Statutární město Ostrava
městský obvod Ostrava - Jih
úřad městského obvodu

Smlouva

Příloha č. 1

- ke Smlouvě na dodávku software dle GDPR pro počítačovou síť
nedílná součást zadávací dokumentace k podmínkám výzvy VZ 145.18

Specifikace minimálních požadavků na software

I. Účel předmětu dodávky

Software musí naplňovat požadovaný účel dodávky.

1. Úřad při zpracování osobních údajů dle požadavků Nařízení EU 2016/679 (dále jen „GDPR") zavedl potřebná opatření a data s osobními údaji ukládá v příslušných agendových systémech a na koncových stanicích. Z tohoto pohledu osobní údaje proudí počítačovou sítí (dále jen „**síť**") a je nutno je chránit před možným zneužitím v síti v souladu se zásadami GDPR.
2. **Dodávka softwarového řešení** pro počítačovou síť, zavede kontrolní mechanismy pro detekci narušení bezpečnosti včetně centrálního logu a monitorování síťové infrastruktury jako ucelený systém (dále jen „**systém**", „**řešení**" nebo „**software**").
3. Dodané software bude tvořit funkční celek, který může být složen z různých samostatných částí jednoho nebo více dílčích řešení.
4. Součástí dodávky řešení může být i dodávka appliance pro přísluný software nebo jeho část.
5. **Správce (administrátor)** software bude mít k dispozici **jednotnou centrální webovou konzoli** pro přístup k logům, alertům, reportům a pro správu systému. Z této konzole se provádí veškerá konfigurace, správa a analýza logů. Není přípustné, aby dodaný systém měl jen více různodých konzolí pro jednotlivé části systému. Dále:
   1. Systém musí umožňovat snadné vytváření uživatelských rolí definujících přístupová práva k uloženým událostem a jednotlivým ovládacím komponentům systému.
   2. Systém musí podporovat ověřování uživatele systému na externím LDAP serveru. V případě výpadku externího LDAP systému musí podporovat ověření z lokální databáze.
   3. Systém musí obsahovat API pro integraci s externím monitorovacím systémem (Zabbix, Nagios, MRTG a další) a umožnovat autorizovaný přístup ke strukturované databázi logů.
   4. Řešení musí umožňovat správu zařízení s agentem (operační systémy Linux a Microsoft v různých verzích) minimálně pro 250 zařízení a správu zařízení bezagentově pro minimálně 1000 spravovaných IP adres min. protokoly SNMP v2, SNMP v3, IMPI, JMX, WMI, Telnet/SSH.
6. Zadavatel požaduje **licenci bez omezení** na počet spravovaných zařízení, ukládanou kapacitu dat a počet uživatelů.
7. **Řešení musí zahrnovat v ceně dodávky všechny náklady** na provoz řešení, tedy včetně licence na operační systémy pro nabízené řešení, databázi, middleware a pod. (bez omezení ukládané kapcity).
8. Dodané řešení nesmí být řešeno formou pronájmu, po skončení technické podpory musí být dále schopno pracovat.
9. Dodavatel může nabídnout hardwarovou appliance a nevyužít volnou kapacitu zadavatele, pokud je zahrnuta v ceně za implementaci dodávky.
10. **Záruka a technická podpora.** Zadavatel požaduje **technickou podporu na řešení po dobu 5 let**, součástí podpory musí být **periodické kontroly stavu systému** a kontrola incidentů v rozsahu 3 hod. měsíčně s písemným reportem zadavateli.

