Příloha č. 3– Technická specifikace

Systém musí splňovat následující minimální (nepodkročitelné) technické požadavky:

Sonda (generátor flow)

- 100% přesný nezávislý autonomní zdroj NetFlow a IPFIX statistik s podporou IPv4, IPv6, VLAN, MPLS, GRE, ERSPAN, VxLAN, ESP
- detekce aplikací dle standardu NBAR2, monitorování a analýza MAC adres, HTTP provozu (včetně položek URL, hostname), VoIP statistik (jiter, zpoždění, ztráta paketů), DNS provozu, DHCP, HTTP, SMTP, Samba a MSSQL
- rack mount zařízení – max. velikost 1RU
- 4× 10 GbE monitorovací port typu SFP+, včetně osazených SFP+ modulů SM
- pasivní zapojení bez vlivu na monitorovanou síť (prostřednictvím SPAN portu aktivních zařízení)
- dva administrativní porty 10/100/1000Mb/s (UTP kabeláž) pro zabezpečenou vzdálenou správu
- zabezpečená vzdálená správa, dohled a konfigurace – SSH, HTTPS
- správa uživatelů a přístupových práv na zařízení
- časová synchronizace zařízení proti centrálnímu zdroji času na síti
- minimální výkon 4 Mp/s na každém portu
- instalace a nastavení zařízení prostřednictvím příkazové řádky
- použití DNS cache na zařízení pro rychlejší překlad IP adres na doménová jména
- podpora autentizace vůči LDAP (Active Directory)
- podpora pro nastavení časů u aktivní a neaktivní expirace toků
- podpora vzorkování na úrovni paketů
- podpora vzorkování na úrovni toků
- podpora filtrování dat na základě IP prefixů a VLAN
- podpora vyplňování AS na základě vestavěného či dodaného seznamu
- podpora filtrování a export datových toků na základě AS

Kolektor

- zabezpečený kolektor NetFlow statistik s databází pro plné uložení síťových statistik o velikosti minimálně 3 TB
- možnost dohledání každé komunikace, průběžné grafy, podpora upozornění, rozšiřitelnost o pluginy na míru
- hardwarové provedení pro montáž do racku
- dva administrativní porty 10/100/1000Mb/s (UTP kabeláž) 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)
- za provozu vyměnitelné disky (hot-swap), HW RAID včetně SMART detekce
- integrace dohledového systému pro kontrolu dostupnosti (SNMP)
- časová synchronizace zařízení proti centrálnímu zdroji času na síti
- instalace a nastavení zařízení prostřednictvím příkazové řádky
- použití DNS cache na zařízení pro rychlejší překlad IP adres na doménová jména
- ukládání síťových statistik bez jakékoliv redukce
- možnost dohledání každé komunikace, průběžné grafy, podpora upozornění, rozšiřitelnost o pluginy na míru
- víceuživatelský přístup - včetně možnosti definovat k jakým datům má jednotlivý uživatel přístup
- analýza HTTP provozu - včetně položek typu URL, hostname,

- analýza VoIP statistik (jitter, latence, ztrátovost), podrobné textové výpisy jednotlivých toků s možnostmi filtrování a agregace
- DNS provozu, DHCP, HTTP, SMTP, Samba a MSSQL včetně obsahu daného dotazu
- drill-down – možnost dohledat každý jednotlivý zaznamenaný tok
- detekce aktivních zařízení na sítí - pro podporu konceptu BYOD
- podpora geolokace na základě IP adresy
- otevřené rozhraní s možnostmi skriptování a zpracování dávkových úloh

Požadavky na bezpečnostní analýzu

Součástí systému (kolektoru) musí být také nástroj pro automatickou detekci anomálií na základě behaviorální analýzy, aby bylo sledováno a vyhodnocováno nestandardní chování a anomálie na úrovni datové sítě a to zejména:

- útoky na síťové služby s cílem získat neoprávněný přístup k zařízení nebo službě
- podpora pro jednu instanci vyhodnocování dat a výkon pro analýzu alespoň 1000 toků za vteřinu
- komunikaci s potenciálně nežádoucími IP adresami, mezi které patří stanice šířící malware, botnet comman & control centra, známí útočníci nebo systémy šířící nevyžádanou poštu
- anomálie DNS provozu indikující infikované stanice, nežádoucí software nebo chybné konfigurace
- anomálie DHCP provozu indikující stanice pokoušející se o odposlech síťové komunikace nebo chybné konfigurace
- skenování portů a další projevy infikovaných stanic nebo nežádoucího software
- potenciálně nežádoucí síťové aplikace jako jsou P2P sítě nebo on-line komunikátory
- anonymizační služby jako např. TOR (The Onion Router) s cílem obcházet bezpečnostní opatření a přistupovat na zablokované webové stránky, obcházení PROXY serveru
- výpadky síťových služeb a špatné konfigurace síťových služeb
- pohyb dat z interní sítě do internetu, tj. potenciální únik dat a využívání služeb pro výměnu dat na internetu (webová úložiště apod.)
- útoky na internetovou telefonii, ústředny a přístroje připojené do IP sítě
- nestandardní poštovní komunikace a síření nevyžádané pošty

