včasné zastavenie útoku máte. A ak nie, aspoň viete infraštruktúru rýchlo obnoviť.



Prečo hlásiť incidenty NBÚ/SK-CERT
- pretože pre nás je to každodenná rutina,
- pretože vám vieme dať odporúčania a odnavigovať vás ďalšími krokmi,
- pretože môžeme disponovať informáciami, ku ktorým nemá verejnosť prístup. Informáciami, zdieľanými v rámci medzinárodnej komunity CSIRTov,
- a možno práve vy pomôžete odhaliť a zablokovať novú kampaň…

Zdroj: https://borngeekblog.com/wp-content/uploads/2015/09/dont-panic-775x480.jpg

69/2018 Z. z. Zákon o kybernetickej bezpečnosti

§ 12 Mlčanlivosť a ochrana osobných údajov

(1) Kto plní alebo plnil úlohy na základe tohto zákona alebo v súvislosti s ním, je povinný zachovávať mlčanlivosť o skutočnostiach, o ktorých sa v súvislosti s plnením úloh podľa tohto zákona dozvedel a ktoré nie sú verejne známe. Povinnosť zachovávať mlčanlivosť trvá aj po skončení dohody o spolupráci podľa § 5 ods. 3, pracovnoprávneho vzťahu alebo obdobného pracovného vzťahu vrátane služobného pomeru.[14]) Ustanoveniami o povinnosti zachovávať mlčanlivosť podľa tohto zákona nie je dotknutá povinnosť mlčanlivosti alebo zachovania tajomstva podľa osobitných predpisov.

Vyhláška NBÚ 227/2025 Z. z. o bezpečnostných opatreniach

AI

Oheň je dobrý sluha ale zlý pán…
AI je ako oheň.
AI je skvelé, ale:

- spochybňujme,
- preverujme,
- buďme kritickí,
- nezabudnime rozmýšľať,
- nezdieľajme to čo nechceme,
- opatrne s agentmi, v snahe vyhovieť dokážu napáchať veľa zlého.