EVROPSKÁ UNIE
Evropský fond pro regionální rozvoj
Integrovaný regionální operační program

MINISTERSTVO PRO MÍSTNÍ ROZVOJ ČR

Výzva k podání nabídky na dodávku Centrálního logování a systému pro vyhodnocování auditních logů (SIEM)

podle §6 zákona č. 134/2016 Sb., o veřejných zakázkách ve znění pozdějších předpisů, dále dle směrnice č. 9 – Zadávání veřejných zakázek dle zák. č. 134/2016 Sb. k podání nabídky

Zadavatel:

Statutární město Brno, městská část Brno-střed,
Dominikánská 2, 601 69 Brno
IČ: 44992785 01
DIČ: CZ44992785
Kontaktní osoba: Arnošt Kolbábek, vedoucí odboru informatiky, Dominikánská 2, Brno,
e-mail: arnost.kolbabek@brno-stred.cz.

Název zakázky: „Dodávka kompletního systému log managementu a systému vyhodnocení (SIEM)“

Druh zakázky: veřejná zakázka malého rozsahu na dodávku zboží a služeb

Lhůta pro podání nabídky začíná běžet dnem doručení výzvy a končí 10.09.2018 ve 14:00 hod.
Místo pro podání nabídky:
Portál veřejných zakázek – EZAK - https://zakazky.brno-stred.cz

Předmět zakázky:
Předmětem veřejné zakázky je dodání, instalace, podpora hardwarového a softwarového řešení centrálního logování a managementu včetně systému vyhodnocení událostí (dále jen „SIEM “). Součástí je i školení zaměstnanců zadavatele. Následná podpora (vyhodnocování) po dobu pěti (5) let.
Implementace systému bude v provedena v souladu s § 23 Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí Vyhlášky č.316/2014 Sb. k Zákonu č. 181/2014 Sb., o kybernetické bezpečnosti.
Cílový stav:
- Implementací systému SIEM (Security Information and Event Management) musí dojít k zastřešení infrastrukturních, informačních a bezpečnostních systémů úřadu a získání přehledu o jejich provozu.
- Informace o provozu a potenciálních zranitelnostech informačních systémů musí umožnit zavádění preventivních opatření a předcházení případným bezpečnostním incidentům.
- Zavedením systému získat schopnost detekce bezpečnostních incidentů a informací pro jejich rychlejší a efektivnější řešení.
- Reporty systému budou sloužit pro přehlednou kontrolu stavu a chování informačních systémů a uživatelů a ke kontrole dodržování nařízení.

Požadavky na zavedení systému :

- Detailní analýza – identifikace zdrojů dat, jejichž provozně bezpečnostní informace bude nutné sbírat, korelovat a analyzovat
- Zdroje dat budou vybrány z tzv. primárních a podpůrných (technických) aktiv zadavatele. K jejich určení bude využito Vyhlášky č.317/2014 Sb. o významných informačních systémech a jejich určujících kritérií přiměřeně uzpůsobených a aplikovaných na MČ (zadavatel neprovozuje významný informační systém, ale využívá kritické informační infrastruktury). Dále požadujeme, aby pro určení zdrojů dat bylo využito vstupního osobního setkání v rozsahu jednoho pracovního dne.
- Předimplementační analýza bude obsahovat následující oblasti:
    - -specifikace profilu pro každý napojovaný zdroj dat, včetně určení vhodné úrovně detailu logování, odpovídající jeho roli v infrastruktuře,
    - -klasifikaci zdrojů informací pro stanovení priority události (stejná událost z různých zdrojů může mít různou prioritu) a z hlediska poskytovaných logů (obsažené informace, struktura logu),
    - -doporučení nastavení logování pro jednotlivé zdroje,
    - -výběr událostí a parametry jejich záznamů a metody sběru z jednotlivých zdrojů,
    - -návrh parserů pro zdroje, které nebudou systéme přímo podporovány,
    - -návrh doplňování logovaných informací z dalších zdrojů pro zlepšení jejich relevantnosti či srozumitelnosti,
    - -metody a pravidla identifikace, zpracování a vyhodnocování událostí, návrhy korelací,
    - -pravidla pro vznik varováni, upozornění, incidentů včetně priority,
    - -doporučenou strukturu oprávnění a řízení přístupových práv
    - -proaktivní a reaktivní procesy (aktivity, role, výstupy, doba odezvy) v případě výskytu varování, upozornění, incidentu a apod.
    - -popis zajištění autentičnosti logů,
    - -definice pohledů na události v konzole uživatelů (např. setřídění událostí podle zdroje, typu, priority, stupně důležitosti, času vzniku apod.),
    - -návrh zálohování konfigurace a dat, návrh retence logů a archivů,
    - -návrh průběhu Zkušebního provozu pro ověření funkčnosti systému v reálném provozu,
    - -návrh způsobu napojení řešení na monitorovací systém uchazeče a definice procesů reakce,
- Návrh a případné provedení konfigurací dotčených a souvisejících systémů
- Návrh a provedení akceptačních testů (musí zahrnovat výkonové testy, testy archivace a obnovy logů a ověření detekce jejich neoprávněně modifikace).

