Národní plán obnovy

Financováno Evropskou unií
NextGenerationEU

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

PŘÍLOHA č. 8

Analýza výchozího stavu

pro projekty výzvy č. 40 - 45

Analýza výchozího stavu

obsahující jednotlivá technická opatření

1. Základní informace o projektu

Žadatel - konečný příjemce (instituce)	Městská část Praha 14
IČ žadatele	00231312
Adresa žadatele	Bratří Venclíků 1073, 198 21 Praha 9
Správce rozpočtové kapitoly (instituce)	Ministerstvo vnitra ČR
Ředitel projektu	Ing. Martin Dušek Email: martin.dusek@praha14.cz; Tel: +420 608 431 472
Statutární zástupce organizace	Jiří Zajac Email: jiri.zajac@praha14.cz, Tel: +420 777 708 305
Název projektu	Posílení kybernetické bezpečnosti Úřadu městské části Praha 14

2. Podrobný popis výchozího stavu – problémy, které má realizace projektu vyřešit

Za současného stavu provozování IS a KS lze identifikovat následující **problémy v oblasti kybernetické bezpečnosti**:[1]

V oblasti systém řízení bezpečnosti informací (§ 3):
Výchozí situace – problémy, které má realizace projektu vyřešit: Městská část Praha 14 není aktuálně povinným subjektem podle ZoKB, nicméně se povinným stane s novelizací zákona (implementace NIS2) v druhé polovině roku 2024. V současné době Městská část Praha 14 postrádá jakýkoli ucelený systém řízení kybernetické bezpečnosti, což ji vystavuje značnému riziku kybernetických útoků a nesouladu s legislativními požadavky. Chybí zavedený systém ISMS dle standardů ISO/IEC 27001 a 27002, který by definoval jednotný rámec pro řízení rizik a bezpečnostních opatření. Organizace nemá obsazenou

[1] Žadatel vybere, ve které oblasti byly identifikovány problémy, které budou řešeny realizací předkládaného projektu a tyto problémy popíše. Dále popíše, jakými technickými opatřeními budou problémy řešeny.

klíčovou pozici manažera kybernetické bezpečnosti, což znamená, že neexistuje žádná koordinovaná strategie ochrany digitálních aktiv. Nedostatek pravidelných bezpečnostních auditů a přezkumů vede k neodhalování nových hrozeb a chyb v zabezpečení. Zaměstnanci nejsou dostatečně školeni v oblasti kybernetické bezpečnosti a neexistují jasně definované bezpečnostní směrnice, což zvyšuje riziko lidské chyby a úniku citlivých dat. ICT infrastruktura není systematicky monitorována a chybí přehled o kritičnosti jednotlivých systémů a souvisejících rizicích. Absence vazby na strukturovanou Configuration Management Database (CMDB) znemožňuje efektivní správu aktiv a jejich klasifikaci. Organizace také postrádá vazbu kybrnetické bezpečnosti na Enterprise Architecture přístup, který by umožnil lepší pochopení vztahů mezi informačními systémy, procesy a daty. Rizika nejsou pravidelně vyhodnocována a chybí systém pro systematické mapování hrozeb a určování prioritních opatření. Dokumentace bezpečnostních opatření a ICT prostředí je neaktuální a nepřehledná, což komplikuje rychlou reakci na bezpečnostní incidenty a ohrožuje kontinuitu provozu.

Opatření ID06 - Zavedení systému řízení kybernetické bezpečnosti včetně sledování a vyhodnocování rizik a atributů na úrovni podpůrných aktiv a výkon role manažera KB

Stručný popis opatření:
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 usnadňujícího následnou správu systému a plnění zákonných povinností včetně plného řízení aktiv a rizik a možnosti automatizovaně a dynamicky definovat případné nové normy formou katalogů hrozeb, zranitelností a opatření. Součástí opatření bude dodavatelské zajištění výkonu role osoby odpovědné za kybernetickou bezpečnost v organizaci žadatele.

Technický popis realizace opatření:

V rámci činnosti dodavatele bude vytvořen komplexní systém řízení bezpečnosti informací odpovídající povinnostem stanovených novelizací zákona č. 181/2014 Sb., o kybernetické bezpečnosti (implementace NIS2).

Vytvořená dokumentace musí jasně definovat odpovědnosti, jak pro organizační opatření (např. řízení přístupu, bezpečnost dodavatelského řetězce, správu změn a konfigurací), oblast lidských zdrojů (např. změna pracovního poměru, práce na dálku), tak opatření technická - fyzická bezpečnost (např. fyzický vstup, zabezpečení kanceláří, místností a vybavení) a technologická oblast (např. logování, oddělení sítí, kryptografie).

Součástí musí být také vytvoření základních metodických pokynů pro zaměstnance, dodavatele a třetí strany, které stanoví závazné postupy a pravidla pro bezpečné nakládání s informacemi a aktivy organizace. Výsledkem bude ucelený systém řízení bezpečnosti informací, podpořený odpovídající dokumentací, který zajistí soulad s požadavky NIS2 a umožní efektivní řízení bezpečnostních rizik. Součástí dodávky bude implementace systému do standardisovaného softwarového prostředí/platformy, které bude propojovat obecné výsledky a vytvořené postupy s reálnými daty z monitorovacích systémů provozovaných v prostředí zadavatele (např. servisdesk, logmanagement nebo monitoring).

Vytvořený systém v rámci online platformy musí podporovat provádění těchto činností v souladu s vybranými EU normami a jejich implementacemi do národních prostředí tedy standardy ISO 27001, NIS2, DORA, TISAX. V případě NIS a NIS2 bude podporovat jejich

implementace národní legislativy v podobě zákonů o kybernetické bezpečnosti a aktuálně chystaného zákona pro NIS2. Systém umožní automatizovaně a dynamicky definovat nové normy formou katalogů hrozeb, zranitelností a opatření. Součástí řešení musí být mapa aktiv a jejich souvztažností.

V případě kontroly ze strany NÚKIB bude systém obsahovat veškerou nutnou dokumentaci a záznamy v rámci dané úrovně povinností, včetně ad hoc generovaných záznamů v oblasti řízení aktiv a rizik např. plán opatření a aktivit (PoA), plán zvládání rizik (PZR) či zhodnocení rizik (ZHR).

V oblasti bezpečnost komunikačních sítí (§ 18):

