|  |  |
| --- | --- |
| Zadavatel | Město Ústí nad Orlicí, Sychrova 16, 562 24 Ústí nad Orlicí, IČ: 00279676 |
| Veřejná zakázka | Pořízení nástroje pro monitoring síťového provozu **LAN** |
| Evidenční číslo VZ | …. |
| Velikost a druh ZŘ | Veřejná zakázka malého rozsahu na dodávku |

Technická specifikace

**Předmětem poptávky je pořízení nástroje pro online monitoring sítě a síťového provozu, který umožní sbírat a vyhodnocovat datové toky a provádět jejich behaviorální analýzu.**

Požadovaná je forma **hardwarové appliance**, která bude schopná bez dalšího hardware plnit požadované funkce, bude dostávat kopii síťového (datového) provozu a bude provádět jeho analýzu s cílem detekovat potenciální kybernetické hrozby, detekovat kybernetické útoky, vyhodnocovat trendy týkající se objemu provozu, analyzovat využití síťové kapacity podle protokolů, aplikací a uživatelů.

Součástí dodávky musí být veškeré potřebné programové vybavení, tj. všechny licence potřebné pro instalaci a provoz.

Předpokládáme zrcadlení veškerého zájmového provozu do jednoho 10 Gb/s monitorovacího portu sondy. Předpokládáme zrcadlení provozu přes perimetr a provozu mezi klienty a servery. Na stávající infrastruktuře (páteřním switchi HP A5800) je k dispozici port pro SFP+ modul i vlastní SFP+ modul. Součástí dodávky musí být optický kabel pro připojení sondy včetně modulu pro připojení na straně sondy.

Dodávka musí zahrnout potřebný hardware a software včetně podpory a aktualizací signatur na období 1 rok.

**Součástí dodávky musí být dodávka, instalace a základní konfigurace systému včetně nastavení detekčních metod pro ADS.**

1. **Požadavky na monitorovací systém**

Monitorovací systém musí umožňovat dlouhodobé detailní monitorování veškerého provozu na počítačové síti. Získané statistiky o provozu datové sítě musí umožnit v reálném čase sledovat a vyhodnocovat objemy a strukturu provozu, analyzovat příčiny provozních nebo výkonnostních problémů a odhalovat bezpečnostní hrozby. Je nezbytné, aby monitorovací systém byl zcela nezávislý na použité síťové infrastruktuře a svou funkcí monitorovanou síť neovlivňoval. Ze strany sledované sítě nesmí být monitorovací systém detekovatelný.

Systém musí umožňovat uložení a zpracování statistik a musí poskytovat grafické uživatelské rozhraní a analytické nástroje pro práci se síťovými statistikami bez nutnosti instalovat jakýkoliv software na klientské stanice a dále pak poskytovat automatizované reporty i notifikace na nestandardní situace. Ukládání dat musí probíhat kontinuálně s dostupností bez jakékoliv ztrátové agregace po dobu několika měsíců. Musí dále umožňovat customizaci způsobu prezentace dat a reportů.

Systém musí pracovat s technologií datových toků (NetFlow/IPFIX/jFlow/NetStream/cflow).

|  |  |
| --- | --- |
| Požadavek | Popis |
| Ucelený, škálovatelný NetFlow/IPFIX monitorovací systém | Ucelené škálovatelné řešení umožňující dlouhodobé monitorování sítě na bázi technologie datových toků (NetFlow, IPFIX, jFlow, cflowd, NetStream). |
| Podpora infrastruktury | Podpora IPv4, IPv6, VLAN, MPLS, Ethernet 10Mb/s až 10Gb/s. |
| Decentralizovaný monitoring lokalit s centrální správou | Sběr síťových statistik ze vzdálených lokalit s centrálním přístupem k reportům, incidentům a síťovým statistikám a centrální správou systému. |
| Nezávislost na stávající infrastruktuře | Nezávislost na stávající síťové infrastruktuře (optické či metalické datové rozvody) a použitých aktivních prvcích (typ nebo výrobce). |
| Zdroje NetFlow statistik (sondy) | Specializovaná dedikovaná zařízení (sondy) pro vytváření detailních statistik IP toků o dění na síti, standardizovaný protokol pro výměnu dat o IP tocích (NetFlow v5,v9, IPFIX) |
| Bezeztrátový sběr flow statistik z více zdrojů | Bezeztrátový sběr dat na kolektorech z různých datových zdrojů, podpora standardizovaných protokolů pro výměnu dat o IP tocích (NetFlowv v5, NetFlow v9 – RFC3954, IPFIX, jFlow, cflowd, NetStream). |
| Ukládání statistik a vyhodnocování bezpečnostních hrozeb | Dlouhodobé ukládání statistik IP toků a jejich centrální sledování a vyhodnocování bezpečnostních hrozeb v síti, prokazování bezpečnostních incidentů. |
| Zákaznická podpora | Plná zákaznická podpora v českém jazyce. |
| Rozhraní pro integraci nástrojů třetích stran | Otevřené rozhraní a dokumentované API s možností integrace nástrojů i třetích stran. |