Požadavky na podporu při provozu:

Minimální rozsah podpory v rámci paušálu:

-Pravidelné servisní prohlídky a revize předepsané výrobci

-Průběžné monitorování prvků IT

-Analýza požadavků a incidentů – dle podmínek SLA

-Profylaxe - minimálně každých 12 měsíců

-Hotline podpora v režimu 9x5

-Odborná podpora v režimu 9x5 – vzdálené konzultace pro podporované služby/produkty.

Celkový rozsah služeb Hotline a Odborné podpory v rámci měsíčního paušálu min. 8 hodin.

-Zajištění tj. dodávku, instalaci a zprovoznění maintenance a aktualizací (včetně bezpečnostních signatur apod.) pro veškerý dodaný software – min. 1x ročně a v případech vynucených změnou legislativy či změnou navázaného systému.

-Helpdeskový systém s on-line přístupem pro kompletní správu požadavků včetně uchování historie požadavků a jejich řešení.
-Rozšířený monitoring a specifické služby provozního zajištění komodity SIEM
-Provádění monitoringu systému a zpracovávaných dat v rozsahu potřebném pro provádění následujících služeb v režimu 9x5
- Informování odpovědných osob zadavatele o vzniku bezpečnostního incidentu v reálném čase za pomocí základních komunikačních nástrojů (mail / tel)
- Zahájení řešení bezpečnostního incidentu do 4hodin od vzniku, řízení souvisejících činností správců a případných dalších dotčených osob.
- Zakládání tiketů, proaktivní komunikace o jejich řešení. Komunikace s třetí stranou jako NBU, NUKIB, NCKB, CSIRT, MMB – Technické sítě, ÚOOU atd.
- Rozšířený reporting - detailní report o událostech a incidentech s návrhy systematických opatření 1x měsíčně.
- Pravidelné skenování aktiv a zranitelností min. 1x týdně.
- Zpracování a poskytnutí měsíčního Report, ve kterém je popsán průběh realizace Plnění za uplynulé období, provedené služby a návrh doporučených opatření pro další období pro zvýšení bezpečnosti a dostupnosti TC ORP a prevenci incidentů.

