# Město Kroměříž

Název projektu: Kroměříž - zlepšení kybernetické bezpečnosti infrastruktury

Registrační číslo projektu: CZ.31.2.0/0.0/0.0/23\_093/0008490

# Obecné požadavky

Část 2:

* Pořízení a implementace Endpoint protection řešení dvoufaktorové ověření uživatelů (2FA) a management mobilních zařízení (MDM

**Důležité upozornění:**

Dodavatel, který se stane vybraným dodavatelem této veřejné zakázky, je vyloučen z možnosti ucházet se o plnění audit kybernetické bezpečnosti.

|  |
| --- |
| **Požadavek** |
| Pokud je k provozu níže uvedených informačních systémů nutné další zařízení, licence nebo prvek podle povahy zvoleného technického řešení s výjimkou nově nakupovaných nebo stávajících, uchazeč ho výslovně uvede a zahrne do ceny svého plnění včetně nutných upgrade a update po dobu udržitelnosti. |
| Dodavatel vždy dodrží uvedené požadavky na instalaci a konfiguraci. |
| Dodavatel zajistí instalaci a konfiguraci dodaných HW a SW komponent v návaznosti na stávající infrastrukturu organizace, a to včetně instalace a implementace do stávající IT infrastruktury v sídle zadavatele |
| V případě dodání více kusů zboží u téhož zboží budou dodány identické kusy. Např. server 3x znamená, že zadavatel požaduje 3x identický server. |
| Dodávané zboží bude, tam kde to je možné, od jednoho výrobce z důvodu zajištění maximální kompatibility a jednotného servisního místa a managementu. |
| **Požadavky na certifikaci dodavatele HW a původ zboží** |
| U zařízení, u kterých je výslovně uveden požadavek na certifikaci, musí být Dodavatelem doložena certifikace nebo čestné prohlášení a garance výrobce nabízeného HW, že nabízené zboží je určené pro český trh, je nové, nepoužité a pochází z oficiálního distribučního kanálu v ČR. Dodavatel dodrží uvedené požadavky na certifikaci dodavatele (subdodavatele) HW a původ zboží. |

# Část 2 Pořízení a implementace Endpoint protection řešení, dvoufaktorového ověření uživatelů (2FA) a managementu mobilních zařízení (MDM), dále jen „Nástroj“

***Zadavatel v současné době používá ESET PROTECT Complete, na obsluhu tohoto programu je zaškolen. Nástroj je nasazen na všech koncových stanicích a serverech.***

Implementace

Součástí dodávky je:

1. Poskytnutí veškerých potřebných licencí – zahrnuje všechny potřebné softwarové a provozní licence pro správný chod nástroje, včetně licencí pro všechny moduly a funkce, které budou součástí implementace.
2. Předimplementační analýza a návrh řešení.
3. Instalace nástroje a zprovoznění přístupu na cloud – zahrnuje kompletní instalaci Nástroje, konfiguraci cloudového prostředí, nastavení přístupu pro administrátory.
4. Zprovoznění, nastavení a optimalizace provozu Nástroje – provedení všech potřebných nastavení pro plně funkční provoz Nástroje, včetně optimalizace výkonu, konfigurace parametrů a zajištění správného chodu všech procesů, aby bylo dosaženo maximální efektivity serverů a klientských stanic.
5. Migrace konfigurace současného řešení včetně politik či instalačních balíčků programů pro PC.
6. Předání instalační a provozní dokumentace – dodání podrobné dokumentace v českém jazyce, která obsahuje kompletní výčet všech potřebných úkonů pro správnou instalaci, konfiguraci a údržbu Nástroje. Dokumentace také zahrnuje návody pro administrátory.
7. Proškolení obsluhy – realizace školení pro administrátory Nástroje, které zahrnuje jak základní, tak pokročilé funkce Nástroje. Školení bude zaměřeno na efektivní využívání Nástroje a jeho správu.

