



Kompetenčné
a certifikačné
centrum
kybernetickej
bezpečnosti

AKO OUTSOURCOVAŤ SLUŽBY KYBERNETICKEJ BEZPEČNOSTI

Teória • legislatíva • praktické príklady



KOMPETENČNÉ A CERTIFIKAČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI

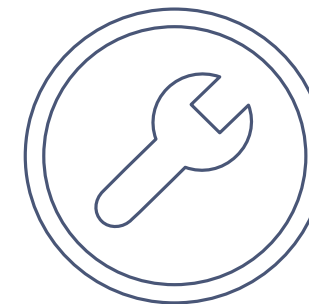
- **Kompetenčné a certifikačné centrum kybernetickej bezpečnosti**, príspevková organizácia NBÚ (skrátene len „Kompetenčné centrum“)
- **Hlavné úlohy** Kompetenčného centra:
 - Certifikácia audítorov, manažérov
 - Vzdelávanie dospelých v kybernetickej bezpečnosti
 - Audit kybernetickej bezpečnosti podľa zákona č. 69/2018 Z. z.
 - Konzultačné služby v oblasti kybernetickej bezpečnosti, utajovaných skutočností a dôveryhodných služieb
 - Organizácia kampaní a publikačná činnosť na zvyšovanie povedomia v kybernetickej bezpečnosti
 - Znalecká a expertízna činnosť podľa zákona č. 382/2004 Z. z. o znalcoch
 - KCCKB plní rolu Národného koordinačného centra (NCC) podľa európskeho nariadenia 2021/887





PREČO VÔBEC OUTSOURCUJEME?

- Nedostatok interných odborných kapacít
- Prístup k špecializovaným znalostiam a technológiám
- Potreba nepretržitej alebo pohotovostnej služby
- Ekonomická efektivita oproti budovaniu vlastného tímu
- Nepravidelná potreba vysoko špecializovaných činností





ČO NIE JE MOŽNÉ OUTSOURCOVAŤ?

- Outsourcovať môžeme výkon služby.
- **Nie zodpovednosť organizácie.**





ČO VŠETKO MOŽNO OUTSOURCOVAŤ?

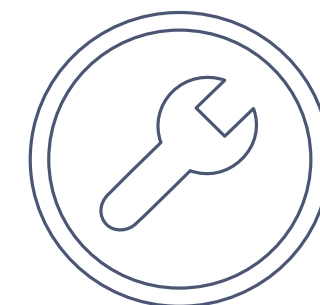
- Manažér kybernetickej bezpečnosti / CISO as a Service
- SOC, SIEM a bezpečnostný monitoring
- Incident response a digitálna forenzná podpora
- Riadenie zraniteľností a penetračné testovanie
- Audity, konzultácie a bezpečnostné posudzovanie
- Školenia a awareness
- Prevádzka a správa vybraných bezpečnostných technológií





NIE VŠETKY SLUŽBY SÚ ROVNAKÉ

- Poradenské – odporúčanie a odborná podpora
- Realizačné – implementácia opatrenia alebo technológie
- Prevádzkové – pravidelný výkon a správa služby
- Monitorovacie – dohľad, detekcia a vyhodnocovanie
- Reaktívne – zásah pri incidente alebo krízovej situácii
- Rozdielna kritickosť znamená rozdielne požiadavky na dodávateľa.





ČO BY MALO ZOSTAŤ INTERNÉ?

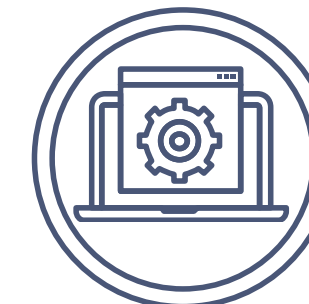
- Vlastníctvo aktív, procesov a rizík
- Rozhodovanie o akceptácii rizika
- Strategické a manažérske rozhodnutia
- Určenie požadovanej úrovne bezpečnosti
- Kontrola a hodnotenie dodávateľa
- Dostatočná znalosť vlastného prostredia





PRAKTICKÝ PŘÍKLAD: „POTREBUJEME SOC“

- Čo tým organizácia skutočne myslí?
 - SIEM a centralizovaný zber logov?
 - 24/7 monitoring?
 - Triage a analýzu alertov?
 - Eskaláciu incidentov?
 - Aktívny zásah a incident response?
 - Forenznú analýzu?
 - Pravidelný report?



Zle definovaná potreba vedie k zle obstarávanej službe.



