Příloha č.3 – Detailní specifikace

Detailní specifikace – monitoring sítě

Obecné požadavky na monitorovací systém

Monitorovací systém musí umožňovat dlouhodobé detailní monitorování dění na počítačové síti. Získané informace o dění na síti a chování uživatelů musí umožnit v reálném čase sledovat a vyhodnocovat bezpečnostní hrozby v síti. Je nezbytné, aby monitorovací systém byl nezávislý na použité síťové infrastruktuře a svou funkcí neovlivňoval sledovanou síť. Ze strany monitorované sítě nesmí být zařízení detekovatelné. Vytváření síťových statistik musí být prováděno pomocí nezávislých a k tomuto účelu určených zařízení.

Uložení a zpracování statistik musí být redundantní na k tomu určených zařízeních – kolektorech. Ty musí být vybaveny SW či HW RAIDem. Kolektory musí poskytovat analytické nástroje pro práci se statistikami, musí být schopny zaznamenat každou komunikaci po dobu několika měsíců bez jakékoliv ztrátové agregace, poskytovat upozornění a rozhraní pro práci bezpečnostního technika.

Systém musí pracovat s technologií NetFlow ve verzi 5 a 9. Tato technologie je v současné době nejpřesnějším a nejmodernějším prostředkem pro monitorování sítě a oproti konkurenčním technologiím nabízí výhody zpracování všech paketů bez vzorkování, imunitu vůči šifrovanému provozu, škálovatelnost i pro vysokorychlostní a zatížené sítě a průmyslovou standardizaci. Díky standardizaci je možné jeden zdroj statistik využít i v dalších systémech, jako je tiketovací nástroj, systém pro log managemet, či SIEM.

Požadavky na monitorovací systém:

- ucelené škálovatelné řešení umožňující dlouhodobé monitorování sítě na bázi technologie NetFlow (nutná podpora NetFlow v5 a NetFlow v9),
- podpora standardů NEL, NSEL a NBAR2,
- sledování bezpečnostních incidentů v několika lokalitách s centrální správou,
- nezávislost na stávající síťové infrastruktuře (optické či metalické datové rozvody) a použitých aktivních prvcích, nesmí docházet k ovlivňování chování sítě,
- 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),
- bezeztrátový sběr dat na kolektorech z několika datových zdrojů, podpora standardizovaných protokolů pro výměnu dat o IP tocích (NetFlow v5, v9 - RFC3954),
- dlouhodobé ukládání statistik IP toků a jejich centrální sledování a vyhodnocování bezpečnostních hrozeb v síti, prokazování bezpečnostních incidentů,
- plná zákaznická podpora v českém jazyce,
- systém ověřený instalacemi na páteřních linkách (10GE) minimálně u 5 poskytovatelů internetu nejméně ve třech zemích světa,
- podpora IPv4, IPv6, VLAN, MPLS, Ethernet 10Mb/s až 10Gb/s, otevřené rozhraní s možností integrace nástrojů i třetích stran.

Obecné požadavky na zdroje dat NetFlow (síťové sondy)

Je nezbytné, aby zdroje dat NetFlow byly nezávislé na použité síťové infrastruktuře a svou funkcí nijak neovlivňovaly sledovanou síť. Ze strany monitorovacích rozhraní připojených do sledované sítě nesmí být zařízení detekovatelné. Vytváření síťových statistik musí být prováděno autonomními, nezávislými a k tomuto účelu navrženými zařízeními.

Obecné požadavky na technické a programové vybavení sondy:

- 100% přesný nezávislý autonomní zdroj NetFlow statistik s podporou IPv4, IPv6, VLAN, MPLS, GRE, NetFlow v5/v9,
- detekce aplikací dle standardu NBAR2, monitorování a analýza HTTP provozu a VoIP statistik,
- snadná instalace do stávající síťové infrastruktury,
- rack mount zařízení,
- pasivní zapojení bez vlivu na monitorovanou síť (zapojení pomocí TAP, případně v kombinaci se SPAN porty),
- jeden administrativní port 10/100/1000Mb/s (UTP kabeláž) pro zabezpečenou vzdálenou správu a přenos NetFlow dat,
- zabezpečená vzdálená správa, dohled a konfigurace – SSH, HTTPS,
- správa uživatelů a přístupových práv na zařízení,
- možnost nastavení rychlosti monitorované linky 10/100/1000Mb/s na metalických rozhraních,
- vestavěný kolektor pro dočasné ukládání NetFlow statistik (zajištění redundance), který zahrnuje uživatelsky definovaný dashboard, automatickou tvorbu reportů, detekci aktivních zařízení a detailní analytické možnosti,
- časová synchronizace zařízení proti centrálnímu zdroji času na síti,
- minimální výkon 1,48 milionů paketů za sekundu na každém portu,
- jednoduchá instalace a nastavení zařízení prostřednictvím příkazové řádky,
- možnost přístupu a konfigurace zařízení prostřednictvím sériové linky (RS-232),
- použití DNS cache na zařízení pro rychlejší překlad IP adres na doménová jména,
- podpora autentizace vůči LDAP (Active Directory).

