PŘÍLOHA Č. 1

Technická specifikace

Aktuální stav řešení:

Magistrát hlavního města Prahy (MHMP) dnes využívá pro zabezpečení perimetru sítě a sítě MEPNET bezpečnostní technologie Check Point. V případě bodu prostupu se jedná o clusterované řešení (postavené na Check Point 21400 VSX), které ale fyzicky neodděluje vnitřní části sítě a interní uživatele od vnějších sítí (včetně MEPNET) a brány pro vzdálené přístupy, a představuje tak zranitelný bod (single point of failure) z hlediska bezpečnostní architektury. Zároveň neumožňuje dostatečnou detailizaci nasazení IPS pro ochranu připojených organizací. V případě nasazené technologie pro extrakci hrozeb (SandBlast Appliance TE1000X) se jedná pouze o jednu appliance a její výpadek znamená kompletní výpadek celého subsystému – i proto, že SandBlast technologie je nasazená pouze na perimetru, nikoli na koncových stanicích.

ŘEŠENÍ MUSÍ ZAJISTIT A PODPOROVAT:

řešení zajistí fyzické oddělení všech služeb souvisejících s přístupy z externích sítí (externí sítě mimo sítě MHMP a síť MEPNet), jedná se především o:

- VPN přístupy spolupracujících subjektů a mobilních uživatelů,
- internetový přístup uživatelů MHMP
- publikace veřejných informačních zdrojů MHMP,
- integrace do centrální správy stávajícího bezpečnostního řešení,
- detekce a ochrana proti tradičním, ale i novým pokročilým zero-day útokům minimálně v SMTP a HTTP provozu
- ochrana proti zero-day útokům a ransomware na úrovni koncových stanic a uživatelů
- lokální emulace zero-day útoků (soubory neopouštějí síť MHMP) z koncových stanic

MINIMÁLNÍ POŽADAVKY NA NABÍZENÉ ŘEŠENÍ:

Firewall cluster pro externí perimeter

- detekce a ochrana proti tradičním, ale i novým pokročilým útokům minimálně v SMTP a HTTP provozu
- ochrana proti Zero-day útokům,
- ochrana proti Ransomware útokům,
- ochrana proti průniku dalších typů škodlivého SW,
- detekce a prevence neoprávněných síťových aktivit,
- detekce a prevence zapojení interních stanic do BOTNET sítí,
- detekce a ochrana proti rizikovým aplikacím,
- prevence přístupu uživatelů na servery se závadným obsahem,
- požadované funkcionality a licence: L3/L4 firewall, ochrana proti Zero-day útokům, IPS, kontrola aplikací, URL filtering, Anti-Virus, detekce a blokování botnetů
- podpora IPSec a SSL VPN tunelů pro vzdálený přístup uživatelů
- jednotná správa řešení - ze stávajícího centrálního firewall management serveru Check Point Smart Center

- režim vysoké dostupnosti (aktivní/pasivní, případně aktivní/aktivní),
- řešení je navrženo ve formě HW zařízení (tzv. appliance)

MINIMÁLNÍ POŽADAVKY NA HW pro Firewall cluster pro externí perimeter:

- propustnost stavového firewallu (RFC 3511, 2544, 2647, 1242) - 75 Gbps
- propustnost 18 Gbps systému IPS při plné inspekci celého síťového provozu,
- propustnost 15 Gbps systému NGFW (Firewall, IPS, Aplikační kontrola)
- propustnost 5 Gbps Threat ochrana (Firewall, IPS, Aplikační kontrola, Antivir, URL filtering, Zero day)
- počet nových spojení 180.000 za 1 sekundu,
- typy a počet komunikačních rozhraní:
    - 1Gbps (RJ45 a SFP) - 10x RJ45
    - 10 Gbps (SFP+) - 6x SFP+, včetně 6x SR transcieverů
    - podpora rozhraní 40 Gbps QSFP - možnost rozšíření o 2x 40Gb QSFP+ rozhraní
    - samostatné vyhrazené rozhraní pro správu HW i v případě výpadku (Out of Band Management) - tzv. LOM card
- podpora IPv6
- hot-swappable redundantní ventilátory
- hot-swappable redundantní napájecí zdroje (AC)
- lokální HDD, pro případ výpadku centrálního management log server – min. 800GB
- montáž do standardních rozvodných skříní (rack 19"),

Zero-day ochrana pro koncové stanice

- Management server licence pro 2000 uživatelů
- Ochrana proti "zero day" malwaru na koncových stanicích pomocí emulace souborů
- Detekce/blokování komunikace malwaru na řídící botnet C&C centra
- Detailní automatická forenzní analýza malware incidentů
- Ochrana proti Ransomware včetně možnosti automatického obnovení zašifrovaných datových souborů na lokálním disku (nezávisle na funkc iVolume Shadow Copy Service (VSS))
- Ochrana proti Ransomware i v off-line režimu (bez přístupu k reputačním cloudovým službám)
- Anti-phishing ochrana, s reputací web formulářů pomocí analýz v reálném čase
- Funkce bezpečného stahování dokumentů: konverze/očištění souborů do čisté formy, nebo filtrace dynamických částí dokumentu (např. filtrace maker, javascript…)
- podpora klientů pro operační systémy MS Windows (verze Windows 7, Windows 8.1 a Windows 10)
- Privátní sandbox appliance pro emulaci souborů z koncových stanic
- Privátní sandbox appliance musí umožňovat identifikaci malwaru skrytého v souborech těchto typů: pdf, doc, docx, dot, docm, dotm, ppt, pptx, exe, com, tar, zip, rar, 7z, gz, tgz, bz2, cab, iso, swf, jar, js, jse, scr, csv, rtf, pif, wsf, wsh, vbs, vba, vbe
- Pokročilá ochrana dat využitím transparentního šifrování disků (Full Disk Encryption)
- Jednotná správa řešení Zero-day ochrana pro koncové stanice - integrace do stávající log analytické platformy Check Point SmartEvent

MINIMÁLNÍ POŽADAVKY pro Sandbox private HW appliance:

- Podporováno pro emulaci 1.000.000 souborů za měsíc (cca 30.000 souborů denně)
- Inspekční propustnost – 2000 Mbps
- Min. 28 paralelně běžících VM s licencemi pro Windows OS a MS Office
- Redundantní HDD s minimální kapacitou 1 TB
- Redundantní napájení
- 4x 10/100/1000, 2x 10Gbps SFP+

PŘEHLED POPTÁVANÝCH KOMPONENT:

Popis komponent	Počet kusů
CPAP-SBTE1000X-28VM (On Premise HW appliance pro podporu mobilních uživatelů a emulaci ZeroDay hozeb)	1
CPSB-NGTX-SBTE1000X-3Y (licence na 3 roky)	1
CPAP-SG15600-NGTX-HPP (HW appliance zabezpečující externí perimetr, včetně licence na 1 rok)	2
CPSB-NGTX-15600-2Y (licence na 2 roky)	2
CPEP-COMPLETE-3Y (SW licence – ochrana mobilních uživatelů před ZeroDay útoky + Data protection modul/ Full Disk Encryption)	2000
CPSM-P2503-E (centrální management pro správu mobilních uživatelů)	1
Podpora výrobce CPCES-CO-PREMIUM na všechny výše uvedené položky	36 měsíců