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Minimální požadavek** | **Dodavatel uvede, jestli splňuje požadavky (ano/ne) a navíc popíše jakým způsobem** |
| Výrobce, název, verze a licenční program |  |  |
| Licence | Nevýhradní licence v délce trvání minimálně 5 let |  |
| Ochrana před škodlivým SW | * Nástroj bude obsahovat podporované klientské platformy - OS: Windows, Linux, MacOS, Android, vše v českém jazyce. * Nástroj bude obsahovat antimalware, antiransomware, antispyware a anti-phishing pro aktivní ochranu před všemi typy hrozeb. * Nástroj bude obsahovat personální firewall pro zabránění neautorizovanému přístupu k zařízení se schopností automatického přebrání pravidel z brány Windows Firewall. * Nástroj bude obsahovat modul pro ochranu operačního systému a eliminaci aktivit ohrožujících bezpečnost zařízení s možností definovat pravidla pro systémové registry, procesy, aplikace a soubory. * Nástroj bude obsahovat ochranu před neautorizovanou změnou nastavení a vyřazením z provozu / odinstalací antimalware řešení a kritických nastavení a souborů operačního systému. * Nástroj bude obsahovat aktivní i pasivní heuristickou analýzu pro detekci dosud neznámých hrozeb. * Nástroj bude obsahovat blokaci exploitů zneužívajících zero-day zranitelnosti, jenž pokrývá nejpoužívanější vektory útoku: o síťové protokoly, o Flash Player, o Javu, o Microsoft Office, o webové prohlížeče, o e-mailové klienty, o PDF čtečky. * Nástroj bude obsahovat detekci malwaru již na síťové úrovni poskytující ochranu i před zneužitím zranitelností na síťové vrstvě. * Nástroj bude obsahovat kontrolu šifrovaných spojení (SSL, TLS, HTTPS, IMAPS…). * Nástroj bude obsahovat anti-phishing se schopností detekce homoglyph útoků. * Nástroj bude obsahovat kontrolu RAM paměti pro lepší detekci malwaru využívajícího silnou obfuskaci a šifrování. * Nástroj bude obsahovat cloud kontrolu souborů pro urychlení skenování fungující na základě reputace souborů. * Nástroj bude obsahovat kontrolu souborů v průběhu stahování pro snížení celkového času kontroly. * Nástroj bude obsahovat kontrolu souborů při zapisování na disku a extrahování archivačních souborů. * Nástroj bude obsahovat detekci s využitím strojového učení. * Nástroj bude obsahovat funkci ochrany proti zapojení do botnetu pracující s detekcí síťových signatur. * Nástroj bude obsahovat ochranu před síťovými útoky skenující síťovou komunikaci a blokující pokusy o zneužití zranitelností na síťové úrovni. * Nástroj bude obsahovat kontrolu s podporou cloudu pro odesílání a online vyhodnocování neznámých a potenciálně škodlivých aplikací. * Nástroj bude obsahovat lokální sandbox. * Nástroj bude umožňovat rollback souborů zasažených ransomwarem s možností reportovat do konzole obnovené soubory zasažené ransomwarem, nevyužívá se shadow copy a pro svou správnou funkci nevyžaduje dodatečnou konfiguraci. * Nástroj bude obsahovat modul behaviorální analýzy pro detekci chování nových typů ransomwaru. * Nástroj bude obsahovat systém reputace pro získání informací o závadnosti souborů a URL adres. * Nástroj bude obsahovat cloudový systém pro detekci nového malwaru ještě nezaneseného v aktualizacích signatur. * Nástroj bude obsahovat technologii pro detekci rootkitů obvykle se maskujících za součásti operačního systému. * Nástroj bude obsahovat skener firmwaru BIOSu a UEFI. * Nástroj bude obsahovat skenování souborů v cloudu OneDrive. * Nástroj bude obsahovat funkcionalitu pro klienty MS Windows – Antimalware, Antispyware, Personal Firewall, Personal IPS, Application Control, Device Control, Security Memory (zabraňuje útokům na běžící aplikace), kontrolu integrity systémových komponent. * Nástroj bude obsahovat funkcionalitu pro klienty MacOS – Antimalware, Personal Firewall, Device Control, autoupgrade. * Nástroj bude obsahovat funkcionalitu pro klienty Linux – Antimalware, ICAPs scan, Botnet Protection. * Nástroj bude umožňovat aplikování bezpečnostních politik i v offline režimu na základě podmínek. * Nástroj bude obsahovat ochranu proti pokročilým hrozbám (APT) a 0-day zranitelnostem. * Nástroj bude podporovat automatické vytváření dump souborů na stanici na základě nálezů. * Nástroj bude umožňovat okamžité blokování/mazání napadených souborů na stanici (s možností stažení administrátorem k další analýze). * Nástroj bude obsahovat duální aktualizační profil pro možnost stahování aktualizací z mirroru v lokální síti a zároveň vzdálených serverů při nedostupnosti lokálního mirroru (pro cestující uživatele s notebooky). * Nástroj bude umožňovat definovat webové stránky, které se spustí v chráněném režimu prohlížeče, pro bezpečnou práci s kritickými systémy nebo internetovým bankovnictvím. * Nástroj bude obsahovat ochranu před útokem hrubou silou na protokol SMB a RDP. * Nástroj bude umožňovat zablokování konkrétní IP adresy po sérii neúspěšných pokusů o přihlášení pro protokoly SMB a RDP s možností výjimek ve vnitřních sítích. |  |
