NÁRODNÍ PLÁN OBNOVY

Financováno Evropskou unií
NextGenerationEU

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

Příloha č. 1 zadávací dokumentace – Technická specifikace

1. 1. Specifikace předmětu plnění

Příloha č. 1 smlouvy – Specifikace předmětu plnění

Vstupní audit

1.1. Identifikace regulovaných služeb v rámci NIS2 a určení úrovně povinností

a) Analýza služeb objednatele

1. Rozbor procesů a produktů objednatele
2. Identifikace všech služeb, které jsou dle nového zákona regulované

b) Určení velikosti objednatele ve smyslu NIS2

1. Rozbor holdingové struktury objednatele a určení s ním propojených osob
2. Zhodnocení velikosti objednatele (malý, střední, velký podnik) se zohledněním propojených osob

c) Určení úrovně povinností ve smyslu ZoKB/NIS2

1. Propojení identifikovaných regulovaných služeb a velikosti podniku, případně zvláštních oborových kritérií
2. Identifikace úrovně povinností objednatele dle nového ZoKB/NIS2.

d) Povinnosti dodavatele pro regulovanou službu

1. V případě, že v rámci předchozích kroků nebude identifikována povinnost objednatele, bude proveden základní rozbor smluvních a zákonných vztahů ve kterých vystupuje objednatel jako významný dodavatel/provozovatel nějaké regulované služby třetí strany.
2. Objednatel bude zařazen do úrovně povinností dle služby třetí osoby, na které se podílí.
3. Vytvoření mapy regulovaných služeb včetně určení jejich úrovně ze zákona a regulovaných služeb třetích stran v rámci kterých je objednatel v pozici významného dodavatele (registrovat se na NÚKIB, dodržovat politiky a pravidla objednatelovy organizace).

1.2. Popis stavu systému kybernetické bezpečnosti objednatele

a) Služba zajistí popis stavu systému kybernetické bezpečnosti (organizační, procesní a technická stránka) v jednotlivých oblastech regulace se zvláštním zaměřením a zvýšenou podrobností popisu v následujících oblastech:

1. Systém řízení bezpečnosti informací (§ 3 ZoKB) se zaměřením na dokumentaci, nastavení procesů a výkon rolí, včetně SW podpory systému řízení ISMS
2. Bezpečnost komunikačních sítí (§ 18 ZoKB) se zaměřením na stav oblasti nástrojů pro detekci kybernetických bezpečnostních událostí, síťový monitoring a reálný stav používaných aktivních prvků, wifi, zálohovací infrastruktury a síťovou ochranu detašovaných pracovišť,

3. Správa a ověřování identit (§ 19 ZoKB) se zaměřením na autentifikaci (vícefaktorovou autentifikaci), identity management a jeho správu v prostředí bezpečnostních nástrojů Microsoft,
4. Řízení přístupových oprávnění (§ 20) se zaměřením na autorizaci a řízení přístupových práv, zejména v prostředí bezpečnostních nástrojů Microsoft,
5. Ochrana před škodlivým kódem (§ 21 ZoKB) se zaměřením na funkčnost antimalwarové ochrany detašovaných pracovišť a poboček, faktickou funkčnost vulnerability managementu a funkčnost a implementaci bezpečnostních nástrojů prostředí Microsoft,
6. Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů (§ 22 ZoKB), Detekce kybernetických bezpečnostních událostí (§ 23 ZoKB) a Sběr a vyhodnocování kybernetických bezpečnostních událostí (§ 24 ZoKB) se zaměřením na systémy detekce nestandardního chování (XDR, EDR), kvalitu a dostatečnost standardního logování, síťový monitoring a schopnost zachycení a reakce na provozní/bezpečnostní anomálii /událost
7. Aplikační bezpečnost (§ 25) se zaměřením na faktickou funkčnost vulnerability managementu
8. Zajišťování úrovně dostupnosti informací (§ 27) se zaměřením na podrobný popis stavu dostupnosti a slabin primárního datového centra, aktivních síťových prvků, wifi infrastruktury a systému zálohování.

b) Výstupem tohoto kroku bude popis využitelný jako přesné zachycení stavu systému kybernetické bezpečnosti objednatele ke dni ukončení auditu.

1.3. Assessment souladu aktuálního stavu vůči ZoKB a novele ZoKB/NIS2

a) Služba zajistí komplexní zhodnocení organizace z hlediska povinností kybernetické bezpečnosti (stávající právní úpravy a také z pohledu nového zákona).

1.4. Stanovení opatření k nápravě

a) V návaznosti na audit budou dodavatelem identifikována a navržena obecná opatření k dosažení shody.

