

ČO ROBIŤ, KEĎ VAŠU FIRMU ZASIAHNE KYBERNETICKÝ ÚTOK

Praktický plán od prvého podozrenia po bezpečný návrat do prevádzky

LiveTalk by T Business | diel #3 | 10. 09. 2026

Bezpečnosť neznamená, že sa firme nikdy nič nestane. Znamená, že dokáže incident včas rozpoznať, udržať si kontrolu, obnoviť fungovanie a poučiť sa. Tento checklist, ktorý vznikol na základe LiveTalku s Tomášom Masným, CISO Slovak Telekom a T-Mobile Czech Republic, vám pomôže overiť, či je firma pripravená a ukáže vám, ako postupovať počas prvých 60 minút incidentu.

PRED INCIDENTOM MUSÍ BYŤ JASNÉ

- ☐ **COMMAND** – kto je Incident Commander a jeho zástupca
- ☐ **ACCESS** – viacfaktorové overovanie (MFA) na kritických a administrátorských prístupoch
- ☐ **RECOVERY** – obnova zo zálohy bola úspešne otestovaná
- ☐ **SUPPLIER** – kontakt na kritického IT dodávateľa pre prípad incidentu
- ☐ **COMMUNICATION** – vieme, kto komunikuje navonok
- ☐ **LEGAL** – kto posúdi oznamovaciu povinnosť
- ☐ **PRACTICE** – vedenie si prešlo jeden „zlý deň“ nanečisto

PRVÝCH 60 MINÚT

1. KTO VELÍ?

Potvrďte Incident Commandera. Jedno miesto koordinácie a rozhodovania.

2. OBMEDZTE ĎALŠIU ŠKODU.

Izolujte zasiahnuté systémy od siete. Svojevoľne ich nevypínajte.

3. ZACHOVAJTE DŮKAZY.

Nemažte ani neprepisujte logy. Neinštalujte nový softvér a nezačínajte s obnovou bez koordinácie s IT alebo IR expertom.

4. ČO VIEME – A ČO EŠTE NEVIEME?

Rozhodujte podľa dostupných faktov. Nečakajte na dokonalý obraz, ale jasne odlišujte potvrdené informácie od predpokladov.

5. KOMUNIKUJTE JEDNÝM KOORDINOVANÝM HLASOM.

Fakty, žiadne špekulácie. Povedzte, čo viete, čo ešte overujete, čo robíte a kedy poskytnete ďalšiu aktualizáciu.

6. OVERTE OZNAMOVACIU POVINNOSŤ.

Zapojte právnika alebo zodpovednú osobu. Overte, či, komu a dokedy treba incident oznámiť.

7. NAJPRV ZATVORTE DVERE.

Pred návratom do bežnej prevádzky overte, že bola odstránená cesta, ktorou sa útočník dostal dnu, a že už nemá prístup. Až potom bezpečne obnovujte systémy.

SLUŽBA BEŽÍ ≠ INCIDENT JE VYRIEŠENÝ

7 BODOV, KTORÉ POSUNÚ FIRMU K VÄČŠEJ ODOLNOSTI

1 VIEME, ČO MUSÍ FUNGOVAŤ, ABY FIRMA PREŽILA?

Ktoré tri služby alebo systémy sú pre fungovanie firmy kritické – a kedy sme naposledy dokázali ich reálnu obnovu?

Záloha nie je odolnosť. Rozhoduje schopnosť obnoviť fungovanie firmy.

2 PRVÝCH 60 MINÚT: VIEME, ČO UROBÍME?

Kto velí? Komu voláme? Čo zastavíme alebo izolujeme? Ako bude pokračovať fungovanie firmy? Kto komunikuje?

Prvých 60 minút nie je čas na tvorbu procesu. Je to čas na jeho použitie. Dobrý Incident Commander neriadi technológiu. Riadi rozhodovanie v chaose.

3 VIEME, KDE MÁ FIRMA OTVORENÉ DVERE?

Aká je dnes najjednoduchšia cesta do firmy? Identita, privilegovaný účet, zraniteľnosť, externista alebo dodávateľ?

