Příloha č. 7 Zadávací dokumentace
Příloha A smlouvy

Požadavky na technické řešení

Popis

Dodání systému – řešení bezpečnostního dohledu pro vyhodnocování a detekci bezpečnostních událostí v oblasti IT v souladu s § 21 vyhlášky č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti.

Současné nasazené prostředky

V současné době využíváme pro log management řešení Splunk Enterprise s jednou licencí 5 GB/den. (Licence je platná, ale z důvodu této veřejné zakázky nebyla obnovena podpora. Před podáním nabídky je nezbytné, aby dodavatel požadované obnovení podpory konzultoval s výrobcem řešení Splunk Enterprise.) Toto řešení plánujeme využít zároveň jako základ nového bezpečnostního dohledu. Splunk Enterprise nyní zajišťuje sběr logů ze všech systémů nad kterými je prováděna základní a provozní analýza.

Obecné požadavky na poptávaný systém

Požadované funkcionality budou popsány v dokumentaci požadované současně s nabídkou dle bodu 2.3. Zadávací dokumentace.

Systém bezpečnostního dohledu:

- musí zahrnovat všechny potřebné licence pro provoz Bezpečnostního monitoringu, včetně podpory,
- bude využívat pouze stávající log management, nebo bude nahrazen novým log managementem bez využití současného řešení Splunk Enterprise,
- musí zpracovávat a vyhodnocovat min. 10GB příchozích dat za den v jedné síťové infrastuktuře,
- musí zpracovávat a vyhodnocovat min. 5GB v jiné fyzicky oddělené síťové infrastuktuře,
- musí zajistit, aby celé řešení fungovalo i bez přístupu na internet,
- musí zpracovávat data z neomezeného počtu zařízení (do systému je možné zasílat data z jakéhokoliv počtu typu zařízení s neomezeným počtem datových zdrojů),
- musí být dodán do virtualizačního prostředí RedHat Enterprise Virtualization, kdy dodané řešení musí toto virtualizační řešení podporovat,
- musí umožňovat správu uživatelů jako jednotné přihlášení do celého řešení, a to pomocí lokálních účtů, LDAP, AD,
- nesmí být licencován na počet uživatelů (bez rozlišení rolí uživatel, administrátor, atd. .....),
- musí zajistit, aby se zadavatel po převzetí díla (zaplacení) stal vlastníkem dodaných licencí na neomezenou dobu (tzn., že po ukončení smlouvou dané podpory bude řešení dále využíváno bez další podpory a aktualizací),
- musí zajistit, aby při překročení objemu zpracovaných dat za den nedošlo k zastavení/zahazování nových příchozích dat (vztahuje se na licenční omezení, HW požadavky řeší zadavatel). Zadavatel musí

mít možnost tyto jednorázové problémy vyřešit, aniž by byla ovlivněna funkcionalita celého řešení,

- musí být dodán jako samostatný virtuální stroj nebo nástavba nad stávajícím řešením (viz odstavec Současné nasazené prostředky),
- musí mít prostředí v českém nebo anglickém jazyce,
- musí po nastavitelnou dobu zaznamenávat vlastní auditní logy (viz § 21 vyhlášky č. 316/2014 Sb.), které musí být chráněny proti modifikaci,
- musí umožnit v grafickém prostředí nastavovat/spravovat/vytvářet veškeré základní konfigurace definic zdrojů logů, definic korelačních pravidel, tvorbu reportů atd.; zpřesňující nastavení je možné provádět v textovém nebo jiném režimu,
- musí obsahovat auditní informace o systému a uživatelích,
- musí být podporován výrobcem po dobu požadované podpory,
- nebude prototypem vyvinutým pro účel této veřejné zakázky; veškerou funkcionalitu musí být dodavatel schopen na vyžádání zadavatele demonstrovat,
- musí být z aktuální produktové řady výrobce,
- musí umožňovat rozšíření řešení až do min. množství zpracovaných dat 50GB/den v každé síťové infrastruktuře.