1.5. Dílo musí odpovídat právním předpisům a platným českým technickým normám, které se na něj vztahují, a to včetně technických norem, které nejsou obecně závazné.

Výstupní audit

1.6. Městská část Praha 14 bude v roce 2025 realizovat projekt „Posílení kybernetické bezpečnosti Úřadu městské části Praha 14“, v rámci něhož budou realizována následující technicko-organizační opatření:

a) ID01 Pokročilý síťový monitoring - Nástroj pro sběr, analýzu a ukládání síťových toků (netflow), detekci nestandardního síťového provozu a činnosti informačních systémů, jejich uživatelů a administrátorů,

b) ID02 Posílení primárního datového centra – redundance - posílení stávajících 3–4 node clusterů tak, aby byla zajištěna vysoká dostupnost a minimalizovány možné výpadky (SPOF),

c) ID03 Výměna a implementace aktivních síťových prvků - implementace moderního modulárního switche s podporou bezpečnostních funkcí,

d) ID04 Výměna a implementace WiFi infrastruktury - implementace moderních access pointů. Nejnovější standard 802.11be (WiFi 7). Nasazení WPA3 a případné nadstavby pro robustnější ochranu. Oddělená SSID a segmentace a centralizovaný monitoring a správa přístupových bodů a kontrolérů,

e) ID05 Výměna a implementace zálohovací infrastruktury – pásková knihovna 2x LTO 9, diskové pole 100TB, 2x NAS (redundantní), 100TB, 2x server pro zálohování (redundantní) a veškeré potřebné licence,

f) ID06 Zavedení systému řízení kybernetické bezpečnosti včetně sledování a vyhodnocování rizik a atributů na úrovni podpůrných aktiv a výkon role manažera KB – v rámci realizace opatření dojde k vytvoření dokumentace, nastavení procesů a rolí tak, aby byl žadatel plně v souladu s novelizací zákona č. 181/2014 Sb. – implementaci směrnice NIS2. Systém bude implementován do online provozovaného standardního nástroje,

g) ID07 Firewally pro detašovaná pracoviště – nákup osmi Next generation firewall pro pracovní skupiny/detašované pracoviště. Součástí dodávaného FW bude i dopovídající software a implementace,

h) ID08 Kompletní správa životního cyklu logů – pro zlepšení sběru, správy a ochrany logů (záznamů událostí) bude implementován pokročilý nástroj pro správu logů (log management). Nástroj bude automaticky sbírat, normalizovat a archivovat logy provozní i bezpečnostní povahy včetně infrastrukturních systémů. Systém bude obsahovat reportovací a notifikační systém. Notifikace bude možné navázat na výskyt provozní či bezpečnostní nestandardní události,

i) ID09 Automatická, periodická kontrola stavu bezpečnosti IT systémů a aplikací – Automatizované vyhledávání známých zranitelností (CVE) ve vnitřních i vnějších systémech. Reportování výsledků, generování přehledů o nalezených slabinách včetně doporučení k nápravě a přiřazení priorit. Integrace s ticketovacím systémem,

j) ID10 Konfigurace a implementace bezpečnostních funkcí prostředí Microsoft (Microsoft Entra ID PIM, MFA, AD hardening a zavedení bezpečnostních nástrojl office) - Konfigurace a implementace správy privilegovaných účtů, Centralizovaná kontrola uživatelů s rozšířenými oprávněními (administrátoři, servisní účty), Just-In-Time (JIT) přidělování, PAM – privileged access management, hardening Active Directory, pravidelné auditování, kontrola konfigurace, hesel a událostí v AD (logování). Vyšší úroveň ochrany identit, včetně adaptivních bezpečnostních politik. Multi-Factor Authentication (MFA). PLné nasazení a zkušební provoz Microsoft Defender for Office 365, Safe Attachments a Safe Links. Data Loss Prevention (DLP) - nastavení pravidel pro zamezení únikům citlivých informací (např. automatické blokace, šifrování),

k) ID11 Posílení dostupnosti primárního datového centra a zálohování - Zpětně uplatněné náklady na nákup tří serverů k zajištění HA datového centra, zálohovacího serveru a rozšíření diskového pole z roku 2023,

l) ID12 Bezpečnostní nástroje Microsoft Uplatnění perpetuálních licencí Microsoft Business Premium a Microsoft Defender for Business servers zakoupených v roce 2023, 2024 a obnovy licencí v roce 2025.

1.7. Cílem výstupního auditu bude kontrola stavu po provedených opatřeních

a) a podrobný popis situace v oblastech, kde byla realizována opatření v rámci dotačního projektu,

b) konstatování, zda došlo realizací opatření k posílení kybernetické bezpečnosti dotčených informačních a komunikačních systémů ve smyslu dotačního projektu.