Výchozí situace – problémy, které má realizace projektu vyřešit:
Městská část Praha 14 se aktuálně potýká s vážnými nedostatky v oblasti bezpečnosti komunikačních sítí, které představují významné riziko pro ochranu dat, dostupnost služeb a splnění legislativních požadavků dle NIS2 a novely zákona o kybernetické bezpečnosti. Většina síťových aktivních prvků a přístupových bodů pochází z let 2012–2016, což znamená, že jsou již bez bezpečnostních aktualizací a podpory, a tedy neschopné splnit současné standardy kybernetické bezpečnosti. Technologické zastarání znemožňuje efektivní mikrosegmentaci sítě, čímž dochází k nekontrolovatelnému pohybu dat a potenciálním bezpečnostním incidentům. Chybí prostředky pro segmentaci sítě, což vede k absenci důsledného řízení komunikace v rámci interních i externích připojení. Neexistence autentizačního systému dle standardu IEEE 802.1X znamená, že v síti mohou operovat neznámá a potenciálně nebezpečná zařízení bez jakékoli kontroly. Nedostatek pokročilých bezpečnostních nástrojů znemožňuje organizaci monitorovat síťový provoz a detekovat anomálie v reálném čase. V současné době není zajištěna důvěrnost a integrita dat při vzdáleném přístupu, protože síť nevyužívá moderní kryptografické mechanismy a šifrování. Organizace nemá efektivní řešení pro blokování nežádoucí komunikace, což zvyšuje riziko cílených útoků a neoprávněných přístupů. Síťová infrastruktura není dostatečně robustní pro ochranu proti DDoS útokům a jiným formám kybernetických hrozeb. Stávající WiFi infrastruktura není schopna splnit moderní bezpečnostní požadavky, protože nepodporuje nejnovější standardy, jako je WPA3 a WiFi 7, a neumožňuje oddělenou segmentaci SSID. Chybějící systém pro pokročilý monitoring síťových toků neumožňuje organizaci včas identifikovat podezřelé aktivity ani efektivně reagovat na bezpečnostní incidenty. Neexistence centralizované správy síťových prvků vede k roztříštěné infrastruktuře a složitému řízení bezpečnostních politik. V případě výpadku nebo kybernetického útoku nejsou zavedeny dostatečně robustní mechanismy pro obnovu dat a kontinuity provozu, což zvyšuje riziko dlouhodobé nefunkčnosti kritických systémů. Nejsou implementovány moderní firewallové prvky pro vzdálená pracoviště, což oslabuje perimetrální ochranu sítě a umožňuje potenciálním útočníkům snadnější průnik do interní infrastruktury. Absence centralizovaného řízení přístupu, pokročilé autentizace a šifrování představuje zásadní

bezpečnostní hrozbu, kterou je nutné bezodkladně řešit modernizací infrastruktury a implementací pokročilých bezpečnostních opatření.

Opatření ID01 - Pokročilý síťový monitoring

Stručný popis opatření:

Pro zajištění „viditelnosti síťového provozu“, detekci nestandardního síťového provozu a činnosti informačních systémů, jejich uživatelů a administrátorů na úrovni síťového provozu bude implementován nástroj pro sběr, analýzu a ukládání síťových toků (netflow). Síťové toky budou získávány ze zrcadlených portů (SPAN) síťových přepínačů a/nebo pomocí speciálních sond. Získané toky budou odesílány do kolektoru, který provede jejich zpracování, uložení a analýzu včetně detekce nestandardních či podezřelých síťových aktivit. Detekované události budou odesílány do centrálního nástroje správy logů a na potenciálně nebezpečné události bude upozorněn správce KS a případně obsluha externího SOC (Security operations center). Kolektor umožní vyhledávání v uložení historii síťového provozu, aby správci IS a KS i členové SOC týmu mohli systém využít při odhalování příčin a průběhů kybernetických událostí, ale i provozních problémů.

Technický popis realizace opatření:

Pro realizaci opatření bude pořízen systém pro sběr a vyhodnocování síťových toků. Požadavky na systém:

1. Server nebo hardwarová appliance pro sběr, ukládání a vyhodnocování síťových toků, předpokládané 2-3 místa sběru dat (sondy), trvalý výkon cca. 0,5-2 Gbit/s, 2000 toků/sec. Ukládání historie cca. 30 dnů
2. Software pro zaznamenávání a vyhodnocování síťových toků s detekcí nestandardní či nebezpečné komunikace

Součástí dodávky bude technická podpora výrobce včetně poskytování aktualizací a nových verzí software/firmware.

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

Opatření ID03 - Výměna a implementace aktivních síťových prvků

Stručný popis opatření:

Implementace moderních switchů. Switche s podporou bezpečnostních funkcí (např. ACL, ochrana proti DDoS na L2/L3 úrovni). Logická mikrosegmentace sítě a IPv6 ready a 802.1X, včetně centralizovaného managementu.

Technický popis realizace opatření:

HW: 1x Modulární switch

Chassis 5 slotů

Redundantní napájení

Redundantní chlazení

Moduly: 2x 48 portů 10G/25G, 1x 12 portů 40G/100G

SW: Součástí dodávaného HW, pokročilé funkce správy a směrování

Podpora: 6 Hrs CTR (Zahájení opravy do 6 hodin od nahlášení v místě instalace)

Implementace: Kompletní instalace a implementace v místě instalace.

Opatření ID04 - Výměna a implementace WiFi infrastruktury

Stručný popis opatření:

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.

Technický popis realizace opatření:

HW: 101 x AP, 17 x Switch, 9x Controller

Lokality: (Plechárna, KD Kyje, Gen. Jan., G14, KC Kardašovská, H55, Polyfunkční budova), Správa majetku, Bratří Venclíků 1073, 1072, 1070)

SW: Součástí dodávaného HW

Podpora: NBD (Následující pracovní den v místě instalace a/nebo vzdáleně)

Implementace: Kompletní instalace a implementace v místě instalace.

•Nejnovější standard 802.11be (WiFi 7)

Zajištění vysoké propustnosti, snížení latence a vyspělé správy šířky pásma pro rostoucí počet zařízení.

•Podpora bezpečnostních protokolů

Nasazení WPA3 a případné nadstavby pro robustnější ochranu (např. Enhanced Open, OWE).

•Oddělená SSID a segmentace

Samostatné sítě pro hosty, zaměstnance a IoT zařízení; zamezení nežádoucího pohybu v síti.

•Centralizovaný monitoring a management

Centralizovaná správa přístupových bodů a kontrolérů, integrace s dohledovými nástroji (SIEM/NMS).

Opatření ID05 - Výměna a implementace zálohovací infrastruktury

Stručný popis opatření:

Výměna stávající infrastruktury za moderní zálohovací systémy a úložiště. Nasazení vysoce dostupných řešení (disková a pásková), která umožňují rychlou obnovu a minimalizaci dopadu výpadku. Automatizace a pravidelné testy obnovy. Nastavení plánovaných záloh, průběžná kontrola konzistence a pravidelné testování disaster recovery scénářů. Šifrování záloh. Řízení kontinuity provozu ICT s důrazem na rychlou obnovu klíčových služeb.

Technický popis realizace opatření:

HW: Pásková knihovna 2x LTO 9, 40 pozic, včetně příslušenství pro optické připojení.

Diskové pole 100TB, optické připojení

2x NAS (redundantní), 100TB, optické připojení

2x server pro zálohování (redundantní napájení / chlazení, 1CPU, 2xSSD 480GB)

SW: Veškeré licence pro kompletní pokrytí zálohovaného hybridního prostředí na 60 měsíců

Podpora: NBD (Následující pracovní den v místě instalace a/nebo vzdáleně)

Implementace: Kompletní instalace a implementace v místě instalace.

Opatření ID07 - Firewally pro detašovaná pracoviště

Stručný popis opatření:

Instalace dedikovaných firewall, s centrálním managementem pro vzdálené lokality (detašovaná pracoviště). Bezpečnostní pravidla a VPN. Zajištění šifrovaného spojení s centrálou a jednotných pravidel pro přístup k aplikacím. Integrované IPS/IDS (Intrusion Prevention/Detection System) pro zachycení útoků v reálném čase. Kompatibilita s NIST CSF. Aplikace best practices pro ochranu sítě na perimetru. Centrální management, jednotné rozhraní pro konfiguraci a dohled, nasazování politik a vzdálený monitoring.

8 x NGFW pro pracovní skupiny / detašované pracoviště, Lokality: (Plechárna, KD Kyje, Gen. Jan., G14, KC Kardašovská, H55, Polyfunkční budova), Správa majetku), včetně odpovídajícího SW.