Požadavky na sondy z pohledu generování NetFlow dat:

- pasivní odposlech dat ze sítě pomocí specializovaných zařízení (TAPů) či SPAN portů,
- podpora protokolů pro výměnu dat – programové vybavení sondy musí umožnit vytváření NetFlow dat ve formátech verzi 5 a 9,
- zpracování datového provozu IPv4 a IPv6, VLAN, MPLS, GRE a jejich reportování na kolektor,
- uživatelsky definovatelné šablony pro protokoly NetFlow v9 a případně IPFIX,
- podpora monitorování MAC adres,
- detekce aplikací dle standardu NBAR2,
- monitorování a analýza HTTP provozu - včetně položek typu URL, hostname,
- monitorování VoIP statistik - položky typu jitter, latence, ztrátovost paketů,
- hloubkový monitoring DNS provozu, včetně identifikátorů, značek a response kódů
- dlouhodobé a stabilní zpracování na všech měřících rozhraních,
- minimální kapacita paměti současných toků na sondě 500 tisíc toků,
- podpora pro nastavení časů u aktivní a neaktivní expirace toků,
- podpora vzorkování na úrovni paketů,
- podpora vzorkování na úrovni toků,
- podpora simultánního exportu NetFlow statistik na libovolný počet cílů (redundantní kolektory v různých lokalitách, lokální uložení dat na sondě),
- podpora filtrování dat na sondě na základě IP prefixů a VLAN (pro různé cíle exportu různé statistiky),
- podpora vyplňování AS na základě vestavěného či dodaného seznamu,
- podpora filtrování a export datových toků na základě AS.

Požadavky na zdroje NetFlow dat (sondy) závislé na kokrétním modelu sondy

- počty a rychlosti/typy rozhraní – 1x – 4x 1GbE, metalika – RJ-45,
- podpora 1 Gigabit Ethernetu,
- 1U či 2U velikost,
- minimální výkon 1,48 milionu paketů za sekundu na každém 1GbE portu,
- minimální kapacita paměti současných toků na sondě 4 miliony toků – 1Gb/s modely
- současné měření síťového provozu na minimálně čtyřech gigabitových rozhraních současně pomocí jednoho zařízení,
- připojení na měřenou síť pomocí metalických či optických konektorů či SFP transceiverů – umožňuje ad hoc změnu typu monitorované linky (metalická/optické single mód či optická multi mód) nebo kombinaci více typů linek na jedné sondě.

Obecné požadavky na kolektory NetFlow dat

Kolektory jsou zařízení (datová úložiště) s vysokou diskovou kapacitou určená pro uložení, vizualizaci a vyhodnocení síťových statistik exportovaných NetFlow dat. Zobrazení uložených NetFlow dat a jejich analýzy (vyhledávání, agregace, výpisy aj.) probíhají na kolektoru a jsou zpřístupněna operátorovi prostřednictvím zabezpečeného rozhraní.

Požadavky na technické a programové vybavení kolektoru:

- zabezpečené kolektory NetFlow statistik s databází pro plné uložení síťových statistik na multigigabitových linkách bez jakékoliv redukce,
- možnost dohledání každé komunikace, průběžné grafy, podpora upozornění, rozšiřitelnost o pluginy na míru,
- snadná instalace do stávající síťové infrastruktury
- jedno administrativní rozhraní pro zabezpečenou vzdálenou správu a přenos NetFlow dat,
- zabezpečená vzdálená správa, dohled a konfigurace – SSH, HTTPS,
- víceuživatelský přístup - včetně možnosti definovat k jakým datům má jednotlivý uživatel přístup,
- podpora autentizace vůči LDAP (Active Directory),
- integrace dohledového systému pro kontrolu dostupnosti (SNMP),
- časová synchronizace zařízení proti centrálnímu zdroji času na síti,
- jednoduchá instalace a nastavení zařízení prostřednictvím příkazové řádky,
- použití DNS cache na zařízení pro rychlejší překlad IP adres na doménová jména.