| SW pro sandboxing | * Nástroj bude obsahovat funkci cloudového sandboxu integrovanou do produktu pro koncové a serverové zařízení * Nástroj bude umožňovat spuštění vzorků malwaru pro: Windows, Linux, MacOS. * Nástroj bude umožňovat využití na koncových bodech a serverech pro aktivní detekci škodlivých souborů. * Nástroj bude obsahovat analýzu neznámých vzorků v řádu jednotek minut. * Nástroj bude obsahovat optimalizaci pro znemožnění obejití anti-sandbox mechanismy. * Nástroj bude umožňovat analýzu rootkitů a ransomwaru. * Nástroj bude obsahovat schopnost detekce a zastavení zneužití nebo pokusu o zneužití zero day zranitelnosti. * Nástroj bude řešit behaviorální analýzu. * Nástroj bude umožňovat reportování o analyzovaném souboru včetně exportu do PDF s informacemi o nalezeném škodlivém chování daného souboru formou webového reportu. * Nástroj bude umožňovat manuální odeslání vzorku do sandboxu. * Nástroj bude obsahovat blokování hrozby dokud není znám výsledek analýzy ze sandboxu. * Nástroj bude umožňovat neomezené množství odesílaných souborů. * Nástroj bude obsahovat veškerou komunikaci probíhající šifrovaným kanálem. * Nástroj bude obsahovat okamžité odstranění souboru po dokončení analýzy v cloudovém sandboxu. * Nástroj bude umožňovat volbu, jaké kategorie souborů do cloudového sandboxu budou odcházet (spustitelné soubory, archivy, skripty, pravděpodobný spam, dokumenty atp.). |  |
| SW pro odhalení škodlivé, či podezřelé aktivity včetně analýzy | * Nástroj bude umožňovat výběr mezi provozem EDR serveru v on-premise prostředí nebo cloud prostředí výrobce. * Nástroj bude umožňovat provoz on-premise s databázemi: MS SQL, MySQL. * Nástroj bude podporovat offline prostředí, technologie EDR vyhodnocuje a reaguje na události lokálně, nevyžaduje pro svou činnost připojení k internetu. * Nástroj bude obsahovat EDR řešení zajišťující stejnou ochranu i bez připojení k internetu. Pracuje autonomně a připojení k internetu neovlivní kvalitu detekční technologie na koncovém bodu. * Nástroj bude umožňovat logování činností administrátora. * Nástroj bude obsahovat EDR agenta pro prostředí Windows, Windows server, MacOS a linuxové distribuce. * Nástroj bude obsahovat autentizaci do management konzole EDR pomocí 2FA. * Nástroj bude umožňovat nutnost aktivace 2FA pro používání pokročilých nástrojů typu terminal. * Nástroj bude umožňovat řízení managementu EDR prostřednictvím API, a to jak pro: přijímání informací z EDR serveru, zasílání příkazů na EDR serveru. * Nástroj bude podporovat vzdálené pouštění příkazů přímo z EDR konzole na platformě Windows s nejvyšším oprávněním SYSTEM. * Nástroj bude umožňovat logování vzdáleného spouštění příkazů z konzole v EDR systému. * Nástroj bude umožňovat izolaci zařízení od sítě prostřednictvím EDR agenta přímo z konzole. * Nástroj bude umožňovat tvorbu vlastních indikátorů zneužití. * Nástroj bude umožňovat škálování množství historických dat vyhodnocených v EDR minimálně 2 měsíce pro low-level-data, minimálně 1,5 roku pro detekované incidenty při provozu v on-premise prostředí. * Nástroj bude obsahovat možnost aktivace „učícího režimu“ pro automatizované vytváření výjimek k detekčním pravidlům. * Nástroj bude obsahovat indikátory útoku pracující s behaviorální detekcí. * Nástroj bude obsahovat indikátory útoku pracující s reputací. * Nástroj bude umožňovat analýzu vektorů útoku. * Nástroj bude obsahovat schopnost detekce: škodlivých spustitelných souborů, skriptů, exploitů, rootkitů, síťových útoků, zneužití WMI nástrojů, bezsouborového malwaru. * Nástroj bude obsahovat schopnost detekce pokusů o dumpování přihlašovacích údajů uživatele. * Nástroj bude obsahovat schopnost detekovat laterální pohyb útočníka. * Nástroj bude obsahovat schopnost ukončit infikovaný proces. * Nástroj bude umožňovat ruční analýzu procesů veškerých spustitelných souborů a DLL knihoven. * Nástroj bude umožňovat náhled na spuštěné skripty použité v daném incidentu. * Nástroj bude umožňovat zabezpečené vzdálené spojení přes servery výrobce do on-premise konzole EDR. * Nástroj bude umožňovat vytváření automatizovaného response úkonu v podobě izolace stanice, blokace konkrétního hashe, odhlášení uživatele, restartování počítače pro jednotlivé scénáře nebo detekce. * Nástroj bude umožňovat automatické vyřešení incidentu definovaného administrátorem. * Nástroj bude obsahovat schopnost prioritizace vzniklých incidentů. * Nástroj bude umožňovat stažení podezřelého souboru ze stanice přes konzoli EDR. * Nástroj bude obsahovat schopnost zobrazení detekcí provedených antimalware produktem. * Nástroj bude umožňovat generování tzv. forest / full execution tree modelu. * Nástroj bude umožňovat vyhledávání pomocí nově vytvořených indikátorů zneužitelnosti nad historickými daty. * Nástroj bude obsahovat provázání s technikami popsanými v knowledge base MITRE ATT&CK. * Nástroj bude podporovat offline režim minimálně s možností detekce pravidel a setů detekčních pravidel. * Nástroj bude obsahovat průběžně aktualizovaná detekční pravidla EDR systému bez nutnosti aktualizace centrální správy/klienta. * Nástroj bude umožnovat EDR založit definice vlastních incidentů i s časovým pořadím detekce událostí * Nástroj bude obsahovat pokročilé detekční mechanismy pro detekci útoku i při nedostupnosti cloudového/centrálního serveru výrobce * Nástroj bude umožňovat export raw dat (veškerých dat) na externí úložiště, např. lokální disk, Azure Blob * Nástroj bude podporovat SHA256 algoritmus * Nástroj bude umožňovat filtrování určitého typu dat zpracovávaného z klientem * platnost licence min. 60 měsíců, včetně nároku na opravné a nové verze software, vč. technické podpory výrobce. |  |
