**Příloha č. 3:** *Specifikace předmětu VZ*

**Specifikace předmětu veřejné zakázky** **„Dodávka antimalware zabezpečení“ vedené pod označením zakázky VZ2020-070-PRO-IT:**

Zadavatel požaduje kompletně vyplněné tabulky Specifikace v rozsahu všech částí A, B, C, D, E a F.

Nabízené řešení musí být plně kompatibilní se stávajícím ICT prostředím Zadavatele a musí splňovat všechny požadavky Zadavatele uvedené v níže uvedené tabulce Technická specifikace.

Součástí dodaného řešení bude také jeho implementace v prostředí Zadavatele a následné poskytování lokální technické podpory nejen od výrobce dodané technologie, ale také vybraného lokálního dodavatele a to na 3 roky s možností automatického prodloužení podpory na další období za stejných cenových podmínek.

Poskytnuté řešení musí být plně kompatibilní se stávajícím ICT prostředím Zadavatele a musí splňovat všechny požadavky Zadavatele uvedené v níže uvedené tabulce Technická specifikace.

ICT Prostředí zadavatele :

* PC a NTB s provozovaným aktualizovaným systémem Microsoft Windows 10
* HW servery osazeny technologií VMware
* Virutální servery provozovány s operačním systémem Microsoft Windows Server 2012-2019
* Moblní zařízení provozováné mají systém iOS (dle možností zařízení aktuální verze) a Android od verze 8.

1. **Obecné požadavky**

|  |  |  |
| --- | --- | --- |
| **Požadavek** | **Splněno**  **(ANO / NE)** | **Poznámka**  **(jakým způsobem řešeno)** |
| Název nabízeného řešení – varianta (business, corporate apod.) včetně verze uvedené varianty a doplňkových modulů |  |  |
| Nabízené antimalware řešení včetně všech požadovaných funkcí pro ochranu stanic, serverů, virtuálního prostředí a BYOD mobilních zařízení je od jednoho výrobce. |  |  |
| Nabízená technologie je v posledním hodnocení „Endpoint Protection Platforms“ (srpen 2019) společnosti Gartner, [www.gartner.com](http://www.gartner.com) zařazena v MagicQuadrantu mezi *Leaders, Visionaries* nebo *Challengers.* |  |  |
| Nabízená technologie je v posledním hodnocení testu AV Comparatives, [www.av-comparatives.org](http://www.av-comparatives.org), kategorie Enterprise / Real-World Protection Test (srpen-září 2020) zařazena mezi 5 technologií s nejlepším hodnocením poměru úspěšnost detekce/false-positives. |  |  |
| Účast minimálně v 8 samostatných testech VB100, [www.virusbulletin.com](http://www.virusbulletin.com) za období 2019-2020 s úspěšností „Passed 100%“ |  |  |
| Plná lokalizace GUI rozhraní aplikace na koncových zařízeních typu PC, notebook nebo BYOD mobilních zařízeních v češtině. |  |  |
| Výrobce antimalware technologie má obchodní a technické zastoupení v ČR. |  |  |
| Bezpečnostní cloud infrastruktura výrobce nabízeného řešení využívaná pro detekci malware mimo prostředí klienta se nachází na území EU nebo některého z přidružených států v Evropě. |  |  |
| Výrobce nabízené technologie disponuje certifikátem ISO/IEC 27001. |  |  |