Min. požadavky na HW, na kterém systém poběží:
1x Procesor Intel 2,1 G, min. 16 Core
Min 4x 8GB RDIM, 266MT/s
Diskové pole Raid 1 – min. velikost 8TB 7,2 K RPM SATA 6Gbps
Diskové pole Raid 1 – min velikost 3,6 TB SAS 12 Gb
2x zdroj Hot Plug
6x Ethernet 1Gbe
Podpora 5 let – Next Business Day

Požadavky na SW:

Základní funkce	Integrovaný systém zpracování logů a událostí z definovaných zdrojů napříč výrobci aplikací, operačních systémů a síťového hardware a sledování síťových toků a detekce anomálií
Ovládání	Uživatelsky přívětivý přístup ke všem komponentám systému z jednotného grafického uživatelského rozhraní (GUI). Konfigurace, definice zdrojů logů, definice korelačních pravidel, tvorba reportů, řešení událostí a další běžné operace musí probíhat z jediné řídící konzole s jednotným GUI.
Správa prvků	Automatické jednorázové i plánované vyhledávání i ruční přidávání Prvků a detekce jejich typů a vlastností. Prvkem se rozumí hw i sw (např. OS) s IP adresou. Prvky jsou typicky zdroji dat - logů a událostí.
Skupiny Prvků	Podpora zařazování Prvků do skupin/kategorií dle vlastností (typ, operační systém, dostupné služby, síť apod.) i metadat (umístění, hodnota apod.)
Metadata Prvků	Možnost konfigurace metadat Prvku - min. hodnota, priorita a spolehlivost (věrohodnost) událostí
Monitorování Prvků	Automatické monitorování stavu Prvku - min. dostupnost poskytované služby a základní dostupnost (odezva na ping)

Vyhledávání Prvků	Víceparametrové vyhledávání a filtrování Prvků podle vlastností i metadat, export do souboru v běžném strojově zpracovatelném formátu (např. csv, xml apod.)
Vazby	Detekce síťových prvků standardními protokoly a mapovaní jejich vazeb
Detekce zranitelností	Automatická ruční i plánovaná detekce zranitelností Prvků (i nezařazených) - porovnání stavu Prvků s databází známých zranitelností průběžně aktualizovanou výrobcem
Profily zranitelností	Vestavěné i uživatelsky definované profily detekce zranitelností - definice typů zranitelností, které mají být kontrolovány.
Autentizace	Podpora detekce zranitelností s i bez přihlášení (autentizací) ke kontrolovanému Prvku.
Detekce průniku	Víceúrovňová detekce průniku (intrusion detection) - min. na úrovni sledování síťového provozu a na úrovní Prvků.
Instalace agentů	Podpora vzdálené instalace ID agentů (intrusion detection) min. pro operační systémy Microsoft Windows
Detekce průniku - assety	Monitoring a analýza uživatelských aktivit, logů, integrity souborů a registrů, rootkitů či obdobného škodlivého kódu
Detekce průniků - síť	Analýza monitorovaných síťových toků a detekce anomálií indikujících možné narušení bezpečností politiky (NBA - Network Behavior Analysis)
Detekce anomálií	Monitorování síťových toků technologií netflow (min. verze 5,9,10) či kompatibilní (ipfix, netstream) dle nabízených sond a přepínačů.
Síťové toky hyervizor	Podpora sledování síťových toků (netflow či kompatibilní) virtuálních síťových přepínačů VMware vSphere
Viditelnost síťových toků	Viditelnost síťového provozu - zobrazení, prohledávání, filtrování síťových toků včetně historie
IP reputace	Integrovaná služba aktualizovaná výrobcem ohodnocující reputaci a spolehlivost veřejné IP adresy s možností změny priorit událostí, alarmů apod. Reputace založena na detekovaných (aktivitách IP adresy (spam, skenování, phising, distribuce malware, botnet apod.
Protokoly	podporované protokoly min. syslog, windows events collection (pomocí agenta i bezagentově (např. WMI), snmp, s/ftp, nfs, cifs, netflow
Ukládání logů	Bezpečné ukládání logů s řízeným přístupem v nezměněné (nefiltrované) podobě (tzv. raw logy)
Zpracování logů	Centrální zpracování logů, jejich normalizace, korelaci, grafická interpretace a archivace, včetně logů generovaných samotným řešením
Rozšíření logů	Vytváření vlastních atributů v událostech. Automatické doplňování atributů aktuálními hodnotymi z externího zdrojů. Podpora atributů v celým systému - vyhledávání, filtrace, korelace atd.
Prohledávání logů	Pokročilé prohledávání a filtrování raw logů, podpora indexování pro zrychlení hledání
Expirace logů	Podpora automatické rotace raw logů s nastavením doby expirace
Zálohování logů	Podpora zálohování logů na externí síťové úložiště