Technický popis realizace opatření:

HW: 8 x NGFW pro pracovní skupiny / detašované pracoviště

7x – minimální propustnost - Firewall Throughput (1518/512/64 byte UDP) 5/5/4 Gbps

1x – minimální propustnost - Firewall Throughput (1518/512/64 byte UDP) 10/10/6 Gbps

SW: Součástí dodávaného FW

Podpora: NBD (Následující pracovní den v místě instalace a/nebo vzdáleně)

Implementace: Kompletní instalace a implementace v místě instalace, včetně zajištění Site-To-Site VPN na centrální FW MČ Praha 14

V oblasti správy a ověřování identit (§ 19):

Výchozí situace – problémy, které má realizace projektu vyřešit:

V současné době Městská část Praha 14 postrádá robustní systém správy a ověřování identit, což představuje významné bezpečnostní riziko v oblasti přístupu k citlivým datům a klíčovým informačním systémům. Organizace nevyužívá pokročilé mechanismy správy privilegovaných účtů (PAM), což znamená, že administrátorské a servisní účty mají trvale vysoká oprávnění, čímž se zvyšuje riziko jejich zneužití nebo kompromitace. Chybí také Just-In-Time (JIT) model přidělování práv, což znamená, že uživatelé mají nadměrná

oprávnění i ve chvílích, kdy je nepotřebují. Active Directory není dostatečně zabezpečeno (hardening), neexistují pravidelné audity konfigurace, hesel ani aktivit v síti, což usnadňuje případné neoprávněné přístupy nebo interní hrozby. Organizace nemá povinně nasazené vícefaktorové ověřování (MFA), což výrazně snižuje odolnost vůči phishingovým útokům a neoprávněným pokusům o přihlášení. Bez adaptivních bezpečnostních politik nejsou identity chráněny proti podezřelým přístupům, například z neobvyklých míst nebo zařízení. Přestože organizace disponuje licencemi pro pokročilé bezpečnostní nástroje Microsoft, dosud je plně neimplementovala, čímž nevyužívá jejich potenciál pro ochranu dat a systémů. Nejsou nastavena pravidla pro Data Loss Prevention (DLP), což znamená, že citlivé informace mohou být volně sdíleny nebo odesílány mimo organizaci bez automatických kontrol a šifrování. Organizace také nevyužívá Microsoft Defender for Office 365 k ochraně proti pokročilým hrozbám, jako jsou škodlivé přílohy nebo odkazy v e-mailech. Absence komplexního řízení přístupu vede k neefektivnímu monitorování uživatelských aktivit a potenciálním bezpečnostním incidentům, které by mohly ohrozit provoz klíčových systémů.

Opatření ID10 - Konfigurace a implementace bezpečnostních funkcí prostředí Microsoft (Microsoft Entra ID PIM, MFA, AD hardening a zavedení bezpečnostních nástrojů office)

Stručný popis opatření:

Konfigurace a implementace bezpečnostních funkcí v existujícím prostředí Microsoft – již vlastněných žadatelem v rámci perpetuálních licencí. Specificky správy privilegovaných účtů (PAM). Just-In-Time (JIT). Hardening Active Directory - nastavení pravidelného auditování, kontrola konfigurace, hesel a událostí. 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).

Technický popis realizace opatření:

Implementace: Kompletní instalace a implementace v prostředí, včetně zajištění napojení na další systémy v souladu se standardy.

Poznámka: 250 uživatelů, více než 500 koncových zařízení (stanice, NTB, tablety, mobily ad.), 60 serverů (fyzických i virtuálních). Více než 100 privilegovaných / servisních účtů. Podpora federovaných identit ad.

•Správa privilegovaných účtů

Centralizovaná kontrola uživatelů s rozšířenými oprávněními (administrátoři, servisní účty).

•Just-In-Time (JIT) přidělování práv - udělení vyšších oprávnění pouze na nezbytně nutnou dobu.

•Audit a schvalování Každá žádost o privilegovaný přístup podléhá schválení a je auditována.

•V souladu s ISO/IEC 27001 Řízení přístupu k důležitým systémům a rizikům spojeným s privilegovanými účty.

Pokročilé ověřování - důraz na protokol Kerberos a vyšší úroveň ochrany identit, včetně adaptivních bezpečnostních politik.

•Zavedení Multi-Factor Authentication (MFA) - Povinné dvou- nebo vícefaktorové ověření pro přístup k citlivým aplikacím a službám.

•Podpora různých autentizačních metod (mobilní aplikace, SMS, HW tokeny, biometrika). Flexibilní přístup pro uživatele, přizpůsobení potřebám (např. čipové karty, biometrika).

•Snížení rizika kompromitace účtů - ři úniku hesel zůstává účet chráněn dodatečnou vrstvou zabezpečení.

ID12 - Bezpečnostní nástroje Microsoft

Stručný popis opatření:

Žadatel v roce 2023 navýšil úrovně perpetuálních licencí produktů Microsoft z úrovně Standard na Microsoft Business Premium a zakoupil Microsoft Defender for Business servers. V rámci povýšení licencí došlo k výraznému posílení kyberntické bezpečnosti žadatele, ač nejsou licencované nástroje zcela implementovány a zkušebně odladěny. Žadatel zpětně uplatňuje upgrade licencí a zároveň jejich obnovu na období od 1.3.2025 do 31.5.2026.

Technický popis realizace opatření:

Smlouva	Licence	Počet licencí	Dní
30.10.2023	**Microsoft 365 Business PREMIUM - roční**	1	42
30.10.2023	**Microsoft 365 Business PREMIUM - měsíční**	9	42
30.10.2023	**Microsoft 365 Business PREMIUM - roční**	223	127
15.03.2024	**Microsoft 365 Business PREMIUM - roční**	223	365
15.03.2024	**Microsoft Defender for Business servers**	60	156
Obnova 2025	**Microsoft 365 Business PREMIUM - roční**	223	456
Obnova 2025	**Microsoft Defender for Business servers**	60	456

Licence Microsoft 365 Business PREMIUM obsahuje následující bezpečnostní funkce:

•Správa privilegovaných účtů

Centralizovaná kontrola uživatelů s rozšířenými oprávněními (administrátoři, servisní účty).

•Just-In-Time (JIT) přidělování práv - udělení vyšších oprávnění pouze na nezbytně nutnou dobu.

•Audit a schvalování Každá žádost o privilegovaný přístup podléhá schválení a je auditována.

•V souladu s ISO/IEC 27001 Řízení přístupu k důležitým systémům a rizikům spojeným s privilegovanými účty.

Pokročilé ověřování - důraz na protokol Kerberos a vyšší úroveň ochrany identit, včetně adaptivních bezpečnostních politik.

•Zavedení Multi-Factor Authentication (MFA) - Povinné dvou- nebo vícefaktorové ověření pro přístup k citlivým aplikacím a službám.

•Podpora různých autentizačních metod (mobilní aplikace, SMS, HW tokeny, biometrika). Flexibilní přístup pro uživatele, přizpůsobení potřebám (např. čipové karty, biometrika).

•Snížení rizika kompromitace účtů - ři úniku hesel zůstává účet chráněn dodatečnou vrstvou zabezpečení.

