Technická specifikace - zabezpečení koncových bodů

1. Specifikace zabezpečení

Předmětem je řešení zabezpečení operačních systémů na koncových (uživatelských) počítačích a serverech.

Musí jít o moduly jednoho výrobce a tyto moduly musí být integrovány do jednoho celku s jednou, centrální správou přes webové rozhraní. Řešení je přípustné implementovat jako software appliance nebo cloud řešení. Součástí dodávky musí být veškeré potřebné programové vybavení, tj. všechny licence potřebné pro instalaci a provoz.
Podpora a záruka na dodaný software musí být 3 roky pro následující prostředí:
Počet serverů (operačních systémů): **30**
Počet stanic: **240**

2. Požadované funkce

a. Základní požadavky

Požadované vlastnosti a funkce	POPIS
Podporované klientské systémy	Windows 7 a vyšší
Podporované serverové systémy	Windows 2008 R2 a vyšší
Podporované další operační systémy (min. rezidentní antimalware ochrana)	Mac, Linux
Podpora agentů pro operační systémy ve virtuálním prostředí v rozsahu popisu.	VMware vSphere a Microsoft Hyper-V
Integrace s Active Directory	
Aktualizační cache a optimalizace komunikace	Komponenta zajišťující centrální stahování aktualizací a jejich redistribuci v rámci lokální sítě + komunikační proxy pro komunikaci s centrální správou
Instalace nových verzí klientů koncových agentů v rámci aktualizačního procesu (navíc k běžné aktualizaci bezpečnostních signatur).	Nesmí vyžadovat manuální aktualizaci programových komponent.
Agentskou (klientskou) část musí být možné skriptovat (například instalovat v režimu tiché instalace a instalovat novou verzi přímo z lokální cache)	-

Instalace (aktualizace) nových verzí centrální správy v ceně licencí po celou dobu platnosti licence	-
Logování bezpečnostních incidentů	Globální logování ze všech komponent software dostupné z centrální správy. Filtrace dle uživatele, počítače nebo skupin (uživatelů a počítačů)
Nastavení politik na úrovni skupina/uživatel/server	-
API rozhraní pro propojení s nástroji třetích stran	-

b. Běžná antimalware kontrola

Požadované vlastnosti a funkce	POPIS
Rezidentní antimalware ochrana	-
Heuristická analýza	-
Použití online signatur při výskytu podezřelých souborů	-
Skenování souborů před stažením z internetu	Před uložením na disk
Aktualizace bezpečnostních signatur	Min. 4 x denně
Plánované skenování	-
Definice výjimek	Na plánovaný sken i anti-malware ochranu, a to minimálně na soubor, složku, proces, exploit, webovou stránku a C&C komunikaci.

c. Proaktivní ochrana

Požadované vlastnosti a funkce	POPIS
Blokování C&C komunikace a komunikace typu Botnet	Požadováno
HIPS (Host-Based IPS)	Požadováno
Kontrola vyjímatelných zařízení (minimálně USB vyjímatelná zařízení, USB šifrovatelná vyjímatelná zařízení, optická média, infračervené přenosy, bluetooth, disketové jednotky, multimediální zařízení)	Požadováno včetně možnosti samostatného monitorování nebo blokování nepovolených zařízení na základě ID nebo module zařízení i globálně.
Data Loss Prevention	Blokace přenosů dat na základě datového typu nebo obsahu souboru.
Aplikační kontrola	Požadováno včetně možnosti samostatného monitorování výskytu nepovolených aplikací a

	blokace aplikací z pravidelně aktualizovaného seznamu výrobce
Ochrana přístupu na internet minimálně v rozsahu, URL filtrování (30+ kategorií, Data Loss, blokování web-based emailů)	Požadováno
Logování	Globální logování ze všech komponent software dostupné z centrální správy. Filtrace dle uživatele, počítače nebo skupin (uživatelů a počítačů)

d. Ochrana nové generace

Požadované vlastnosti a funkce	POPIS
Anti – Exploit	Požadována ochrana blokování útoků využívajících exploitů v operačním systému nebo aplikacích.
Anti – Exploit alespoň pro základní aplikace (MS Office, Java, Internetové prohlížeče apod.)	Požadováno
Anti – Cryptoransomware	Požadováno blokování i neznámých malware kategorie „Crypto-Ransomware" vč. funkcionality roll-back (vrácení původních, již zašifrovaných souborů po zastavení Crypto-Ransomware)
Ochrana MBR	Například proti ransomware
Ochrana proti zvýšení oprávnění	-
Ochrana proti přepisování kódu v paměti	-
Ochrana proti odcizení přihlašovacích údajů	-
Deep Learning	Včetně analýzy důvodu označení za škodlivý kód
Automatické vyčištění systému na aplikační úrovni	-
Automatická izolace postižených stanic od sítě na úrovni agenta endpoint protection.	-

e. EDR (Endpoit Detection & Response)

Požadované vlastnosti a funkce	POPIS
Zjednodušený náhled na nákazu	Minimálně v rozsahu, vstupní bod malware do systému (aplikace), malware, přijaté opatření
Grafické znázornění průběhu nákazy	Minimálně v rozsahu, vstupní bod malware do systému (aplikace), zápisy do systému a

	souborové úrovni a do registrů OS, komunikace na internet včetně zobrazí IP a URL adres, analýza souborů přes Deep Learning
Možnost globálního vyčištění a blokování nalezeného malware na všech systémech najednou (pomocí jedné akce).	-
Vytvoření „hash" pro soubor na úrovni lokálního agenta a vyhledání infikovaných počítačů na základě tohoto „hash" malware	-
Automatické vyhodnocení incidentů	-
Zobrazení obecných informací o proběhnutých útocích (alespoň z poslední doby)	Minimálně v rozsahu jméno malware, počet postižených systémů a hodnocení nebezpečnosti malware výrobcem.