# Příloha č. 1 – Technická specifikace

**příloha č. 1\_Technická specifikace\_část 3**

# Bezpečnostní technologie a práce

# 1.1 Více faktorová autentizace

|  |  |
| --- | --- |
| **Parametr** | **Minimální požadavek** |
| Výrobce, název, verze software | **MONET+, a. s. SW - Licence Kartového centra, SW licence CMS** |
| Požadavek | * Prostředky pro zajištění dvoufaktorového ověřování včetně karet |
| Vlastnosti karet | * Celkem 900 kusů QSCD hybridních čipových karet ve formátu ID-1 (velikost bankovní karty) z toho 300 kusů, které budou mít navíc čipy Mifare 4K a RFID 125 kHz. * Kontaktní čipy a aplikace nahraná do kontaktního čipu umožňuje správu kryptografických klíčů určených k vytváření kvalifikovaného elektronického podpisu. * Dodané karty budou podporovat paralelní zpracování komunikace mezi kartou a čtečkou. * Možnost garantovaného dokoupení dalších kontaktních karet stejného typu po dobu platnosti smlouvy. * Dodat 200 kusů kontaktních čteček čipových karet, které budou kompatibilní s dodanými hybridními čipovými kartami. * Garantovaná kompatibilita se stávajícím přístupovým systémem (dle standardu Mifare DesFire viz <https://en.wikipedia.org/wiki/MIFARE> respektive <https://www.mifare.net/en/about-mifare/certification/>) * Dodané karty budou obsahovat i bezkontaktní čip, kompatibilní s naším stávajícím řešením (dle standardu Mifare DesFire.) * Dodat SW aplikace pro správu hybridních čipových karet a certifikátů s licencí na dobu neurčitou pro 1000 uživatelů. * Pomocí hybridních čipových karet zajistit 2faktorovou autentizaci uživatelů, pomocí PKI uživatelských certifikátů uložených v kontaktním čipu ID-1 karty, tak aby byly naplněny podmínky ZoKB. * Implementace dodaných systémů a vyškolení příslušných osob odběratele na obsluhu všech dodaných systémů * Poskytnou 5letou udržitelnost celého dodaného systému. |
| Funkční specifikace | * Umožnit vytvářet pro zaměstnance zadavatele kvalifikovaný elektronický podpis podle nařízení eIDAS pomocí kryptografických klíčů bezpečně chráněných v hardwarovém prostředku – hybridní čipové kartě. * Karta musí také umožňovat společné uložení certifikátu z interní certifikační autority založené na produktech Microsoft. Pomocí tohoto certifikátu se držitel karty bude moci v budoucnu přihlásit do doménových počítačů (technologie Smartcard Logon). * Základní požadavky na zařízení: * Hybridní čipové karta a ovladače: * Pro uložení elektronických certifikátů X.509 (a generování / uložení příslušných kryptografických klíčů) * Budou dodány hybridní čipové karty ve formátu ID-1 (velikost bankovní karty): * kontaktní čip na bázi GlobalPlatform/JavaCard s personalizovanou PKI aplikací. * Certifikované karty musí být v souladu: * s normou ČSN EN ISO 7816, část 1-4 a * standardem EN 419 211 a profily: BSI-CC-PP-0059, BSI-CC-PP-0075, BSI-CC-PP-0071, BSI-CC-PP-0072, BSI-CC-PP-0076 * Vlastnosti kontaktního čipu a PKI aplikace: * Všechny operace s privátním klíčem probíhají uvnitř čipu – klíč neopustí prostředí karty * Privátní klíč uložený na kartě nelze z karty vyexportovat * Vytváření kvalifikovaného elektronického podpisu splňující nařízení eIDAS * Podporuje uložení kvalifikovaných certifikátů minimálně od tří poskytovatelů * Součástí podpory uložení kvalifikovaných certifikátů na čipovou kartu jsou také moduly pro ověření původu klíče (důkaz, že privátní klíč vznikl generováním uvnitř čipu kvalifikovaného prostředku), které je integrované se systémy kvalifikovaných certifikačních autorit. * Klíče pro kvalifikovaný elektronický podpis jsou generovány v čipu. * Klíče, které nejsou určeny pro kvalifikovaný