Ochrana logů	Zajištění integrity raw logů aplikací digitální podpisu. Možnost jednoduchého uživatelského ověření integrity
Centralizace logů	Konsolidace logů na jednom centrálním místě.
Geolokace	Automatické doplňování geolokačních informací k událostem a jejich grafické znázornění na mapě
Doplňování názvů	Automatické doplňování reverzních DNS a hostname záznamů k IP adresám.
Identifikace MAC	Automatické doplňování výrobce zařízení podle MAC adresy
Grafy událostí	Grafické znázornění událostí - četnost, typ, časová osa
Parsery	Možnost vytváření uživatelských parserů bez nutnosti externí spolupráce
Ladění parserů	On-line ladění uživatelsky vytvářených parserů v reálném čase- okamžité zobrazení rozparsovaných dat při vložení testovací zprávy/události.
Standardizace logů	Standardizace přijatých logů do jednotného formátu, parsování parametrů do předepsaných polí
Pohledy	Předpřipravené pohledy a podpora vytváření vlastních pohledů na data uživateli a jejich ukládání pro pozdější využití a zpracování dat. Včetně grafické reprezentace dat - grafy, mapy apod.
Reporty	Integrovaný reportovací nástroj s přednastavenými obvyklými reporty a možností vlastních úprav a vytvoření nových reportů. Včetně grafické reprezentace dat - grafy, mapy apod.
Upozornění	Zasílání uživatelsky vytvořených upozornění podle uživatelsky definovaných podmínek. Možnost zahrnutí přijatých rozparsovaných dat do upozornění.
Správa uživatelů	Správa uživatelů systému musí být integrovatelná s MS Active Directory. Systém musí umožňovat i přihlašování pomocí lokálních účtů. Podpora lokálního nastavení uživatelských oprávnění
Tikety	Možnost vytváření tiketů k bezpečnostním událostem s možností přiřazení řešiteli. Možnost sledování průběhu tiketů včetně historie - obsah, vykonané činnosti, eskalace. Podpora jednoduchého manuálního vytváření tiketů v průběhu vyšetřování incidentu.
Automatizace tiketů	Tikety lze vytvářet automaticky na základě vytvořené policy k jednotlivým událostem / zranitelnostem.
Politiky	Podpora vestavěných a tvorby vlastních komplexních politik zpracování událostí Politiky musí umožnit spustit minimálně následující akce: odeslání emailu, vytvoření tiketu, spuštění skriptu.
Korelace	Podpora korelací události na základě definovaných parametru bez závislosti na typu zdroje. Vestavěné a výrobcem aktualizované korelace, podpora vytváření vlastních
Rozšířené korelace	Systém musí umožňovat tvorbu korelacínejen napříč zdroji, ale také napříč daty z interních subsystémů (např. detekce zranitelnosti, průniků, IP reputace). V závislosti na datech interních subsystémů je případně upravena vážnost incidentu (oproti standardní korelaci).
Upozornění	Podpora vytvářet upozornění (alertů) na základě korelovaných událostí včetně zahrnutí rozšířených korelací. Vestavěná upozornění i podpora ručního vytváření.