Útočník sa nepýta iba na veľkosť firmy. Hľadá cestu s najmenším odporom a ak môže, vojde potichu.

4 VIEME, AKO JE FIRMA PREPOJENÁ S RIZIKOM ZÁKAZNÍKOV A DODÁVATEĽOV?

ZÁKAZNÍK ← NAŠA FIRMA ← DODÁVATEĽ. Komu poskytujeme kritickú službu? Ktorí dodávatelia majú prístup k našim systémom, dátam alebo prevádzke?

Outsourcovať môžete službu. Zodpovednosť za kontinuitu fungovania firmy nie.

5 KEĎ FIRMA ZRÝCHĽUJE, ZRÝCHĽUJE S ŇOU AJ KONTROLA?

AI, cloud a automatizácia umožňujú robiť viac a rýchlejšie. Dokážeme rovnako rýchlo overovať výsledok?

AI nám nerozbila bezpečnosť. Predbehla našu schopnosť overovať. Ak zrýchľuje fungovanie firmy, musí s ňou zrýchľovať aj kontrola.

6 DOSTANE SA ZLÝ SIGNÁL K SPRÁVNEMU ČLOVEKU DOSTATOČNE RÝCHLO?

Keď človek urobí chybu, všimne si anomáliu alebo má pochybnosť – dokáže o tom okamžite hovoriť bez strachu z hľadania vinníka?

VŠIMNÚŤ SI → POVEDAŤ → REAGOVAŤ → POUČIŤ SA ↻

Najdrahšia chyba môže byť tá, o ktorej ľudia vedia, ale boja sa o nej hovoriť. Speak-Up je súčasťou kontrolného systému.

7 PO INCIDENTE: OBNOVILI SME SLUŽBU, ALEBO SME ZLEPŠILI FIRMU?

Vieme, kadiaľ útočník vošiel? Zavreli sme tú cestu? Overili sme, že nemá inú? Čo sme po incidente zmenili?

RÝCHLY TEST PRIPRAVENOSTI

Po prečítaní checklistu si úprimne označte, čo má firma zvládnuté a kde ešte zostáva priestor na zlepšenie.

- | | | | | |
|----|--|------------------------------|------------------------------------|------------------------------|
| 1. | VIEME, KTORÉ SYSTÉMY MUSIA FUNGOVAŤ? A NAOZAJ SME ICH OBNOVILI ZO ZÁLOHY? | ☐ Áno | ☐ Čiastočne | ☐ Nie |
| 2. | VŠIMOL BY SI NIEKTO ÚTOK A VEDEL BY, ČO UROBIŤ AKO PRVÉ? | ☐ Áno | ☐ Čiastočne | ☐ Nie |
| 3. | VIEME EŠTE PRED INCIDENTOM, KTO HO BUDE RIADIŤ? | ☐ Áno | ☐ Čiastočne | ☐ Nie |
| 4. | VIEME OBMEDZIŤ ŠKODU BEZ ZNIČENIA DÔKAZOV? | ☐ Áno | ☐ Čiastočne | ☐ Nie |
| 5. | VIEME KOMUNIKOVAŤ RÝCHLO, FAKTICKY A JEDNÝM HLASOM? | ☐ Áno | ☐ Čiastočne | ☐ Nie |
| 6. | VIEME SA BEZPEČNE OBNOVIŤ A OVERIŤ, ŽE ÚTOČNÍK JE PREČ? | ☐ Áno | ☐ Čiastočne | ☐ Nie |
| 7. | POUČÍME SA Z INCIDENTU BEZ HĽADANIA VINNÍKA? | ☐ Áno | ☐ Čiastočne | ☐ Nie |

Každé „**NIE**“ alebo „**ČIASTOČNE**“ ukazuje konkrétnu oblasť, ktorú je lepšie vyriešiť pred incidentom než počas neho.

Zaujala vás táto téma alebo máte otázky k vašej konkrétnej situácii?
Radi sa na to s vami pozrieme. Stačí nás kontaktovať cez [online formulár](#).