Technická specifikace

Dodávka technických opatření kybernetické bezpečnosti SŠTE Brno

1. Modernizace a doplnění síťové infrastruktury

Stručný popis opatření:

Předmětem tohoto bezpečnostního opatření je modernizace distribučních síťových aktivních prvků v celkovém počtu 20ks formou náhrady novými prvky tak, aby splňovaly parametry bezpečnosti, správy a managementu, zajištění dostupnosti služeb a zejména implementaci a provoz systémů a prostředků požadovaných vyhláškou č. 316/2014 Sb.

Požadavky na řešení:

- Unifikovaná řada síťových prvků (switchů) jednoho výrobce s konektivitou 48 portů ETH (100/1G), min. 2ks 1G uplink portů (SFP) s technickou podporou výrobce
- Podpora standardů 802.1Q, 802.1x (PNAC/EAP), 802.1p, 802.1D MAC Bridges, 802.1s Multiple Spanning Trees, 802.1w Rapid Reconfiguration of Spanning Tree
- Podpora dálkové správy a managementu (konzole, web)
- Podpora SNMP v3
- Monitorování síťového provozu, sledování výkonových parametrů sítě a aplikací umožňující sledovaní stavu sítě v reálném čase (plná podpora NetFlow, IPFIX)
- Zabezpečený a auditovatelný přístup ke konfiguracím a nastavení prvků (TACACS+)
- Pokročilé řízení kvality služeb (podpora Advanced QoS)

Pořizované položky řešení:

- Modernizace a doplnění síťové infrastruktury formou nákupu 20 kusů 48 portových switchů včetně minimálně 5-leté záruky a všech potřebných licencí a průběžných aktualizací na dobu minimálně 5 let
- Kompletní instalace a nastavení, včetně bezpečnostních politik

Detailní technické specifikace:

Třída L3
Velikost zařízení max. 1U
Počet 1Gbit/s metalických portů min. 48x10/100/1000Mbit RJ45
Min. 4x10Gbit/s optických portů s volitelným fyzickým rozhraním
10GE interface zpětně kompatibilní s 1Gbit/s a 100Mbit/s transceivery
Všechny ethernet porty dostupné zepředu
Primární napájecí zdroj
Podpora Energy Efficient Ethernet (802.3az)
Celková propustnost přepínače minimálně 175.94 Gb/s
Celkový paketový výkon přepínače minimálně 109 mpps
Pamětový buffer min. 12 MB

Maximální hloubka přepínače 26 cm
Podpora "jumbo rámců" včetně velikosti 9220 Byte
Podpora linkové agregace IEEE 802.1AX
Konfigurovatelné rozkládání LACP zátěže podle L3 a L4
Alespoň 15 000 záznamů v tabulce MAC adres
Min. 1000 záznamů v tabulce ARP
Protokol pro definici šířených VLAN MVRP
Podpora VLAN podle IEEE 802.1Q, minimálně 512 aktivních VLAN
Zařazování do VLAN podle protokolu 802.1v
Zařazování do VLAN podle MAC adresy bez nutnosti externího řízení (Radius)
IEEE 802.1s - Multiple Spanning Tree
STP instance per VLAN s 802.1Q tagováním BPDU (např. PVST+)
Detekce protilehlého zařízení pomocí LLDP a rozšíření LLDP-MED
Detekce jednosměrnosti optické linky (např. UDLD)
DHCP server
DHCP relay pro IPv4 a IPv6 včetně option 82 a 79
NTP pro IPv4 a IPv6 včetně MD5 autentizace
Statické směrování IPv4 a IPv6
Dynamické směrování RIPv2 a RIPng
Minimálně 1900 záznamů ve směrovací tabulce
IGMP v3 a MLD v2
Hardware podpora IPv4 a IPv6 ACL
ACL definice na základě skupiny fyzických portů
ACL aplikovatelný na rozhraní IN včetně virtuálních VLAN
BPDU Guard a Root Guard
DHCP snooping pro IPv4 a IPv6
HW ochrana proti zahlcení (broadcast/multicast storm) nastavitelná na % rychlosti portu a množství paketů za vteřinu
ICMPv4 a ICMPv6 rate-limiting per port
Podpora ověřování 802.1X včetně více uživatelů per-port (min.30)
RADIUS MAC autentizace, probíhající před 802.1x pro případy, že koncové zařízení není softwarově vybaveno pro 802.1x autentizaci
Dynamické zařazování do VLAN a přidělení QoS podle RFC 4675
Podpora 802.1X Guest VLAN
Podpora IPv6 RA Guard
IP source guard / dynamic IP lockdown pro IPv4 a IPv6

