

Kybernetická odolnosť v štátnej správe: čo musíte mať pripravené skôr, než príde incident?

Datum 12.10.2026

Subjekt SOITRON

Region Slowakei

Kategorie IT und Kommunikation, Staatsverwaltung und Selbstverwaltung, Sicherheit

Kybernetickému incidentu sa nedá vždy zabrániť. O tom, či ho štátna inštitúcia zvládne, rozhoduje to, čo má pripravené vopred: kto rozhoduje, komu volá, čo má v zmluve s dodávateľom a či svoje postupy niekedy vyskúšala.

To boli spoločné témy nášho odborného brunchu Kybernetická odolnosť v štátnej správe, ktorý sme zorganizovali 6. októbra 2026 v Bratislave. Vystúpili Štefan Porubčan (Soitron), Martin Lohnert (void SOC) a Pavol Dovičovič (KCCKB), ktorí v paneli diskutovali aj so zástupcom SK-CERT – Milanom Pikulom, a Radoslavom Zlackým z NASES. V článku sme zhrnuli to najpodstatnejšie, vrátane postrehov z diskusie, ktoré v prezentáciách nenájdete.

- **Incident príde.** Rozhoduje, či inštitúcia udrží prevádzku: má otestované zálohy, plán obnovy a jasné roly.
- **Mandát sa nedá outsourcovať.** O odpojení systému v noci rozhoduje človek z inštitúcie, preto treba mať vopred schválené scenáre reakcie.
- **Outsourcovať môžete výkon, nie zodpovednosť.** Za kybernetickú bezpečnosť vždy zodpovedá štatutár.
- **Zmluva je len taká dobrá, aký presný je jej rozsah.** Potrebujete merateľné KPI, pravidlá eskalácie a exit stratégiu.
- **Podpisom to nekončí.** Dodávateľa treba priebežne kontrolovať a reporty čítať v kontexte.
- **Pri ransomvéri volajte hneď.** Na začiatku incidentu vám SK-CERT dokáže pomôcť, po troch dňoch toho už veľa nezmôže.

Od prevencie k odolnosti

Ešte pred niekoľkými rokmi sa mohlo zdať, že firewall novej generácie a dobré technológie stačia. Dnes je jasné, že incidentu treba nielen predchádzať a odhaliť ho, ale aj počítať s tým, že sa raz stane aj nám. Výpadok štátnej inštitúcie nepociťuje len úrad, ale aj občania, ktorí na jej služby čakajú.

Prevencia, politiky, procesy a vzdelávanie používateľov zostávajú rovnako dôležité. Zákon o kybernetickej bezpečnosti a predpisy pre informačné technológie verejnej správy však od inštitúcií očakávajú aj zvládnutú reakciu na incident. Naš bezpečnostný expert Štefan Porubčan vo svojom vystúpení položil otázky, na ktoré by mala mať odpoveď každá inštitúcia:

- Vieme hneď zistiť, že sa niečo deje?
- Vieme, ako obnoviť kritické systémy?
- Máme plán obnovy po havárii a plán kontinuity činnosti? A testujeme ich?
- Testujeme zálohy, alebo len veríme, že fungujú?
- Máme zmapované závislosti medzi systémami?

- Vieme, kto pri incidente čo robí a kto komunikuje navonok – s verejnosťou a médiami?

Cieľom nie je incidentom sa za každú cenu vyhnúť, pretože to ani nie je reálne. Cieľom je zvládnuť ich bez fatálnych následkov pre inštitúciu aj pre jej štatutára.

Kto rozhodne v sobotu o 4:18h?

Útočníci útočia najmä vtedy, keď nie sme v práci: v noci, cez víkend a cez sviatky. Zákon pritom očakáva včasné varovanie už do 24 hodín a od monitoringu sa očakáva nepretržitá dostupnosť. Jedno pracovné miesto, ktoré pokrýva prevádzku 24/7, pritom znamená zamestnávať 5 – 6 ľudí na plný úväzok, keď započítate zmeny, dovolenky a choroby.

Technológia incident odhalí. Rozhodnúť o odpojení produkčného systému však stále musí človek s mandátom. Tento mandát zostáva v inštitúcii bez ohľadu na to, či má vlastný SOC, hybridný model alebo SOC ako službu. Pri externej službe sa časť zásahu dá preniesť na dodávateľa, ale len v rozsahu, ktorý je dohodnutý v zmluve a SLA.

V praxi sa osvedčujú vopred schválené scenáre reakcie

Ešte pred spustením služby sa inštitúcia so SOC dodávateľom dohodne, za akých podmienok smú vypnúť systém, zablokovat prístup alebo resetovať identity. O 4:18h potom netreba nikoho budiť kvôli súhlasu. Riaditeľ nášho SOCu Martin Lohnert k tomu dodal dôležitý rozmer: ak hrozí, že incident prerastie do veľkých rozmerov, reakcia naň by mala mať prednosť pred parametrami SLA prevádzky.