elektronický podpis, mohou být generovány v čipu anebo mohou být na kartu importovány * Generování RSA i ECC klíčů v čipu i import klíčů s certifikáty do čipu, ze souboru formátu PKCS#12 * Archivaci privátních klíčů v procesech vydávání šifrovacích certifikátů * Podporované jsou minimálně kryptografické algoritmy: * Symetrické: 3DES, AES * Hash: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512. * RSA: 1024, 2048 bitů * Eliptické křivky: P-224, P-256, P-384, P-521 * Zablokování bezpečnostního kódu PIN, QPIN resp. PUK po opakovaném chybném zadání PIN, QPIN resp. PUK * Podpora PIN Proxy pro možnost opakovaného podpisu kvalifikovaným certifikátem bez nutnosti opakovaného zadávání PINu. * Podpora odblokování bezpečnostního kódu PIN pomocí PIN nebo PUK, podpora odblokování bezpečnostního kódu QPIN pomocí QPIN nebo PUK. * Podpora procesu ověření uživatele manažerem pro obnovu PIN * Omezit možnost měnit PUK, aby uživatel mohl měnit pouze PIN * Podpora správy PUK administrátorem * Zabezpečení komunikace na bázi e-mailů (S/MIME, elektronický podpis a šifrování e-mailů) * Dvoufaktorovou autentizaci na bázi certifikátů X.509 (do PC v prostředí Microsoft AD, webových služeb, VPN, aplikací atd.) * Vytváření elektronického podpisu na bázi certifikátů ve formě: * kvalifikovaného elektronického podpisu, * zaručeného elektronického podpisu, * uznávaného elektronického podpisu a * jiné formy elektronického podpisu. * Generování a práce s RSA a ECC klíči v čipu * Hybridní čipová karta podporuje získání následného certifikátu prostřednictvím aplikace pro automatizovanou obnovu certifikátů. V případě kvalifikovaného certifikátu je požadována podpora minimálně dvou poskytovatelů kvalifikovaných certifikátů. * Hybridní čipová karta podporuje konfigurovatelné množství kontejnerů pro RSA / ECC klíče a certifikáty,  minimálně v rozsahu 10  kontejnerů pro RSA (až do velikosti privátního klíče 4096 b a 10 kontejnerů pro ECC (až do velikosti privátního klíče 521 b) * Ovládací software karty: * Čipové karty budou dodány s ovládacím software, pro integraci kontaktního čipu karty do operačního systému. Vlastnosti ovládacího software: * podléhá specifikaci Microsoft Smart Card minidriver for Windows Base CSP V5.07 nebo vyšší * podpora Microsoft CryptoAPI, Microsoft CNG i PKCS#11 * použití na O MS Windows 10 nebo vyšších verzích; * případné použití i na Linux – LTS (Long Term Support) verze pro Ubuntu a RHEL (PKCS#11) OS X (PKCS#11) * Podpora MacOS * instalace z MSI balíčků (podpora obslužné a bezobslužné instalace), RPM, DEB * Součástí instalačního balíčku ovladačů karet je aplikace, která je dostupná pro uživatele i administrátory a umožňuje správu objektů čipové karty, např.   ·        Změna PIN / PUK  ·        Prohlížení obsahu kontejnerů (klíčů, certifikátů)  ·        Mazání kontejnerů  ·      Import klíčů a certifikátů do čipové karty   * Stav dodané karty: * Inicializovaná PKI aplikace s PIN, QPIN a PUK. * Předání seznamu personalizovaných karet, pro import do evidence CMS. U každé karty uvedeno číslo kontaktního, případně i bezkontaktního čipu. * Inicializovaná PKI aplikace výchozími hodnotami PIN, QPIN a PUK. Technickými prostředky bude vynuceno, aby si uživatel po přijetí karty změnil hodnotu bezpečnostních kódů. * Dodané čtečky čipových karet * Maximální hmotnost 60g * USB propojení (není požadována podpora bluetooth) * Podporované operační systémy: * MacOS, Linux, Windows * Požadavky na aplikace pro správu a podporu čipových karet a certifikátů a dalších bezpečnostních předmětů: * Zjednodušení životního cyklu karet a certifikátů, automatizace procesů životního cyklu karet formou průvodců pro správce životního cyklu i pro držitele certifikátů. Odstínění koncových uživatelů od technologie. * Automatizovaná obnova kvalifikovaných i komerčních certifikátů alespoň od dvou různých externích poskytovatelů v ČR. Automatizovaná obnova interních certifikátů z doménové CA * Implementace aplikace, které prostřednictvím e-mailové notifikace upozorní uživatele na blížící se konec platnosti certifikátu   a.  