LEGISLATÍVA VSTUPUJE DO HRY

- Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti – povinnosti prevádzkovateľa a riadenie bezpečnosti
- Vykonávacie predpisy vrátane vyhlášky č. 227/2025 Z. z.
- Požiadavky na riadenie dodávateľov a dodávateľského reťazca

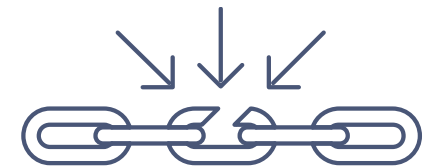


Externé zabezpečenie činnosti nemení potrebu preukázať plnenie povinností.



DODÁVATEĽSKÝ REŤAZEC

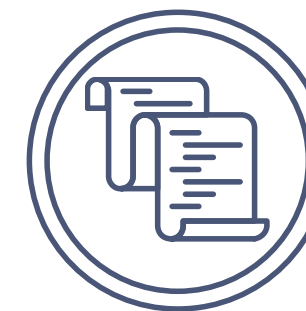
- Identifikovať služby a dodávateľov, ktorí môžu ovplyvniť kybernetickú bezpečnosť
- Posudzovať riziká spojené s dodávateľom a poskytovanou službou
- Stanoviť bezpečnostné požiadavky pred začatím spolupráce
- Priebežne sledovať plnenie dohodnutých požiadaviek
- Riadiť zmeny, subdodávateľov a ukončenie služby





ČO MUSÍME OD DODÁVATEĽA POŽADOVAŤ

- Jasný predmet, rozsah a hranice služby
- Bezpečnostné a personálne požiadavky
- Ochranu informácií a prístupových údajov
- Pravidlá oznamovania a riešenia incidentov
- Kontrolu, reporting a možnosť auditu
- Kontinuitu služby a obnovu
- Pravidlá pre subdodávateľov
- Podmienky ukončenia a odovzdania služby





„RED FLAGS“ PRI VÝBERE DODÁVATEĽA

- „To máme vyriešené interne.“
- „To vám nemôžeme ukázať.“
- „Incident sme ešte nikdy nemali.“
- „SLA nepotrebuje, reagujeme vždy rýchlo.“
- „Subdodávateľov neriešate.“
- „Po ukončení zmluvy vám dáta nejako odovzdáme.“
- „ISO certifikát máme, scope teraz neviem.“





„MÁME TO OUTSOURCOVANÉ“ NIE JE OPATRENIE

Povinnosť



Externá služba



Kontrola organizácie



Dôkaz

Musíme vedieť preukázať nielen existenciu služby, ale aj jej riadenie a účinnosť.



CENA NIE JE JEDINÁ POŽIADAVKA

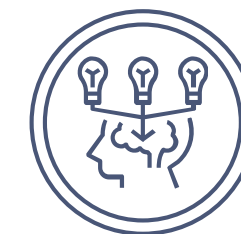
- Najnižšia cena nemusí znamenať najnižšie riziko
- Rozhoduje schopnosť dodávateľa splniť konkrétne požiadavky organizácie
- Požiadavky musia vzniknúť pred hodnotením ponúk
- Bez definovaných požiadaviek porovnávame iba obchodné ponuky, nie bezpečnostné služby.





PRAKTICKÝ PŘÍKLAD: TRAJA DODÁVATELIA

- Dodávateľ A – nízka cena, obmedzené SLA, bez 24/7 reakcie
- Dodávateľ B – vyššia cena, 24/7 monitoring, incident response, auditovateľnosť
- Dodávateľ C – najvyššia cena, široký rozsah služieb a silné zmluvné garancie
- **Ktorý je najlepší?**



Bez definovaných potrieb, rizík a požiadaviek to nevieme rozhodnúť.



ČO MUSÍ BYŤ DEFINOVANÉ PRED PODPISOM ZMLUVY

- Predmet a rozsah služby
- Roly a zodpovednosti oboch strán
- Bezpečnostné požiadavky
- Komunikačné a eskalačné pravidlá
- SLA, KPI a reporting
- Incident management
- Kontinuita a dostupnosť
- Kontrola a audit
- Ukončenie služby





ROZSAH (SCOPE) SLUŽBY

- „Dodávateľ zabezpečuje bezpečnostný monitoring.“
 - Čo monitoruje?
 - V akom čase?
 - Aké udalosti analyzuje?
 - Čo považuje za incident?
 - Koho a ako kontaktuje?
 - Kto vykonáva zásah?



Jedna veta v zmluve môže skrývať desiatky nezodpovedaných otázok.