| Správa a funkce konzole pro administraci | * Nástroj bude obsahovat konzoli dostupnou v internetovém prohlížeči. * Nástroj bude umožňovat instalaci v on-premise prostředí na Windows nebo Linux. * Nástroj bude umožňovat provoz konzole v cloudu výrobce. * Nástroj bude umožňovat instalaci formou virtual appliance pro virtuální prostředí VMware, Microsoft Hyper-V a Microsoft Azure, Oracle Virtual Box připravenou výrobcem. * Nástroj bude obsahovat server/proxy architekturu pro síťovou pružnost – snížení zátěže při stahování aktualizací detekčních modulů výrobce. * Nástroj bude umožňovat probuzení klientů pomocí Wake On Lan. * Nástroj bude obsahovat offline agent vzdálené správy pro zajištění komunikace a ovládání operačního systému klienta. * Nástroj bude umožňovat aktivaci politik a spouštění úloh při výskytu definované události i bez přístupu k internetu (například: odpojení od sítě při nalezení škodlivého kódu). * Nástroj bude obsahovat administraci v nejpoužívanějších jazycích včetně češtiny. * Nástroj bude umožňovat široké možnosti konfigurace oprávnění administrátorů (například možnost správy pouze části infrastruktury, které konkrétnímu administrátorovi podléhá). * Nástroj bude obsahovat zabezpečení přístupu administrátorů do vzdálené správy pomocí 2FA. * Nástroj bude obsahovat informace o aktuálně přihlášených uživatelích na daném zařízení. * Nástroj bude podporovat štítky/tagování pro snazší správu a vyhledávání. * Nástroj bude obsahovat správu karantény s možností vzdáleného vymazání / obnovení / obnovení a vyloučení objektu z detekce. * Nástroj bude umožňovat vzdálené získání zachyceného škodlivého souboru z klienta. * Nástroj bude obsahovat detekci nespravovaných (rizikových) počítačů komunikujících na síti. * Nástroj bude umožňovat instalaci a odinstalaci aplikací 3. stran. * Nástroj bude umožňovat vyčítání informací o verzích softwaru 3. stran. * Nástroj bude umožňovat vyčítání informací o hardwaru na spravovaných zařízeních (CPU, RAM, diskové jednotky, grafické karty…). * Nástroj bude umožňovat odeslání zprávy na počítač / mobilní zařízení, které se následně zobrazí uživateli na obrazovce. * Nástroj bude umožňovat vzdálené spuštění jakéhokoli příkazu na cílové stanici pomocí Příkazového řádku. * Nástroj bude obsahovat dynamické skupiny pro možnost definování podmínek, za kterých dojde k automatickému zařazení klienta do požadované skupiny a automatickému uplatnění klientské úlohy. * Nástroj bude podporovat klientské úlohy pro dynamické skupiny. * Nástroj bude umožňovat automatické zasílání upozornění při dosažení definovaného počtu nebo procent ovlivněných klientů (například: 5 % všech počítačů / 50 klientů hlásí problémy). * Nástroj bude podporovat SNMP Trap, Syslog, Rest API. * Nástroj bude podporovat instalaci agenta skriptem - \*.bat, \*.sh, \*.ini (GPO, SSCM…). * Nástroj bude umožňovat rychlé připojení na klienta pomocí RDP z konzole pro vzdálenou správu. * Nástroj bude obsahovat reportování stavu klientů chráněných jinými bezpečnostními programy. * Nástroj bude umožňovat zasílání reportů a upozornění na e-mail. * Nástroj bude umožňovat odesílání notifikací o vybraných událostech prostřednictvím tzv. Webhooků. * Nástroj bude umožňovat integraci s řešeními třetích stran podporujícími MDM (např. MS Intune, Workspace One). * Nástroj bude umožňovat řízení managementu konzole a jeho komponent prostřednictvím API, a to jak pro: Centrální správu samotnou, Komponenty antimalware řešení, jeho správy, politik a nastavení, EDR řešení, Export informací o detekcích, incidentech, Úpravu detekčních pravidel EDR. * Nástroj bude umožňovat správu zařízení a jeho nastavení, instalačních balíčků, včetně možnosti automatizace jednotlivých úkonů. * Nástroj bude umožňovat přidání zařízení do vzdálené správy pomocí: Synchronizace s Active Directory (jedné nebo více Active Directory), včetně možnosti synchronizace počítačů a uživatelů, Ručního přidání pomocí IP adresy nebo názvu zařízení, Síťového skenu nechráněných zařízení v síti. |  |
| Chráněné služby | * Nástroj bude umožňovat přihlášení do webových aplikací společnosti Microsoft (OWA, SharePoint…). * Nástroj bude umožňovat přihlášení přes RDP. * Nástroj bude umožňovat přístup k Exchange Control Panel & Exchange Administrator Center. * Nástroj bude umožňovat integraci s VMware Horizon View. * Nástroj bude umožňovat integraci s Citrix XenApp. * Nástroj bude umožňovat autentizaci pro VPN služby využívající protokol RADIUS (Cisco, Citrix, Fortinet, Juniper, Microsoft, OpenVPN…). * Nástroj bude umožňovat připojení ke cloudovým službám Office 365, G Suite a identity providerům (podpora SAML protokolu, podpora AD FS). * Nástroj bude umožňovat lokální přihlášení do Windows, Linux, macOS účtů. * Nástroj bude umožňovat vyžádání 2FA v nouzovém režimu Windows. * Nástroj bude umožňovat vyžádání 2FA při vyvolání UAC dialogu ve Windows. * Nástroj bude umožňovat vyžádání 2FA při uzamčeném účtu. |  |
| Požadavky na správu | * Nástroj bude obsahovat webové konzole provozované v cloudu výrobce s možností nasazení v on-premise prostředí. * Nástroj bude umožňovat přístup do konzole chráněný 2FA ověřením. * Nástroj bude umožňovat multitenantní provoz (možnost spravovat vícero uživatelských struktur v jedné konzoli). * Nástroj bude umožňovat synchronizaci uživatelských účtů z Active Directory. * Nástroj bude umožňovat tvorbu výjimek pro vnitřní sítě, kde není 2FA vyžadováno. * Nástroj bude umožňovat uživatelům přihlášení bez použití 2FA pro vybrané služby. * Nástroj bude umožňovat dočasné pozastavení požadavku na 2FA pro uživatele. * Nástroj bude umožňovat nastavení limitu pro počet neúspěšných zadání OTP. * Nástroj bude umožňovat centrální správu a přidělování hardwarových tokenů jednotlivým uživatelům. * Nástroj bude umožňovat reportování o úspěšných/neúspěšných přihlášeních uživatelů a způsobu použité autentizace (SMS, Push, OTP). |  |