Požadavky na zdroje NetFlow/IPFIX dat (sondy)

Zdroj flow (NetFlow/IPFIX) dat (sonda) musí být autonomní zařízení, monitorující síťový provoz.

Sonda musí monitorovat síťový provoz na síťové (L3) a transportní (L4) vrstvě OSI modelu, ale musí rovněž umožňovat analýzu aplikační vrstvy (L7), identifikaci aplikací (NBAR2) a podrobný monitoring hlavních aplikačních protokolů (např. HTTP, DNS, DHCP).

Mimo objemových charakteristik provozu musí sondy poskytovat i výkonové parametry datové sítě (např. RTT, SRT, jitter) pro analýzu zpoždění na síti pro usnadnění řešení síťových problémů, správu a optimalizaci sítě a zvyšování její bezpečnosti.

Sondy musí být nezávislé na použité síťové infrastruktuře a svou funkcí nesmí nijak ovlivňovat sledovanou síť.~~.~~ Ze strany monitorovacích rozhraní připojených do sledované sítě nesmí být zařízení detekovatelné. Sonda musí být vybavena vlastní kolektorovou aplikací umožňující lokální ukládání a analýzu vlastních NetFlow/IPFIX dat.

|  |  |
| --- | --- |
| Požadavek | Popis požadavku |
| Pasivní zapojení | Pasivní zapojení bez vlivu na monitorovanou síť (zapojení pomocí TAPů, případně v kombinaci se SPAN/mirror porty). |
| Instalace | Snadná instalace do stávající síťové infrastruktury – racková montáž nebo šablony pro nasazení virtuálního stroje. |
| Management rozhraní | Dva plnohodnotné management (administrativní) porty 10/100/1000Mb/s (UTP kabeláž) pro zabezpečenou vzdálenou správu a přenos NetFlow dat. |
| Zabezpečená vzdálená správa | Zabezpečená vzdálená správa, dohled a konfigurace – SSH, HTTPS. |
| Správa uživatelů a přístupových práv | Správa uživatelů a přístupových práv na zařízení prostřednictvím uživatelských rolí. |
| Nastavitelná rychlost monitorovací linky | Možnost nastavení rychlosti monitorované linky 10/100/1000Mb/s na metalických rozhraních. |
| Dohled | Sondu je možné integrovat do dohledového systému pro kontrolu dostupnosti a vytížení zdrojů technologií SNMP. |
| Vestavěný kolektor | Vestavěný kolektor pro dočasné ukládání flow statistik (zajištění redundance), který zahrnuje plnohodnotnou funkcionalitu flow kolektoru. |
| Časová synchronizace | Časová synchronizace zařízení proti centrálnímu zdroji času na síti. |
| Minimální výkon | Minimální výkon 1 milion paketů za sekundu na každém portu, možnost upgradu na verzi s wire-speed garancí zpracování všech paketů. |
| Podpora příkazové řádky | Jednoduchá instalace a nastavení zařízení prostřednictvím příkazové řádky. Základní správa prostřednictvím příkazové řádky. |
| Sériová linka pro konfiguraci zařízení | Možnost přístupu a konfigurace hardwarových zařízení prostřednictvím sériové linky (RS-232). |
| DNS cache | Použití DNS cache na zařízení pro rychlejší překlad IP adres na doménová jména. |
| LDAP autentizace | Podpora autentizace vůči LDAP (Active Directory). |
| TACACS+ autentizace | Podpora autentizace vůči TACACS+ |
| Podpora protokolů pro výměnu dat | Programové vybavení sondy musí umožnit vytváření NetFlow dat ve formátech verzi 5 a 9, IPFIX. |
| Podpora spolehlivého a šifrovaného exportu toků dle standardu | Zařízení umožňuje exportovat statistiky o síťovém provoze (toky) pomocí spolehlivého a zabezpečeného komunikačního kanálu dle standardu RFC 5153. |
| Zpracování datového provozu | Zpracování datového provozu IPv4 a IPv6, VLAN, MPLS a jejich reportování na kolektor. |
| Analýza tunelovaného provozu | Monitorování provozu v tunelu (deenkapsulace) GRE, ESP a OTV. |
| Uživatelsky definované šablony | Uživatelsky definovatelné šablony pro protokoly NetFlow v9 a IPFIX. |
| Monitorování MAC adres | Monitorování a reportování MAC adres ve flow statistikách. Možnost použít MAC adresu jako položku klíče flow záznamu. |