SLA NESTAČÍ

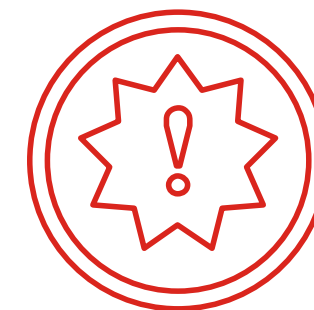
- SLA – akú úroveň služby dodávateľ garantuje
- KPI – ako meriame výkon a kvalitu služby
- KRI – čo nám signalizuje rastúce riziko
- Príklady:
 - Dostupnosť služby 99,9 %
 - Triage kritického alertu do 15 minút
 - Eskalácia incidentu do 30 minút
 - Počet neanalyzovaných alertov
 - Pokrytie požadovaných logových zdrojov





INCIDENT O 02:17 RÁNO

- Externý SOC identifikuje podozrenie na ransomware o 02:17 hod.
 - Koho kontaktuje?
 - Kto môže izolovať server alebo endpoint?
 - Kto môže odstaviť produkčnú službu?
 - Čo ak kontaktná osoba nedvíha telefón?
 - Kto rozhoduje o aktivácii incident response?

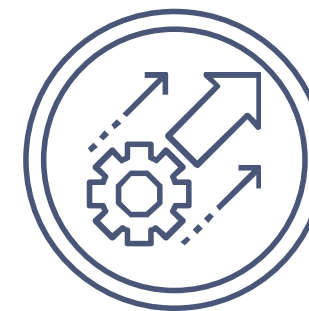


Technická detekcia bez procesného nastavenia nemusí viesť k účinnej reakcii.



PODPISOM ZMLUVY OUTSOURCING IBA ZAČÍNA

- Služba sa musí riadiť počas celého životného cyklu.
- Mení sa infraštruktúra, riziká, legislatíva aj samotný dodávateľ.
- Požiadavky nastavené pri podpise zmluvy nemusia byť o dva roky dostatočné.
- Organizácia potrebuje vlastníka služby a pravidelný proces jej hodnotenia.





AKO KONTROLOVAŤ DODÁVATEĽA

- Pravidelný reporting
- Service review stretnutia
- Vyhodnocovanie SLA, KPI a KRI
- Kontrola incidentov a eskalácií
- Audit alebo iná forma overenia
- Riadenie zmien
- Aktualizácia rizík
- Kontrola subdodávateľov a významných zmien služby





MESAČNÝ REPORT ≠ RIADENIE SLUŽBY

- **12 482 921 events**
- **4 217 alerts**
- **23 incidents**



Sme teda bezpečnejší ako minulý mesiac? Samotné čísla bez kontextu často neposkytujú odpoveď.



ČO BY MAL MANAGEMENT SKUTOČNE VEDIEŤ

- Čo sa od posledného obdobia zmenilo?
- Aké nové alebo zvýšené riziká vznikli?
- Ktoré opatrenia alebo časti služby nefungujú podľa očakávania?
- Aké významné incidenty nastali a čo sme sa z nich naučili?
- Čo potrebuje manažérske rozhodnutie?
- Kde je potrebná investícia alebo zmena priority?





NAJČASTEJŠIE CHYBY

- „Dodávateľ sa o to postará.“
- Nejasný alebo príliš všeobecný scope
- SLA bez reálneho merania a kontroly
- Chýbajúci interný vlastník služby
- Závislosť od jedného človeka na strane dodávateľa
- Nekontrolovaní subdodávatelia
- Vendor lock-in
- Chýbajúca exit stratégia





MODELOVÝ PRÍKLAD ZLYHANIA

SOC incident správne detegoval.

Podľa dohodnutého postupu
odoslal upozornenie e-mailom.