| Ochrana poštovních serverů | * Nástroj bude obsahovat víceúrovňovou ochranu celého serveru – databáze schránek, transport zpráv i souborový systém serveru. * Nástroj bude podporovat MS Exchange 2019 a novější. * Nástroj bude obsahovat antivirus, antispyware a antispoofing technologie. * Nástroj bude obsahovat antispam s funkcí graylisting. * Nástroj bude umožňovat blokování nevyžádané pošty a phishingu bez potřeby manuální úpravy hodnot SCL (Spam Confidence Level). * Nástroj bude umožňovat vytváření pokročilých antispamových pravidel s možností vyhodnocení více podmínek v jednom pravidlu. * Nástroj bude umožňovat kontrolu jednotlivých MBX databází nebo konkrétních uživatelských schránek. * Nástroj bude umožňovat uživatelům poštovních schránek pracovat v samostatném prohlížeči se spamovými a potenciálně infikovanými zprávami, které nebyly doručeny do jejich e-mailové schránky. * Nástroj bude umožňovat tvorbu vlastních pravidel s vlastním hodnocením obsahu. * Nástroj bude podporovat více-serverové prostředí a zajišťovat P2P komunikaci. * Nástroj bude umožňovat detekci škodlivých souborů v reálném čase. * Nástroj bude podporovat správu přes příkazovou řádku (podpora edice Windows Server Core). * Nástroj bude obsahovat komplexní protokoly blokovaného spamu a zobrazovat greylistingované odesílatele. * Nástroj bude umožňovat sledování výkonu serveru v reálném čase. * Nástroj bude umožňovat nastavení pravidel inspekce souborů, například mazání spustitelných souborů a skriptů. * Nástroj bude obsahovat cloudovou reputační službu pro kontrolu příloh e-mailových zpráv. * Nástroj bude umožňovat správu ochrany na Exchange Serveru samostatně nebo prostřednictvím management konzole v cloudu. * Nástroj bude umožňovat export protokolů událostí produktu do protokolu operačního systému. * Nástroj bude podporovat tvorbu pravidel "Z hlavičky" pro přesnější detekci podvržených e-mailů na základě vyhodnocení pole From:. * Nástroj bude obsahovat backscatter ochranu. * Nástroj bude umožňovat synchronizaci lokální karantény zpráv napříč uzly clusteru. * Nástroj bude podporovat hybridní prostředí s možností kontroly poštovních schránek v Office 365. * Nástroj bude umožňovat zasílání přehledů o zachycených e-mailových hrozbách koncovým uživatelům. * Nástroj bude umožňovat zabezpečení poštovního serveru a jeho komponent heslem proti neautorizovaným úpravám. * Nástroj bude umožňovat dočasnou deaktivaci heslového zabezpečení pro vybrané uživatele na základě ověření administrátora vůči doméně. * Nástroj bude podporovat správu karantény prostřednictvím webového portálu pro vybrané uživatele i administrátory. * Nástroj bude umožňovat ochranu nastavení dodatečným heslem před neoprávněnou změnou konfigurace produktu. * Nástroj bude umožňovat editaci zpráv o stavu karantény a zachycených souborů (úprava těla e-mailu, předmětu a odkazu na blokovaný e-mail). * Nástroj bude obsahovat integrovanou funkci cloudového sandboxu pro e-mailovou ochranu MS Exchange, která nevyžaduje instalaci dalších komponent. * Nástroj bude řešit zpracování dat odesílaných v rámci cloudového sandboxu v rámci EU. * Nástroj bude umožňovat sandboxovou analýzu vzorků malwaru pro Windows, macOS a Linux. * Nástroj bude umožňovat využití sandboxu na koncových bodech a Exchange serveru pro aktivní detekci škodlivých souborů v e-mailech. * Nástroj bude podporovat analýzu neznámých vzorků v řádu jednotek minut. * Nástroj bude optimalizován pro znemožnění obejití anti-sandbox mechanismů. * Nástroj bude umožňovat analýzu rootkitů a ransomwaru. * Nástroj bude podporovat detekci a zastavení zneužití nebo pokusů o zneužití zero-day zranitelností. * Nástroj bude využívat behaviorální analýzu. * Nástroj bude poskytovat kompletní výsledky analýzy souboru v centrálním managementu včetně informací o nalezeném i nenalezeném škodlivém chování. * Nástroj bude umožňovat manuální odesílání vzorků do sandboxu. * Nástroj bude podporovat proaktivní ochranu, kdy je potenciální hrozba blokována do doby dokončení analýzy v sandboxu. * Nástroj bude umožňovat neomezené množství odesílaných souborů. * Nástroj bude zabezpečovat veškerou komunikaci šifrovaným kanálem. * Nástroj bude umožňovat okamžité odstranění souborů po dokončení analýzy z cloudového sandboxu. * Nástroj bude umožňovat výběr kategorií souborů odesílaných do cloudového sandboxu (spustitelné soubory, archivy, skripty, pravděpodobný spam, dokumenty atd.). * Nástroj bude podporovat odesílání souborů do cloudového sandboxu o velikosti až 64 MB. |  |
| Ochrana cloud Microsoft 365 | * Nástroj bude poskytovat komplexní ochranu pro prostředí Microsoft 365, včetně Exchange Online, OneDrive, SharePoint Online a Microsoft Teams. * Nástroj bude umožňovat nezávislou cloudovou správu pro vyhodnocení zachycených hrozeb. * Nástroj bude obsahovat neinvazivní technologii, která při nedostupnosti neovlivní fungování Microsoft 365. * Nástroj bude zahrnovat funkce Antimalware, Antispam a Antiphishing. * Nástroj bude umožňovat detekci útoků využívajících homoglyf techniku. * Nástroj bude umožňovat zasílání pravidelných reportů. * Nástroj bude podporovat vícenásobnou kontrolu podezřelých e-mailů. * Nástroj bude umožňovat export událostí, detekcí a audit logů přes Syslog. * Nástroj bude umožňovat ochranu celého tenantu nebo jednotlivých uživatelů. * Nástroj bude umožňovat automatickou aplikaci ochrany pro nově vzniklé uživatele v Microsoft 365 nebo Google Workspace. * Nástroj bude obsahovat integrovanou funkci analýzy neznámých vzorků v prostředí cloudového sandboxu. |  |
