Předmět zakázky

Předmětem zakázky je **komplexní zajištění služeb bezpečnostního dohledu typu Security Operation Center nad prostředím a informačními systémy ČSÚ** (dále jen „Služby SOC“) po dobu 36 měsíců.

Služby SOC budou zajišťovány formou provozu nástrojů pro vyhodnocování kybernetických bezpečnostních událostí v komunikačních sítích Českého statistického úřadu. Zadavatel pro účely poskytování služby zpřístupní dodavateli vlastní bezpečnostní dohledové systémy (SIEM, NetFlow/IPFIX monitoring) v potřebném rozsahu, včetně základní konfigurace (vytvoření jmenných účtů, nastavení rolí, apod.).

Rozsah prostředí

Služby SOC jsou v tuto chvíli provozovány nad 5 informačními systémy ČSÚ a související infrastruktuře. Počet aktivních připojených zdrojů logů do nástroje SIEM je cca 150, generované množství logů do nástroje SIEM dosahuje cca 400 EPS. V závislosti na nepravidelných projektech (např. volby nebo Sčítání lidu, domů a bytů) se dočasně množství logů může navýšit (řádově o malé stovky EPS). V závislosti s případnými změnami i přirozeným vývojem prostředí ČSÚ se může množství logů měnit i dlouhodobě.

Technická specifikace

Dohledové centrum kybernetické bezpečnosti (SOC)

Předmětem poptávky je komplexní řešení pro centralizovanou správu, ukládání a vyhodnocování logů v nezměnitelné podobě z libovolných síťových aktivních prvků, operačních systémů a používaného aplikačního software provozované formou služby Sdíleného dohledového centra kybernetické bezpečnosti (SOC – Security Operation Centra). Implementace systému bude provedena v souladu s *§ 23 Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí* dle Vyhlášky č. 82/2018 Sb. k Zákonu č. 181/2014 Sb., o kybernetické bezpečnosti v platném znění.

Požadavky na SOC

1. Zadavatel předpokládá realizaci uvedených úloh prostředky a technologiemi Zadavatele, nejméně v rozsahu řešení sběru NetFlow a SIEM řešení jež zadavatel sám vlastní. Služba dodavatele zohlední přítomnost těchto prostředků na straně zadavatele v tom smyslu, že jako primární a rozhodné nástroje dodavatel využije tyto prostředky. Konfigurační změny a úpravy uvedených prostředků provede Dodavatel vlastním nákladem jako součást služby a předá je do vlastnictví zadavatele.
2. Bezpečnostní dohledové centrum dodavatele musí podporovat práci s nástroji Zadavatele, dle předmětu zakázky (SIEM – IBM QRadar, NetFlow – Flowmon). Zadavatel si vyhrazuje právo během trvání smlouvy na Služby SOC jednotlivé produkty obměnit za jiné v dané kategorii, na základě výsledků případných veřejných zakázek.
3. Dodavatel navrhne modifikaci relevantních procesů na straně Zadavatele, včetně atributů a parametrů procesů potřebných pro doručení služby.
4. Služba je dostupná v českém, případně slovenském jazyce.
5. Služba dohledu je zajišťována z území ČR.
6. V rámci služby bude vytvořeno bezpečné uložiště pro sdílení kompletních materiálů k poskytované službě.
7. Správa a dohled zdrojů – Performance a Capacity management je zajištěn nástroji Zadavatele využívaných Službou SOC

