PŘÍLOHA Č. 1 Specifikace Dodávky

PŘEDMĚT ZADÁNÍ

Vytvoření ochrany interní datové sítě Magistrátu hl. m. Prahy (dále jen MHMP) proti hrozbám v reálném čase (Advanced Persistent Threats), které cíleně napadají interní systémy s cílem získat úplný přístup k celé síti a všem jejím datům. Vzhledem ke skutečnosti, že tyto útoky nemusí být založeny na již známých zranitelnostech a tudíž se nedá využít standardní postupy a nástroje (Antivirus, AntiSpam), je třeba aktivovat nástroj schopný tyto hrozby identifikovat a zabránit průniku útočníků do interní datové sítě.

TECHNICKÉ POŽADAVKY

Dodávané řešení pro ochranu před neznámými malware hrozbami v reálném čase se nesmí spoléhat na signatury známých útoků, ale musí využívat jiný způsob detekce nežádoucího kódu. Požadovaným způsobem je využití emulovaného sandbox prostředí, kde se v izolovaném prostoru virtualizovaných operačních systémů budou jednotlivé hrozby detekovat. Předpokládá se dodání dedikovaného hardware pro privátní cloud a software oboje s podporou výrobce (maintenance) na dobu 12 měsíců v režimu hlášení závad 7x24 a vyřešení následující pracovní den (NBD). Řešení bude rozšiřovat a doplňovat stávající bezpečnostní systém Check Point SG21400 a integruje se tak do stávajícího managementu bezpečnostního systému.

ŘEŠENÍ MUSÍ ZAJISTIT A PODPOROVAT:

- Ochranu webového a email provozu
- Sledování chování každého souboru a jeho vyhodnocování z více hledisek (bez závislosti na signatuře)
- Sledování změn souborů (změny na file systému)
- Změny registrů
- Analýza procesů
- Analýza síťové komunikace
- Podpora více než 30 běžných typů souborů včetně emulace archivů, spustitelných souborů, pdf a Microsoft Office dokumentů
- Efektivita prevence neznámých hrozeb 99%
- Schopnost detekce nežádoucího malware
- Funkcionalitu bezpečného doručování dokumentů (extrakce dynamických a ostatních zneužitelných částí a komponent z dokumentů typu pdf a MS Office)

MINIMÁLNÍ POŽADAVKY NA NABÍZENÉ ŘEŠENÍ:

- Návaznost na stávající technologie firewall Check Point SG21400
- Musí umožňovat identifikaci malwaru skrytého v souborech těchto typů:
    - Adobe Acrobat dokument (pdf)
    - Microsoft Word dokument (doc, docx, dot, docm, dotm)
    - Microsoft Excel dokument (xls, xlsx, xlm, xlsm)
    - Microsoft PowerPoint dokument (ppt, pptx,)
    - Spustitelné soubory (exe, com)
    - Archivní soubory (tar, zip, rar, 7z, gz, tgz, bz2, cab, iso)
    - Flash soubory (swf)
    - Java soubory (jar, js, jse)
    - SCR a CSV soubory
    - Soubory typu rtf
    - Soubory typu pif
    - Skript soubory (wsf, wsh, vbs, vba, vbe)
- Dynamická analýza souborů a dokumentů na detekci kybernetických hrozeb ve virtuálním prostředí (sandboxu)
- Zabezpečení dynamické analýzy proti útokům na různé verze operačního systému MS Windows
- Zabezpečení dynamické analýzy s podporou následujících protokolů:
    - HTTP
    - HTTPs (dekrypce SSL provozu)
    - SMTP, s podporou MTA agenta
    - SMTPs (dekrypce TLS provozu), s podporou MTA agenta
- Možnost aktivní blokace útoku již při prvním výskytu hrozby (hold mód) pro SMTP i HTTP provoz
- Možnost manuálního nahrání souborů přímo na emulation appliance přes API rozhraní
- Možnost integrace do stávajícího bezpečnostního managementu, log managementu a reportingu
- Monitorování chování spuštěného souboru se zaměřením na změny v systému souborů, systémových registrů, procesů a navázání síťových spojení
- Analýza souborů uvnitř SSL a TLS komunikace
- Monitorování emailové komunikace s kontrolou příloh
- Zabezpečení aktualizace signatur pro již známé soubory
- Tvorba vlastních signatur
- Definice politik a reporting:
    - Granulární definice politik – per IP adresa/síť
    - Granulární definice politik – per uživatelská identita
    - Výjimky v definici politik – per IP adresa/síť/uživatel
    - Výjimky v definici email politik – per odesílatel/příjemce/doména
    - Výjimky v definici politik – per soubor (MD5)
    - Reporting

  - Detailní analýza všech aktivit (zápisy do registrů, změny ve filesystem, síťové spojení, analýza systémových procesů)
  - Detailní popis všech volání procesů
  - Export reportu do pdf
- Řešení musí umožnovat plně preventivní režim s blokováním vstupu malware do interní sítě

MINIMÁLNÍ POŽADAVKY NA HW:

- 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
- Redundadní HDD s minimální kapacitou 1 TB
- Redundadní napájení
- 4x 10/100/1000, 2x 10Gbps SFP+

IMPLEMENTAČNÍ PRÁCE

Požadujeme implementaci dodávané technologie do prostředí serverové infrastruktury MHMP, napojení na stávající management Check Point a konfiguraci politiky. Řešení musí dynamicky analyzovat soubory v rámci HTTP komunikace a emailového provozu. Výstupem je zprovozněné řešení s nakonfigurovanou a funkční politikou a zaškolení odborného personálu MHMP pro následný provoz systému. Odhadovaný rozsah implementačních prací 30 MD.

PŘEHLED POPTÁVANÝCH KOMPONENT

Popis komponent	Počet kusů
CPAP-SBTE1000X-28VM (HW appliance)	1ks
CPSB-NGTX-SBTE1000-1Y (SW pro appl.)	1ks
CPSB-TETX-21400-1Y (SW rozš. pro stáv. FW)	2ks
Podpora výrobce CPCES-CO-PREMIUM na všechny výše uvedené položky	12 měsíců