IT Compliance	Podpora compliance (jednání v souladu s pravidly") - certifikace dle obvyklých bezpečnostních standardů a norem PCI DSS, HIPAA
Auditní reporty	Vestavěné, výrobcem aktualizované šablony reportů pro podporů kontrolních a certifikačních auditů - min. dle standardů PCI DSS, HIPAA, NIST CSF, ISO 27001
Legislativa	Systém musí zajistit bezpečné, úplné a nezpochybnitelné ukládání, vyhodnocování a archivaci logů ICT prostředí zadavatele a naplnění požadavků dle zákona č. 181/2014 Sb. (ZKB) a vyhlášky č.316/2014 Sb. (VKB), o kybernetické bezpečnosti, a to v platných zněních
Provedení	Centrální část systému bude realizována jako jedna virtuální appliance
Licence	Licence pro minimálně 150 Prvků. Součástí licence bude centrální část systému a dále samostatný (sub)systém (virtuální appliance) zajišťující sběr dat a vykonávání funkcí systému (např. detekci Prvků, testy zranitelností, monitoring síťových tok, sběr logů atd.) lokálně ve vzdálené lokalitě (U spořitelny) a předávání dat a událostí do centrální části systému).
Výkon	Trvalé zpracování celého subsystému 1500 EPS (events per second - událostí za sekundu)
Škálovatelnost	Možnost zvýšení výkonu doplněním dalších appliance pro sběr dat a vykovávání funkcí systémů, popřípadě rozdělením systému na více serverů.
Vysoká dostupnost	Možnost doplnění dalšího systému (nodu)
Záruka	Min. 60 měsíců včetně nároku na nové verze software a včetně aktualizací bezpečnostní a funkčních signatur (zranitelnosti, korelační pravidla, detekce průniku, detekce Prvků (typy zařízení, aplikace, operační systémy), aktualizací reportů popř. další.

Podmínky a požadavky na zpracování a podání nabídky:

Nabídka bude podána prostřednictvím Portálu veřejných zakázek _EZAK
https://zakazky.brno-stred.cz

požadavky na zpracování nabídky: součástí nabídky bude

- Krycí list nabídky – obsahuje:
  - identifikační údaje uchazeče
  - kontaktní informace,
  - Celkovou nabídková cena v Kč bez DPH i s DPH, včetně dopravy do místa plnění – sídlo zadavatele. Součástí celkové nabídkové ceny budou nabídkové ceny za každé zařízení/položku samostatně v Kč bez DPH a s DPH (pokud není dodáváno jako celek);
- Podrobné technické parametry všech nabízených zařízení
- Cena za hardware, instalaci a licenci – jednorázová platba
- Cena za roční podporu a vyhodnocování událostí

Doba plnění zakázky: říjen 2018

Místo plnění zakázky: Statutární město Brno, městská část Brno-střed, Dominikánská 2, 601 69 Brno

Způsob hodnocení nabídek:

Základním hodnotícím kritériem je ekonomická výhodnost předložených nabídek. Hodnocena bude celková nabídková cena včetně DPH s vahou kritéria 100%
Jako nejvýhodnější nabídka bude vybrána nabídka s nejnižší nabídkovou cenou.

Zadavatel nepřipouští variantní nabídky.

Ostatní:

- Dodavatel je oprávněn po zadavateli požadovat vysvětlení zadávacích podmínek. Pokud bude. písemná žádost o vysvětlení, tak musí být zadavateli doručena nejpozději 4 pracovní dny před uplynutím lhůty pro podání nabídek.
- Zadavatel si vyhrazuje právo veřejnou zakázku zrušit i bez udání důvodů
- Zadavatel si vyhrazuje právo změnit nebo doplnit soutěžní podmínky, upřesnit technickou specifikaci u zařízení v průběhu lhůty pro podání nabídek a to všem zájemcům shodně
- Smlouva na podporu a vyhodnocování systému událostí bude uzavřena na 5 let
- Smlouva (objednávka), uzavřená z vítězným dodavatelem, včetně jejích případných změn, bude zveřejněna na základě zákona č. 106/1999 Sb., o svobodném přístupu k informacím, vyjma informací uvedených v §7- §11 zákona. Veškeré údaje, které požívají ochrany dle zvláštních zákonů, zejména osobní a citlivé údaje, obchodní tajemství, aj. budou anonymizovány.

Bc. Arnošt Kolbábek

vedoucí Odboru informatika