Požadavky na vyhodnocování bezpečnostních událostí

Požadované funkcionality budou popsány v dokumentaci požadované současně s nabídkou dle bodu 2.3. Zadávací dokumentace

Systém musí (některé z následujících bodů mohou být řešeny i v rámci log managementu):

- umožňovat vyhledávání dle klíčových slov (řetězců) v názvech zdrojů, v korelačních pravidlech, v uložených log souborech a v auditních log souborech řešení, to celé v grafickém prostředí,
- rozlišovat zdroj log souborů,
- podporovat tagování pro jednotlivé události,
- zajistit dostupnost logu v nezměněném tvaru, tak jak byl poslán ze zdrojového zařízení po dobu minimálně 90 dní,
- mít evidenci aktiv (pro zadavatele důležitých prvků IT, může se jednat například o službu nebo prvek v síti)
    - u aktiv a identit je možné definovat jejich váhu a riziko, se kterou dále pracuje risk management,
- nad logy provádět parsování:
    - tzn., že z jakéhokoliv čitelného formátu je možné pomocí regulárních výrazů vybírat části logů a přidávat je do proměnných/pojmenovaných hodnot,
- nad logy provádět normalizaci:
    - tzn., že je možné zvolit datovou strukturu (Datovou strukturou je myšlen souhrn informací, které jsou důležité pro jednu oblast. Například pro autentizaci by měla datová struktura

obsahovat informace o zařízení, kam se uživatel hlásil, jaký uživatel se hlásil, kdy se hlásil, zda byla akce úspěšná či neúspěšná. Všechny tyto informace pak mají stejný formát a obsah napříč každým zdrojem přijímaných dat, například autentizace. Do této struktury musí být možné automatiky zařazovat logy, které odpovídají regulárnímu výrazu. Těchto regulárních výrazů však může být více pro jednu skupinu),

- tzn., že jednotlivé hodnoty v datové struktuře budou v jednotném tvaru a formátu a popsány v dokumentaci,
- minimálně musí systém obsahovat datové struktury normalizovaných logů vyplývajících z § 21 vyhlášky č. 316/2014 Sb.,
- uživatel může v grafickém rozhraní tvořit vlastní datovou strukturu normalizovaných logů, definovat jejich strukturu a určovat, jaké typy logů budou normalizovány do takových struktur,
- příchozí logy mohou být normalizovány a uloženy v jedné nebo více datových strukturách,
- při normalizaci lze provádět datové obohacování z jiných zdrojů (např. doplnit jméno počítače za základu jeho IP adresy, doplnit lokalitu dle GEO informace, provést dotaz do LDAP, spuštěného skriptu apod.).

- nad logy provádět korelace
  - korelace lze provádět jak nad normalizovanými logy, tak i nad logy v původním formátu,
  - automaticky stanovit závažnost událostí na základě předchozí činnosti zdroje / cíle nebo jiných dostupných informací apod.,
  - vyhledávat anomálie v událostech nebo v datových tocích (nárůst počtu neúspěšných pokusů o přihlášení v určitém čase, neúspěšné pokusy o přihlášení v mimopracovní době, neobvyklé toky dat apod.),
  - využívat predikční algoritmy při realizaci korelací,
  - definování / přidávání vlastních korelačních pravidel a log parserů přímo v grafickém uživatelském rozhraní (GUI) bez nutnosti spolupráce s dodavatelem nebo výrobcem, např. pomocí wizardu nebo regulárních výrazů,
  - real-time korelaci a korelaci v časovém okně několika hodin mezi událostmi z různých zdrojů (libovolných a nezávislých zdrojů předávajících data do systému),
  - korelaci událostí dávkově importovaných do systému, tj. korelaci událostí, které nejsou zařazovány real-time, ale např. prostřednictvím importů logů,
  - musí obsahovat komplexní sadu funkcionalit a přednastavených korelačních pravidel, které řeší klasické hrozby a bezpečnostní rizika i sofistikované bezpečnostní problémy z oblastí:
    - Útoky robotů, červů a virů (chyby antivirů)
    - Monitorování databází (Chyby a varování, přístupy do DB, konfigurace)
    - Neoprávněný přístup k aplikacím (ověřování uživatelů, změny administrace a konfigurace)
    - Monitorování serverů a desktopů (administrace privilegovaných uživatelů, přístupy a

změny konfigurace, odmítnutá připojení, úspěšné a chybné přihlašovací aktivity, varování systémů IPS/IDS a využívání šíře pásma)