8. Sítový dohled - Network Performance Monitoring and Diagnostics je zajištěn nástrojem Zadavatele
9. Bezpečnostní dohled – SIEM je zajištěn nástrojem Zadavatele
10. Incident management – Operátorské činnosti, Incident handling, Incident Response.
11. Analýza incidentů – Odborné činnosti spočívající v detekci a lokalizaci příčin incidentů.
12. Návrhy systematických opatření – Sestavení opatření v organizační a technické úrovni pro posouzení Zadavatelem.
13. Návrhy řešení incidentů – Odborné činnosti pro kategorizaci na interní a externí příčiny incidentů a k nim příslušných opatření.
14. Reporting a analýza stavů, událostí a incidentů – Odborné činnosti pro doložení úrovně bezpečnosti vůči interním kontrolním procesům nebo pro doložení vůči externím kontrolním autoritám.
15. Personální zajištění služby SOC pracovníky Dodavatele s odbornou způsobilostí vyhovující požadavkům stanovaným v kvalifikačních požadavcích.
16. Plánování odstávek poskytované služby se zajištěnou náhradou.
17. Služba, včetně všech komponent poskytovaných dodavatelem, které využívá, musí být odolná proti výpadkům a poruchám. Všechny komponenty musí být schopny dlouhodobého provozu bez změny chování a úbytku výkonu.
18. Všechny parametry služby musí zajistit na úrovni technologií i procesů splnění požadavků na zajištění potřebné míry informační bezpečnosti, zejména pak: Důvěrnost, Citlivost, Dostupnost, Autentizaci, Autorizaci, Nepopiratelnost.
19. Služba musí zajistit odbavení všech monitorovaných atributů a parametrů, a to jak na úrovni přístupu ke vstupním/zdrojovým datům systému, tak i k incidentům.
20. Součástí služby bude rovněž odhalování zranitelností spravovaných aktiv, provázané s monitoringem a správou korelačních vrstev dat o spravovaných a dohledovaných celcích tak, aby umožňoval automatické stanovení relevance jednotlivých událostí. Služba zajistí rovněž prověřování evidovaných aktiv na dostupné zranitelnosti.
21. Služba zajistí klasifikaci incidentů a vytváření reportů v souladu s normami řady ISO / IEC 27000.
22. Služba zajistí řízení celého životního cyklu každého typu incidentu.
23. Služba zajistí vytváření vlastního auditního žurnálu (záznam změn konfigurace služby v nastavení přístupů personálu Dodavatele ke klasifikovaným informacím a systémům Zadavatele) po nastavitelnou dobu a tento musí být chráněn proti modifikaci, a být přístupný ke kontrole Zadavateli nebo k výkonu interního auditu Zadavatele.
24. Služba využije SIEM (bezpečnostní dohledové systémy) Zadavatele jako primární výpočetní prostředí a jako primární zdroj dat. Vrstva sběru dat a vyhodnocení informací bude funkčně i technicky integrována na prostředky Zadavatele tak, že veškeré změny v nastavení prostředků budou provedeny vždy primárně na straně těchto prostředků Zadavatele.
25. Služba zajistí úpravu procesů na straně Dodavatele a návrh na jejich integraci s relevantními procesy na straně Zadavatele (adaptace a akceptace sdílených procesů).
26. SLA procesních vstupů a výstupů – Služba zajistí monitoring procesů na straně Dodavatele a Zadavatele.
27. Dodavatel před podpisem smlouvy umožní Zadavateli návštěvu vlastního bezpečnostního dohledového centra, aby si mohl ověřit splnění požadavků. Zjištění nedodržení požadavků je důvod pro vyloučení Dodavatele.
28. Služba musí být rozšiřitelná způsobem, který umožní u každé části služby rozdělení nebo vydělení v samostatné části, funkčně shodné s originálem. V případě potřeby musí služba

Dodavatele umožnit separaci na úrovní procesů, systémů, dat, přístupových oprávnění, včetně transferu historických dat a informací do prostředí Zadavatele.

Technické požadavky na SOC

29. Dodavatel provozuje vlastní Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí, který umožňuje napojení na nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí Zadavatele (SIEM – IBM QRadar).
30. Rozhodné operace a manipulace jsou prováděny prostředky Zadavatele a nástroje Dodavatele budou sloužit na jeho straně pro případnou agregaci v rámci jeho procesů. Žádný ze způsobů propojení nesmí omezit nebo narušit primární autonomní fungování celého řešení jen prostředky Zadavatele.
31. Dodavatel zajistí provozní monitoring bezpečnostních nástrojů zadavatele, dle předmětu zakázky v rozsahu:
    - dostupnost a funkčnost nástrojů,
    - vytíženost nástrojů,
    - detekce vyčerpání kapacitních zdrojů.
32. V rámci služby Dodavatel zajišťuje nastavování nástrojů Zadavatele, dle předmětu zakázky, v rozsahu:
    - úprava a optimalizace korelačních pravidel,
    - přidávání nových zařízení,
    - vytváření nových scénářů pro detekci KBU,
    - úprava nastavení nástrojů dle novelizace legislativních požadavků.