OSTRAVA!!!
OSTRAVA-JIH

II. Bližší specifikace předmětu dodávky

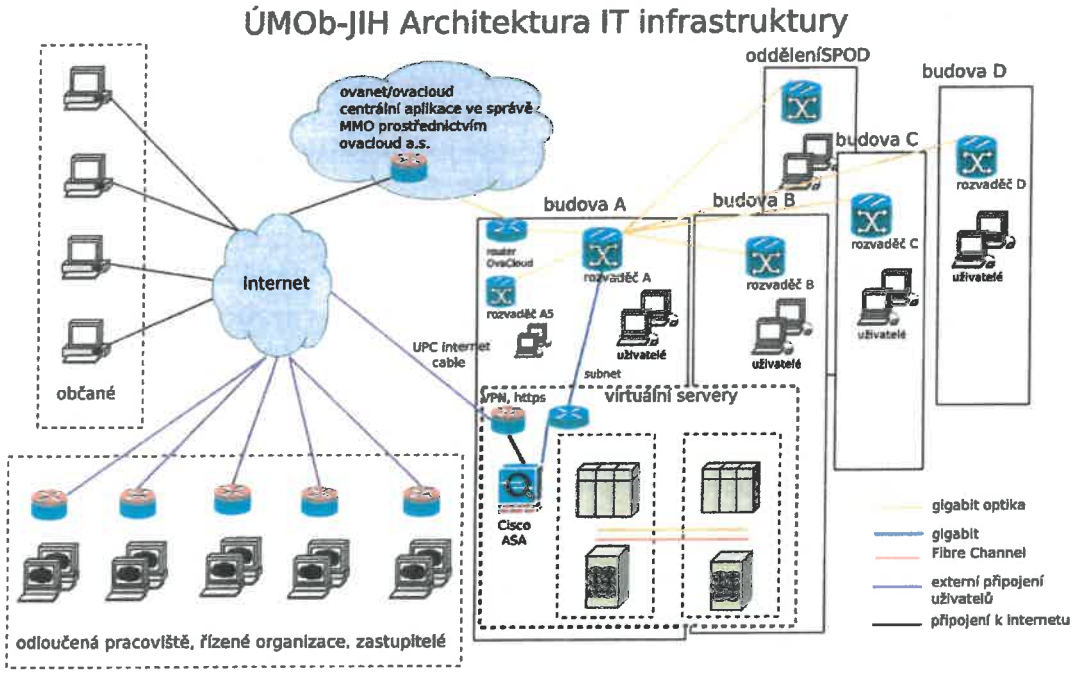
1. **Detekce narušení bezpečnosti a centrální log** - Zadavatel požaduje řešení splňující následující kritéria (Dodavatel do nabídky uvede formou odkazu do dokumentace nabízeného řešení, jak je vlastnost splněna):
   1. Škálovatelné a robustní řešení s licenčně neomezeným množstvím EPS. Výkon minimálně 10000 EPS (srovnávací výkon - nezohledňuje zadavatelem použitý storage)
   2. Redundance všech komponent řešení
   3. Systém může pracovat jako více nodová virtuální appliance avšak s jedním uceleným rozhraním pro všechny administrátorské i operátorské činnosti.
   4. Systém provádí zpracování událostí z předdefinovaných zdrojů logů napříč výrobci aplikací, operačních systémů a síťového hardware
   5. Systém umožňuje dopsání parseru logů bez nutnosti spolupráce s výrobcem nebo dodavatelem
   6. Integrace NetFlow/Sflow (protokoly pro monitorování IP toků) kolektoru
   7. Systém přijímá a zpracovává logy, události a další strojově generovaná data prostřednictvím běžně dostupných UDP/TCP portů. Systém musí umožnovat přijímat logy i na uživatelsky definovaných UDP a TPC portech. Přijaté logy systém standardizuje do jednotného formátu a logy jsou rozdělovány do příslušných polí dle jejich typu
   8. Eventy zasílané koncovými zařízeními do SIEM řešení (Security Information and Event Management - management bezpečnostních informací a událostí) je možno přenášet v šifrované podobě
   9. Všechny pole a položky přijaté systémem jsou automaticky indexovány. Nad všemi položkami je možné ihned provádět vyhledávání bez nutnosti dodatečného ručního indexování administrátorem.
   10. Podpora OSINT (Open-Source Intelligence)
   11. Systém provádí konsolidaci logů na centrálním místě. Databáze logů je redundantní
   12. Systém umožňuje snadné vyhledávání událostí (ad hoc) bez nutnosti dodatečného programování nebo aplikování dotazů v SQL jazyce.
   13. Systém provádí ucelenou vizualizaci logů a událostí (grafy událostí). Vizualizace musí být dynamická, tj volbou v jednom grafu se ostatní příslušné grafy v pohledu na data upraví dle požadované volby automaticky.
   14. Systém umožňuje snadno vytvářet grafické znázornění TOP událostí nad všemi daty za určité časové období.
   15. Systém provádí automatické doplňování GeoIP informací k událostem a jejich grafické znázornění na mapě.
   16. Systém provádí automatické doplňování reverzních DNS záznamů k IP adresám.
   17. V případě přetížení systému nesmí dojít ke ztrátě logů. Všechny přijaté nezpracované logy/události musí být ukládány do vyrovnávací paměti.
   18. Systém musí umožňovat unifikované vyhledávání napříč všemi typy dat a zařízení.
   19. Systém musí mít možnost uložení uživatelem vytvořených pohledů na data (dashboardů) pro budoucí zpracování.

20. Systém obsahuje reportovací nástroj s přednastavenými nejběžnějšími reporty a možností vlastních úprav a vytvoření nových pohledů. Pro vytváření nových pohledů na data není přípustné používat povinně SQL jazyk.
21. Systém obsahuje předpřipravené pohledy na uložená data dle jednotlivých kategorií zdrojových zařízení i dle logického členění.
22. Systém podporuje i automatizuje průběžné aktualizace reportů a pohledů výrobcem.
23. Monitoring stavu systému - alertování při překročení prahových hodnot nebo chybě systému, přeposlání upozornění pomocí SMTP nebo Syslog.