| Detekce aplikací | Detekce aplikací dle standardu NBAR2. |
| Analýza zpoždění na síti | Reportování RTT, SRT, delay, jitter, retransmise, out-of-order pakety jako součást flow statistik. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX). |
| Monitorování a analýza HTTP provozu | Monitorování a analýza HTTP provozu - včetně položek typu URL, hostname, stavový kód HTTP, dotazovací metoda. Pro HTTPS reportování hostname jako SNI. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX). |
| Profilování zařízení v síti | Identifikace operačního systému vč. jeho verze. Identifikace internetového prohlížeče vč. jeho verze. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX). |
| Monitorování VoIP | Monitorování VoIP statistik, protokol SIP – položky typu SIP URI, jitter, latence, ztrátovost paketů. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX). |
| Monitorování DNS provozu | Monitorování a analýza DNS provozu - položky jako typ dotazu, dotazovaná doména, návratová hodnota, odpověď. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX). |
| Monitorování SMB/CIFS provozu | Monitorování a analýza SMB/CISF provozu – položky typu síťová cesta, název souboru, typ operace. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX). |
| Monitorování DHCP provozu | Monitorování DHCP provozu – položky jako typ DHCP požadavku, originální MAC adresa. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX). |
| Monitorování e-mailového provozu | Monitorování e-mailového provozu – protokolů SMTP, POP3, IMAP a položek jako uživatelské jméno, jméno odesílatele, selhání autentizace a další. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX). |
| Monitorování MS SQL (TDS protokolu) provozu | Monitorování Microsoft SQL provozu (TDS protokolu) – položky jako typ dotazu, verze klienta a serveru, uživatelské jméno a další. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX). |
| Monitorování rozšířených L3/L4 informací | Monitorování rozšířených L3/L4 informací - TTL (Time to live), TCP Window size, TCP SYN packet size umožňujících detekci NATů. |
| Kapacita paměti současných toků | Minimální kapacita paměti současných toků na sondě 500 tisíc toků per monitorovací port. |
| Nastavení času pro expiraci toků | Podpora pro nastavení časů u aktivní a neaktivní expirace toků. |
| Vzorkování | Podpora vzorkování na úrovni paketů. Podpora vzorkování na úrovni toků. |
| Simultánní export NetFlow statistik | Podpora simultánního exportu flow statistik na libovolný počet cílů (redundantní kolektory v různých lokalitách, lokální uložení dat na sondě). Pro různé cíle exportu lze použít různé flow standardy (NetFlow v5, NetFlow v9, IPFIX). |
| Export na základě filtrování dat na sondě | Podpora filtrování dat na sondě na základě IP prefixů, VLAN, AS (pro různé cíle exportu různé statistiky). |
| Vyplňování identifikace AS | Podpora vyplňování AS na základě vestavěného či dodaného seznamu. |
| Vyplňování čísla interface | Podpora pro nastavení hodnoty interface index pro exportované flow statistiky per monitorovací port. |
| Záchyt provozu v plném rozsahu | Sonda umožňuje rozšíření o funkcionalitu záznamu provozu v plném rozsahu na základě uživatelem definovaného pravidla záchytu. Rozšíření je řešeno formou licence/instalace SW bez nutnosti změny HW konfigurace. |
| Výkonnostní parametry - sonda | HW appliance  1 x 10GE monitorovací port  výkon na port 1,5 Mp/s  4M flow záznamů ve flow cache na monitorovací port |

Požadavky na kolektory NetFlow dat

Kolektor musí podporovat flow data ve formátech jFlow, sFlow, NetStream a další kompatibilní s NetFlow.