Požadovaná podpora SOC

33. Ticketovací systém s on-line přístupem pro kompletní správu požadavků včetně uchování historie požadavků a jejich řešení. Jeho dostupnost musí být v režimu 24x7. Zadavatel má přístup do tohoto systému prostřednictvím webGUI rozhraní.
34. Přístup k podpoře provozu systémů – HotLine
35. Přístup k podpoře Incident Response – telefon, email
36. Informování odpovědných osob Zadavatele o vzniku bezpečnostního incidentu v reálném čase za pomocí základních komunikačních nástrojů (e-mail / SMS / telefon).
37. Zakládání tiketů, proaktivní komunikace o jejich řešení. Komunikace s třetí stranou jako NBÚ, NUKIB, CSIRT atd.
38. Rozšířený reporting – detailní report o událostech a incidentech s návrhy systematických opatření 1x měsíčně. Vzdálená prezentace reportu např. formou videokonference. Prezentace měsíčních reportů v rozsahu 2 hod.
39. Kontinuální skenování aktiv definovaných danou sítí/sítěmi a zranitelností relevantních pro daná aktiva. Minimálně na začátku poskytování služby budou provedeny plné skeny a dále vždy 1x měsíčně skeny rozdílové. K tomuto účelu může Zadavatel poskytnout přístup k nástroji pro skenování zranitelností (Nexpose).
40. Přístup administrátorů Zadavatele ke sledovaným parametrům alespoň v režimu čtení prostřednictvím grafického rozhraní (GUI – dashboard apod.).
41. Dodavatel zpracuje a poskytne zadavateli každý měsíc Report, ve kterém je popsán průběh realizace Plnění za uplynulé období, provedené služby a návrh doporučených opatření pro další období pro zvýšení bezpečnosti, dostupnosti a prevenci incidentů.
42. Technologie sběru dat – Služba zajistí užití SIEM systému Zadavatele jako základního zdroje dat a bude s ním komunikovat průmyslově standardními protokoly. Řešení na straně Zadavatele zajišťuje sběr, přenos a uložení logů a jejich vyhodnocování v rámci SIEM.
43. Base line analýza – Služba zajistí porovnání neobvyklých počtů určitých událostí oproti jinému období z minulosti.

44. Členění aktiv – Aktiva musí být možno rozdělit, dle jejich důležitosti. Aktiva musí mít uživatelsky definovatelné kategorie a parametry.
45. Relevance zranitelnosti – U aktiv musí být ověřena relevantnost incidentů pro dané aktivum vulnerability scannerem.
46. Kategorizace aktiv/zdrojů – Služba zajistí evidenci a vyhodnocení kategorie aktiv dle povahy zdrojových dat a dle těchto kategorií bude utvářet další pravidla nebo reporty v prostředcích Zadavatele.
47. Manuální parsovací pravidla – Služba zajistí generování parsovacích pravidel a reportů v prostředcích Zadavatele.
48. Historická korelace – Služba zajistí ověření nového korelačního pravidla proti historickým datům.
49. Reporty – Služba zajistí provádění on-demand spouštění některých pravidel a z výstupu bude vytvářet reporty.
50. Režim Maintenance – Služba musí být schopna běhu v režimu údržby, kdy se nebudou z jednotlivých zdrojů/aktiv vyhlašovat alerty.
51. Sdílené účty – Služba zajistí detekci privilegovaných přístupů pro konkrétního uživatele.
52. Služba Monitoringu a detekce:
    - Průběžné sledování provozu prostředí Zadavatele.
    - Real-time analýza situace v napojených zařízeních podle skupin, kategorií zařízení a podle kontextu log záznamů nebo událostí.
    - 2x denně odborné posouzení bezpečnostní situace a provozního stavu. V případě anomálie posouzení její relevance a závažnosti.
    - Posouzení kontextu anomálie a příčin vzniku situace s případnou eskalací problému zadavatele na analytického specialistu dodavatele.
53. Služba včasné výstrahy a reakce na nestandardní situace v provozu bezpečnostních systémů:
    - Zpracování analytických scénářů na aktuální kybernetické hrozby.
    - Posouzení eskalovaného problému zadavatele analytickým specialistou.
    - Detekce a vyhodnocení závažnosti identifikovaných anomálií.
    - Posouzení a případná eskalace nestandardní situace v provozu zadavatele na službu včasné výstrahy a reakce na incident v rámci bezpečnostních struktur ČR.