Aký model SOC zvoliť a ako sa medzi nimi rozhodnúť, podrobne rozoberáme v samostatnom článku.

Outsourcovať môžete výkon, nie zodpovednosť

Najväčším problémom inštitúcií zvyčajne nie sú technológie, ale ľudia. Vlastné odborné kapacity chýbajú, a preto si často bezpečnosť objednávajú ako službu. Pavol Dovičovič z KCCKB nám však pripomenul zásadnú vec: outsourcovať sa dá výkon služby, nie zodpovednosť organizácie. Podľa zákona o kybernetickej bezpečnosti za ňu zodpovedá štatutár. A manažér kybernetickej bezpečnosti (MKB) nemá spadať pod IT, ale reportovať priamo štatutárovi.

Čo sa dá outsourcovať?

- úloha manažéra kybernetickej bezpečnosti alebo CISO ako služba,
- bezpečnostný monitoring, SIEM a SOC,
- reakcia na incidenty a digitálna forenzná analýza,
- penetračné testy a riadenie zraniteľností,
- audity, bezpečnostné posudky a konzultácie,
- školenia bezpečnostného povedomia.

Nie všetky služby sú rovnaké. Niektorí potrebujú len dohľad, iní zálohu, konzultanta alebo reaktívnu službu pre prípad incidentu.

Čo musí zostať v inštitúcii?

- vlastníctvo aktív, procesov a rizík (dobrá rada: analýzu rizík vám žiadna tretia strana neurobí na kľúč bez vašej súčinnosti),
- strategické a manažérske rozhodnutia (odpojíme organizáciu od siete? vypneme server tretej strany?),

- určenie požadovanej úrovne bezpečnosti,
- kontrola a hodnotenie dodávateľa,
- dostatočná znalosť vlastného prostredia.

Zákon a vyhláška navyše vyžadujú riadenie dodávateľského reťazca. To, že činnosť zabezpečuje niekto iný, nemení vašu povinnosť preukázať plnenie požiadaviek. A preukázať treba nielen to, že služba existuje, ale aj to, že v praxi funguje.

Najprv domáca úloha, potom zmluva

Zle definovaná potreba vedie k zle obstaranej službe. Skôr než inštitúcia vyhlási obstarávanie, mala by vedieť, čo vlastne chce: SIEM? monitoring? interný tím? Ako bude riešiť incidenty a ako začleniť novú službu do svojich procesov? A koľko to bude stáť?

Na brunchi zaznel príklad organizácie, ktorá si kúpila jednorazovú službu na rok aj s licenciami a až potom zistila, že nepokrýva to, čo potrebuje. Dodatkom k zmluve sa situácia nevyrieši – dodávateľ veľmi pravdepodobne buď odstúpi, alebo zvýši cenu. Riešením je zadefinovať si aspoň v bodoch, čo má služba spĺňať, nechať si odhadnúť náklady (napríklad od konzultanta) a urobiť si malú analýzu rizík: čo mi služba prinesie a čo sa môže stať, ak ju mať nebudem.

Vo verejnom obstarávaní je hlavným kritériom často cena. Najnižšia cena však neznamená najnižšie riziko. Požiadavky preto musia vzniknúť skôr, než začnete hodnotiť ponuky, inak sa nemáte podľa čoho rozhodnúť.

Čo musí byť jasné pred podpisom zmluvy

1. Predmet a rozsah služby
2. Roly a zodpovednosti oboch strán
3. Bezpečnostné požiadavky
4. Komunikačné a eskalačné pravidlá
5. SLA, KPI a reporting
6. Riadenie incidentov
7. Kontinuita a dostupnosť
8. Kontrola a audit
9. Ukončenie služby a exit stratégia

Najdôležitejší je rozsah. Veta „Dodávateľ zabezpečí bezpečnostný monitoring“ nie je špecifikácia služby. Čo sa monitoruje a v akom čase? Čo sa považuje za incident? Koho a ako dodávateľ kontaktuje? Jedna veta v zmluve môže skrývať desiatky nezodpovedaných otázok.

Samotné SLA nestačí, potrebujete aj merateľné ukazovatele výkonu (KPI) a rizika (KRI). Napríklad: dostupnosť služby 99,9 %, triáž kritického alertu do 15 minút či eskalácia incidentu do 30 minút.

Varovné signály pri výbere dodávateľa

Spozornieť by ste mali, ak počujete:

- „Máme audit kybernetickej bezpečnosti, takže ste v pohode.“ (Audit mohol skončiť s 5 % súladom.)
- „SLA nepotrebujeme.“
- „Incident sme ešte nemali.“
- „To vám nemôžeme ukázať.“

Podpisom zmluvy sa to len začína

Outsourcing nie je jednorazový nákup. Služba sa musí riadiť počas celého životného cyklu, pretože sa mení infraštruktúra, riziká, legislatíva aj samotný dodávateľ. Požiadavky, ktoré boli dobré pri podpise, nemusia o dva roky stačiť.