Podpora Dynamic ARP protection
Port security - omezení počtu MAC adres na port, statické MAC, možnost definování akcí při překročení
Ochrana proti opakovaným výpadkům linek (flapování) s možností konfigurace citlivosti a akce při překročení
Ochrana control plane (CPU) před útoky typu DoS
Podpora IPv4 a IPv6 QoS
IEEE 802.1p - minimální počet front 8
Management
CLI formou RJ45 serial konsole port
USB konzolový port
Konfigurace zařízení v člověku čitelné textové formě
Podpora managementu přes IPv4 i IPv6
SSHv2 a SFTP
Podpora SNMPv2c a SNMPv3
RMON
Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL
Lokálně vynucené RBAC na úrovni přepínače
Dualní flash image
TCP a UDP SYSLOG pro IPv4 a IPv6 s možností logováni do více syslog serverů
Podpora oddělených čítačů paketů pro IPv4 a IPv6 provoz
Podpora RADIUS včetně RADIUS CoA (RFC3576)
Aktivní monitoring dostupnosti RADIUSu přednastaveným jménem a heslem
Podpora TACACS+
Konfigurační změny pomocí naplánovaných pracovních úloh (Job scheduler)
Analýza síťového provozu sFlow podle RFC 3176
Podpora zrcadlení portů (SPAN) v režimu N:1
Podpora IP SLA pro měření zpoždění provozu VoIP
Podpora Zero Touch Provisioning (ZTP)
REST API pro automatizaci nastavení, včetně popory CLI a batch CLI příkazů
Podpora Chromecast Gateway
Funkce mDNS brány pro distribuci a filtraci multicast služeb napříč IP subenty. (Apple Bonjour Gateway)
Automatická konfigurace portu dle připojeného zařízení
Podpora Cloud based management

2. Systém řízené segmentované WiFi sítě

Stručný popis opatření:

Pro zvýšení bezpečnosti a správné fungování bezdrátové datové sítě bude provedena její modernizace náhradou, které bude podporovat segmentaci WiFi pomocí oddělených sítích (ESSID), dále bude využívat nejaktuálnějších bezpečných protokolů a bude podporovat ověřování uživatelů pomocí 802.1x. WiFi řešení umožní dále použití „sítě pro hosty", kde bude možné izolovat jednotlivé připojené klienty, omezit přístupy do vnitřních sítí a omezit i rychlost spojení. Všechny přístupové body WiFi sítě budou připojeny na centrální správu řízené pomocí centrálního kontroleru. Celkový počet přístupových bodů WiFi AP bude 30 ks.

Pořizované položky řešení:

- Systém řízené segmentované WiFi sítě formou nákupu 30 kusů přístupových WiFi bodů a kontroleru. Minimální záruční doba bude 5 let a součástí budou veškeré potřebné licence a průběžné aktualizace na dobu minimálně 5 let
- Instalace a konfigurace síťových prvků

Detailní technické specifikace:

Uzavřená konstrukce bez ventilátorů
Podpora bezdrátových standardů 802.11a, 802.11b/g, 802.11n, 802.11ac
Plnohodnotná certifikace Wi-Fi Aliance IEEE 802.11a/b/g/n/ac
Pracovní režimu AP bez kontroléru (autonomní)
Pracovní režimu AP pod kontrolérem (lightweight)
Pracovní režim AP v roli WLAN kontroléru s možností správy až 100 AP
Počet portů ethernet LAN 1x10/100/1000 Mbit/s RJ45
Energy Efficient Ethernet (EEE)
Podpora napájení ze switche
Možnost napájení z AC napájecího zdroje
Interní anténa MU-MIMO všesměrová
MIMO a počet nezávislých streamů na jedno rádio 4x4:4
Radiová část: dual band, současná podpora pásem 2,4GHz a 5GHz
Automatické ladění kanálu a síly signálu v koordinaci s ostatními AP
Komunikační rychlost na fyzické vrstvě (Max data rate) minimálně 1.728 Gbit
Integrovaný TPM pro bezpečné uložení certifikátů a klíčů
Podpora 802.11ac beamforming
Podpora airtime fairness
Prioritizace jednotlivých SSID na základě vysílacího času
USB port s podporou 3G/4G USB modemu jako WAN uplink