| Detekci a správu zranitelností (VAPM) | * Nástroj bude obsahovat integrovanou součást agenta poskytovatele bezpečnostní platformy bez nutnosti instalace dalších komponent. * Nástroj bude podporovat operační systémy Windows, Linux a macOS. * Nástroj bude umožňovat správu všech detekovaných zranitelností a jejich dostupných záplat přes centrální správu výrobce bezpečnostního řešení. * Nástroj bude obsahovat informace o zranitelnostech ve standardizovaném formátu CVE, včetně data zařazení, popisu povahy zranitelnosti a odkazu na zdroj s podrobnostmi. * Nástroj bude přidělovat každé zranitelnosti "bezpečnostní skóre" dle databáze CVSS 3.0 či novější. * Nástroj bude integrovaný v centrálním managementu bezpečnostního nástroje výrobce. * Nástroj bude umožňovat skenování zranitelností na vyžádání. * Nástroj bude umožňovat ruční spuštění záplaty podporované aplikace. * Nástroj bude umožňovat automatické spuštění záplaty podporované aplikace podle časových kritérií s možností výběru aplikací pomocí blacklist/whitelist logiky. * Nástroj bude umožňovat automatizované spuštění záplaty vybrané aplikace podle definovaných podmínek, například dle skóringu zranitelnosti, konkrétních CVE nebo verzí aplikací. * Nástroj bude umožňovat automatické záplatování Windows OS s možností definice typů aktualizací, včetně kritických a důležitých updatů. * Nástroj bude umožňovat definovat minimální prostor na disku potřebný pro stažení a aplikaci záplat. * Nástroj bude umožňovat vynucení instalace záplaty po uplynutí stanovené lhůty. * Nástroj bude řešit notifikaci uživatele v případě potřeby restartu aplikace, přičemž aplikace nebude bez vyzvání restartována. * Nástroj bude řešit možnost odložení restartu zařízení v případě potřeby jeho restartování po instalaci záplaty. |  |
| Správa mobilních zařízení | * Nástroj bude obsahovat podporu operačních systémů Android, iOS a iPadOS. * Nástroj bude umožňovat centrální správu zařízení pomocí management konzole výrobce bezpečnostního řešení. * Nástroj bude umožňovat registraci zařízení v režimu vlastníka nebo prostřednictvím Apple Business Manager (ABM). * Nástroj bude umožňovat integraci s managementem zařízení Microsoft Intune. * Nástroj bude řešit správu účtů (email, LDAP, Exchange…). * Nástroj bude umožňovat konfiguraci restrikcí na spravovaných zařízeních. * Nástroj bude umožňovat vynucení složitosti zámku obrazovky zařízení. * Nástroj bude umožňovat definici informací na zamčené obrazovce (např. kontaktní údaje společnosti). * Nástroj bude obsahovat ochranu před výměnou SIM karty s možností definice důvěryhodné SIM. * Nástroj bude obsahovat detekci roamingu. * Nástroj bude umožňovat lokalizaci zařízení. * Nástroj bude obsahovat podporu anti-theft akcí (siréna, zámek telefonu, vzdálené smazání dat). * Nástroj bude umožňovat filtrování hovorů a SMS s definicí časových slotů pro uplatnění pravidel. * Nástroj bude umožňovat WebControl s možností filtrování obsahu webu. * Nástroj bude umožňovat Application Control s možností vynucení požadovaných aplikací. * Nástroj bude umožňovat správu aktualizací systému. * Požadavky na antivirové zabezpečení:   + Nástroj bude obsahovat podporu antivirového zabezpečení pro operační systém Android.   + Nástroj bude obsahovat rezidentní ochranu běžící a chránící zařízení v reálném čase.   + Nástroj bude umožňovat definici naplánovaných kontrol.   + Nástroj bude umožňovat kontrolu výměnných zařízení.   + Nástroj bude obsahovat detekci potenciálně nechtěných aplikací.   + Nástroj bude umožňovat definici aktualizačního serveru.   + Nástroj bude obsahovat ochranu proti phishingu.   + Nástroj bude obsahovat detekci phishingových URL v SMS zprávách.   + Nástroj bude umožňovat instalaci a odinstalaci aplikací třetích stran.   + Nástroj bude umožňovat vyčítání informací o verzích softwaru třetích stran.   + Nástroj bude umožňovat vyčítání informací o hardwaru na spravovaných zařízeních. |  |
| Dvoufaktorová autentizace | * Nástroj bude umožňovat doručení OTP aplikací v mobilním zařízení. * Nástroj bude umožňovat doručení OTP e-mailem. * Nástroj bude umožňovat doručení OTP bezpečnostním tokenem. * Nástroj bude umožňovat doručení OTP SMS zprávou. * Nástroj bude umožňovat konfiguraci vlastní SMS brány pro doručení OTP kódu. * Nástroj bude umožňovat doručení OTP vlastní aplikací. * Nástroj bude podporovat ověřování metodou FIDO. * Nástroj bude umožňovat ověřování pomocí Push Authentication. * Aplikace výrobce s podporou Push-Notifications pro platformy: * Nástroj bude podporovat push notifikace pro iOS. * Nástroj bude podporovat push notifikace pro Android. * Nástroj bude podporovat push notifikace pro watchOS a Wear OS. * Požadavky na aplikaci výrobce systému:   + Nástroj bude obsahovat mobilní aplikaci v hlavních jazykových lokalizacích včetně češtiny.   + Nástroj bude umožňovat přístup do mobilní aplikace chráněný PINem nebo biometrikou.   + Nástroj bude umožňovat generování OTP v off-line prostředí (bez internetového připojení, bez GSM spojení). * Další požadavky:   + Nástroj bude podporovat hardwarové tokeny HOTP splňující standard OATH.   + Nástroj bude podporovat hardwarové tokeny certifikované výrobcem.   + Nástroj bude umožňovat kompletně softwarové řešení bez nutnosti nákupu dalšího hardwaru.   + Nástroj bude podporovat time-based hardwarové tokeny (PSKC).   + Nástroj bude umožňovat self-enrollment uživatelů. |  |
| Další požadavky | * Nástroj bude v souladu s:   + ISO27001 Standard,   + PCI/DSS - The Payment Card Industry Data Security Standard,   + ISAE 3402 – International Standards for Assurance Engagements no. 3402,   + HIPAA - Health Insurance Portability and Accountability Act,   + FFIEC - Federal Financial Institutions Examination Council compliances,   + Technická podpora v češtině. |  |