- na události navázat automatické akce, spuštění externího skriptu,
- umožňovat notifikaci přes email s možností definovat pravidla pro zasílání na různé adresy podle kritičnosti, zdroje apod.,
- podporovat napojení nezávislých zdrojů obohacujících informací např. (DNS, IDM, LDAP, DHCP, AD, Radius, atd.),
- podporovat možnost tvorby vlastních editovatelných Dashboardů a Vizuálních Analýz v GUI,
- podporovat pokročilý Alert Management (výpočet Alert Score události se skládá z více vstupů a musí obsahovat položku váhy aktiva,
- bude podporovat Anotace/Poznámky pro detekované alerty,
- bude obsahovat workflow pro podporu řešení detekovaných událostí a incidentů. Incidenty je možno předávat mezi jednotlivými řešiteli, přiřazovat jim závažnost a sledovat jejich stav. K jednotlivým incidentům je možno vázat další související informace, např. přiřadit výsledek vyhledávání dalších souvislostí apod. Workflow ke každému incidentu bude obsahovat časovou osu, kde je možno sledovat veškeré akce řešitelů.

Požadavky na reporting **(některé z následujících bodů mohou být řešeny i v rámci log managementu)**

- reporty řešení musí být předdefinovatelné a modifikovatelné
- musí umožňovat definovat vlastní reporty
- musí poskytovat reporty i ve formě grafů a tabulek
- umožňuje vytvářet reporty ve formátech PDF, HTML a CSV, popř. dalších strojově čitelných datech
- umožňuje poskytovat report o aktivitách vybraných uživatelů resp. skupiny uživatelů
- umožňuje poskytovat pro každého uživatele vlastní personalizovaný dashboard
- umožňuje drill-down analýzu v GUI tj. od obecnějších informací vedou linky na konkrétnější informace a to s využitím minimálního počtů kroků
- umožňuje podporu automatického spouštění definovaných reportů (měsíčně, týdně, denně, nebo v definovaném čase), ukládání na síťové úložiště a jejich zasílání e-mailem přímo ze systému

Požadavky na dodavatele

- dodavatel je partnerem výrobce dodaného systému
- termín dodání celého řešení je do 90 kalendářních dnů od podpisu smlouvy
- dodavatel prokáže formou potvrzené reference provedenou implementaci nabízeného řešení minimálně v obdobném rozsahu. Součástí reference bude stručný technický popis řešení. Zadavatel si

vyhrazuje právo možnosti v době posuzování nabídek vyzvat dodavatele k sjednání technické konzultační schůzky s provozovatelem referenčního řešení.

- podpora celého řešení bude poskytována po dobu 5 let a bude zahrnovat:
  - aktualizace softwarových produktů poskytnutých v rámci dodávky systému – řešení
  - komunikace s dodavatelem (směrem k výrobci) v případě potřeby řešení chyb

Požadavky na implementaci

- implementace bude realizována včetně všech požadovaných funkcionalit
- implementace bude prováděna formou praktického školení administrátorů zadavatele
- dodavatel si zajistí dokumentaci ke komerčně dodávaným řešením provozovaným zadavatelem; zadavatel dodá dokumentaci k řešením, které mu byly realizovány na míru třetí stranou
- každý ze zdrojů dat musí být dopracován tak, aby splnil podmínky § 21 vyhlášky č. 316/2014 Sb. jako kritický informační systém
- v procesu implementace zadavatelem definovaných zdrojů dat zajistí dodavatel:
  - analýzu možností jednotlivých zdrojů
  - dodání jednotlivých kroků pro nastavení zdrojů dat (nastavení na prvcích provede zadavatel)
  - provedení parsování
  - zapojení do datových struktur
  - přípravu a optimalizaci korelací
  - tvorbu dashboardů
  - nastavení nezbytná pro zajištění funkčnosti řešení

Zdroje dat

Seznam zdrojů dat je specifikován v příloze č. 10 Zadávací dokumentace – Seznam zdrojů dat, která je zároveň přílohou F smlouvy – Seznam zdrojů dat a jedná se o NEVEŘEJNOU INFORMACI.