Band Steering či obdobné (prioritizace 5GHz pásma v případě je-li podporováno)
Detekce Rogue AP
Počet inzerovaných SSID (BSSID) na rádio min. 8
Nastavitelný DTIM interval pro jednotlivé SSID
Mapování SSID do různých VLAN podle IEEE 802.1Q
VLAN Pooling
Podpora wireless MESH funkcionality s protokolem pro optimální výběr cesty v rámci MESH stromu
Podpora Layer-2 izolace bezdrátových klientů
Hardware filtry pro filtraci intermodulačního rušením pocházejícím z mobilních sítí (Advanced Cellular Coexistence nebo obdobné)
Detekce a monitorování problémů WLAN odchytáváním provozu na AP ve formátu PCAP a jeho zasíláním do Ethernetového analyzátoru, schopnost zachytávat rámce včetně 802.11 hlaviček.
DHCP server, směrování a NAT pro bezdrátové klienty
AP v režimu IPSec VPN klient s možností tvorby L2 či L3 VPN
Automatická identifikace připojeného zařízení a jeho operačního systému
Předávání konektivity mezi AP při pohybu bez výpadku spojení – roaming
Dynamické vyvažování zátěže klientů mezi AP se zohledněním zátěže, počtu klientů, síly signálu v koordinaci s ostatními AP
Optimalizace provozu: multicast-to-unicast konverze
Možnost řízení QoS (šířky pásma) na základě aplikací (Office 365, Dropbox, Facebook, P2P sdílení, VoIP, video aplikace)
Filtrování přístupu na web
802.11w ochrana management rámců
Podpora Kensington lock
Podpora MAC ověřování
Podpora 802.1X ověřování
Volitelně možnost spravovat AP cloud management nástrojem
SSHv2, SNMPv2c a SNMPv3
Součástí AP je příslušenství pro montáž na zeď nebo strop, PoE injektor a další potřebné prvky

3. Modernizace firewallu

Stručný popis opatření:

Bude provedena modernizace firewallového řešení na síťovém perimetru organizace s tím, že toto řešení budou implementovány další bezpečnostní funkcionality jako IPS, VPN. Dále bude implementovaný modul pro antivirovou kontrolu a řízení internetového provozu.

Pro zvýšení bezpečnosti a odolnosti je navržena modernizace firewallového řešení na síťovém perimetru organizace s tím, že v tomto řešení budou implementovány další bezpečnostní funkcionality jako IPS, VPN. Ochrana síťového perimetru musí zabránit útokům na vnitřní sítě, včetně detekce spoofingu, ochrany před hrozbami DoS, DDoS a různých paketových útoků (ICMP). Dále je navržena implementace modulu pro detekci škodlivého kódu v datovém provozu (antivirová kontrola) a řízení internetového provozu (minimálně pro http, https a ftp provoz).

- Propustnost Firewallu minimálně 20 Gb/s
- Alespoň 2 WAN porty pro připojení dvou nezávislých datových poskytovatelů
- Možnost zapojit stejný typ Firewall a vytvořit cluster (Active/Passive nebo Active/Active)
- Funkcionalita IPS (Intrusion prevention systém)
- Funkcionality VPN gatevay minimálně protokol IPSec, volitelně další VPN protokoly jako L2TP, PPTP
- HTTPS proxy na Firewallu, která ukončí SSL/TLS spojení na Firewallu a provede inspekci datového spojení
- Softwarově rozšiřovatelné funkcionality Firewallu

Pořizované položky řešení:

- Modernizace Firewallu formou nákupu. Součástí bude záruka minimálně 5 let a veškeré potřebné licence a průběžné aktualizace na dobu minimálně 5 let
- Kompletní instalace, implementace, nastavení bezpečnostních politika zaškolení uživatelů

Detailnější technická specifikace:

Výkon:
FW propustnost: alespoň 26 Gbps
FW IMIX propustnost: min. 9 Gbps
VPN propustnost: min. 2.7 Gbps
IPS propustnost: min. 5.5 Gbps
NGFW propustnost (IPS + App Ctrl + WebFilter):min. 4 Gbps
AV proxy propustnost: 3.3 Gbps
Počet současných spojení alespoň: 17 500 000
Počet nových spojení za sekundu: min. 200 000
Minimální požadavky na HW
Integrovaný SSD disk (alespoň 180GB)