Zobrazení uložených flow dat a jejich analýza (vyhledávání, agregace, výpisy aj.) musí probíhat na kolektoru prostřednictvím zabezpečeného webového rozhraní. Uložená data a výsledky analýz musí být dostupné ve formě dlouhodobých grafů a top statistik s možností zobrazení dat až na úrovni jednotlivých komunikací (jednotlivých NetFlow/IPFIX záznamů).

Kolektor musí dále poskytovat funkce reportování statistik o síťovém provozu a systém notifikací v případě výskytu definované události/anomálie.

|  |  |
| --- | --- |
| Název požadavku | Popis požadavku |
| Úložná kapacita | 0,5 TB |
| Výkon | až 50 000 toků/s |

1. Požadavky na automatické vyhodnocování NetFlow dat

Systém pro automatické vyhodnocování IP toků musí umožňovat automatickou detekci bezpečnostních nebo provozních a anomálií datové sítě a jejich hlášení formou událostí. Systém musí být založen na pokročilých metodách behaviorální analýzy a umožňovat odhalování hrozeb a incidentů, které překonaly zabezpečení na perimetru nebo bezpečnostních ochranu koncových stanic, a pro které dosud není dostupná signatura.

Musí tak představovat systém včasné detekce a reakce na bezpečností incidenty. Detekované události musí být možné dále analyzovat, vizualizovat nebo automaticky reportovat, případně integrovat s dohledovými systémy, incident handling systémy a systémy typu SIEM.