Požadavky na měření výkonu webových a DB aplikací

Součástí systému (kolektoru) musí být také nástroj pro měření výkonu webových a databázových aplikací, aby bylo možno sledovat a vyhodnocovat výkon a spolehlivost těchto aplikací. Tento nástroj musí splňovat následující požadavky:

- webové uživatelské rozhraní v českém jazyce (vizualizuje stavu aplikace, výkonu aplikace, počtu transakcí a dalších informací ve formě grafů a tabulek. Umožnuje analyzovat stav jednotlivých částí aplikace a transakcí
- uživatelsky definovatelný dashboard pro okamžitou vizualizaci stavu aplikace pomocí widgetů. Možnost přizpůsobení a vkládání vybraných widgetů uživatelem i souhrnné informace a další statistiky vztažené k definovatelnému časovému intervalu (předcházejících x hodin/dnů)
- systém reportuje pro definované aplikace a každou uživatelskou transakci realizovanou nad aplikací včetně doby odezvy aplikace, zpoždění sítě, zpoždění aplikace
- systém musí monitorovat aplikace bez nutnosti instalovat jakýkoliv SW na servery nebo klientské stanice
- systém umožnuje monitorovat aplikace bez jakéhokoliv vlivu na aplikaci nebo síťovou infrastrukturu

- možnost nasadit monitoring výkonu samostatně na jedné sondě, nebo na více sondách s centrální správou a webovým uživatelským rozhraním na kolektoru
- možnost monitorovat komunikaci mezi klienty aplikace a aplikační serverem na bázi protokolu HTTP a HTTPS. V případě použití protokolu HTTPS podporuje automatické dešifrování komunikace se znalostí privátního klíče pro šifrovací protokoly, které toto umožňují
- systém musí umožňovat monitorovat komunikaci mezi aplikačními servery a databázovými servery Oracle, MS SQL, PostgreSQL, MySQL
- systém umožňuje definovat pro každou aplikaci, resp. i její část definovat SLA pro dobu odezvy. Systém kontinuálně vyhodnocuje všechny transakce a stanovuje celkový status výkonu aplikace na základě plnění SLA
- flexibilita možnosti definice aplikace pro monitoring a to minimálně v rozsahu IP adresy, porty, host, URL vč. regulárních výrazů
- systém umožňuje korelovat zpoždění na úrovni uživatelské transakce na aplikačním serveru a transakce mezi aplikačním a databázovým serverem. Pro každou uživatelskou transakci je pak možné zobrazit SQL transakce, které byly v rámci uživatelské transakce vykonány
- systém umožňuje definovat skupiny pro sledování metrik pouze pro zvolenou podmnožinu transakcí (např. skupina pro PHP soubory, multimediální soubory, část klientů a uživatelů)
- systém umožnuje přepočítat historické statistiky pro nově vytvořené skupiny
- systém umožňuje vytvářet reporty dostupné prostřednictvím webového GUI, ve formátu PDF. Reporty je možné automaticky odesílat e-mailem
- pro každou transakci jsou dostupné detaily minimálně v rozsahu URL, parametry, user agenty, objem přenesených dat, návratová hodnota, cookie
- pro každou transakci jsou dostupné detaily minimálně v rozsahu SQL dotazu v plném rozsahu, velikost dotazu a odpovědi, typ SQL dotazu, čas vzniku dotazu i odpovědi a doba odezvy
- systém umožňuje filtrovat nad seznamem jednotlivých transakcí pomocí různých kritérií (např. IP adresa uživatele, doba odezvy, SLA, uživatelské jméno, začátek a konec transakce a další). Díky tomu lze získat informace o tom, jaká skupina uživatelů komunikovala s aplikací, jaká byla odezva aplikace, pro jaké uživatele a transakce byla aplikace nedostupná, atd.
- systém umožňuje exportovat informace o transakcích ve formátu CSV