Notifikační profil lze konfigurovat podle potřeb, tj. vzhled a textace mailu, pravidla notifikace podle vlastností certifikátu (např. na základě vydavatele certifikátu, šablony certifikátu (pro MS CA), atp.  b.  Notifikační zprávu lze zároveň odesílat na mail správců, aby byli informování o blížící se expiraci certifikátů v organizaci  c.  Notifikaci lze odeslat nejen při blížící se expiraci certifikátů, ale také při jejich vydání  d.   Notifikační zpráva pro správce IT o nově vydaných certifikátech   * Implementace aplikace pro podporu činností spojených se správou životního cyklu čipových karet a certifikátů, zastřešení registračního místa doménové CA. * Implementace webové aplikace, určené správcům certifikátů. Možnost vyhledávat a prohlížet informace o čipových kartách - jejich držitelích, stavech čipové karty, datového obsahu čipové karty, prohlížení statistik karet v organizaci a  generování a prohlížení reportů. * . * Implementace PKI Zadavatele * Zadavatel požaduje v infrastruktuře svých podřízených organizací vybudovat bezpečnostní vrstvu vybudovanou na bázi PKI MS Windows, která je primárně určena pro vydávání klientských karetních a infrastrukturních certifikátů. * Nově se plánuje z doménového PKI vydávat uživatelské certifikáty na čipové karty za účelem zavedení primárně dvoufaktorové autentizace (náhrada autentizace jménem/heslem). Mimo přihlášení do PC budou z interní CA vydávány případně certifikáty pro přihlášení do VPN a interní elektronický podpis. Interní PKI bude také poskytovat infrastrukturní certifikáty pro interní použití, např certifikáty pro web servery a DC. * V rámci dodávky je Zadavatelem požadované pro každou z podřízených organizací: * Provést a předat návrh PKI * Implementace PKI dle návrhu, součástí minimálně bude: * Implementace zvolené architektury hierarchie PKI, zprovoznění PKI v prostředí zákazníka * Předat podklady na implementaci šablon pro vydání certifikátů pro autentizaci uživatelů do domény, případně další uživatelské akce. * Implementace šablon uživatelských certifikátů * Definici distribučníc h bodů CRL * Ochrana a uložení klíče CA * Dodání havarijní a provozní dokumentace k vybudované vrstvě PKI |
| Záruky a podpora | * Udržitelnost nabízeného řešení musí zahrnovat podporu po dobu 5 let ode dne podpisu předávacího protokolu (delší podpora je volitelná a zadavatel ji nemusí využít): * čipových karet do konce životnosti * čteček pro práci s kartou * instalovaných aplikací pro správu životního cyklu karet a certifikátů * formou Service Desku v režimu 5 x 8, jehož provozní doba musí být min. od 8:00 do 16:00 v pracovní dny. * Požadované reakční doby: * Přijetí požadavku do 2 hodin od nahlášení. * Dočasné řešení do 1 pracovního dne od přijetí požadavku. * Vyřešení požadavku do 5 pracovních dnů od dodání dočasného řešení. * Reakční doby musí být garantovány pro serverové komponenty řešení. * Součástí ceny je podpora v rozsahu 24 MDs * Součástí dodávky musí být zaškolení obsluhy (administrátorů) v sídle zadavatele v rozsahu minimálně 1 x 3 hodiny. Předpokládaná účast 3 lidé.   + Školení administrátorů bude v délce 3 hodin.   + Hodinou je míněno 60 minut. |