1. **Ochrana pracovních stanic a serverů**

|  |  |  |
| --- | --- | --- |
| **Požadavek** | **Splněno**  **(ANO / NE)** | **Poznámka**  **(jakým způsobem řešeno)** |
| Podpora pro OS Windows 7 a výše, Windows Server 2008 a výše, Linux (CentOS, Debian, RedHat, Ubuntu, SUSE), Mac 10.9 a výše |  |  |
| Antimalware ochrana před škodlivými kódy (viry, červy, trojské koně, backdoors, spyware, adware, ransomware, keyloggery, crimeware, phishing, rootkit), skripty (PowerShell, WSH, Java, VB, …) vč. Zero Day útoky atd. |  |  |
| Ochrana před exploitací instalovaných aplikací a OS |  |  |
| Detekce malware prostřednictvím technologií virových signatur, heuristiky, behaviorální analýzy a strojového učení (Machine Learning) |  |  |
| Detekce malwaru na bázi reputace a cloudové kontroly (lokální i globální služby výrobce) |  |  |
| Kontrola paměti a detekce Fileless Threats ve Windows. |  |  |
| Antiransomware detekce pokusů o neoprávněné šifrování dat na úrovni Windows, Linux a Windows Servers. |  |  |
| Roll-back nechtěných změn v systému v reakci na detekované aktivity malware (body obnovy). |  |  |
| Možnost přepnutí do cloud režimu ochrany pro snížení lokálního zatížení RAM a HDD prostředků u méně výkonných zařízení v síti |  |  |
| Možnost rozšíření o Endpoint Detection and Response (EDR) a on-premise Sandbox technologii od stejného výrobce jako je dodané řešení |  |  |
| Možnost konfigurovat firewall pravidla ve Windows Server a Linux prostřednictvím centrální konzole nabízeného řešení |  |  |
| Manuální a plánované spouštění skenování, blokování skriptů, kontrola Windows registrů, Buffer overflow ochrana a skenování na pozadí |  |  |
| Self-Defense ochrana heslem před neoprávněnou deaktivací antivirové ochrany včetně blokování neoprávněné vzdálené správy |  |  |
| Kontrola archivů (ZIP, ARJ, CAB, RAR, LHA, JAR, ICE) |  |  |
| Pravidelná automatická aktualizace systému (v závislosti na síťovém prostředí se aktualizace stahují buď z centrálního uložiště, nebo přímo z Internetu). Lokální aktualizační servery (mirrory) si mohou vzájemně replikovat data. Pro externí pracovníky lze nastavit sekundární profil aktualizace z internetu. |  |  |
| Centrálně konfigurovaný personální firewall + Host Intrusion Prevention (HIPS). Pravidla firewallu lze automaticky měnit v závislosti na prostředí |  |  |
| Ochrana elektronické pošty na úrovni protokolů (POP3, IMAP) vč. plug-in pro MS Outlook |  |  |
| Inspekce síťového provozu HTTP(S) a FTP |  |  |
| Blokování uživatelských přístupů na webové stránky s nechtěným nebo škodlivým obsahem na základě URL, webové kategorie, uživatele a času přístupu |  |  |
| Kontrola URL vůči globální cloudové službě výrobce |  |  |
| Uživatelské bezpečnostní politiky zvlášť na zařízení, web a aplikace. |  |  |
| Application Control – možnost povolovat/blokovat spouštění vybraných aplikací dle nastavené firemní politiky (blacklisty/whitelisty) a na základě výrobcem aktualizované reputace spouštěných aplikací |  |  |
| Whitelist aplikací na základě digitálního certifikátu, HASH, metadat, souborového umístění nebo výrobcem předdefinovaných kategorií |  |  |
| Monitorování aplikací využívajících speciální nebo náhodné porty |  |  |
| Možnost omezit práva spouštěných aplikací s ohledem na jejich reputaci |  |  |
| Device Control - možnost blokovat vybraná USB a jiná přídavná zařízení na úrovni sběrnice s možností whitelist zařízení a řízení oprávnění (read/write) |  |  |
| Automatická kategorizace připojovaných USB zařízení dle jejich typu s možností blokace upravených USB zařízení emulujících standardní klávesnici |  |  |
| Automatická kontrola výměnných zařízení a blokace spuštění spustitelných souborů |  |  |
| Kontrola audio a video zařízení pro nahrávání |  |  |
| Blokace několika současných síťových připojení |  |  |
| Automatické skenování stanice po dobu nečinnosti (screensaver, uzamčený počítač apod.) a možnost vynechat již dříve zkontrolované a nezměněné objekty |  |  |
| Umožňuje uložit protokoly o činnostech v běžných formátech (CSV, text, Windows event log) |  |  |
| Rozhraní klientské části antiviru je plně lokalizováno do ČJ |  |  |
| Šifrování celého disku vč. OS, pouze vybraných souborů a složek ve Windows, výměnných paměťových úložišť a správa nativního šifrování ve Windows Bit Locker a v MacOS FileVault. |  |  |
| Data Recovery šifrovaných zařízení v případě havárie včetně centrální správy šifrovacích klíčů |  |  |
| Podpora dvoufaktorové autentizace v preboot režimu u šifrovaných zařízení a to pomocí USB autentizačních tokenů/čipové karty |  |  |
| Patch Management - přehled zranitelností u min. 150+ Microsoft a aplikací třetích stran včetně možnosti automatické instalace příslušných oprav a aktualizací s podporou jejich agregace |  |  |
| Možnost instalace pouze administrátorem schválených aktualizací s možností využít testovací režim na nastavitelném vzorku zařízení |  |  |
| Remote Desktop – možnost správy koncového zařízení prostřednictvím funkce vzdálené plochy s podporou logování provedených akcí |  |  |
| Vytváření bitových záloh koncových zařízení a jejich deployment |  |  |
| Inventarizace HW komponent a SW instalovaného na koncových bodech včetně sledování platnosti licencí |  |  |

1. **Ochrana a správa mobilních zařízení typu SmartPhone/tablet**

|  |  |  |
| --- | --- | --- |
| **Požadavek** | **Splněno**  **(ANO / NE)** | **Poznámka**  **(jakým způsobem řešeno)** |
| Podpora pro OS Android a iOS |  |  |
| Antimalware ochrana Android zařízení na úrovni souborů a síťové komunikace (virové signatury, heuristika, cloud reputace, strojové učení) |  |  |
| Detekce root/jailbreak zařízení |  |  |
| SMS/MMS AntiSpam a filtr nevyžádaných hovorů |  |  |
| Anti-Theft funkce (vzdálené uzamčení, smazání, SIM kontrola, foto a GPS lokace) |  |  |
| Zabezpečení on-line komunikace (firewall) |  |  |
| Zašifrování obsahu mobilního zařízení |  |  |
| Správa přístupu uživatelů na web umožňující blokovat škodlivé nebo nevhodné webové stránky také na základě jejich kategorií |  |  |
| Ochrana uživatelů před phishingovými weby, které hrozí krádeží informací a identifikačních údajů |  |  |
| Konfigurace správy aplikací umožňující určit, které aplikace bude možné spouštět |  |  |
| Správa zařízení - povolení/blokování použití paměťových karet, kamery, WiFi, Bluetooth, IR, … |  |  |
| Uživatelský Self-Service portal pro správu zařízení |  |  |
| Příprava zařízení, centrální nastavení politik a push instalace/odinstalace vybraných aplikací |  |  |