V oblasti řízení přístupových oprávnění (§ 20):

Výchozí situace – problémy, které má realizace projektu vyřešit:

Městská část Praha 14 v současnosti čelí závažným nedostatkům v oblasti řízení přístupových oprávnění, které výrazně zvyšují riziko neoprávněného přístupu k citlivým datům a systémům. Neexistuje centralizovaný systém pro správu privilegovaných účtů (PAM), což znamená, že administrátorské účty mají trvale vysoká oprávnění bez jakéhokoli omezení nebo dohledu. Chybí implementace Just-In-Time (JIT) modelu, který by umožnil přidělování rozšířených oprávnění pouze po nezbytně nutnou dobu, čímž by se snížilo riziko jejich zneužití. Organizace nemá zavedený systematický audit a schvalovací proces pro přidělování oprávnění, což vede k netransparentnímu řízení přístupů a potenciálním bezpečnostním incidentům. Active Directory není dostatečně zabezpečeno (hardening), přičemž nejsou zakázány zastaralé protokoly, jako je NTLM a SMBv1, což zvyšuje zranitelnost vůči útokům typu Pass-the-Hash. Chybí také pravidelné auditování a monitorování událostí v AD, což znamená, že neexistuje efektivní způsob odhalování podezřelých aktivit a neobvyklých přístupů. Organizace nevyužívá pokročilé ověřovací mechanismy, jako je Multi-Factor Authentication (MFA), což umožňuje snadné zneužití účtů v případě úniku hesel. Chybí adaptivní bezpečnostní politiky, které by zohledňovaly rizikové přihlašovací pokusy, například z neznámých zařízení nebo geografických lokalit. Přestože organizace disponuje pokročilými bezpečnostními nástroji Microsoft v rámci Business Premium licencí, dosud nebyly plně implementovány a odladěny. Absence efektivního řízení přístupových oprávnění tak představuje zásadní bezpečnostní riziko, které je nutné neodkladně řešit modernizací identitní správy a posílením bezpečnostních politik.

Opatření ID10 - Konfigurace a implementace bezpečnostních funkcí prostředí Microsoft (Microsoft Entra ID PIM, MFA, AD hardening a zavedení bezpečnostních nástrojů office)

Stručný popis opatření:
Konfigurace a implementace bezpečnostních funkcí v existujícím prostředí Microsoft – již vlastněných žadatelem v rámci perpetuálních licencí. Specificky správy privilegovaných účtů (PAM). Just-In-Time (JIT). Hardening Active Directory - nastavení pravidelného auditování, kontrola konfigurace, hesel a událostí. 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).

Technický popis realizace opatření:
Implementace: Kompletní instalace a implementace v prostředí, včetně zajištění napojení na další systémy v souladu se standardy.

•Správa privilegovaných účtů

Centralizovaná kontrola uživatelů s rozšířenými oprávněními (administrátoři, servisní účty).

•Just-In-Time (JIT) přidělování práv - udělení vyšších oprávnění pouze na nezbytně nutnou dobu.

•Audit a schvalování Každá žádost o privilegovaný přístup podléhá schválení a je auditována.

•V souladu s ISO/IEC 27001 Řízení přístupu k důležitým systémům a rizikům spojeným s privilegovanými účty.

•Bezpečnostní nastavení Active Directory - zákaz nevyužívaných protokolů (NTLM, SMBv1), komplexní GPO politiky a omezení útoků typu Pass-the-Hash.

•Pravidelné auditování, kontrola konfigurace, hesel, událostí v AD (logování), odhalení neobvyklých událostí.

•CIS Benchmarks - postupy pro nastavení bezpečného AD prostředí, např. omezení privilegovaných skupin.

•Pokročilé ověřování - důraz na protokol Kerberos a vyšší úroveň ochrany identit, včetně adaptivních bezpečnostních politik.

•V souladu s doporučeními CIS Benchmarks - benchmarks pro Active Directory a pravidly NIST SP 800-53.

•Snížení rizika kompromitace účtů - při úniku hesel zůstává účet chráněn dodatečnou vrstvou zabezpečení.

ID12 - Bezpečnostní nástroje Microsoft

Stručný popis opatření:

Žadatel v roce 2023 navýšil úrovně perpetuálních licencí produktů Microsoft z úrovně Standard na Microsoft Business Premium a zakoupil Microsoft Defender for Business servers. V rámci povýšení licencí došlo k výraznému posílení kyberntické bezpečnosti žadatele, ač nejsou licencované nástroje zcela implementovány a zkušebně odladěny. Žadatel zpětně uplatňuje upgrade licencí a zároveň jejich obnovu na období od 1.3.2025 do 31.5.2026.

Technický popis realizace opatření:

Smlouva	Licence	Počet licencí	Dní
30.10.2023	**Microsoft 365 Business PREMIUM - roční**	1	42
30.10.2023	**Microsoft 365 Business PREMIUM - měsíční**	9	42
30.10.2023	**Microsoft 365 Business PREMIUM - roční**	223	127
15.03.2024	**Microsoft 365 Business PREMIUM - roční**	223	365
15.03.2024	**Microsoft Defender for Business servers**	60	156
Obnova 2025	**Microsoft 365 Business PREMIUM - roční**	223	456
Obnova 2025	**Microsoft Defender for Business servers**	60	456

Licence Microsoft 365 Business PREMIUM obsahuje následující bezpečnostní funkce:

•Správa privilegovaných účtů

Centralizovaná kontrola uživatelů s rozšířenými oprávněními (administrátoři, servisní účty).

•Just-In-Time (JIT) přidělování práv - udělení vyšších oprávnění pouze na nezbytně nutnou dobu.

•Audit a schvalování Každá žádost o privilegovaný přístup podléhá schválení a je auditována.

•V souladu s ISO/IEC 27001 Řízení přístupu k důležitým systémům a rizikům spojeným s privilegovanými účty.

•Bezpečnostní nastavení Active Directory - zákaz nevyužívaných protokolů (NTLM, SMBv1), komplexní GPO politiky a omezení útoků typu Pass-the-Hash.

•Pravidelné auditování, kontrola konfigurace, hesel, událostí v AD (logování), odhalení neobvyklých událostí.

•CIS Benchmarks - postupy pro nastavení bezpečného AD prostředí, např. omezení privilegovaných skupin.

•Pokročilé ověřování - důraz na protokol Kerberos a vyšší úroveň ochrany identit, včetně adaptivních bezpečnostních politik.

•V souladu s doporučeními CIS Benchmarks - benchmarks pro Active Directory a pravidly NIST SP 800-53.

•Snížení rizika kompromitace účtů - při úniku hesel zůstává účet chráněn dodatečnou vrstvou zabezpečení.

V oblasti ochrana před škodlivým kódem (§ 21):

Výchozí situace – problémy, které má realizace projektu vyřešit:

Městská část Praha 14 v současné době čelí zásadním nedostatkům v oblasti ochrany před škodlivým kódem, což výrazně zvyšuje riziko napadení informačních systémů malwarem, ransomwarem a dalšími kybernetickými hrozbami. Organizace nemá implementováno efektivní zabezpečení vzdálených pracovišť, což vede k nedostatečné kontrole nad síťovou komunikací a možností šifrovaného připojení k interním systémům. Chybí pokročilé bezpečnostní prvky, jako jsou integrované systémy prevence a detekce průniků (IPS/IDS), které by umožnily včasné zachycení a blokování škodlivých aktivit. Současné firewally nejsou schopny efektivně filtrovat škodlivý provoz, což zvyšuje pravděpodobnost šíření malwaru v rámci organizace. Neexistuje také pravidelný a automatizovaný monitoring bezpečnostních zranitelností, což znamená, že zranitelná zařízení (a existujícími exploity) nejsou včas identifikována a zabezpečena. Ochrana e-mailové komunikace je nedostatečná, protože nejsou nasazeny moderní nástroje, jako jsou Safe Attachments a Safe Links, které by dynamicky kontrolovaly přílohy a odkazy na škodlivé URL. Organizace také nevyužívá pokročilé antimalwarové řešení na úrovni koncových zařízení a serverů, čímž je zranitelná vůči cíleným útokům. Chybí systematická implementace Microsoft Defender for Office 365, který by mohl automaticky detekovat phishingové útoky a podezřelé aktivity v e-mailové komunikaci. Neexistence centralizovaného řízení a auditu

bezpečnostních politik vede k nekontrolovanému přístupu uživatelů k citlivým datům a aplikacím. Všechny tyto faktory způsobují, že organizace není dostatečně chráněna před moderními kybernetickými hrozbami, což vyžaduje urychlenou implementaci plánovaných bezpečnostních opatření.