# 1.2 Analýza síťového provozu

* Systém pro analýzu síťového provozu a bezpečnostní monitoring, který okamžitě identifikuje bezpečnostní rizika a události a který splňuje klíčové požadavky uvedené níže.
* Nabízená technologie musí být určena pro český trh.
* Při definici technických požadavků jsou všechny uvedené požadavky závazné. Je-li definice požadavku „umožňuje, lze, je možné, možnost, …“ je uvedený parametr závazný a požadovaná funkcionalita musí být v rámci Systému dodána/naimplementována a případně licencována. Tyto technické požadavky jsou minimální možné, Poskytovatel (dále také „dodavatel“) může nabídnout charakteristiky (funkce) lepší.

|  |  |
| --- | --- |
| **Parametr** | **Minimální požadavek** |
| Výrobce, název, verze a licenční program | **GREYCORTEX s.r.o. - Mendel SW licence** |
| Obecné požadavky na nástroj | * Nástroj slouží k opatření ve smyslu §23 Vyhláška č. 82/2018 Sb. Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti) * Nástroj zajištující detailní viditelnost síťového provozu s možností vizualizace komunikace všech hostů a jejich služeb s možností forenzní analýzy v řádu měsíců. Nástroj je schopen detekovat anomálií na úrovni toků a dále rozpoznávat známé hrozby na základě DPI za pomoci detekčních signatur. * Nástroj na analýzu síťového provozu se logicky skládá z jedné nebo více sond pro sběr dat a z jedné centrální konzole pro vyhodnocování dat o síťovém provozu. Fyzicky jde o jednu hardwarovou applianci, nebo o několik hardwarových appliance. * Celá softwarová část je od jednoho výrobce. * Jedna centrální konzole pro vyhodnocování dat o síťovém provozu je schopná analyzovat všechna data (tj. až 500 Mbps) od všech sond a zobrazovat je v jednom jednotném aplikačním rozhraní. * Nástroj neobsahuje žádný skrytý (backdoor) přístup. * Nástroj obsahuje veškerý hardware a software potřebný pro zprovoznění a provoz. * Licence na aktualizace veškerého software nástroje a jeho dat (filtry, signatury, databáze třetích stran, threat intelligence, atd.) na 60 měsíců. * Fungování s přístupem na Internet i bez nutnosti přístupu na Internet. |
| Požadavky na analýzu provozu | * Podpora IPv4, IPv6, VLAN, MPLS, Ethernet 10Mb/s až 10 Gb/s * Stejné funkce pro IPv4 a IPv6 (s výjimkou funkcí, které v IPv4, respektive IPv6 vůbec neexistují). * Podpora VLAN podle IEEE 802.1Q. * Nástroj zpracuje veškerá data odeslaná na jeho síťová rozhraní pro příjem síťového provozu. * Nástroj provádí analýzu (kopie) datového provozu, který obdrží ze zrcadlených (SPAN, mirror) portů aktivních síťových prvků. * Komunikace mezi sondou a kolektorem je plně šifrována na úrovni SSL/TLS. * Aplikace umožnuje jednotné vyhledávání ve všech datových pohledech, tj. jeden vyhledávací dotaz je možné aplikovat na síťová data, bezpečnostní incidenty případně jiná zobrazení jako přehledové informace, bez nutnosti kopírovat nebo jinak přenášet, či modifikovat vyhledávací filtr. * V datech lze vyhledávat/filtrovat dle libovolného parametru, případně kombinace parametrů datového toku – minimálně hostname, jméno uživatele z Active Directory, IP adresa, MAC adresa, lokální služba (local service), vzdálená služba (remote service), příchozí provoz, odchozí provoz, interní provoz. * Je možné použít aplikačního průvodce pro vytváření uživatelských filtrů a jejich uložení případně sdílení mezi ostatními uživateli. * Aplikace průběžně vytváří a ukládá statistická dat o síťovém provozu na všech podsítích, všech hostech a všech službách v rámci monitorované sítě. * Aplikace umožňuje okamžitou grafickou vizualizaci a výpis průběhu komunikace u všech zařízení v monitorované síti, všech služeb a všech podsítí s možností řazení dle libovolné hodnoty – např. přenesená (odchozí, příchozí) data, pakety, toky, množství komunikačních partnerů, výkonnostní metriky (RTT – Round Trip Time, ART – Application Response Time, EUT – End User Experience Time …). * Síťové toky jsou prezentovány při každém zobrazení v aplikaci jako obousměrné. Tj. prezentace, zda daný tok (požadavek) měl i opačný provoz (odpověď), bez nutnosti vytváření dalších filtrů či dohledávání zpětné komunikace