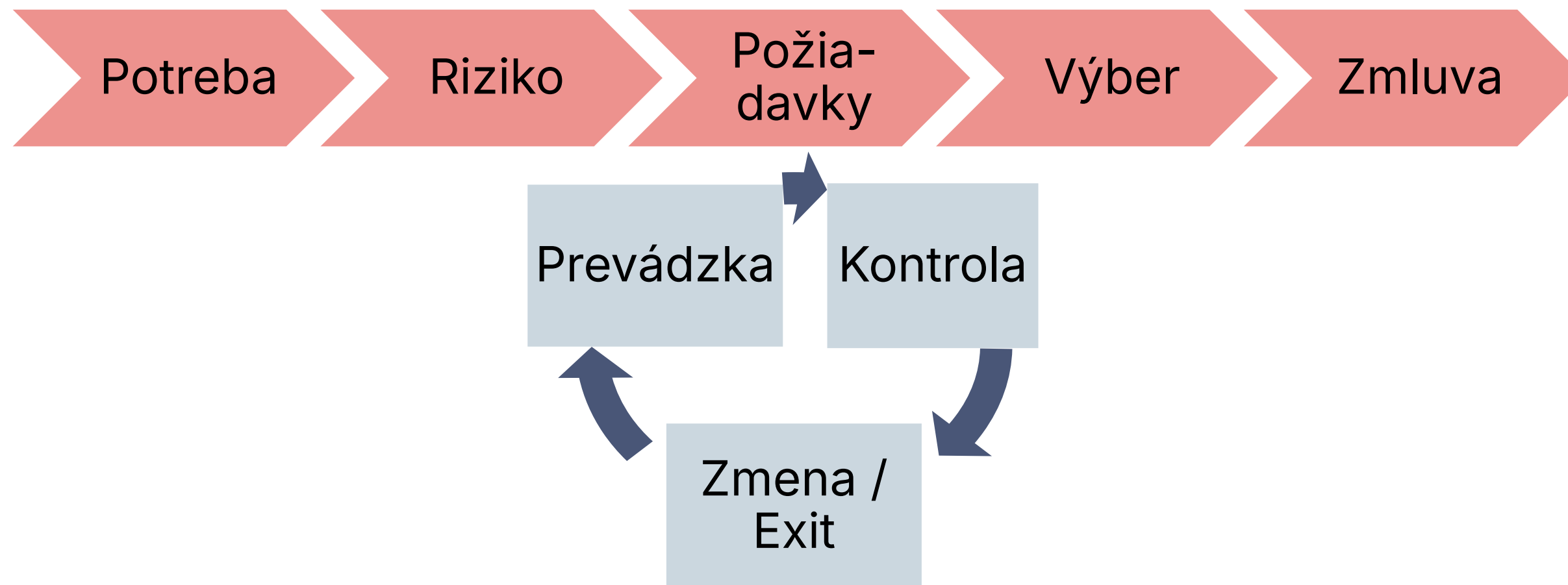
Na strane zákazníka si správu
nikto nevšimol.

K zásahu prišlo až po prejavení
dopadu incidentu.

- Dodávateľ mohol formálne splniť SLA – a organizácia napriek tomu zlyhala.
- Otázka preto nie je iba „splnil dodávateľ zmluvu?“, ale „fungoval celý proces?“



AKO VYZERÁ DOBRE NASTAVENÝ OUTSOURCING



- Outsourcing je životný cyklus, nie jednorazový nákup.



7 OTÁZOK PRED OUTSOURCINGOM

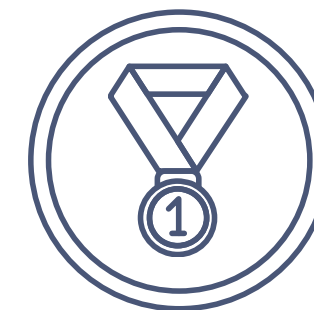
1. Vieme presne, čo kupujeme?
2. Vieme, aké riziko tým riešime?
3. Vieme, čo od dodávateľa požadujeme?
4. Vieme, kto za službu interne zodpovedá?
5. Vieme, ako budeme merať jej kvalitu?
6. Vieme, čo sa stane pri incidente?
7. Vieme, ako zo služby odídeme?





ZÁVER

- **Outsourcovať môžeme službu**
- **Nie zodpovednosť**



Dobre nastavený outsourcing musí byť definovaný, zmluvne ošetrený, merateľný a priebežne kontrolovaný.



Ochrana vlastnických práv

Všetky autorské práva k tomuto dokumentu sú vyhradené pre Kompetenčné a certifikačné centrum kybernetickej bezpečnosti (ďalej len „KCCKB“). Autorské práva k tomuto dokumentu má a autorské práva k tomuto dokumentu vykonáva KCCKB.

Vlastnícke práva tretích strán

Všetky ochranné známky a iné obdobné právne chránené označenia spomenuté v tomto dokumente sú výhradným vlastníctvom ich vlastníkov, ktorí sú, pokiaľ sa nejedná o KCCKB, v dokumente označení vo forme príslušnej citácie.

Akémkoľvek kopírovanie či iné neoprávnené použitie celého dokumentu alebo jeho časti, v elektronickej alebo listinnej podobe, bez predchádzajúceho písomného súhlasu jeho autorov, napr. KCCKB, je zakázané. Porušenie vlastnických a iných súvisiacich práv bude riešené v zmysle právnych predpisov Slovenskej republiky.

Limity informácií

Informácie obsiahnuté v tomto dokumente sú poskytované iba na informačné účely a bez akejkoľvek záruky, výslovnej či implicitnej. Názov KCCKB, logo KCCKB a ďalšie produkty a služby KCCKB sú ochrannými známkami KCCKB. Ostatné názvy spoločností, produktov alebo služieb môžu byť ochrannými známkami, alebo značkami služieb iných organizácií.



www.cybercompetence.sk



www.linkedin.com/company/cybercompetence



[@CybercenterSk](https://twitter.com/CybercenterSk)