## Požadavky na záruky

Zadavatel požaduje záruku na veškeré dodané technologie v délce trvání minimálně **24 měsíců** od okamžiku předání díla, není-li u konkrétního zařízení či komponenty požadováno jinak v specifikaci ZD

Veškeré opravy po dobu záruky budou provedeny bez dalších nákladů pro zadavatele. Veškeré komponenty, náhradní díly a práce, poskytnuté v rámci záruky budou poskytnuty bezplatně.

## Požadavky na technickou podporu

Dodavatel nacení i potřebnou technickou podporu - je proces pravidelného udržování, vylepšování a opravování softwarových aplikací po jejich prvotním vývoji a nasazení. Zadavatel v rámci stanovení nabídkové ceny nacení veškerou potřebnou technickou podporu k řádnému provozovaní dodaného řešení. Potřebnou technickou podporu dodavatel nacení po dobu udržitelnosti projektu 5let. Technická podpora bude dle povahy dodaného řešení pokrývat minimálně níže uvedené scénáře:

* **Technická podpora:** Oprava chyb a problémů, které se objeví po nasazení softwaru. To může zahrnovat opravy bezpečnostních zranitelností, chyb v kódu nebo jiné problémy, které ovlivňují funkčnost softwaru.
* **Nové verze a aktualizace:** Úpravy a změny softwaru, aby zůstal kompatibilní s měnícím se prostředím. To může zahrnovat aktualizace pro nové operační systémy, hardware nebo jiné softwarové závislosti. Soulad SW s platnou legislativou.
* **Optimalizace provozu:** Vylepšení softwaru za účelem zvýšení jeho výkonu nebo použitelnosti. To může zahrnovat optimalizaci kódu, zlepšení uživatelského rozhraní nebo zavádění nových funkcí.

Údržba softwaru je klíčová pro zajištění, že software zůstane funkční, bezpečný a relevantní i po dlouhou dobu po jeho původním nasazení.

**Garantovaná doba reakce Poskytovatele od nahlášení požadavku na poskytnutí technické podpory**

1. Služba je poskytována Pracovníky Poskytovatele v okamžiku, kdy dojde k zadání Požadavku.
2. Obsahem této služby je reakce Poskytovatele na Požadavky dle jejich priority a zahájení řešení v rámci **Servisního kalendáře, tj. pracovní dny od 7:00 do 17:00**.
   1. Je-li požadavek nahlášen mimo pracovní dobu, je počátkem uvedené doby 7:00 hodin nejbližšího pracovního dne.
   2. Dodavatel je povinen zahájit řešení požadavku bezodkladně, nejpozději však do níže uvedených časů, viz tabulka Klasifikace požadavku a stavů.
3. Požadavek na provedení této služby zadávají Kontaktní osoby Objednatele nebo Poskytovatele zadáním Požadavku na Helpdesk Poskytovatele.
4. Zahájení řešení je primárně poskytováno Vzdáleným připojením pracovníka Poskytovatele. Pokud to technická povaha řešení Požadavku vyžaduje, bude realizován fyzický zásah pracovníka Poskytovatele v místě technologických center města Kroměříže, přesné místo bude vždy specifikováno v zadaném požadavku.