na jiném řádku. * Záznam každého síťového toku obsahuje stejné informace vždy pro požadavek i odpověď. Minimálně však: IP adresa, MAC adresa, port, počet paketů, velikost dat přenášených po sítí, velikost aplikačních dat přenesených po síti, identifikovaný aplikační protokol, aplikační metadata všech provedených transakcí v rámci daného toku. * Ukládání aplikačních metadat (transakcí) minimálně pro HTTP (minimálně URL požadavku a návratový kód odpovědi pro každou transakci), DNS (plné znění požadavku i odpovědi) a HTTPS (použité certifikáty). * Možnost nastavení obsahu ukládaných metadat, včetně možnosti úplného vypnutí ukládání aplikačních metadat. * Ukládání plného záznamu síťové komunikace ve formátu PCAP dle uživatelem definovaných filtrů. * Nastavení systémového času manuálně a formou synchronizace s časovými servery protokolem NTP. * Geolokace externích IP adres dle databáze platné v době zaznamenání síťového toku. * Aplikace přiřazuje všem IP adresám hostname dle aktuálních DNS záznamů. * Aplikace přiřazuje všem IP adresám hostname dle aktuálních DHCP záznamů. * Aplikace umožnuje dešifrování libovolné komunikace na úrovni SSL/TLS vložením privátního šifrovacího klíče/certifikátu. Po dešifrování je provedená plnohodnotná inspekce provozu, tj. bezpečnostní analýza za pomocí známých hrozeb (signatur), uložení metadat atd. |
| Provádění a metody detekce | * Metoda detekce kybernetických útoků na základě rozpoznání anomálií v síťovém provozu. Anomálie jsou detekovány porovnáním aktuálního chování vůči chování za minulé období. Detekce minimálně pro jednotlivá zařízení v síti, pro jednotlivé služby v síti a pro jednotlivé podsítě. * Detekce na základě modelování koncových hostů. Detekce odchylek od predikovaného chování dle historického modelu chování všech hostů v síti, všech služeb na každém hostu v síti a jednotlivých podsítí. * Metoda detekce kybernetických útoků na základě síťové behaviorální analýzy komunikace, tj. detekce vzorů chování za pomoci detekčních pravidel. * Detekce opakujícího se chování se zpětnou analýzou každého hosta a každé služby alespoň 6 hodin. * Metoda detekce porušení interních bezpečnostních politik za pomocí síťové behaviorální analýzy cílená na dodržování politikou definovaných komunikačních matic a komunikačních vektorů. * Metoda detekce kybernetických útoků na základě síťové behaviorální analýzy cílené na rozpoznání strojového a lidského chování v dlouhodobých časových intervalech. * Metoda pro detekci aplikačních a síťových výkonnostních problémů a anomálií za pomoci analýzy síťových výkonnostních metrik (alespoň. RTT, ART). * Metoda detekce kybernetických útoků na základě automaticky a pravidelně aktualizovaných detekčních signatur známých hrozeb typu Snort. Aplikace obsahuje alespoň 30.000 aktivních detekčních signatur. * Detekční signatury rozděleny do kategorií dle zaměření detekce na určitý typ kybernetické hrozby. Například: Trojan, Exploit, Webové útoky, Malware, Mobilní malware, zneužití zranitelnosti dle CVE kódu, atd. * Vytváření a nasazení vlastních signatur pro detekci určitého vzoru v obsahu komunikace v jazyce, který je obdobný (nemusí být identický, ale má obdobné možnosti), jako je jazyk pro psaní pravidel pro SNORT. * Analýza plného obsahu komunikace pomocí DPI (Deep Packet Inspection). Nejedná se o analýzy jen zaznamenaných metadat komunikace. * Aplikace poskytuje možnost vytváření vlastních detekčních signatur ekvivalentních s typem Snort. |
| Detekční schopnosti | * Detekce minimálně následujících typů skenování portů: TCP, SYN, FIN, NULL. * Detekce hádání hesel pro minimálně následující protokoly: TELNET, HTTP, SSH, RDP, FTP, SMTP, IMAP, POP3, SMB, SMB2. * Detekce známých (vyskytujících se v signaturách nástroje) hrozeb a škodlivého kódu (malware). * Detekce DDoS útoků. * Měření výkonnosti všech aplikací vyskytujících se v monitorované síti, které používají TCP, minimálně podle RTT (Round Trip Time) a ART (Application Response Time). S grafickou vizualizací pro jednotlivé hosty v síti a všechny služby obsažené v monitorované síti. * Detekce komunikace s adresami s nízkou