1. **Optimalizovaná ochrana pro virtuální prostředí**

|  |  |  |  |
| --- | --- | --- | --- |
| **Požadavek** | **Splněno**  **(ANO / NE)** | **Poznámka**  **(jakým způsobem řešeno)** | |
| Agentless antimalware zabezpečení pro VMware |  |  | |
| Antimalware Light Agent zabezpečení pro VMware, Hyper-V, Citrix |  |  | |
| Podpora AWS a MS Azure veřejného/privátního cloudu |  |  | |
| Antimalware kontrola za využití virových signatur, heuristiky, strojového učení a behaviorální analýzy |  |  | |
| Zabezpečení pomocí napojení na cloud reputační službu výrobce a ochrana před exploitací instalovaných aplikací |  |  | |
| Kontrola poštovní (IMAP, SMTP, POP3) a síťové komunikace (HTTP a FTP) |  |  | |
| Kontrola integrity systémových souborů, logů a kritických aplikací |  |  | |
| Přenesení skenovacích úloh a tím i zatížení na samostatnou virtuální appliance a eliminace opakovaného skenování nezměněných objektů |  |  | |
| Application Control – možnost omezit oprávnění běžících aplikací na základě jejich reputace |  |  | |
| Roll-back nechtěných změn v systému v reakci na detekované aktivity malware (body obnovy). |  | |  |
| Vestavěný firewall a Host Intrusion Prevention (HIPS) |  |  | |
| Device Control – správa připojování výměnných zařízení |  |  | |

1. **Centrální správa**

|  |  |  |
| --- | --- | --- |
| **Požadavek** | **Splněno**  **(ANO / NE)** | **Poznámka**  **(jakým způsobem řešeno)** |
| Konzole centrální správy v provedení tlustého klienta (lokálně instalované aplikace) s možností webové konzole |  |  |
| Podpora Windows Server 2008 a výše, MS SQL Server 2008 (Express) a výše, MySQL 5.5 a výše |  |  |
| Vzdálená centrální správa všech komponent antimalware řešení včetně šifrování, Patch Management, BYOD … |  |  |
| Možnost vzdálené instalace, odinstalace a konfigurace všech komponent na PC, serverech včetně mobilních zařízení typu SmartPhone a tablet |  |  |
| Deployment klientů na koncová zařízení pomocí RPC, GPO, síťový agent popř. standalone instalačního balíčku |  |  |
| Instalace endpoint aplikace na serverech bez nutnosti restartu |  |  |
| Zabezpečené spojení mezi serverem centrální správy a endpoint agenty |  |  |
| Podpora manuální/automatické instalace/odinstalace nekompatibilních aplikací (vč. současné ochrany Kaspersky) |  |  |
| Podpora Active Directory a IPv6 |  |  |
| Tvorba politik s jednotlivým nastavením komponent řešení a jejich aplikace na úrovni skupin. |  |  |
| Přidělování práv administrátorů na úrovni skupin nebo serverů s předdefinovanými security právy pro role auditor, supervisor a security officer. |  |  |
| Centrální správa a nastavení jednotlivých klientů na úrovni skupin nebo hierarchie |  |  |
| Správa zařízení na základě dynamických profilů a tagů (síť, OS, AD, virtualizace, aplikace). |  |  |
| Možnost stahování aktualizací z centrálního serveru nebo Internetu na základě kvality sítě |  |  |
| Možnost distribuovat události z vybrané skupiny PC prostřednictvím vybraného počítače v síti. |  |  |
| Podpora virtuálního prostředí (VMware, Hyper-V, Citrix) |  |  |
| Možnost prohlížení všech bezpečnostních událostí na spravovaných zařízení v síti. |  |  |
| Notifikace pomocí e-mail, syslog, SMS, SIEM. |  |  |
| Možnost generovat a odesílat reporty e-mailem ve formátu .PDF nebo .XML včetně možnosti jejich přizpůsobení. |  |  |

1. **Služby lokální technické podpory**

|  |  |  |
| --- | --- | --- |
| **Požadavek** | **Splněno**  **(ANO / NE)** | **Poznámka**  **(jakým způsobem řešeno)** |
| Instalace a základní konfigurace SW v prostředí Zadavatele |  |  |
| Úvodní zaškolení obsluhy na správu a používání dodaného systému |  |  |
| Lokální technická podpora dodavatele nabízeného řešení v ČJ v rozsahu HOT LINE (e-mail/telefon) v pracovních dnech od 8:00 hod. – 16:00 hod. |  |  |