Opatření ID07 - Firewally pro detašovaná pracoviště

Stručný popis opatření:

Instalace dedikovaných firewall, s centrálním managementem pro vzdálené lokality (detašovaná pracoviště). Bezpečnostní pravidla a VPN. Zajištění šifrovaného spojení s centrálou a jednotných pravidel pro přístup k aplikacím. Integrované IPS/IDS (Intrusion Prevention/Detection System) pro zachycení útoků v reálném čase. Kompatibilita s NIST CSF. Aplikace best practices pro ochranu sítě na perimetru. Centrální management, jednotné rozhraní pro konfiguraci a dohled, nasazování politik a vzdálený monitoring.

8 x NGFW pro pracovní skupiny / detašované pracoviště, Lokality: (Plechárna, KD Kyje, Gen. Jan., G14, KC Kardašovská, H55, Polyfunkční budova), Správa majetku), včetně odpovídajícího SW.

Technický popis realizace opatření:

HW: 8 x NGFW pro pracovní skupiny / detašované pracoviště

7x – minimální propustnost - Firewall Throughput (1518/512/64 byte UDP) 5/5/4 Gbps

1x – minimální propustnost - Firewall Throughput (1518/512/64 byte UDP) 10/10/6 Gbps

SW: Součástí dodávaného FW

Podpora: NBD (Následující pracovní den v místě instalace a/nebo vzdáleně)

Implementace: Kompletní instalace a implementace v místě instalace, včetně zajištění Site-To-Site VPN na centrální FW MČ Praha 14

Opatření ID09 Automatická, periodická kontrola stavu bezpečnosti IT systémů a aplikací

Stručný popis opatření:

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. Soulad s ISO/IEC 27002 (řízení technických zranitelností) a NIST SP 800-40. "

Technický popis realizace opatření:

Cca. 700 monitorovaných zařízení

Podpora: NBD (Následující pracovní den v místě instalace a/nebo vzdáleně)

Implementace: Kompletní instalace a implementace v místě instalace.

•Pravidelné skenování

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

Přímé vytváření úkolů pro zodpovědné týmy; sledování průběhu jejich řešení.

•Soulad s ISO/IEC 27002 (řízení technických zranitelností) a NIST SP 800-40."

Opatření ID10 - Konfigurace a implementace bezpečnostních funkcí prostředí Microsoft (Microsoft Entra ID PIM, MFA, AD hardening a zavedení bezpečnostních nástrojů office)

Stručný popis opatření:
Konfigurace a implementace bezpečnostních funkcí v existujícím prostředí Microsoft – již vlastněných žadatelem v rámci perpetuálních licencí. Specificky správy privilegovaných účtů (PAM). Just-In-Time (JIT). Hardening Active Directory - nastavení pravidelného auditování, kontrola konfigurace, hesel a událostí. 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).

Technický popis realizace opatření:
Implementace: Kompletní instalace a implementace v prostředí, včetně zajištění napojení na další systémy v souladu se standardy.

Poznámka: 250 uživatelů, více než 500 koncových zařízení (stanice, NTB, tablety, mobily ad.), 60 serverů (fyzických i virtuálních). Více než 100 privilegovaných / servisních účtů. Podpora federovaných identit ad.

•Microsoft Defender for Office 365 - pokročilá ochrana proti phishingu, ransomwaru a malwaru s automatickým vyhodnocením hrozeb.

•Safe Attachments a Safe Links - dynamická kontrola příloh a odkazů v e-mailech, prevence proti exploitům a škodlivým URL.

ID12 - Bezpečnostní nástroje Microsoft

Stručný popis opatření:
Žadatel v roce 2023 navýšil úrovně perpetuálních licencí produktů Microsoft z úrovně Standard na Microsoft Business Premium a zakoupil Microsoft Defender for Business servers. V rámci povýšení licencí došlo k výraznému posílení kyberntické bezpečnosti žadatele, ač nejsou licencované nástroje zcela implementovány a zkušebně odladěny. Žadatel zpětně uplatňuje upgrade licencí a zároveň jejich obnovu na období od 1.3.2025 do 31.5.2026.

Technický popis realizace opatření:

Smlouva	Licence	Počet licencí	Dní

30.10.2023	**Microsoft 365 Business PREMIUM - roční**	1	42
30.10.2023	**Microsoft 365 Business PREMIUM - měsíční**	9	42
30.10.2023	**Microsoft 365 Business PREMIUM - roční**	223	127
15.03.2024	**Microsoft 365 Business PREMIUM - roční**	223	365
15.03.2024	**Microsoft Defender for Business servers**	60	156
Obnova 2025	**Microsoft 365 Business PREMIUM - roční**	223	456
Obnova 2025	**Microsoft Defender for Business servers**	60	456

Licence Microsoft 365 Business PREMIUM obsahuje následující bezpečnostní funkce:

•Microsoft Defender for Office 365 - pokročilá ochrana proti phishingu, ransomwaru a malwaru s automatickým vyhodnocením hrozeb.

•Safe Attachments a Safe Links - dynamická kontrola příloh a odkazů v e-mailech, prevence proti exploitům a škodlivým URL.

Součástí je i antimalwarová ochrana formou Microsoft Defender for Business servers.

V oblasti zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů (§ 22):

Výchozí situace – problémy, které má realizace projektu vyřešit:

Městská část Praha 14 v současnosti čelí zásadním nedostatkům v oblasti zaznamenávání a správy událostí v informačních a komunikačních systémech, což výrazně snižuje její schopnost detekovat a reagovat na bezpečnostní incidenty. Chybí centrální systém pro sběr, analýzu a archivaci logů, což znamená, že události v síti, činnost uživatelů a administrátorů nejsou efektivně monitorovány ani uchovávány pro následnou forenzní analýzu. Neexistuje automatizovaný mechanismus pro detekci nestandardního síťového provozu, což znemožňuje včasné odhalení podezřelých aktivit nebo kybernetických útoků. Logy z jednotlivých systémů nejsou centralizovaně ukládány ani chráněny proti neoprávněné manipulaci, což ztěžuje jejich využití jako důkazního materiálu při vyšetřování bezpečnostních incidentů. Organizace nemá implementovaný systém pokročilé analýzy síťových toků (NetFlow), který by umožňoval identifikaci anomálií v reálném čase. Chybí také strukturovaný přístup ke správě životního cyklu logů, což vede k jejich nekonzistentnímu uchovávání a absenci pravidelného vyhodnocování bezpečnostních událostí. Současné řešení neumožňuje efektivní notifikaci správců IT a bezpečnostních týmů při výskytu kritických událostí, což prodlužuje reakční dobu na kybernetické hrozby. Absence pokročilého systému správy logů znamená, že organizace není schopna v souladu s legislativními požadavky archivovat logy po předepsanou dobu a zajistit jejich integritu. Neexistence strojového učení a automatizované analýzy logů omezuje schopnost odhalovat pokročilé útoky a vnitřní hrozby. Tyto zásadní nedostatky vyžadují neodkladnou implementaci plánovaných opatření, která posílí monitorování a ochranu ICT infrastruktury proti moderním kybernetickým hrozbám. Žadatel nevyužívá pro ochranu sítě žádnou formu provozního ani bezpečnostního síťového monitoringu, nevyhodnocuje síťový provoz a nedetekuje provozní anomálie/bezpečnostní události a případné bezpečnostní incidenty.