8 x RJ45 metalických portů
2 x 1G SPF porty
2 x 10G SPF+ porty
možnost rozšíření o 2x 40 GE QSFP+ porty nebo 4x 10G SFP+ porty
redundantní zdroj napájení (externí)
konektor HDMI pro přímé napojení na monitor
3x USB 3.0 port
1x micro USB port
RAM alespoň 12GB DDR3
Obecná specifikace
Řešení je Leader v Gartner Magic Quadrant – UTM (2017)
Možnost správy WiFi AP od on box (integrovaný WiFi controler)
Řešení nabízí User Portal s možností správy emailové karantény pro uživatele v případě nákupu licence pro zabezpečení emailového provozu
Řešení disponuje funkcí tzv. Selective HTTPS Scanning, která umožňuje správci vybrat určitý HTTPS obsah, na kterém má být provedeno skenování a kontrola protokolu SSL.
Řešení poskytuje vhled do uživatelské aktivity tzv. User Threat Quocientem – automatickým nástrojem, který uděluje skóre rizikovosti jednotlivým uživatelům
Řešení je schopno na základě automatizovaného procesu zjistit aktuální bezpečnostní stav koncové stanice (zda nebyla na stanici identifikována nákaza malwarem, agent AV je plně aktualizován atd.) a případně uplatnit restriktivní politiky na konkrétní zařízení. Platí v případě nákupu AV od stejného výrobce.
Řešení musí umožnit identifikaci všech aplikací, které běží na koncové stanici a v rámci FW uplatnit zvolenou politiku per aplikace. Platí v případě nákupu AV od stejného výrobce.
FW musí mít integrovaný tester pro FW a web filter politiky
Řešení musí nabízet on-box reporting
Podpora Wildcard pro Domain Name Host Objects
Funkcionality
Zahrnuje ochranu pomocí Intrusion Prevention (IPS) - možnost definování vlastních signatur
Možnost rozšíření o cloud Sandbox Protection, které nabízí machine learning (datacentrum s umístěním v zemích EU)
Nabízí možnost rozšíření o Web Application Firewall a reverzní proxy
Nabízí plně transparentní proxy pro AV kontrolu a filtrování webu
Dva nezávislé skenovací AV enginy (různí výrobci) v rámci nabízené licence pro kontrolu webového provozu

Zajišťuje kontrolu emailového provozu včetně šifrování emailové komunikace a ochraně proti ztrátě dat, tzv. DLP Dva nezávislé skenovací AV enginy (různí výrobci) v rámci nabízené licence
Umožňuje nasazení v clusteru Active/Active nebo Active/Passive, přičemž v režimu A/P není nutné pro pasivní HW applianci kupovat licenci

4. Systém antimalwarové ochrany PC (Endpoint advanced protection)

Stručný popis opatření:

Implementace systému pokročilé ochrany koncových stanic, antimalwarové ochrany hybridní infrastruktury fyzických i virtuálních koncových stanic s důrazem na snížení utilizace potřebných IT zdrojů a ochranu proti pokročilým hrozbám nultého dne, APT, Kryptovirům (Ransomware). Řešení bude umět chránit file system, operační paměť, služby i registry a dále musí umět centrální správu všech endpointů včetně dedikované virtuální Appliance instalované virtualizační platformě. Řešení musí disponovat pokročilým firewall s Application white listingem (součást efektivní ochrany proti útokům nultého dne). Řešení musí umět blokovat a řídit přístup ke všem přenositelným zařízením.

Pro zvýšení bezpečnosti a správné fungování všech koncových stanic PC je navržena implementace systému pokročilé antimalwarové ochrany koncových stanic s důrazem na snížení utilizace potřebných IT zdrojů a ochranu proti pokročilým hrozbám typu nultého dne (zero-day), APT – přetrvávající pokročilé hrozby (Advanced Persistent Threat), Ransomware (kryptoviry).

Řešení musí chránit celou infrastrukturu koncových bodů s důrazem na snížení systémových nároků na provoz bez dopadů na úroveň bezpečnosti. To bude umět chránit file system, operační paměť, služby i registry a dále musí umět centrální správu všech endpointů včetně dedikované virtuální Appliance instalované virtualizační platformě. Řešení musí disponovat pokročilým firewallem s Application white listingem (součást efektivní ochrany proti útokům nultého dne). Řešení musí umět blokovat a řídit přístup ke všem přenositelným zařízením.

Pořizované položky řešení:

- Bezpečnostní řešení antimalvarové ochrany PC (Endpoint advanced protection) včetně všech potřebných licencí a průběžných aktualizací na dobu minimálně 5 let
- Kompletní instalace a implementace včetně zaškolení obsluhy

Detailnější technická specifikace:

Antimalware ochrana (ochrana před rootkit, spyware, adware, PUP atd.)
Centrální správa přes management rozhraní umístěné v datacentru výrobce (možnost volby DC v zemích EU)
Host Intrusion Prevention
Application Control musí zamezovat instalaci aplikací, které představují bezpečnostní nebo právní hrozby pro společnost.
Blokování URL na základě kategorií
Data Loss Prevention musí umožňovat blokovat dokumenty označené jako důvěrné, aby nemohly být zaslány přes email, webový prohlížeč nebo nahrány na USD disky.
Musí umožňovat automatizované propojení s firewallem na perimetru a odesílat informace o svém stavu na tento firewall
Řešení musí být schopné blokovat pokusy o komunikaci na C&C servery
Veškeré bezpečnostní moduly nabízeného AV řešení musí být součástí jednoho agenta pro snížení HW nároků