SLA parametry SOC

54. Dodavatel musí provozovat vlastní bezpečnostní dohledovou službu v režimu 24x7x365. Ve smyslu zajištění provozu systémů a pohotovosti role Operátor SOC. Služby ostatních procesních rolí jsou poskytovány minimálně v režimu 10x5.
55. **Kategorie III** – eskalace do 30 minut (Detekce: 5 minut, Vyhodnocení: 20 minut, Klasifikace: 5 minut) - velmi významný kybernetický bezpečnostní incident, při kterém je přímo a významně narušena bezpečnost poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje neprodlené zásahy obsluhy s tím, že musí být všemi dostupnými prostředky zabráněno dalšímu šíření kybernetického bezpečnostního incidentu včetně minimalizace vzniklých i potenciálních škod.
56. **Kategorie II** – eskalace do 2 hodin - významný kybernetický bezpečnostní incident, při kterém je narušena bezpečnost poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje neprodlené zásahy obsluhy s tím, že musí být vhodnými prostředky zabráněno dalšímu šíření kybernetického bezpečnostního incidentu včetně minimalizace vzniklých škod.
57. **Kategorie I** – eskalace do 24 hodin - méně významný kybernetický bezpečnostní incident, při kterém dochází k méně významnému narušení bezpečnosti poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje zásahy obsluhy s tím, že musí být vhodnými prostředky omezeno další šíření kybernetického bezpečnostního incidentu včetně minimalizace vzniklých škod. Jedná se bezpečnostní incidenty, které nespadají do kategorií III a II.

Pro každý kybernetický incident (dle §7, ZokB) prochází Dodavatel následným postupem k určení kategorií kybernetických bezpečnostních incidentů (dle §31, VoKB) podle následků a negativních projevů pro doporučení opatření či součinnosti v následné reakci:

Fáze Detekce

- Monitoring prostředí vymezeného Zadavatelem.
- Dohledování bezpečnostní situace Zadavatele.
- Detekce anomálie – rozpoznání odchylky od běžného stavu nebo od Zadavatelem normovaného stavu.

Fáze Přiřazení

- Klasifikace anomálie - určení závažnosti ve škále:
    - False-Positive Alarm – způsobuje falešný alarm z důvodu:
        - chyby v úsudku míry závažnosti anomálie;
        - nepřesnosti rozpoznání odchylky vzniklé při dohledování a monitoringu v předchozí fázi Detekce.
    - Bezpečnostní událost - anomálie, která může způsobit narušení bezpečnosti:
        - informací v informačních systémech Zadavatele;
        - služeb Zadavatele;
        - a integrity datových sítí Zadavatele.
    - Bezpečnostní incident – anomálie, která narušila či narušuje bezpečnost:
        - informací v informačních systémech Zadavatele;
        - služeb Zadavatele;
        - a integritu datových sítí Zadavatele nebo jiných subjektů.

Fáze Analýza

- Vyhodnocení anomálie – vyhodnocení relevance:
    - k systémům Zadavatele;
    - k procesům Zadavatele;
    - k zákonným normám ČR vztažených na Zadavatele.
- Klasifikace incidentu – začlenění incidentu do bezpečnostního typu kategorie dle určení Zadavatelem nebo dle §30, VoKB:
    - Podle příčiny:
        - incident způsobený kybernetickým útokem nebo jinou událostí vedoucí k průniku do systému nebo k omezení dostupnosti služeb;
        - incident způsobený škodlivým kódem;
        - incident způsobený překonáním technických opatření;
        - incident způsobený porušením organizačních opatření;
        - incident spojený s projevem trvale působících hrozeb;
        - ostatní incidenty způsobené kybernetickým útokem.
    - Podle dopadu:
        - incident způsobující narušení důvěrnosti aktiv;
        - incident způsobující narušení integrity aktiv;
        - incident způsobující narušení dostupnosti aktiv;
        - incident způsobující kombinaci výše uvedených dopadů.
    - Kategorizace incidentu – začlenění incidentu podle významnosti:

Fáze Eskalace a Notifikace Zadavatele

Dodavatel podle kategorie incidentu a relevance zajišťuje rozdělení notifikace (telefonní hovor, SMS, e-mail, tiket v ServiceDesk)