Opatření ID01 - Pokročilý síťový monitoring

Stručný popis opatření:

Pro zajištění „viditelnosti síťového provozu“, detekci nestandardního síťového provozu a činnosti informačních systémů, jejich uživatelů a administrátorů na úrovni síťového provozu bude implementován nástroj pro sběr, analýzu a ukládání síťových toků (netflow). Síťové toky budou získávány ze zrcadlených portů (SPAN) síťových přepínačů a/nebo pomocí speciálních sond. Získané toky budou odesílány do kolektoru, který provede jejich zpracování, uložení a analýzu včetně detekce nestandardních či podezřelých síťových aktivit. Detekované události budou odesílány do centrálního nástroje správy logů a na potenciálně nebezpečné události bude upozorněn správce KS a případně obsluha externího SOC (Security operations center). Kolektor umožní vyhledávání v uložení historii síťového provozu, aby správci IS a KS i členové SOC týmu mohli systém využít při odhalování příčin a průběhů kybernetických událostí, ale i provozních problémů.

Technický popis realizace opatření:

Pro realizaci opatření bude pořízen systém pro sběr a vyhodnocování síťových toků. Požadavky na systém:

1. Server nebo hardwarová appliance pro sběr, ukládání a vyhodnocování síťových toků, předpokládané 2-3 místa sběru dat (sondy), trvalý výkon cca. 1-2 Gbit/s, 2000 toků/sec. Ukládání historie cca. 30 dnů

2. Software pro zaznamenávání a vyhodnocování síťových toků s detekcí nestandardní či nebezpečné komunikace

Součástí dodávky bude technická podpora výrobce včetně poskytování aktualizací a nových verzí software/firmware.

Opatření ID08 Kompletní správa životního cyklu logů

Stručný popis opatření:

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. Sbírané logy budou tříděny pomocí strojového učení za účelem správného parsování a normalizace. Uložené logy budou chráněny proti neoprávněným změnám, a to i v případě archivace. Archivované logy budou komprimovány na maximálně 5% jejich původní velikosti. Uložené logy bude možné snadno prohledávat či filtrovat na základě multikriteriálních dotazů napříč zdroji logů a to včetně logů uložených v komprimovaném archivu. Systém bude obsahovat reportovací a notifikační systém. Notifikace bude možné navázat na výskyt provozní či bezpečnostní nestandardní události.

Technický popis realizace opatření:

• hardwarové appliance s možností zajištění režimu vysoké dostupnosti doplněné virtuálním arbitrem včetně software/firmware pro kompletní správu životního cyklu logů

• systém typu „log management“ pro komplexní správu životního cyklu logů s úložištěm pro ukládání 18 měsíční historie a podporou komprimované archivace, zajištění integrity a nezpochybnitelnosti aktuálních i archivovaných dat pomocí digitálních podpisů vstupních "raw" logů

• systém bude provozován na vyhrazeném hardware pro zachování schopnosti logování nezávisle na běhu ostatních prvků

• systém bude obsahovat integrační konektory / parsery dodávaných a udržovaných výrobcem hlavních používaných IT technologií TC z důvodu minimalizace vývoje a údržby vlastních konektorů / parserů

• sběr logů bude plně bez-agentový, tj. bez nutnosti instalace jakéhokoliv software mimo hardware vyhrazená pro log management

• součástí dodávky bude technická podpora výrobce včetně poskytování aktualizací a nových verzí software/firmware.

V oblasti detekce kybernetických bezpečnostních událostí (§ 23):

Výchozí situace – problémy, které má realizace projektu vyřešit:

Městská část Praha 14 v současné době postrádá efektivní systém detekce kybernetických bezpečnostních událostí, což výrazně zvyšuje riziko pozdního odhalení útoků a bezpečnostních incidentů. Organizace nemá implementován centralizovaný nástroj pro monitoring síťového provozu, což znamená, že nedochází k systematickému sledování anomálií nebo podezřelých aktivit v interní i externí síti. Chybí také mechanismus pro sběr a analýzu síťových toků (NetFlow), který by umožnil identifikovat neobvyklé vzorce chování, jako jsou pokusy o neoprávněný přístup, šíření malwaru nebo pokusy o exfiltraci dat. Neexistuje propojení mezi detekovanými událostmi a systémem správy logů, což ztěžuje korelaci bezpečnostních událostí a jejich efektivní vyšetřování. Logy z kritických systémů nejsou automaticky ukládány a analyzovány v reálném čase, což znamená, že organizace není schopna rychle reagovat na potenciální hrozby. Nedostatečné zabezpečení logů a absence mechanismů pro jejich archivaci a ochranu proti neoprávněným změnám způsobuje, že organizace nemá důvěryhodný zdroj informací pro forenzní analýzu. Chybí také automatizovaný systém notifikací, který by upozornil správce IT na podezřelé aktivity, což prodlužuje reakční dobu na bezpečnostní incidenty. Stávající prostředí neumožňuje využití pokročilých metod, jako je strojové učení pro analýzu vzorců síťového provozu, což by mohlo pomoci při identifikaci sofistikovaných kybernetických hrozeb. Organizace není schopna v souladu s legislativními požadavky ukládat a analyzovat logy po předepsanou dobu, což zvyšuje její zranitelnost a ohrožuje schopnost splnit požadavky NIS2 a novely zákona o kybernetické bezpečnosti. Tyto nedostatky jasně ukazují na nutnost implementace plánovaných opatření, která posílí detekci kybernetických hrozeb a umožní rychlejší reakci na bezpečnostní incidenty.

Opatření ID01 Monitoring síťového provozu
Stručný popis opatření:

Pro zajištění „viditelnosti síťového provozu“, detekci nestandardního síťového provozu a činnosti informačních systémů, jejich uživatelů a administrátorů na úrovni síťového provozu bude implementován nástroj pro sběr, analýzu a ukládání síťových toků (netflow). Síťové toky budou získávány ze zrcadlených portů (SPAN) síťových přepínačů a/nebo pomocí speciálních sond. Získané toky budou odesílány do kolektoru, který provede jejich zpracování, uložení a analýzu včetně detekce nestandardních či podezřelých síťových aktivit. Detekované události budou odesílány do centrálního nástroje správy logů a na potenciálně nebezpečné události bude upozorněn správce KS a případně obsluha externího SOC (Security operations center). Kolektor umožní vyhledávání v uložení historii síťového provozu, aby správci IS a KS i členové SOC týmu mohli systém využít při odhalování příčin a průběhů kybernetických událostí, ale i provozních problémů.

Technický popis realizace opatření:

Pro realizaci opatření bude pořízen systém pro sběr a vyhodnocování síťových toků. Požadavky na systém:

1. Server nebo hardwarová appliance pro sběr, ukládání a vyhodnocování síťových toků, předpokládané 2-3 místa sběru dat (sondy), trvalý výkon cca. 1-2 Gbit/s, 2000 toků/sec. Ukládání historie cca. 30 dnů
2. Software pro zaznamenávání a vyhodnocování síťových toků s detekcí nestandardní či nebezpečné komunikace
3. Součástí dodávky bude technická podpora výrobce včetně poskytování aktualizací a nových verzí software/firmware.

Opatření ID08 Kompletní správa životního cyklu logů

Stručný popis opatření:

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. Sbírané logy budou tříděny pomocí strojového učení za účelem správného parsování a normalizace. Uložené logy budou chráněny proti neoprávněným změnám, a to i v případě archivace. Archivované logy budou komprimovány na maximálně 5% jejich původní velikosti. Uložené logy bude možné snadno prohledávat či filtrovat na základě multikriteriálních dotazů napříč zdroji logů a to včetně logů uložených v komprimovaném archivu. Systém bude obsahovat reportovací a notifikační systém. Notifikace bude možné navázat na výskyt provozní či bezpečnostní nestandardní události.