Dobre nastavený outsourcing má jasné poradie: potreba, analýza rizík z pohľadu dodávateľa, požiadavky, výber a zmluva. Potom sa opakuje cyklus prevádzky, kontroly a zmeny, až k prípadnému exitu.

Ako kontrolovať dodávateľa

Pravidelný reporting, vyhodnocovanie dohodnutých parametrov, kontrola incidentov a eskalácií, audit. Treba si uvedomiť, že mesačný report s číslami bez kontextu o kvalite služby nehovorí nič. Oplatí sa vopred zmluvne dohodnúť, že report bude obsahovať napríklad aj vysvetlenie a porovnanie s minulým obdobím. Manažment by z neho mal vyčítať:

- čo sa zmenilo od posledného reportu a aké sú trendy,
- aké významné incidenty sa vyskytli a ako sa vyriešili,
- aké sú odporúčania a či je potrebná investícia,
- čo si vyžaduje manažérske rozhodnutie.

Najčastejšie chyby:

- „Dodávateľ sa o to postará.“
- Nejasný alebo príliš všeobecný rozsah služby. Toto je najzávažnejšia chyba.
- SLA bez reálneho merania a kontroly.
- Závislosť od jedného dodávateľa (vendor lock-in).
- Chýbajúca exit stratégia.
- Závislosť od jedného človeka na strane dodávateľa.

Pred outsourcingom bezpečnosti si skúste položiť týchto 7 otázok:

1. Vieme presne, čo kupujeme?
2. Vieme, aké riziko tým riešime?
3. Vieme, čo od dodávateľa požadujeme?
4. Vieme, kto za službu interne zodpovedá?
5. Vieme, ako budeme merať jej kvalitu?
6. Vieme, čo sa stane pri incidente?
7. Vieme, ako zo služby odideme?

Sme pod útokom. Kam sa obrátiť?

Pri incidente nie je čas klopať od jedných dverí k druhým. Panelisti z SK-CERT, NASES a void SOC vysvetlili, kto čo robí a čo od koho môžete očakávať.

- NBÚ (Národný bezpečnostný úrad) prijíma hlásenia incidentov. Ak ste štátna inštitúcia, incident s vami často rieši aj vládna jednotka CSIRT.SK.
- SK-CERT kontaktujte čo najskôr, ideálne hneď na začiatku incidentu. Pomáha v troch úrovniach. Ak má organizácia procesy a incident zvláda sama, SK-CERT len dozoruje. Ak máte kapacity, ale potrebujete usmernenie, metodicky vám poradia. A ak potrebujete priamu pomoc,

SK-CERT príde na miesto a urobí aj forenznú analýzu. Odmietne len vtedy, keď nemá voľné kapacity.

- NASES je dôležitý partner, ak ste pripojení na sieť GovNet. Informáciami prepája ministerstvá a NBÚ, upozorňuje na hrozby a blokuje IP adresy útočníkov v sieti GovNet. Reakciu na incident za organizáciu nevykonáva, ale poradí, na koho sa obrátiť.
- Komerčný SOC zmluvným klientom garantuje pomoc v dohodnutom čase a rozsahu. Pomáha aj organizáciám bez zmluvy, ktoré potrebujú rýchlu odbornú pomoc, výsledok však garantovať nemôže.

A nezabudnite, že pri ransomvéri platí jedno zásadné pravidlo: ozvite sa hneď. Keď sa organizácia ozve na začiatku útoku, SK-CERT jej vie dokázať dobre poradiť. Keď sa ozve po troch dňoch, už je pravdepodobne neskoro.

A ak sa pri zásahu niečo pokazí? Panelisti sa zhodli, že dobre nastavená spolupráca stojí na dohode vopred. Komerčný SOC nerobí svojvoľný zásah, scenáre schvaľuje zákazník už pri definovaní služby. NASES zasahuje len v rozsahu, na ktorom sa vopred dohodol a na ktorý má mandát. Zodpovednosť za škodu sa dá zmluvne obmedziť alebo poistiť, no v konečnom dôsledku zostáva na inštitúcii.

Tri odporúčania na záver

Na otázku, čo si majú účastníci z brunchu odniesť, sa panelisti zhodli na troch slovách:

1. **Dokumentujte.** Majte dokumentáciu skôr, než príde incident.
2. **Poznajte.** Vedzte, čo máte doma: aktíva, systémy, závislosti.
3. **Trénujte.** Simulujte a testujte, aby postupy fungovali aj o 4:18 ráno.

Kybernetická odolnosť nie je produkt, ktorý si inštitúcia kúpi. Je to schopnosť, ktorú si musí vybudovať, preveriť a udržiavať, s dodávateľmi alebo bez nich.

Prezentácie zo všetkých vystúpení nájdete na stránke podujatia. Ako si vybrať vhodný model SOC, rozoberáme v článku na webe void SOC.

A nevíete, kde je vaša inštitúcia dnes a čo by mala riešiť ako prvé, ozvite sa nám, radi sa s vami porozprávame.

<https://www.soitron.sk/kyberneticka-odolnost-v-statnej-sprave>