reputací, známými botnety a C&C centry, darknetem (nelegitimní služby a aplikace provozované v internetu). * Detekce P2P komunikace. * Detekce aplikací. Minimálně Skype, Jabber/GTalk, Torrent, TOR. * Detekce standardních protokolů, i když běží na nestandardních portech – např. HTTP nebo SSH na portu 443 atd. * Detekce datových tunelů v komunikaci. Například HTTP v DNS, SMTP v HTTP, IPv6 v IPv4. * Detekce anomálií v komunikačních protokolech, minimálně DNS, DHCP, HTTP, SMTP, SMB. * Detekce událostí:   + MAC Spoofing   + IP Spoofing   + Duplikace/změna IP   + Duplikace/změna MAC   + Detekce neočekávaného přenosu objemu dat (Bandwidth anomaly detectiom) * Detekce neočekávaného počtu spojení (Connection rate detection) * Detekce nedostupnosti vybraných zařízení a služeb. * Detekce vzniku nových služeb, či komunikačních vektorů nedopovídajících uživatelem definované komunikační matici monitorované sítě. * Možnost dešifrování SSL/TLS komunikace obsahu komunikace pro vybraná zařízení s využitím privátního klíče. * Každá detekované bezpečnostní událost poskytuje odkaz na konkrétní tok, nebo toky, které bezpečnostní událost způsobily. Tento síťový tok události obsahuje vždy záznam s informacemi o požadavku i odpovědi. |
| Správa a reporting | * Nástroj obsahuje integrovaný centrální reporting, který je součástí produktu. Nesmí jít o externí komponentu. * Reporty minimálně ve formátech PDF a DOCX. * Reporty v českém nebo anglickém jazyce. * Rozesílání reportů elektronickou poštou. * Uživatelsky definované reporty. * Zálohování dat na externí datové úložiště dostupné minimálně přes protokol CIFS. * Logování ve formátu syslog, syslog CEF, LEEF s možností konfigurovatelné struktury obsahu generovaných záznamů. * Konfigurovatelná možnost, že zpráva syslog obsahuje URL odkaz do centrální konzole na událost, která způsobila odeslání syslog zprávy. * Minimálně 2 DNS servery pro překlad mezi jmény a IP adresami. * Základní administrace (nastavení sítě, restart aplikace, ověření stavu aplikace) možná přes řádkové rozhraní s využitím SSH2. * Pokročilá administrace přes jedno jednotné uživatelské grafické rozhraní s využitím standardního web prohlížeče. * Procesní podpora nástroje při řešení detekovaných událostí. Tj. nástroj podporuje přiřazení více stavů (např. detekovaná, řešená, vyřešená) jednotlivým událostem (detekovaný incident). Vše je součástí jednoho jednotného uživatelského grafického webového rozhraní. * Možnost zobrazení (filtrování) událostí v GUI dle aktuálního stavu (např. detekovaná, řešená, vyřešená) * Autentizace uživatelů nástroje vůči LDAP, MS Active Directory a lokální databázi. * Administrátorské profily s možností přidělování práv (read only, read-write, none) pro jednotlivé skupiny administračních funkcí, pro jednotlivé metody detekce, pro jednotlivé rozsahy IP adres, MAC adres, atd. |
| Implementace a požadavky na nasazení nástroje | * Implementace a provoz nástroje nemodifikuje stávající provoz a bezpečnost počítačové sítě. * Montáž všech appliance do standardních 19“ skříní (rack). * Napájení všech appliance 230 V AC / 16 A. * Vestavěné napájecí zásuvky IEC typ C13 ve všech appliance. * Provoz všech appliance v teplotním rozsahu minimálně 10–35 stupňů Celsia. * Minimálně jedno síťové rozhraní pro správu appliance na každé appliance. * V síti je předpokládáno cca 500 aktivních IP adres zařízení s průměrným celkový průtokem do 200Mbps. * Je požadován 1x HW datový kolektor/sensor o průměrné propustnosti minimálně 200Gbps s monitorovacím rozhraním 2x10GbE a 2x1GbE. * Na zařízení je požadována dostupná historie dat minimálně 12 měsíců zpětně, uložená na rychlém úložišti typu SSD o velikosti alespoň 3TB. Požadován je minimálně RAID10 nebo RAID6 se schopností hot-swap. |
| Podpora | * Výrobcem automaticky aktualizovaná databáze adres a jmen s nízkou reputací na Internetu (SPAM listy, black listy, weby s malware atd.) po dobu 60 měsíců. * Výrobcem automaticky aktualizovaná databáze IP adres známých botnet C&C center po dobu 60 měsíců. * Výrobcem automaticky aktualizovaná databáze signatur hrozeb a útoků po dobu 60 měsíců. |