Technický popis realizace opatření:

- hardwarové appliance s možností zajištění režimu vysoké dostupnosti doplněné virtuálním arbitrem včetně software/firmware pro kompletní správu životního cyklu logů
- systém typu „log management“ pro komplexní správu životního cyklu logů s úložištěm pro ukládání 18 měsíční historie a podporou komprimované archivace, zajištění integrity a nezpochybnitelnosti aktuálních i archivovaných dat pomocí digitálních podpisů vstupních "raw" logů
- systém bude provozován na vyhrazeném hardware pro zachování schopnosti logování nezávisle na běhu ostatních prvků

• systém bude obsahovat integrační konektory / parsery dodávaných a udržovaných výrobcem hlavních používaných IT technologií TC z důvodu minimalizace vývoje a údržby vlastních konektorů / parserů
• sběr logů bude plně bez-agentový, tj. bez nutnosti instalace jakéhokoliv software mimo hardware vyhrazená pro log management
• součástí dodávky bude technická podpora výrobce včetně poskytování aktualizací a nových verzí software/firmware.

Sběr a vyhodnocování kybernetických bezpečnostních událostí (§ 24):

Výchozí situace – problémy, které má realizace projektu vyřešit:

Městská část Praha 14 v současné době postrádá ucelený systém pro sběr, analýzu a vyhodnocování kybernetických bezpečnostních událostí, což výrazně snižuje její schopnost efektivně reagovat na bezpečnostní incidenty. Neexistuje centralizovaný nástroj pro správu logů, což znamená, že záznamy z různých systémů nejsou shromažďovány na jednom místě a není možné je efektivně analyzovat. Chybí mechanismus pro automatickou normalizaci a třídění logů, což vede k nekonzistentnímu uchovávání dat a komplikovanému vyhledávání relevantních informací. Nejsou implementovány pokročilé metody analýzy, jako je strojové učení, které by mohly pomoci identifikovat anomálie a potenciální bezpečnostní hrozby v reálném čase. Ukládané logy nejsou dostatečně chráněny proti neoprávněným změnám, což ohrožuje jejich integritu a využitelnost při forenzních analýzách. Organizace nemá zavedený efektivní systém notifikací, který by okamžitě upozornil odpovědné pracovníky na kritické bezpečnostní události. Chybí také možnost dlouhodobé archivace logů v souladu s legislativními požadavky, což znamená, že organizace nesplňuje podmínky stanovené směrnicí NIS2 a novelou zákona o kybernetické bezpečnosti. Nedostatečná viditelnost událostí v informačních systémech způsobuje, že kybernetické útoky mohou být detekovány se zpožděním, což výrazně zvyšuje jejich potenciální dopad. Neexistence centralizovaného systému také ztěžuje dohled a audit bezpečnostních opatření, což oslabuje celkovou odolnost organizace vůči kybernetickým hrozbám. Tyto nedostatky jasně ukazují na nutnost implementace plánovaných opatření, která umožní efektivní sběr a vyhodnocování bezpečnostních událostí v souladu s moderními standardy kybernetické bezpečnosti.

Opatření ID08 Kompletní správa životního cyklu logů

Stručný popis opatření:

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. Sbírané logy budou tříděny pomocí strojového učení za účelem správného parsování a normalizace. Uložené logy budou chráněny proti neoprávněným změnám, a to i v případě archivace. Archivované logy budou komprimovány na maximálně 5% jejich původní velikosti. Uložené logy bude možné snadno prohledávat či filtrovat na základě multikriteriálních dotazů napříč zdroji logů a to včetně logů uložených v komprimovaném

archivu. Systém bude obsahovat reportovací a notifikační systém. Notifikace bude možné navázat na výskyt provozní či bezpečnostní nestandardní události.

Technický popis realizace opatření:
• hardwarové appliance s možností zajištění režimu vysoké dostupnosti doplněné virtuálním arbitrem včetně software/firmware pro kompletní správu životního cyklu logů
• systém typu „log management“ pro komplexní správu životního cyklu logů s úložištěm pro ukládání 18 měsíční historie a podporou komprimované archivace, zajištění integrity a nezpochybnitelnosti aktuálních i archivovaných dat pomocí digitálních podpisů vstupních "raw" logů
• systém bude provozován na vyhrazeném hardware pro zachování schopnosti logování nezávisle na běhu ostatních prvků
• systém bude obsahovat integrační konektory / parsery dodávaných a udržovaných výrobcem hlavních používaných IT technologií TC z důvodu minimalizace vývoje a údržby vlastních konektorů / parserů
• sběr logů bude plně bez-agentový, tj. bez nutnosti instalace jakéhokoliv software mimo hardware vyhrazená pro log management
• součástí dodávky bude technická podpora výrobce včetně poskytování aktualizací a nových verzí software/firmware.

Aplikační bezpečnost (§ 25):

Výchozí situace – problémy, které má realizace projektu vyřešit:
Městská část Praha 14 v současnosti čelí významným nedostatkům v oblasti aplikační bezpečnosti, což představuje zvýšené riziko pro její informační systémy a citlivá data. Neexistuje systematický proces pro pravidelnou kontrolu technických zranitelností, což znamená, že bezpečnostní slabiny v aplikacích, operačních systémech a komunikačních protokolech zůstávají neodhaleny a neopraveny. Chybí mechanismus pro pravidelné testování odolnosti aplikací proti kybernetickým útokům, což organizaci vystavuje nebezpečí zneužití zranitelností ze strany útočníků. Nejsou prováděny penetrační testy ani hloubkové audity bezpečnosti, což znemožňuje včasnou identifikaci rizikových oblastí a následnou nápravu. V současnosti neexistuje ani žádný systematický přístup k řízení životního cyklu zranitelností (Vulnerability Management), což vede k neefektivnímu řešení bezpečnostních problémů a absenci prioritizace oprav kritických chyb. Bez pravidelného externího skenování a testování bezpečnosti IT systémů zůstávají aplikace otevřené potenciálním útokům, například zneužití známých exploitů v zastaralých verzích softwaru. Chybí informační databáze, která by pomohla správcům IT pochopit identifikované zranitelnosti a doporučená opatření k jejich eliminaci. Organizace rovněž nemá zavedený proces školení zaměstnanců IT a bezpečnosti v oblasti efektivního vyhodnocování a řešení bezpečnostních hrozeb. Neexistence automatizovaného nástroje pro detekci a řízení zranitelností způsobuje, že opravy bezpečnostních slabin probíhají nesystematicky a reaktivně, což může vést k závažným bezpečnostním incidentům. Tyto zásadní nedostatky jasně ukazují na nutnost zavedení plánovaných opatření, která umožní pravidelné skenování a vyhodnocování bezpečnostních zranitelností, čímž se výrazně zvýší celková kybernetická odolnost organizace.

Opatření ID09 Automatická, periodická kontrola stavu bezpečnosti IT systémů a aplikací

Stručný popis opatření:

Zadavatel si je vědom stále sofistikovanějších kybernetických hrozeb a nutnosti udržování svých prostředí s vysokou odolností proti nim. V rámci proaktivní kontroly stavu svých prostředí se zadavatel rozhodl o nasazení systému nejen pro jednorázové prověření jednotlivých komponent infrastruktury, ale zavedení celého systému pro udržování životního cyklu tzv. Vulnerability managementu, který vhodně doplní stávající nástroje pro identifikaci hrozeb a jejich nápravu o periodické externí testování a management hrozeb i na zařízeních, které na sobě nemají tradiční operační systém s bezpečnostními produkty.