Řešení nabízí kontrolu stahovaných souborů na základě reputace a jejich skenování AV enginem
Device Control - řízení přístupu pro USB disky apod.
Blokování PUA aplikací
Automatické odstraňování detekovaného malware
Řešení musí být od výrobce, který je Gartner Leader pro oblast Endpoint Protection Platforms v roce 2018 – min v TOP3

5. Systém antimalwarové ochrany pro komunikační servery

Stručný popis opatření:

Pro zvýšení bezpečnosti a spolehlivé fungování emailové komunikace je navržena implementace systému pokročilé ochrany emailového provozu chránící uživatele před spamem, malware i phishingem šířeným poštou. Systém musí disponovat několika antispamovými filtry současně, jako DNS Blacklisty na úrovni SMTP spojení, inteligentní analýzu obsahu e-mailu, IP Sender Reputation System (SRS), detekci obrázkového spamu a analýzu hlavičky e-mailu.

Dále systém musí disponovat minimálně dvěma nezávislými antivirovými jádry ke zvýšení úrovně ochrany poštovního serveru proti trojanům, virům a jinému malwaru. Systém musí být schopen integrace s Active Directory a s poštovním serverem typu Microsoft Exchange. Výhodou je podpora virtualizovaného prostředí, jako je VMware.

Pořizované položky řešení:

- Systém antimalvarové ochrany pro komunikační servery pro minimálně 400 účtů. Součástí budou veškeré potřebné licence a průběžné aktualizace na dobu minimálně 5 let.
- Kompletní instalace, nastavení a zaškolení obsluhy

6. Systém analýzy síťové komunikace (NetFlow, NBA)

Stručný popis opatření:

Jako další technické bezpečnostní opatření pro ochranu interní datové infrastruktury je navrženo využití řešení pro analýzu a detekci anomálií pomocí monitorování sítí na bázi datových toků (NetFlow/IPFIX). Takové řešení musí být schopné provádět diagnostiku výkonnostních problémů datové infrastruktury, provádět detekci pokročilých kybernetických hrozeb a následně provést příslušné automatizované opatření.

Základem takových síťových analýz jsou NetFlow systémy se sondami, které analyzují každý procházející paket podklady = data pro vyhodnocování. Součástí vyhodnocování síťových dat musí být i behaviorální analýza datových toků (NBA). Vznikne tak systém detekce anomálií a nežádoucího chování v datové síti, založený na permanentním vyhodnocování statistik a informací o provozu na síti, který automatizovaně dokáže odhalovat bezpečnostní a provozní problémy, a zvýšit vnější i vnitřní bezpečnosti datové sítě. Tento systém je pak možné propojit do nadřazeného systému SIEM.

Implementace bude provedena pomocí autonomní hardwarové sondy. Tato hardwarová netflow sonda bude připojena k centrálnímu switchi pomocí metalického vedení s kapacitou 1Gb Ethernet.

Další komponentou nebo funkcionalitou musí pak být systém Anomaly Detection System (ADS), které bude provádět vlastní detekce anomálií a analýzy chování sítě síťovou infrastrukturou, klíčová je schopnost detekce cílených útoků nebo identifikace neznámého malware na síťové úrovni schopnost reakce na takové specifické hrozby reagovat. Funkcionalita na rozdíl od provozně – technického monitoringu např. na úrovni SNMP musí sledovat celkové chování zařízení v síti a identifikovat hrozby pro které neexistuje signatura stejně jako Heuristické analýzy antivirových systémů. Takto se doplní základní bezpečnostní opatření na bázi firewallů, IDS/IPS systémů a antivirových systémů.

Pořizované položky řešení:

- Systém analýzy síťové komunikace včetně všech potřebných licencí a průběžných aktualizací na dobu minimálně 5 let
- Kompletní instalace a implementace včetně zaškolení obsluhy
- Nastavení pravidel pro detekci událostí, nastavení reportů a alertů

Detailní technická specifikace:

Specifikace obecných požadavků na nástroj:
Nástroj zajišťující detailní viditelnost síťového provozu s možností vizualizace komunikace všech hostu a jejich služeb s možností forenzní analýzy v řádu měsíců. Nástroj je schopen detekovat anomálií na úrovni toků a dále rozpoznávat známe hrozby na základě DPI za pomoci detekčních signatur.
Nástroj na analýzu síťového provozu se logicky skládá z jedné nebo více sond pro sběr dat a z jedné centrální konzole pro vyhodnocování dat o síťovém provozu. Fyzicky jde o jednu hardwarovou applianci, nebo o několik hardwarových appliance.
Celá softwarová část je od jednoho výrobce.