Požadavky na kolektory z pohledu sběru dat:

- podpora verze NetFlow protokolu – programové vybavení kolektoru musí umožnit sběr a vyhodnocení NetFlow dat ve verzi 5 a 9,
- podpora pro sběr a analýzu sFlow a NetStream dat,
- podpora standardů NEL a NSEL, monitorování MAC adres,
- podpora pro příjem a analýzu informací o detekovaných aplikacích dle NBAR2 standardu,
- podpora pro příjem a analýzu HTTP provozu - včetně položek typu URL, hostname,
- podpora pro příjem a analýzu VoIP statistik (jitter, latence, ztrátovost),
- podpora sběru a analýzy dat z autentizačních systémů,
- kapacita datového úložiště – systém je schopen sbírat a ukládat dlouhodobě data z desítek NetFlow zdrojů. Disková kapacita datového úložiště musí umožnit záznamy statistik bez jakékoliv redukce v horizontu minimálně tří měsíců.
- možnost přeposílání přijímaných NetFlow statistik ke zpracování na další kolektory včetně možnosti filtrace na úrovni NetFlow paketů.

Požadavky na kolektory z pohledu vyhodnocení dat:

- ucelené řešení pro sledování síťové komunikace, jak v reálném čase, tak dlouhodobě,
- uživatelsky definovatelný dashboard (konfigurace per uživatel),
- vytváření dlouhodobých grafů a přehledů s různými typy pohledů rozdělených do kategorií podle objemu (počet přenesených bytů, toků, paketů), IP provozu (TCP, UDP, ICMP, ostatní) nebo protokolu (HTTP, IMAP, SSH),
- generování statistik a podrobných výpisů nad volitelnými časovými intervaly,
- reporty v podobě průběhových i koláčových grafů,
- online reporty včetně možnosti exportu do PDF a CSV formátu,
- automatické zasílání reportů emailem (reporty v českém a anglickém jazyce),
- řízení uživatelského přístupu k jednotlivým typům reportů (uživatel je oprávněn zobrazovat pouze statistiky, ke kterým mu bylo nastaveno oprávnění administrátorem),
- výpis tzv. top N statistiky podle různých kritérií (počet přenesených bytů, paketů, toků atd.) umožňující vypsat nejaktivnější či anomální počítače podílející se na síťovém provozu,
- upozornění administrátorům v případě vzniku uživatelem definované situace (např. nadměrný přenos dat, výskyt nebezpečné anomálie, použití zakázané aplikace atd.) prostřednictví emailu, SNMP trapu a syslogu,
- vytváření profilů pro ukládání dat vyhovující nadefinovaným filtrům (např. HTTP, FTP, SMTP, SSH provoz),
- podrobné textové výpisy jednotlivých toků s možnostmi filtrování a agregace,
- drill-down – možnost dohledat každý jednotlivý tok zaznamenaný sondami,
- detekce aktivních zařízení na sítí - pro podporu konceptu BYOD,
- podpora korelace dat z autentizačních systémů se síťovými statistikami pro tzv. Identity awereness,
- podpora geolokace na základě IP adresy,
- otevřené rozhraní s možnostmi skriptování a zpracování dávkových úloh.

Požadavky na zdroje kolektory dat závislé na konkrétním modelu sondy

- ukládání síťových statistik na multigigabitových linkách bez jakékoliv redukce minimálně po dobu 3 měsíců,
- kapacita minimálně 500GB,
- podpora nasazení do virtuálního prostředí VMware
- výkon 75 000 toků za vteřinu.

Obecné požadavky na automatické vyhodnocování NetFlow dat

Automatické vyhodnocování měřených dat s cílem identifikovat provozní a bezpečnostní incidenty a tyto reportovat/alertovat jako události. Systém je založen na pokročilých metodách tzv. behaviorální analýzy a umožňuje tak odhalovat hrozby a incidenty, pro které dosud není dostupná signatura.

