iDEME 2026 · 21. mája 2026 · Bratislava

# Hackerovi je jedno, aká veľká je vaša obec.

Ján Kratka · Riaditeľ divízie IT služieb, infraštruktúry a kybernetickej bezpečnosti

synchronix.sk | info@synchronix.sk | +421 238 100 014

**1 842 útokov**
**týždenne**
**na jednu slovenskú organizáciu**

**+27 %**
**medziročne**

# SLOVENSKO OČAMI ÚTOČNÍKA

## Toto vidí útočník skôr, než vidí vás.

Prieskum verejne dostupnej infraštruktúry je prvý krok každého cieleného útoku. Trvá hodiny, vyžaduje nulové oprávnenie a v sieti obete sa nezobrazí.

- **1 822 vzdialených prístupov** dostupných z internetu najčastejší vstupný vektor ransomware útokov.
- **405 mailových serverov** s neopravenými zraniteľnosťami.
- **340 priemyselných riadiacich systémov** vystavených bez ochrany - riadia fabriky, čerpadlá, energetiku.

# VEĽKOSŤ CIEĽA NIE JE DÔLEŽITÁ

## Dôležité je, k čomu má cieľ prístup.

- **Stanica vo Vrútkach -** vstupný bod do systémov centrály
- **Pobočka úradu -** vstupný bod do systémov ministerstva
- **Externý dodávateľ s VPN -** vstupný bod do vášho systému
- **2 890 obcí pripojených na ÚPVS -** 2 890 vstupných bodov do registrov štátu

Perimeter vašej organizácie nekončí vašim firewallom.
Končí tam, kde končí prístup posledného dodávateľa.

synchronix.sk | info@synchronix.sk | +421 238 100 014

**48%**
**úspešných útokov**
**v 2025 zahŕňalo tretiu stranu**

**+60 %**
**medziročný nárast supply chain útokov**

**88 %**
**organizácií**
**nepravidelne audituje dodávateľské prístupy**

**207 dní**
**je priemerný čas detekcie útoku cez tretiu stranu**

# BÝVALÝ ZAMESTNANEC. AKTÍVNA VPN.

## Reálny prípad, ktorý som riešil v praxi.

- Externý dodávateľ poskytoval IT službu výrobnému podniku
- Zamestnanec dodávateľa odišiel - VPN účet ostal aktívny
- Účet patril dodávateľovi, audit nad ním mal dodávateľ
- 8 mesiacov bez kontroly z oboch strán
- Cez VPN vstúpil útočník.
- Zašifrované dáta. Zastavená prevádzka aj výroba.

# KB NIE JE PRODUKT

## Aj keď máte všetko, čo máte mať - bezpečnosť tým ešte stále nemáte.

- **Máte audit. ISO certifikát. Súlad so zákonom.** Audit ukáže, čo máte na papieri. Neukáže, či to v praxi reálne funguje. A útočník nepozerá na váš certifikát.
- **Máte drahé bezpečnostné systémy. SOC. Firewally. EDR.** Technológia rieši to, čo pozná. Útočník prichádza s tým, čo technológia ešte nepozná.
- **Máte politiky. Procesy. Dokumentáciu.** Smernice, ktoré nikto nečíta, nezachránia nikoho. Otázka je, či ich niekto reálne dodržiava - a či to niekto kontroluje.

**60 %**
**prienikov**
**v 2025 zahŕňalo ľudský faktor**

**8 %**
**zamestnancov**
**spôsobuje 80 % incidentov**

synchronix.sk | info@synchronix.sk | +421 238 100 014

**8 hodín**
**v 2022.**
**22 sekúnd**
**v 2025.**

**Tak rýchlo dnes útočník predá váš prístup ďalej**

# ANATÓMIA MODERNÉHO ÚTOKU

## Útoky v 2025 nie sú útoky z 2015.

**1. Prieskum.** Verejne dostupné data. Útočník sa nedotkne vašej siete. Trvá týždne.

**2. Vstup.** Cielený phishing. Dodávateľ. Slabé heslo. Trvá hodiny.

**3. Laterálny pohyb.** Z bežného účtu k privilegovanému. Z jedného segmentu siete do druhého. Trvá mesiace.

**4. Exfiltrácia.** Dáta odchádzajú v malých dávkach. Trvá týždne až mesiace.

**5. Ransomware (voliteľne).**

Bežná ochrana zachytí piaty krok.
Útok sa rozhodol v prvom.

# ČO TREBA INAK.

## Technológiu si kúpite. Bezpečnosť nie. Tú treba urobiť.

**1. Ľudia, ktorí poznajú útok skôr, než príde.** Pravidelné školenia. Simulácie phishingu. *Útok začína u človeka. Tam má začať aj obrana.*

**2. Procesy, ktoré sa reálne dodržiavajú.** Patche, MFA, offboarding, audit prístupov, segmentácia. Otázka je, či ich niekto reálne robí. *A niekto kontroluje, že to robí dobre.*

**3. Cvičenia, kde sa neohrozí produkcia.** Tabletop simulácie. Hraný scenár ransomware útoku. Tri hodiny, ktoré vám ukážu, čo nemáte pripravené. *Kým máte ešte čas.*

**4. Niekto, koho zavoláte pred problémom, nie po ňom.** Konzultácia pred zavedením nového systému. Druhý pohľad na zmluvu s dodávateľom. *Vždy lacnejšie než riešiť následky.*

synchronix.sk | info@synchronix.sk | +421 238 100 014

**z 33 % na 4 % kliknutí**
**na podvodný email po roku pravidelných školení**

**47 % organizácií**
**nemá pravidelný bezpečnostný tréning**

**32 rokov**
**v IT službách a infraštruktúre.**

**50+**
**odborníkov**

# SYNCHRONIX.

## Nepredávame krabice.
## Nemáme jedno riešenie pre všetkých.
## Máme riešenie pre vás.

- **Bezpečnostné školenia a simulácie**
- **Tabletop cvičenia**
- **Poradenstvo a konzultácie**
- **Governance, risk & compliance**
- **Bezpečnostné audity**

## Ako pracujeme

Každá organizácia je iná. Aj jej riziká.
Začíname tým, čo už máte. Pozeráme, čo funguje a čo nie.
Doplníme to, čo treba.

synchronix.sk | info@synchronix.sk | +421 238 100 014

# HACKEROVI JE JEDNO, AKÁ VEĽKÁ JE VAŠA OBEC. VÁM BY TO JEDNO BYŤ NEMALO.

Útočníkovi nezáleží na vašej veľkosti.
Záleží mu na ceste, ktorá k vám vedie.
A tá cesta dnes vedie cez váš dodávateľský reťazec.

Bezpečnosť sa nezačína v centre.
Začína sa na okraji.



# ĎAKUJEM

SYNCHRONIX
Ján Kratka
0917 511 579
jan.kratka@synchronix.sk