# 1.3 Identifikace a hodnocení aktiv a rizik a řízení kontinuity činností

Cílem je předcházet rizikům a zároveň minimalizovat následky a náklady na řešení potenciálních kybernetických bezpečnostních incidentů. Předmětem činností je zajištění souladu s požadavky současného zákona č. 141/2014 Sb., o kybernetické bezpečnosti (ZoKB) a vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti. Konkrétně v oblastech §4 VyKB řízení aktiv, §5 VyKB řízení rizik, §8 VyKB řízení dodavatelů, §15 VyKB Řízení kontinuity činností a §27 Zajišťování úrovně dostupnosti informací, §30 Bezpečnostní politika a bezpečnostní dokumentace včetně tvorby přiléhající dokumentace dle požadavků VyKB pro oblast řízení kontinuity činností a zajištění úrovně dostupnosti informací.

Cílem je také zajistit soulad se všemi změnami souvisejícími s povinnostmi ZZSJčK v souvislosti s novelizací ZoKB a VyKB. V případě, že v době plnění veřejné zakázky nevejde nový ZoKB a VyKB v platnost, bude dodavatel vycházet z v té době známých materiálů uveřejněných na oficiálních webových stránkách Národního úřadu pro kybernetickou a informační bezpečnosti a materiálů uveřejněných na oficiálních webových stránkách portálu informačního systému ODok Úřadu vlády České republiky.

ZZSJčK požaduje agilní řízení projektu a aktivit za neustále komunikaci se ZZSJčK a dodavateli ZZSJčK  s cílem maximální efektivity a dosažení požadovaných výstupů projektu. ZZS JčK níže poskytuje svoji představu o jednotlivých činnostech a výstupech s tím, že rozsah a míra detailu se v průběhu může změnit v závislosti na splnění výše uvedeného cíle a předmětu.

### **Identifikace a hodnocení aktiv a rizik**

Prvním krokem bude vytvoření metodiky pro identifikaci a hodnocení aktiv a rizik.