Jedna centrální konzole pro vyhodnocování dat o síťovém provozu je schopná analyzovat všechna data (tj. až 200Mbps) od všech zdrojů dat a zobrazovat je v jednom jednotném aplikačním rozhraní.
Nástroj neobsahuje žádný skrytý (backdoor) přístup.
Řešení obsahuje veškerý hardware a software potřebný pro zprovoznění a provoz.
Licence na aktualizace veškerého software nástroje a jeho dat (filtry, signatury, databáze třetích stran, threat intelligence, atd.) na 60 měsíců.
Licence na neomezený počet uživatelů, kteří používají sondy a centrální konzoli.
Fungování s přístupem na Internet i bez nutnosti přístupu na Internet.
Implementace a provoz nástroje nemodifikuje stávající provoz a bezpečnost počítačové sítě.
Požadavky na nasazení:
Montáž všech appliance do standardních 19" skříní (rack).
Celková velikost všech appliance dohromady maximálně 2U (rack unit).
Minimálně dva napájecí zdroje pro každou appliance.
Napájení všech appliance 230 V AC / 16 A.
Vestavěné napájecí zásuvky IEC typ C13 ve všech appliance.
Provoz všech appliance v teplotním rozsahu minimálně 10–35 stupňů Celsia.
Minimálně jedno síťové rozhraní pro správu appliance na každé appliance.
Požadavky na analýzu provozu a hardwarovou podporu:
Nástroj bude získávat kopii provozu na 1 místě počítačové sítě: – Celkový datový tok maximálně 1Gbps, připojení sondy 1 Gbps metalika. – Možnost napojení dalších lokalit.
Minimálně 1 LAN rozhraní 1 Gbps metalika na appliance, na které je centrální konzole, pouze pro práci s konzolí.
Minimálně 1 volné LAN rozhraní 1 Gbps metalika a minimálně 1 volné LAN rozhraní 1Gbps metalika jako rezerva na sondách pro sběr dat.
Celkem tedy minimálně 4 LAN rozhraní 1 Gbps metalika pro sběr dat a 1 LAN rozhraní 1 Gbps metalika pro práci s centrální konzolí.
Kapacita centrálního diskového úložiště minimálně 1TB (terabyte) na rychlém datovém uložišti SSD.
Stejné funkce pro IPv4 a IPv6 (s výjimkou funkcí, které v IPv4, respektive IPv6 vůbec neexistují).
Podpora VLAN podle IEEE 802.1Q.
Nástroj zpracuje veškerá data odeslaná na jeho síťová rozhraní pro příjem síťového provozu.
Zpracování sítových dat a jejich vizualizace:
Nástroj provádí analýzu (kopie) datového provozu, který obdrží ze zrcadlených (SPAN, mirror) portů aktivních síťových prvků.

Komunikace mezi sondou a kolektorem je plně šifrována na úrovni SSL/TLS.
Aplikace umožnuje jednotné vyhledávání ve všech datových pohledech, tj. jeden vyhledávací dotaz je možné aplikovat na síťová data, bezpečnostní incidenty případně jiná zobrazení jako přehledové informace, bez nutnosti kopírovat nebo jinak přenášet, či modifikovat vyhledávací filtr.
V datech lze vyhledávat/filtrovat dle libovolného parametru, případně kombinace parametrů datového toku – minimálně hostname, jméno uživatele z Active Directory, IP adresa, MAC adresa, lokální služba (local service), vzdálená služba (remote service), příchozí provoz, odchozí provoz, interní provoz.
Je možné použít aplikačního průvodce pro vytváření uživatelských filtrů a jejich uložení případně sdílení mezi ostatními uživateli.
Aplikace průběžně vytváří a ukládá statistická dat o síťovém provozu na všech podsítích, všech hostech a všech službách v rámci monitorované sítě.
Aplikace umožňuje okamžitou grafickou vizualizaci a výpis průběhu komunikace u všech zařízení v monitorované síti, všech služeb a všech podsítí s možností řazení dle libovolné hodnoty – např. přenesená (odchozí, příchozí) data, pakety, toky, množství komunikačních partnerů, výkonnostní metriky (RTT – Round Trip Time, ART – Application Response Time, EUT – End User Experience Time ...).
Síťové toky jsou prezentovány při každém zobrazení v aplikaci jako obousměrné. Tj. prezentace, zda daný tok (požadavek) měl i opačný provoz (odpověď), bez nutnosti vytváření dalších filtrů či dohledávání zpětné komunikace na jiném řádku.
Záznam každého síťového toku obsahuje stejné informace vždy pro požadavek i odpověď. Minimálně však: IP adresa, MAC adresa, port, počet paketů, velikost dat přenášených po sítí, velikost aplikačních dat přenesených po síti, identifikovaný aplikační protokol, aplikační metadata všech provedených transakcí v rámci daného toku.
Ukládání aplikačních metadat (transakcí) minimálně pro HTTP (minimálně URL požadavku a návratový kód odpovědi pro každou transakci), DNS (plné znění požadavku i odpovědi) a HTTPS (použité certifikáty).
Možnost nastavení obsahu ukládaných metadat, včetně možnosti úplného vypnutí ukládání aplikačních metadat.
Ukládání plného záznamu síťové komunikace v formátu PCAP dle uživatelem definovaných filtrů.
Nastavení systémového času manuálně a formou synchronizace s časovými servery protokolem NTP.
Geolokace externích IP adres dle databáze platné v době zaznamenání síťového toku.
Aplikace přiřazuje všem IP adresám hostname dle aktuálních DNS záznamů.
Aplikace přiřazuje všem IP adresám hostname dle aktuálních DHCP záznamů.
Aplikace umožnuje dešifrování libovolné komunikace na úrovni SSL/TLS vložením privátního šifrovacího klíče/certifikátu. Po dešifrování je provedená plnohodnotná inspekce provozu, tj. bezpečnostní analýza za pomocí známých hrozeb (signatur), uložení metadat atd.