|  |  |
| --- | --- |
| Název požadavku | Popis požadavku |
| Podpora flow standardů | Podpora standardů NetFlow v5, NetFlow v9, IPFIX, jFlow, cflowd, NetStream. |
| Deduplikace | Systém umožňuje deduplikovat flow statistiky před jejich vlastní analýzou. |
| Korelace před a za proxy | Systém umožňuje provést korelaci flow statistik před a za proxy serverem před jejich vlastní analýzou s cílem identifikovat provoz procházející proxy serverem a tento provoz přiřadit koncovému uživateli. |
| Vzorkování na úrovni toků | Systém podporuje vzorkování na úrovní toků před jejich vlastním zpracováním. |
| Identita uživatelů | Systém zobrazuje informace o identitě uživatelů obsaženou ve flow datech jako součást události. |
| Persistence doménových jmen | Systém podporuje persistenci doménových jmen, tedy uložení doménové jména původce události v okamžiku zaznamenání výskytu této události. |
| Detekční pravidla a algoritmy | Systém obsahuje předdefinovanou sadu detekčních metod a algoritmů pro analýzu flow statistik, detekci bezpečnostních incidentů, provozních problémů a síťových anomálií. |
| Detekce síťových útoků | Detekce skenování portů, slovníkové útoky, útoky odepření služeb (DoS), útoky na síťové protokoly SSH, RDP, Telnet a další obdobné služby. |
| Detekce anomálií v síťovém provozu | Detekce anomálií v DNS, DHCP, SMTP, multicast provozu a nestandardní komunikace. |
| Detekce nežádoucích aplikací | Detekce P2P sítí, a anonymizačních služeb (např. TOR) |
| Detekce událostí na základě „Threat intelligence“ dat | Systém umožňuje identifikovat bezpečnostní události (např. komunikaci s botnet command & control centry, přístup na phishing servery, apod.) využíváním zdrojů IP a host reputačních databází poskytovaných výrobcem a aktualizovaných nejméně každých 24 hodin. Systém umožňuje zapojit další zdroje IP a host reputačních dat pro automatickou detekci. |
| Detekce provozních problémů | Detekce nadměrné zátěže sítě, výpadků služeb, chybějících reverzních DNS záznamů, nových a cizích zařízení připojených k síti. |
| Detekce síťových anomálií | Detekce síťových anomálií na základě predikce budoucího chování sítě s využíváním znalosti historie komunikace. |
| Konfigurační průvodce | Systém obsahuje konfiguračního průvodce pro nastavení systému při prvním spuštění podle parametrů sítě, do kterého je systém nasazen. |
| Konfigurace detekčních schopností | Jednotlivé detekční schopnosti je možné konfigurovat a parametrizovat tak, aby bylo dosaženo maximální efektivity a minimálního počtu falešných poplachů. Detekční mechanismy je možné konfigurovat různým způsobem (např. s různou citlivostí) pro statistiky z různých segmentů sítě (např. LAN nebo DMZ). |
| Detekce NATů | Detekce NATů v síti s využitím rozšířených informací z L3/L4. |
| Správa filtrů | Systém umožňuje definovat filtry vč. komplexních filtrů složených z dílčích filtrů. Pro zjednodušení definice filtrů je možné používat operace jako inverze nebo rozdíl filtrů. Filtry je možné exportovat do formátu XML nebo z tohoto formátu importovat. |
| Správa falešných poplachů | Případné události, které představují falešné poplachy (false positives) je možné odstranit prostřednictvím jednoduché konfigurace pravidel pro vyloučení falešných poplachů dostupné v uživatelském rozhraní. |
| Definice závažnosti událostí | Předdefinované priority událostí s možností uživatelského nastavení závažnosti událostí na základě IP adresních rozsahů, typů událostí, míst výskytu nebo detailů události. Jedna událost může mít v závislosti na konfiguraci přiřazeno více priorit. |
| Správa uživatelů a přístupových práv | Správa uživatelů a přístupových práv k událostem prostřednictvím uživatelských rolí. Separace událostí s omezením přístupu pro jednotlivé role/uživatele. |
| E-mailové notifikace | Notifikace o detekovaných událostech prostřednictvím e-mailu s podporou různých formátů (HTML, incident handling systém, úsporný textový formát). Možnost připojit vzorek flow dat, na základě kterých byla událost detekována k emailovému reportu. |
| Uživatelské rozhraní | Webové uživatelské rozhraní v českém jazyce. Uživatelsky definovatelný dashboard (konfigurace per uživatel). Vizualizace průběhu provozu s vyznačením detekovaných událostí v závislosti na nastavené závažnosti událostí. |
| Integrace informací z jiných služeb | Systém integruje informace ze služeb DNS, WHOIS, geolokační služby. Uživatelsky definované externí služby fungující na protokolu HTTP. |
| Kategorie a komentáře | Události je možné přiřazovat do uživatelsky definovaných kategorií (např. vyřešeno, důležité, apod.). Událostem je možné přímo v systému pořizovat poznámky a komentáře. |
| Vyhledávání událostí | Systém nabízí flexibilní uživatelské rozhraní pro vyhledávání událostí dle různých parametrů (typ události, IP adrese původce události, filtr, přiřazení události do kategorie, ID události apod.). Události je možné prezentovat různým způsobem (prostý seznam, agregace dle zdrojů, dle cílů apod.). |
| Interaktivní vizualizace událostí | Systém umožňuje interaktivní vizualizaci detekovaných událostí formou grafické reprezentace flow statistik, na základě kterých byla událost rozpoznána. |
| Reporting | Předdefinovaná sada reportů s možností plné konfigurace uživatelem. Reporty dostupné prostřednictvím webového uživatelského rozhraní, ve formátu PDF. Automatická distribuce reportů e-mailem. |
| CSV export | Události je možné exportovat do formátu CSV pro další zpracování. |
| Otevřené rozhraní | Systém detekce anomálií poskytuje dokumentované API pro získávání a zpracování událostí. Prostřednictvím API je možné systém detekce anomálií rovněž konfigurovat (např. vytvářet filtry, měnit nastavení detekčních metod, apod.). |
| Sledování změn konfigurace | Systém loguje veškeré změny konfigurace s cílem zajistit auditovatelnost činnosti uživatelů a provedené změny s dopadem detekci událostí. Změny konfigurace je možné rovněž odesílat protokolem syslog pro auditování formou externího systému typu SIEM nebo log management. |
| Výkonnostní parametry | výkon až 1000 toků/s, velikost sítě (počet IP adres) až 1000 |

**Požadovaná úroveň technické podpory a záruka**

SLA po dobu 1 roku v úrovni:

* NBD ( Next Business Day) on-site hardware
* všechny updaty i upgrady (nová funkcionalita)
* přístup k webovému zákaznickému centru
* podpora telefonem a emailem v českém jazyce v pracovní době (8x5)
* vzdálená podpora přes SSH
* konzultace síťového a bezpečnostního technika.