Následně dojde k identifikaci primárních a podpůrných aktiv. Na základě identifikovaných primárních a podpůrných aktiv budou vedeny rozhovory s garanty primárních a podpůrných aktiv pro zajištění hodnocení primárních a podpůrných aktiv. Současně dojde k proškolení garantů primárních a podpůrných aktiv s jejich rolí v oblasti kybernetické bezpečnosti a Systému řízení bezpečnosti informací.

Následně dojde k identifikace vazeb mezi primárními a podpůrnými aktivy. Následovat bude identifikace a hodnocení a hrozeb, zranitelností a tvorba rizikových scénářů. Výsledkem bude hodnocení rizik a plán zvládání rizik včetně prohlášení o aplikovatelnosti a případně další bezpečnostní dokumentace.

Všechny informace musí být řádně evidovány.

Výstupní dokumentace:

* Metodika pro identifikaci aktiv a rizik
* Výstup identifikace a hodnocení aktiv a rizik včetně:
  + Identifikace, hodnocení a evidence primárních aktiv
  + Identifikace, hodnocení a evidence podpůrných aktiv
  + Identifikace a evidence vazeb mezi primárními a podpůrnými aktivy
  + Identifikace a evidence zranitelností
  + Identifikace a evidence hrozeb
  + Tvorba rizikových scénářů
  + Hodnocení rizik
  + Zvládání rizik
* Prohlášení o aplikovatelnosti
* Plán zvládání rizik
* Bezpečnostní dokumentace Systému řízení bezpečnosti informací

### **Řízení kontinuity činností**

Prvním krokem bude vytvoření metodiky pro provedení analýzy dopadů.

Následně dojde k provedení analýzy dopadů, kdy dojde mj. k vyhodnocení a dokumentaci možných dopadů kybernetických bezpečnostních incidentů a zohlednění hodnocení rizik. Analýza dopadů bude probíhat řízenými rozhovory s garanty primárních a podpůrných aktiv.

Na základě výsledků analýzy dopadů vznikne strategie řízení kontinuity činností, která bude obsahovat, kromě jiného, cíle řízení kontinuity činností formou určení:

* minimální úrovně poskytovaných služeb, která je přijatelná pro užívání, provoz a správu poskytování regulované služby ZZSJčK;
* doby obnovení chodu, během které bude po kybernetickém bezpečnostním incidentu obnovena minimální úroveň poskytovaných služeb regulované služby a
* bodu obnovení dat jako časové období, za které musí být zpětně obnovena data po kybernetickém bezpečnostním incidentu nebo po selhání.

Následně dojde k vytvoření a zavedení plánů kontinuity činností (BCP) a plánů obnovy (DRP). Současně s tvorbou plánu obnovy (DRP) dojde k revizi a optimalizaci plánu zálohování a testování s cílem zajištění, že pro zajištění dostupnosti regulované služby jsou vytvořeny pravidelné zálohy nastavení technických aktiv, informací a dat nezbytných pro účely obnovy regulované služby pro případ kybernetického bezpečnostního incidentu. V rámci plánu zálohování a testování musí být zajištěno:

* testování jejich integrity, dostupnosti a obnovitelnosti;
* dokumentování provedených testů;
* ochrana ukládaných záloh a dat v nich obsažených před narušením jejich integrity a důvěrnosti, a to zejména šifrováním těchto záloh v souladu s VyKB;
* ochrana ukládaných záloh a dat v nich obsažených před narušením jejich dostupnosti;
* segmentace komunikační sítě, včetně oddělení zálohovacího prostředí.

Posledním krokem bude vytvoření politiky řízení kontinuity činností, která bude obsahovat všechny provedené úpravy z předchozích činností a bude obsahovat mj. naplnění cílů řízení kontinuity činností, stanovení práv a povinností garantů podpůrných aktiv (administrátorů a osob zastávající bezpečnostní role.

Výstupní dokumentace:

* metodika analýzy dopadů
* zpráva o analýze dopadů
* strategie řízení kontinuity činností
* politika řízení kontinuity činností
* plány kontinuity (BCP)
* plány obnovy (DRP)
* plán testování
* plán zálohování