Požadavky na metody detekce a detekční schopnosti:
Metoda detekce kybernetických útoků na základě rozpoznání anomálií v síťovém provozu. Anomálie jsou detekovány porovnáním aktuálního chování vůči chování za minulé období. Detekce minimálně pro jednotlivá zařízení v síti, pro jednotlivé služby v síti a pro jednotlivé podsítě.
Detekce na základě modelování koncových hostů EPM - End Point Modeling. Detekce odchylek od predikovaného chování dle historického modelu chování všech hostů v síti, všech služeb na každém hostu v síti a jednotlivých podsítí.
Metoda detekce kybernetických útoků na základě síťové behaviorální analýzy komunikace, tj. detekce vzorů chování za pomoci detekčních pravidel.
Detekce opakujícího se chování se zpětnou analýzou každého hosta a každé služby.
Metoda detekce porušení interních bezpečnostních politik za pomocí síťové behaviorální analýzy cílená na dodržování politikou definovaných komunikačních matic a komunikačních vektorů.
Metoda detekce kybernetických útoků na základě síťové behaviorální analýzy cílené na rozpoznání strojového a lidského chování v dlouhodobých časových intervalech.
Metoda pro detekci aplikačních a síťových výkonnostních problémů a anomálií za pomoci analýzy síťových výkonnostních metrik (alespoň. RTT, ART).
Metoda detekce kybernetických útoků na základě automaticky a pravidelně aktualizovaných detekčních signatur známých hrozeb typu Snort. Aplikace obsahuje alespoň 30.000 aktivních detekčních signatur.
Detekční signatury rozděleny do kategorií dle zaměření detekce na určitý typ kybernetické hrozby. Například: Trojan, Exploit, Webové útoky, Malware, Mobilní malware, zneužití zranitelnosti dle CVE kódu, atd.
Vytváření a nasazení vlastních signatur pro detekci určitého vzoru v obsahu komunikace v jazyce, který je obdobný (nemusí být identický, ale má obdobné možnosti), jako je jazyk pro psaní pravidel pro SNORT.
Analýza plného obsahu komunikace pomocí DPI (Deep Packet Inspection). Nejedná se o analýzy jen zaznamenaných metadat komunikace.
Detekce minimálně následujících typů skenování portů: TCP, SYN, FIN, NULL.
Detekce hádání hesel pro minimálně následující protokoly: TELNET, HTTP, SSH, RDP, FTP, SMTP, IMAP, POP3, SMB, SMB2.
Detekce známých (vyskytujících se v signaturách nástroje) hrozeb a škodlivého kódu (malware).
Detekce DoS útoků.
Měření výkonnosti všech aplikací vyskytujících se v monitorované síti, které používají TCP, minimálně podle RTT (Round Trip Time) a ART (Application Response Time). S grafickou vizualizací pro jednotlivé hosty v síti a všechny služby obsažené v monitorované síti.
Detekce komunikace s adresami s nízkou reputací, známými botnety a C&C centry, darknetem (nelegitimní služby a aplikace provozované v internetu).