2. **Monitorování síťové infrastruktury** - Zadavatel požaduje řešení splňující následující kritéria (Dodavatel do nabídky uvede formou odkazu do dokumentace nabízeného řešení, jak je vlastnost splněna):
   1. možnost tvorby vlastních scriptů pro monitoring, software musí mít dobře definované API s příklady implementace
   2. připravené Templates (šablony) pro typická síťová zařízení, aplikace, databáze a systémy
   3. agregace metrik – sumární datové toky za prvek
   4. autodiscovery - automatické přidání nového prvku
   5. asset managment – evidence sériových čísel aktivních prvků
   6. korelace událostí
   7. možnost definice víceúrovňové závislosti mezi souvisejícími uzly sítě
   8. automatické vytváření vizuálních map infrastruktury
   9. tvorba grafů a jejich zobrazování v mapách
   10. integrace se SW třetí strany (helpdesk, tiketovací systém, SIEM), otevřené API pro napojení na SW třetích stran (zadavatel uvede seznam dostupných API a seznam SW s hotovým konektorem – pouze API a konektory, které jsou součástí cenové nabídky)
   11. automatizace s využitím API
   12. vytváření linků v mapách
   13. možnost vzdáleného přístupu více uživatelů, možnost zobrazení individuálních map
   14. podpora IPv6
   15. napojení na SIEM
   16. backup konfigurací síťových prvků
   17. podpora syslog
   18. email a SMS notifikace

III. Rozsah implementace

1. Rozsah implementace definuje jaké má být provedeno úvodní nastavení dodaného software. Dodávaný software bude provozován ve virtualizačním prostředí vmware, kde má zadavatel pro tento účel rezervovanou kapacitu 4 fyzických jader CPU (PassMark cca 10000), 32GB RAM, 15TB disk (300 iops). Případně může být také provozován z části nebo celý na dodané applianci pro přísluný software. Souhrnně je v Active directory evidováno do 500 účtů (včetně technických). Přehledové schéma architektury IT městského obvodu Ostrava-Jih:



2. Instalace a nastavení software bude provedeno dodavatelem v produkčním prostředí. Během prací nesmí dojít k ohrožení provozu při testování různých nastavení dodaného software.
3. **Detekce narušení bezpečnosti a centrální log** - Zadavatel požaduje implementaci v následujícím rozsahu:
   - **a)** integrace s monitorovacím systémem
   - **b)** nastavení zasílání logů ze síťových zařízení (max. 50)
   - **c)** nastavení zasílání logů z bezpečnostních prvků (max. 5)
   - **d)** nastavení zasílání logů z operačních systémů serverů (max. 50)
   - **e)** základní nastavení pravidel
   - **f)** školení obsluhy v rozsahu 8 hod. (pro max. 5 osob v prostorách zadavatele)

4. **Monitorování síťové infrastruktury** - Zadavatel požaduje monitorovat kritické body všech komponent infrastruktury a vizualizaci aktuálního stavu. Dodavatel zajistí analýzu infrastruktury, navrhne vhodné monitorovací metriky a jejich kritické hodnoty a definuje hierarchické závislosti mezi prvky. Zadavatel odsouhlasí navržené metriky, které pak dodavatel nastaví. Zadavatel požaduje minimálně monitorovat::
   a) L2 prvky
      1. monitoring přibližně 30 prvků
      2. dostupnost management rozhraní prvku
      3. zdraví prvku (CPU, RAM, Teplota, Napájení, síla signálu optických převodníků …)
      4. chyby logované prvkem a SNMP trapy
      5. interface a datové toky

   b) L3 prvky
      1. monitoring přibližně 20 prvků
      2. dostupnost management rozhraní prvku
      3. zdraví prvku (CPU, RAM, Teplota, Napájení, síla signálu optických převodníků …)
      4. chyby logované prvkem a SNMP trapy
      5. interface a datové toky

   c) operační systémy a servery
      1. monitoring přibližně 20 prvků
      2. dostupnost management rozhraní prvku
      3. chyby logované prvkem
      4. vytížení prvku (CPU, RAM, disk)
      5. spuštěné procesy a služby
      6. dostupnost služeb poskytovaných prvkem

IV. Akceptace dodávky

1. Dodavatel předvede **splnění** minimálních požadavků na požadovaný **účel dodávky** uvedený **v části I.** a požadované **vlastnosti software** uvedené **v části II.** této přílohy podle jednotlivých bodů na provedené instalaci nebo předpřipravených ukázek.
2. Dodavatel předvede splnění minimálních požadavků na **rozsah instalace** uvedený **v části III.** této přílohy podle jednotlivých bodů 1 až 4.
3. **Akceptace – hodnocení**
   Pro akceptaci dodaného software je třeba aby akceptace proběhla kladně ve všech částech akceptace IV.1. až IV.2. (průběh akceptace viz smlouva).

Ing. Vladimír Měkota
Digitálně podepsal Ing. Vladimír Měkota
Datum: 2019.03.08 13:40:02 +01'00'

Ing. Milan Juřík
Digitálně podepsal Ing. Milan Juřík
Datum: 2019.03.08 14:00:46 +01'00'