Požadavky funkce poskytované řešením automatické analýzy NetFlow dat:

- Deduplikace a podpora korelace dat před/za PROXY
- Výkon nejméně 2500 toků/s, podpora pro samplování na úrovni toků
- Předdefinovaná sada pravidel a algoritmů pro odhalování nežádoucích vzorů chování
    - Útoky (skenování portů, slovníkové útoky, denial of service, protokol telnet)
    - Anomálie datového provozu (DNS, DHCP, multicast, nestandardní komunikace)
    - Nežádoucí aplikace (P2P sítě, instant messaging, anonymizační služby)
    - Interní bezpečnostní problémy (viry, spyware, botnety)
    - Poštovní provoz (odchozí spam)
    - Vestavěná IP reputační databáze pro detekci útoků a botnetů
    - Provozní problémy (zpoždění, nadměrná zátěž, reverzní DNS záznamy, nefunkční aktualizace)

- Budování dlouhodobých profilů chování zařízení na síti z pohledu služeb, objemů provozu a komunikačních partnerů
    - Objemy datového provozu (přenesená data, počty uskutečněných spojení)
    - Struktura služeb (využívané a poskytované služby)
    - Komunikační partneři
    - Vyhledávání serverů a klientů v síti
    - Vyhledávání zařízení poskytujících nebo využívajících služby v síti
    - Celkový pohled na strukturu provozu
    - Detailní profil pro každou IP adresu, sledování trendů
- Předdefinovaná sada pravidel pro odhalování obecných anomálií v síti
    - Predikce chování sítě a detekce odchylek
- Přehledný dashboard s okamžitou indikací problémů a top statistik
- Definice závažnosti události na základě IP adresních rozsahů, typů a míst v síti
- Víceuživatelský přístup - včetně možnosti definovat k jakým datům a událostem má jednotlivý uživatel přístup
- Integrace informací ze služeb DNS, WHOIS, geolokační služby
- Interaktivní vizualizace událostí
- Export statistik o provozu na síti, které událost způsobily ve vhodné formě pro prokazování incidentů
- Export událostí do CSV
- Automatický export událostí ve formátu CEF protokolem Syslog nebo SNMP, pro možnost odesílání dat do systémů třetích stran, jako jsou tiketovací nástroje, log management či SIEM

Mimofunkční požadavky

- Řešení musí být umožňovat více jazykových mutací, minimálně však češtinu, angličtinu, alespoň v částech řešení, které jsou přístupné pro koncové uživatele
- Řešení musí být umožňovat úpravy vzhledu rozhraní pro koncové uživatele do korporátního designu

Omezení a limity

- Řešení bude implementováno bez přerušení nebo narušení provozu společnosti ČEPRO
- Řešení umožní znovupoužití a využití již pořízených prostředků a služeb na straně zadavatele, a to jak z hlediska již provozované infrastruktury, tak i z hlediska platformy, na níž bude samo vystavěno
- Řešení umožní iterativní nasazení, tedy nasazení po jednotlivých částech
- Řešení nesmí zavádět proprietární protokoly nebo formáty tam, kde jsou k dispozici kvalitativně srovnatelné průmyslové standardy, akceptované dalšími výrobci

Detailní specifikace – Log Management

Požadavky na logmanagement

Navržené řešení musí pokrýt jak HW, tak SW a licenční potřeby zadavatele v této věci a musí obsahovat vše potřebné pro zhotovení bezvadného díla odpovídajícího zde uvedené specifikaci.

Řešení pokryje potřeby zadavatele v rozsahu všech lokalit (cca 25) propojených WAN sítí zadavatele.

V rámci každé lokality zajistí řešení nejméně sběr událostí z platforem: Windows, CISCO IOS, MSSQL, VMWARE a dále z proprietárních aplikací.

V rámci každé lokality řešení aplikuje relay/sberač/konektor. Sběr událostí nelze provádět vzdáleně.

Řešení zajistí uživatelskou dostupnost na úrovni implementovaných prvků. Prezentace dat musí být provedena i v grafické podobě, prezentační rozhraní musí být multiplatformní nebo platformně nezávislé a plně funkční na platformách Windows, Linux, Apple MacOS, Apple iOS.

Řešení musí podporovat zapojení pro High Availability, tj. vysoká dostupnost (zero drop).