Detekce P2P komunikace.
Detekce aplikací. Minimálně Skype, Jabber/GTalk, Torrent, TOR.
Detekce standardních protokolů, i když běží na nestandardních portech – např. HTTP nebo SSH na portu 443 atd.
Detekce datových tunelů v komunikaci. Například HTTP v DNS, SMTP v HTTP, IPv6 v IPv4.
Detekce anomálií v komunikačních protokolech, minimálně DNS, DHCP, HTTP, SMTP, SMB.
Detekce událostí: • MAC Spoofing • IP Spoofing • Duplikace/změna IP • Duplikace/změna MAC • Detekce neočekávaného přenosu objemu dat (Bandwidth anomaly detectiom) Detekce neočekávaného počtu spojení (Connection rate detection)
Detekce nedostupnosti vybraných zařízení a služeb.
Detekce vzniku nových služeb, či komunikačních vektorů nedopovídajících uživatelem definované komunikační matici monitorované sítě.
Možnost dešifrování SSL/TLS komunikace obsahu komunikace pro vybraná zařízení s využitím privátního klíče.
Každá detekované bezpečnostní událost poskytuje odkaz na konkrétní tok, nebo toky, které bezpečnostní událost způsobily. Tento síťový tok události obsahuje vždy záznam s informacemi o požadavku i odpovědi.
Výrobcem automaticky aktualizovaná databáze adres a jmen s nízkou reputací na Internetu (SPAM listy, black listy, weby s malware atd.) po dobu 24 měsíců. Jde o komerční databázi, ne o volně dostupnou nebo komunitní databázi.
Výrobcem automaticky aktualizovaná databáze IP adres známých botnet C&C center po dobu 24 měsíců. Jde o komerční databázi, ne o volně dostupnou nebo komunitní databázi.
Výrobcem automaticky aktualizovaná databáze signatur hrozeb a útoků po dobu 24 měsíců. Jde o komerční databázi, ne o volně dostupnou nebo komunitní databázi.
Aplikace poskytuje možnost vytváření vlastních detekčních signatur ekvivalentních s typem Snort.
Požadavky na administraci a výstupy:
Nástroj obsahuje integrovaný centrální reporting, který je součástí produktu. Nesmí jít o externí komponentu.
Reporty minimálně ve formátech PDF a DOCX.
Reporty v českém nebo anglickém jazyce.
Rozesílání reportů elektronickou poštou.

Uživatelsky definované reporty.
Zálohování dat na externí datové úložiště dostupné minimálně přes protokol CIFS.
Logování ve formátu syslog, CEF, LEEF s možností konfigurovatelné struktury obsahu generovaných záznamů.
Konfigurovatelná možnost, že zpráva syslog obsahuje URL odkaz do centrální konzole na událost, která způsobila odeslání syslog zprávy.
Minimálně 2 DNS servery pro překlad mezi jmény a IP adresami.
Základní administrace (nastavení sítě, restart aplikace, ověření stavu aplikace) možná přes řádkové rozhraní s využitím SSH2.
Pokročilá administrace přes jedno jednotné uživatelské grafické rozhraní s využitím standardního web prohlížeče.
Procesní podpora nástroje při řešení detekovaných událostí. Tj. nástroj podporuje přiřazení více stavů (např. detekovaná, řešená, vyřešená) jednotlivým událostem (detekovaný incident). Vše je součástí jednoho jednotného uživatelského grafického webového rozhraní.
Možnost zobrazení (filtrování) událostí v GUI dle aktuálního stavu (např. detekovaná, řešená, vyřešená)
Autentizace uživatelů nástroje vůči LDAP, MS Active Directory a lokální databázi.
Administrátorské profily s možností přidělování práv (read only, read-write, none) pro jednotlivé skupiny administračních funkcí, pro jednotlivé metody detekce, pro jednotlivé rozsahy IP adres, MAC adres, atd.

7. Systém testování zranitelnosti

Stručný popis opatření:

Pro zajištění technického bezpečnostního opatření bude provedena implementace systému automatizovaného testování zranitelností, které zajistí provádění automatizovaného testování známých zranitelností podpůrných technických aktiv zajišťujících provoz primárních aktiv v definovaných periodách. Systém bude dále detekovat a diagnostikovat možné zranitelnosti a zjištění porovnávat s otevřenými databázemi zranitelností podle standardu CVE (Common vulnerabilities and exposures).

Nástroj umožní automatické spouštění předdefinovaných předloh nebo sestav detekcí, definice šablon nebo předloh nebo sestav detekcí.

Nástroj musí podporovat síťové protokoly IPv4 a IPv6. Dále umožní export výstupů ve formátech vhodných pro další strojové zpracování například strukturovaný text, XML, JSON, apod. a bude schopen integrace s dalšími nástroji prostřednictvím API (JSON / REST API, apod.) nebo s užitím skriptování frameworkem na straně OS.

Nástroj může být nasazen jako virtualizovaný systém ve formě nezávislé SW appliance pro VMWare virtualizační platformu. Nebo musí být jako program pro operační systém Windows 2008 a novější.

Předpokládaný počet zařízení pro pravidelné testování zranitelností je kolem 750.

Pořizované položky řešení:

- Implementace systému testování zranitelností včetně všech případných licencí a průběžných aktualizací po dobu minimálně 5 let
- Kompletní instalace a implementace systému, včetně zaškolení obsluhy

[redacted]

Střední škola technická a ekonomická

[redacted]

22.10.2018

[redacted]