Přípustná řešení:

1. <u>Při použití technologie Splunk:</u>
   Všechny funkcionality budou řešeny v rámci Splunku a rozšíření Splunku. Součástí nabídky bude aktualizace a rozšíření všech potřebných licencí včetně všech souvisejících poplatků a úrovně požadované podpory.

2. <u>Při dodání jiného řešení</u>
   Splunk nebude nijak využit (dojde k jeho kompletnímu nahrazení dodaným řešením).
   Současné řešení Splunk a jeho funkcionality jako log management budou dodaným produktem nahrazeny. Mezi tyto funkcionality patří
   i. Vysoká dostupnost napříč lokalitami
   ii. Zabezpečený přenos dat
   iii. Migrace současného nastavení

iv. Migrace ze stávajících zdrojů dat na nové řešení
v. Redundance dat
vi. Zachovat obdobné funkcionality log managementu

Požadavky na podporu

Podpora řešení (technických a programových prostředků) zahrnuje:

- odstraňování vad programových prostředků,
- poskytování aktualizací programových prostředků (nové verze, opravné verze, bezpečnostní záplaty),
- pomoc při řešení provozních problémů,
- podporu na místě při implementaci aktualizací programových prostředků, a to na základě výzvy objednatele,
- bude poskytována v pracovní dny od 7:45 do 16:30 hod.,
- dodavatel poskytne objednateli aktualizace programových prostředků bez zbytečného odkladu, nejpozději však do 14 dnů od uvedení SW výrobcem na trh,
- dodavatel zahájí práce na odstranění vady programových prostředků do 1 pracovního dne od jejího ohlášení; dodavatel dodá opravnou verzi programových prostředků bez zbytečného odkladu po jejím vydání výrobcem,
- dodavatel poskytne konzultace na rozvoj řešení (čerpání 60% v sídle dodavatele a 40% v sídle zadavatele)
    - v rozsahu 30MD/rok první rok
    - v rozsahu 10MD/rok následující 4 roky
    - všechny nevybrané konzultace automaticky převádí na následující rok až do konce platnosti smlouvy

Požadavky na zálohování

- Zadavatel využívá pro zálohování řešení EMC Networker.
- Dodavatel musí zajistit nejméně jednu z následující možností zálohování:
    - zajištění zálohování pomocí klienta EMC Networkeru tak, že je zajištěno, že veškerá data jsou v kompletní a konzistentním stavu. Bývá řešeno přístupem na API dodaného produktu.
    - zajištění zálohovaní pomocí metody implementované v produktu, které vytvoří soubor/adresář s obsahem klíčových dat pro obnovu dat a obnovu plné funkčnosti
    - zajištění zálohování pomocí skriptu, které vytvoří soubory/adresář s obsahem klíčových dat pro obnovu dat a obnovu plné funkčnosti
    - Záloha musí být provedena tak, aby nedošlo k ovlivnění či výpadku dodaného systému. Výpadkem se v tomto znění myslí, že na straně uživatele nebude zálohovací proces nijak patrný.

Požadavky na školení

- V rámci dodávky musí dodavatel zajistit školení v rozsahu min 5 MD pro 2 osoby
- Školení musí být koncipováno od základního seznámení po pokročilou administraci
- Školení musí být pořádáno výrobce dodaného řešení, nebo musí být v souladu s osnovou školení výrobce
    - V případě, že školení bude pořádáno výrobcem, může být v anglickém nebo českém jazyce
    - Pokud školení nebude pořádáno výrobcem, bude školení v českém jazyce