Podpora vstupních protokolů (sources ~ zdrojů log záznamů) a přenosu dat:

- SNMP
- syslog:
  - UDP (dle RFC 3164)
  - TCP
  - ETF (RFC 5424) + TLS
- Aktivní sběr logů z databází (přes ODBC).
- Agent/Client pro sběr log záznamů jak pro prostředí Windows, tak i pro prostředí Linux/Unix (HP-UX, Solaris, …)/AIX:
  - sběr Windows EVT záznamů i z kontejnerů Windows Server.
  - sběr AIX/Solaris/HP-UX/IRIX auditních OS záznamů.
  - sběr textových logů ze souborů.
  - Sběr logů z databází
  - přenos log dat (tj. forward přes syslog) šifrovaným kanálem.
  - Podpora RELAY funkce (tj. přeposílací servery, např. pro infrastrukturu v DMZ)
- Podpora BUFFER/CACHE na výstupu jak u Agenta, tak pro RELAY, a také pro Server/Appliance.
- Podpora výstupních protokolů (destinations ~ umístění log záznamů):
  - syslog (UDP, TCP, IETF).
  - zápis log dat napřímo do databází (ODBC).
  - SNMP Trap.
- Možnost konfigurace pokročilého filtrování log záznamů (jakýkoli vstup log dat prochází libovolnou sadou filtrů na libovolný výstup).
- Ukládání log dat:
  - Textové úložiště v originálním (RAW) formátu.
  - Šifrované úložiště (logspace) s podporou šifrování privátním klíčem/certifikátem a TSA podpisem, pro zajištění právních potřeb forenzního šetření.
  - Podpora indexace log dat pro rychlé vyhledávání údajů i v nestrukturovaných v datech (položka message u syslog protokolu).
- Řízení přístupů (AAA):
  - řízení přístupu na úrovni jednotlivých úložišť (logspace).

    - podpora GROUP managementu.
    - podpora autentizace přes RADIUS.
    - lokální /externí databáze uživatelů – LDAP.
- Zálohování, Archivace, Export, Sdílení log dat:
    - nezávislé zálohovací politiky jak pro konfiguraci, tak pro jednotlivá úložiště (logspace).
    - nezávislé archivační (retention) politiky pro jednotlivá úložiště.
    - podpora exportu/sdílení log dat v originálním i ve strukturovaném tvaru.
- Alerting:
    - RATE alerting (detekce změn „nestandardního chování zdrojů log záznamů“ pro nastavené limitní hladiny datových přenosů v čase).
    - Výskyt definovaného slova/znaku v logu (Např. „error“, „fail“ nebo „alert“).
    - Artificial Ignorance – funkcionalita, která identifikuje, co je informačně nezajímavé a potlačuje eskalaci. Nebo identifikuje, co informačně systém log managementu ještě nikdy neviděl a eskaluje anomálii.
- Vyhledávání a Reporting:
    - Vyhledávání na základě indexace, umožnění vytváření vlastních analytických pohledů.
    - Dashboardy/Statistiky log management infrastruktury.
    - Uživatelsky konfigurovatelný reporting strukturovaných dat (timestamp, facility, proirity, tag, program, hostname, atd.).

Kapacitní požadavky

Řešení musí výkonově pokrýt špičkový krátkodobý vstup a bezztrátové zpracování alespoň 40.000EPS.

Licence řešení pokryje sběr událostí z minimálně 150 zařízení, v odhadované kapacitě 80GB/den, a zajistí dlouhodobě schopnost sběru 5.000 EPS (událostí za vteřinu - průměr za 24hod.).

Licenční krytí řešení nesmí mít omezení na maxima krátkodobých špiček objemu zpracovaných událostí (EPS).

Řešení musí být škálovatelné tak, aby rychlost i kapacita všech částí mohla být bez ztráty dat navýšena nejméně o 100%.

Mimofunkční požadavky

Řešení musí být umožňovat více jazykových mutací, minimálně však češtinu, angličtinu, alespoň v částech řešení, které jsou přístupné pro koncové uživatele.

Zadavatel předpokládá řešení ve formě HW+SW / appliances.

Omezení a limity

- Zadavatel pro účely zálohování vyhradí kapacitu max. 5TB dat.
- Řešení bude implementováno bez přerušení nebo narušení provozu společnosti ČEPRO
- Řešení umožní znovupoužití a využití již pořízených prostředků a služeb na straně zadavatele, a to jak z hlediska již provozované infrastruktury, tak i z hlediska platformy, na níž bude samo vystavěno
- Řešení umožní iterativní nasazení, tedy nasazení po jednotlivých částech
- Řešení nesmí zavádět proprietární protokoly nebo formáty tam, kde jsou k dispozici kvalitativně srovnatelné průmyslové standardy, akceptované dalšími výrobci