**Klasifikace požadavku a stavů**

|  |  |  |  |
| --- | --- | --- | --- |
| **Klasifikace** | **Definice** | **SLA zahájení řešení** | **Předpokládané vyřešení požadavku** |
| 1. Nahlášení požadavku | Potvrzení přijetí nahlášeného požadavku jedním z výše uvedených způsobů hlášení požadavku. | Nejpozději do 15 minut | Není specifikováno |
| 1. Kritický požadavek (A) | Události, které znemožňují přístup ke službám a datům poskytovaných Prvky IT, nebo jejich využívání, vážně ovlivňují plnění termínů nebo ziskovost, případně mají vliv na většinu uživatelů a služeb. | Nejpozději do 2 hodiny od nahlášení požadavku v rámci Servisního kalendáře | Do 8 hodin od zahájení řešení, dle servisního kalendáře |
| 1. Závažný požadavek (B) | Události, které významným způsobem degradují, nebo silně omezují funkcionalitu nebo službu Prvku IT, ale existuje náhradní řešení (činnost pokračuje v omezeném provozu). | Nejpozději do 5 hodin od nahlášení požadavku v rámci Servisního kalendáře | Do 16 hodin od zahájení řešení, dle servisního kalendáře |
| 1. Ostatní požadavky (C) | Všechny ostatní požadavky, neomezující řádné používání Informačního systému, které tvoří Prvky IT. | Nejpozději do druhého pracovního dne od nahlášení požadavku | Do 32 hodin od zahájení řešení, dle servisního kalendáře |
| 1. Změnové požadavky | Součinnost při implementaci změn a činnostech při nasazovaní nových prvků IT či jejich částí. | Nejpozději do 7 pracovních dní | Stanoveno dohodou |
| 1. Konzultace a návrh řešení, programátorské práce | Konzultace při řešení problémů nebo při úpravách prvků IT. | Nejpozději do 5 pracovních dní | Stanoveno dohodou |

Pro případ, že bude zadavatel požadovat služby rozšířené technické podpory podle písmena e) a f), budou tyto služby vyúčtovány po skončení kalendářního měsíce, ve kterém byly čerpány, v hodinové sazbě uvedené v Kalkulaci ceny, dle skutečně realizovaných hodin rozšířené servisní podpory. Předpokládaný rozsah služeb rozšířené technické podpory pro účely přípravy nabídky je 100 hodin / na 5 let.

# Společné požadavky

|  |
| --- |
| **Požadavek** |
| Dodavatel bere na vědomí, že součástí akceptace plnění jsou výsledky auditu, který bude prověřovat, zda jím implementovaná bezpečnostní opatření jsou funkční. Dodavatel pak poskytne součinnost nebo napraví nalezené chyby vysoké závažnosti v implementaci technických opatření. |
| Součástí je zajištění instalace a konfigurace veškerých komponent v návaznosti na stávající infrastrukturu úřadu (tj. včetně dopravy, montáže, instalace a implementace do stávající IT infrastruktury) v sídle zadavatele. |
| Součástí instalace musí být i zaškolení IT administrátorů minimálně v rozsahu nutném pro samostatnou administraci všech komponent zakázky. Administrací se rozumí zejména: konfigurace, monitoring činnosti, aktualizace, řešení problémů, zálohování konfigurace. |
| Zákaznická dokumentace bude zahrnovat:   * popis všech prvků/zařízení, * popis způsobu zálohy a obnovy konfigurace všech prvků/zařízení * veškeré požadavky na zachování záruky/podpory (např. environmentální, kompatibilita, …) * informaci o způsobu řešení servisních požadavků |
| Dodavatel do své nabídky zahrne veškerý instalační materiál a kabeláž nutnou k plnohodnotnému zprovoznění dodané technologie jako logického a funkčního celku. |
| Dodavatel zajistí instalaci a konfiguraci dodaných HW a SW komponent v návaznosti na stávající infrastrukturu organizace, a to včetně instalace a implementace do stávající IT infrastruktury v sídle zadavatele:   * instalace zařízení do standardní RACK skříně 19“ * implementace Best Practice scénářů pro dané konfigurace * kontroly kompatibility verzí ovladačů a firmware jednotlivých zařízení a jejich aktualizace * registrace záruk u výrobců * umístění do racku a zapojení kabeláže vč. jejího označení, * inicializace a konfigurace všech dodaných zařízení * nastavení IP adres * nastavení vysoké dostupnosti * konfiguraci datových prostor polí, integrace s hypervizorem, nastavení dohledu a instalace SW pro monitoring výkonu * zapojení do stávající SAN |
| Dodavatelé za všechny části si budou poskytovat vzájemnou součinnost při zprovoznění nebo implementaci všech částí zakázky v nezbytném rozsahu. Předpokládaná součinnost pro každého dodavatele v každé části je 1 člověkoden celkem pro všechny části. |

# Provozní podpora

|  |
| --- |
| **Požadavek** |
| Podpora a servis pro dodaný HW a SW budou poskytovány minimálně po celou dobu udržitelnosti projektu (tj. 60 měsíců od předání díla), pokud není specifikováno jinak. |
| Bude zajištěna udržitelnost HW a SW včetně třetích stran, dodaných v rámci veřejné zakázky. |
| Technická podpora a servis zařízení HW a SW budou realizovány dodavatelem, případně prostřednictvím odpovídajícího servisního kanálu výrobce. |
| Technická podpora a servis budou realizovány v místě zadavatele. Výjimku tvoří činnosti realizovatelné vzdáleným připojením. |
| Technická podpora bude zajišťována těmito způsoby:   * Telefonicky prostřednictvím přiděleného tel. kontaktu. * Prostřednictvím elektronické oznamovací služby (tzv. helpdesku). * Prostřednictvím vzdáleného připojení na PC uživatele / server. |
| Telefonická, e-mailová podpora a podpora prostřednictvím vzdáleného připojení bude k dispozici minimálně v pracovních dnech od 7 do 17 hod. |
| Služba HelpDesk umožní příjem požadavku na servisní zásah v českém jazyce prostřednictvím webového rozhraní v režimu 7x24 hod (s výjimkou předem nahlášených servisních zásahů při správě systému HelpDesk). |