Příloha č. 1 ZD veřejné zakázce Komplexní poradenství a realizaci dotačního projektu - Kybernetická bezpečnost

Technologické požadavky projektového záměru

Oblast	Popis
Analytické práce v oblasti bezpečnosti	Součástí je vytvoření bezpečnostních politik, směrnic a další dokumentace vyžadované VoKB. Součástí je také provedení analýzy dopadů (BIA – business impact analysis), na kterou navazuje tvorba plánů kontinuity. Součástí je formální popis interních procesů, tvorba základních směrnic společnosti, a nasazení IT procesů např. dle standardu ITIL. Předpokládá se plná shoda s novou legislativou NIS2.
Výpočetní cluster	Výpočetní cluster o dvou nodech s celkovými paramety 96 cores @2.8 GHz, 1TB ram, 20TB vSAN full SSD, 4x 10 Gbit, vmware 8 Ent+VSAN, vCenter, Windows 2022 DC, 200 device RDP CALs, . Clustr bude sloužit jako podkladový HW pro bezpečnostní technologie, zároveň bude schopen konsolidovat stávající starou infrastrukturu i licenčně. Součastí dodávky musí být pokrytí dvěma UPS s dostatečným výkonem.
Síťová infrastruktura	Nová síťová infrastruktura, která bude obsahovat: 2x CoreSwitch - 32-port 10Gbits SFP+ , 6-port 40Gbits QSFP+ 12x Acess Switch - 48-port 1Gbits RJ45, 4-port 10Gbits SFP+ Předpokládá se zapojení ve vysoké dostupnosti s použitím redundantních propojů
Zálohovací systém	Rozšíření stávajícího nebo nový zálohovací systém, který je navržen v režimu 3-2-1.
Realizace perimetrového firewallu a segmentace sítě	Nasazení perimetrového a centrálních firewallů, které zajistí ochranu sítě. V rámci tohoto kroku budou i naimplementována vhodná pravidla v rámci firewallů. Součástí bude také segmentace sítě. Perimetrový firewall bude obsahovat NextGenration funkce pro vyšší úroveň ochrany – filtrace a kategorizace webu, IPS, kontrola botnetů a DNS překladů). Firewall řešení bude spravována pomocí jednoho centrálního managementu.
Vybudování PKI	Vybudování interní certifikační autority PKI (public key infrastructure – architektura veřejných klíčů), která bude ve správě lázní. Vybudování interní certifikační autority PKI (public key infrastructure – architektura veřejných klíčů), která bude ve správě žadatele.

Příloha č. 1 ZD veřejné zakázce Komplexní poradenství a realizaci dotačního projektu - Kybernetická bezpečnost

Technologické požadavky projektového záměru

Nástroj pro řízení přístupu na síti	Nasazení nástroje nebo použití Windows NPS, který bude řídit přístup na síti. Cílem je, aby se k interní síti mohli připojit pouze autorizovaní uživatelé a zařízení, a aby se tak zamezilo nežádoucím připojením k síti.
Nástroj pro analýzu rizik	Implementace jednoduchého a uživatelsky přívětivého nástroje pro analýzu rizik. Nástroj umožní udržovat vazby mezi primárními a podpůrnými aktivy a celkovou správu aktiv, dále správu hrozeb, zranitelností a správu rizik. Přímá podpora pro zavedení řízení bezpečnosti (ISMS) a řízené dokumentace. Platforma pro správu rizik a dodržování compliance, která umožňuje organizacím snadno identifikovat, hodnotit a řídit bezpečnostní rizika a sledovat, zda jsou dodržovány příslušné zákony a předpisy. Poskytuje ucelený pohled na bezpečnostní a compliance situaci organizace a umožňuje řídit procesy související s řízením rizik a compliance.
IPAM	IPAM (IP Address Management) je nástroj pro řízení IP adres. Tento nástroj slouží ke správě adresního prostoru, zajišťuje plánování, sledování a řízení použitého IP adresního prostoru v síti.
Skener zranitelností a hardeningové politiky	Implementace nástroje, který bude skenovat technické zranitelnosti na zařízeních připojených do interní sítě. Tento nástroj umožní detekovat například neaktualizované nebo neopatchované aplikace a operační systémy, nepodporované systémy apod.
Systém pro správu privilegovaných účtů	Nasazení systému, který zajistí správu privilegovaných účtů a monitoring privilegovaných relací.
Nástroj pro sběr a korelaci událostí a logů (log management)	Nasazení nástroje, který zajistí centralizovaný sběr a korelaci událostí a logů z veškerých významných zařízení a aplikací v zákonem stanovené retence logů.
Automatické penetrační testy	Platforma pro automatické penetrační testy infrastruktury a aplikací. Jedná se o testování bezpečnosti IT systémů a aplikací pomocí simulování útoků hackerů. řešení, která pomáhají organizacím identifikovat, vyhodnotit a eliminovat bezpečnostní rizika v jejich IT prostředí.

Příloha č. 1 ZD veřejné zakázce Komplexní poradenství a realizaci dotačního projektu - Kybernetická bezpečnost

Technologické požadavky projektového záměru

EDR	Nasazení technologie na detekci a reakci na nežádoucí aktivity na koncových zařízeních, která disponuje nejen prevenčními schopnostmi pro zablokování škodlivého kódu a jiných útoků mířených na koncové stanice a servery.
SOC	Nasazení služby Managed Detection & Response, jedná se o bezpečnostní dohled nad detekovanými incidenty, včetně rychlé reakce.
Externí audit kybernetické bezpečnosti	Po vytvoření všech bezpečnostních politik, bezpečnostní dokumentace a nasazení dalších bezpečnostních nástrojů bude proveden audit kybernetické bezpečnosti. Cílem tohoto auditu je přezkoumání technické shody, posouzení souladu bezpečnostních opatření s nejlepší praxí, právními předpisy, vnitřními předpisy, jinými předpisy a smluvními závazky vztahujícími se k informačnímu a komunikačnímu systému.