# DODÁNÍ A IMPLEMENTACE OCHRANY KONCOVÝCH STANIC A SERVERŮ PŘED BEZPEČNOSTNÍMI HROZBAMI

# ochrana koncových stanic a serverů:

1. Detekce a prevence malware: Dodaný systém musí být schopen detekovat a zabránit různým typům malware, včetně virů, trojských koní, ransomwaru, spywaru a dalších hrozeb. Musí umět používat pokročilé algoritmy analýzy chování a heuristiky pro odhalování nových a neznámých hrozeb (tzn. nerozhodovat pouze na základě antivirové databáze).
2. Behaviorální analýza: Dodaný systém musí sledovat chování souborů a procesů v reálném čase a detekovat podezřelé aktivity, které naznačují přítomnost malware, případně jiných hrozeb. Musí používat strojové učení a umělou inteligenci pro identifikaci nových vzorů chování malware.
3. Ochrana před ransomwarem: Dodaný systém musí obsahovat funkce pro ochranu proti ransomwaru, jako je monitorování podezřelých souborových operací.
4. Síťová ochrana: Dodaný systém musí poskytovat funkce ochrany síťové komunikace před neoprávněným přístupem ze sítě třetích stran. (mimo interní prostředí zadavatele, například práce z domova apod.).
5. Kompatibilita a výkon: Dodaný systém musí být kompatibilní s aktuálně podporovanými verzemi MS Windows – desktop i server a aktuálně podporovaných verzí OS Linux. Musí nabízet efektivní skenování zařízení a nesmí zásadním způsobem ovlivnit výkon zařízení. Minimální konfigurace: 2 jádrový CPU, 8GB RAM a SSD disk.
6. Automatické aktualizace: Dodaný systém musí automaticky stahovat a instalovat aktualizace s definicí škodlivého software (virová databáze).
7. Dodaný systém musí umět sám všechny hrozby vyhodnotit a bez nutnosti administrátora sám zakročit a případný útok zastavit dle nastavených pravidel v centrální správě dodaného systému.
8. Dodaný systém musí umožnit automatické skenování všech nově připojených datových zdrojů k zařízení (například USB disk, FlashDisk, paměťové karty apod.).
9. Dodaný systém musí umožnit aktivní správu všech vstupně výstupních portů určených k přenosu dat.
10. Centrální správa a monitorování: Dodaný systém musí mít možnost centrální správy a monitorování, která umožňuje správcům IT prostředí sledovat stav a výkonnost antivirového programu a provádět vzdálené aktualizace antivirových databází a konfigurace z jednoho místa.

# Centrální správa:

1. Centrální správa: Dodaný systém musí poskytovat nástroj, který umožňuje správcům IT sledovat a spravovat všechny stanice a servery z jednoho místa (centrální správa). Dodaný systém musí nabízet uživatelsky přívětivé rozhraní pro snadnou správu (GUI).
2. Instalace klientů pomocí doménové politiky: Dodaný systém musí umožňovat automatizovanou instalaci klientů na koncová zařízení pomocí doménové politiky. Tímto způsobem bude zajištěna automatická instalace a konfigurace na všech koncových zařízeních bez nutnosti manuální intervence na každém koncovém zařízení.
3. Základní přehled stanic: Dodaný systém musí poskytovat přehled o aktuálním stavu všech koncových zařízeních (například: poslední aktualizace databáze a její verze, verze programu, posledním skenování a výsledcích, zda je zařízení aktivní, zda je zařízení v ohrožení apod.).
4. Upozornění na hrozby: Dodaný systém musí disponovat funkcí upozornění a notifikací (minimálně notifikace emailem) v případě detekce hrozeb nebo jiných událostí dle konfigurace.
5. Dashboard: Dodaný systém musí disponovat nástrojem pro centrální sledování stavu všech koncových zařízení (dashboard). Tento dashboard musí být interaktivní a musí reagovat v reálném čase.
6. Analýza hrozeb: Dodaný systém musí poskytovat nástroje pro analýzu hrozeb, včetně detailních informací o detekovaných hrozbách, jejich původu, chování a dopadu na postižené koncové zařízení. Součástí nabízeného řešení je možnost vyhledávání a filtrování hrozeb pro podrobnější analýzu.
7. Vzdálená správa bezpečnostních incidentů: Nabízené řešení musí umožňovat vzdálenou správu bezpečnostních incidentů a jejich řešení (a to i v případě, kdy agent nabízeného řešení instalovaný na koncovém zařízení zablokuje síťovou komunikaci).
8. Přihlášení správce do aplikace musí být zabezpečeno min. dvou-faktorovou autentizací.

# Prostředí:

1. Agent nabízeného řešení musí umět chránit koncové zařízení v každém okamžiku (v prostředí zadavatele i v externím prostředí, i bez aktivního připojení k internetu).
2. Agenta nabízeného řešení musí jít vypnout, pozastavit, nebo zapnout pouze z centrální správy, nebo pověřeným účtem.
3. Agent nabízeného řešení musí umět komunikovat s centrální správou i v případě, kdy je v externím prostředí, ale je připojený k veřejné síti internet.
4. Nabízené řešení musí být provozováno dodavatelem v bezpečném datovém centru, splňující aktuálně platnou legislativu ČR (zvláště pak musí být v souladu s požadavky NUKIB, NIS2, GDPR apod.).

# Maintenance:

1. Po dobu životnosti licence musí být poskytnuty aktualizace software.
2. Po dobu životnosti licence musí být poskytnuty bezpečnostní záplaty.
3. Pro antivirové řešení musí být poskytnuta technická podpora.
4. Pro antivirové řešení musí být poskytnuta konzultace a školení pro zavedení antivirového řešení.