Technický popis realizace opatření:

Je požadováno dodání On-premise nebo Cloud prostředí (v úvahu připadá i hybridní nasazení), které bude spravovat celý životní cyklus pro min. 700 zařízení a min. 5 webových aplikací a systémů publikovaných do internetu s min. podporou na 1 rok. Nedílnou součástí musí být i podrobná informační báze, která napomůže k pochopení identifikovaných zranitelností, související rizika a s doporučením jaká je třeba udělat nápravná opatření k eliminaci takových rizik.

Dodavatel musí být schopen řešení nejen nasadit do prostředí zadavatele, ale také zaškolit v užívání tohoto prostředí jeho zaměstnance pro IT a bezpečnost, aby dokázali využívat širokého spektra možností takovéhoto produktu se schopností eliminovat dle priorit jednotlivé identifikované hrozby. V rámci dodávky je požadováno provedení prvního bezpečnostního „scanu“ a být nápomocni v osvojení schopnosti interpretace úvodních nálezů a podílet se min. na eliminaci kritických nálezů.

V oblasti zajišťování úrovně dostupnosti informací (§ 27):

Výchozí situace – problémy, které má realizace projektu vyřešit:

Městská část Praha 14 v současnosti postrádá odpovídající opatření k zajištění vysoké dostupnosti informací a kontinuity provozu svých informačních systémů, což představuje významné riziko pro stabilitu a bezpečnost poskytovaných služeb. Primární datové centrum není dostatečně redundantní a chybí efektivní mechanismy pro failover mezi jednotlivými uzly clusteru, což vede k vysoké zranitelnosti v případě výpadků. Neexistuje systematická strategie pro zálohování a obnovu dat, což znamená, že v případě kybernetického útoku nebo hardwarové poruchy hrozí ztráta důležitých informací. Chybí robustní řešení pro zálohování na úrovni serverové infrastruktury, včetně odpovídajícího diskového pole s dostatečnou kapacitou a redundantním připojením. Stávající síťová infrastruktura neumožňuje efektivní segmentaci a ochranu proti DDoS útokům na vrstvě L2/L3, což zvyšuje riziko narušení provozu klíčových aplikací. Bezpečnost WiFi připojení je nedostatečná, protože současné přístupové body nepodporují moderní standardy šifrování a segmentace SSID, což umožňuje potenciálním útočníkům snazší přístup k interní síti. Nedostatek automatizovaných testů obnovy záloh a neexistence disaster recovery plánů znamená, že organizace nemá jasně definované postupy pro rychlou obnovu kritických služeb po výpadku. Síťové prvky nejsou centrálně spravovány a neumožňují plně automatizovanou konfiguraci a dohled, což komplikuje operativní správu a snižuje efektivitu řízení IT infrastruktury. Chybějící virtualizační platforma s podporou Hyper-V a vysoké

dostupnosti vede k neefektivnímu využívání serverových zdrojů a prodlužuje dobu odezvy na technické incidenty. Tyto nedostatky jasně ukazují na naléhavou potřebu implementace plánovaných opatření, která zajistí vyšší úroveň dostupnosti, spolehlivosti a bezpečnosti informačních systémů organizace.

ID02 - Posílení primárního datového centra - redundance
Stručný popis opatření:
Redundantní klastrová řešení - posílení stávajících 3–4 node clusterů tak, aby byla zajištěna vysoká dostupnost a minimalizovány možné výpadky (SPOF). Hyper-V virtualizace. Vytvoření záložních scénářů - připravené procedury pro failover mezi clustery a replikace dat pro zajištění kontinuity služeb. Soulad s TIER doporučeními - vyšší úroveň dostupnosti a bezpečnosti v návaznosti na TIA-942. Optimalizace konfigurace a hardening.

Technický popis realizace opatření:

"HW: 6x server, 2 CPU, 384 GB RAM, 2x480GB SSD, redundantní napájení / chlazení
1x server, 2 CPU, 1 TB RAM, 2x480GB SSD, redundantní napájení / chlazení
3x server, 1 CPU, 64 GB RAM, 2x480 GB SSD, redundantní napájení/chlazení)
Diskové pole: 100TB redundantní
SW: Součástí dodávaného HW, Windows Server 2025 Datacentre 6x, Standard 4x
Podpora: NBD (Zahájení opravy následující pracovní den v místě instalace) 5 let
Implementace: Kompletní instalace a implementace v místě instalace.

Opatření ID03 - Výměna a implementace aktivních síťových prvků

Stručný popis opatření:
Implementace moderních switchů. Switche s podporou bezpečnostních funkcí (např. ACL, ochrana proti DDoS na L2/L3 úrovni). Logická mikrosegmentace sítě a IPv6 ready a 802.1X, včetně centralizovaného managementu.

Technický popis realizace opatření:

HW: 1x Modulární switch

Chassis 5 slotů

Redundantní napájení

Redundantní chlazení

Moduly: 2x 48 portů 10G/25G, 1x 12 portů 40G/100G

SW: Součástí dodávaného HW, pokročilé funkce správy a směrování

Podpora: 6 Hrs CTR (Zahájení opravy do 6 hodin od nahlášení v místě instalace)

Implementace: Kompletní instalace a implementace v místě instalace.

Opatření ID04 - Výměna a implementace WiFi infrastruktury

Stručný popis opatření:
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.

Technický popis realizace opatření:

HW: 101 x AP, 17 x Switch, 9x Controller

Lokality: (Plechárna, KD Kyje, Gen. Jan., G14, KC Kardašovská, H55, Polyfunkční budova), Správa majetku, Bratří Venclíků 1073, 1072, 1070)

SW: Součástí dodávaného HW

Podpora: NBD (Následující pracovní den v místě instalace a/nebo vzdáleně)

Implementace: Kompletní instalace a implementace v místě instalace.

•Nejnovější standard 802.11be (WiFi 7)

Zajištění vysoké propustnosti, snížení latence a vyspělé správy šířky pásma pro rostoucí počet zařízení.

•Podpora bezpečnostních protokolů

Nasazení WPA3 a případné nadstavby pro robustnější ochranu (např. Enhanced Open, OWE).

•Oddělená SSID a segmentace

Samostatné sítě pro hosty, zaměstnance a IoT zařízení; zamezení nežádoucího pohybu v síti.

•Centralizovaný monitoring a management

Centralizovaná správa přístupových bodů a kontrolérů, integrace s dohledovými nástroji (SIEM/NMS).

Opatření ID05 - Výměna a implementace zálohovací infrastruktury

Stručný popis opatření:

Výměna stávající infrastruktury za moderní zálohovací systémy a úložiště. Nasazení vysoce dostupných řešení (disková a pásková), která umožňují rychlou obnovu a minimalizaci dopadu výpadku. Automatizace a pravidelné testy obnovy. Nastavení plánovaných záloh, průběžná kontrola konzistence a pravidelné testování disaster recovery scénářů. Šifrování záloh. Řízení kontinuity provozu ICT s důrazem na rychlou obnovu klíčových služeb.

Technický popis realizace opatření:

HW: Pásková knihovna 2x LTO 9, 40 pozic, včetně příslušenství pro optické připojení.

Diskové pole 100TB, optické připojení

2x NAS (redundantní), 100TB, optické připojení

2x server pro zálohování (redundantní napájení / chlazení, 1CPU, 2xSSD 480GB)

SW: Veškeré licence pro kompletní pokrytí zálohovaného hybridního prostředí na 60 měsíců

Podpora: NBD (Následující pracovní den v místě instalace a/nebo vzdáleně)

Implementace: Kompletní instalace a implementace v místě instalace.

Opatření ID11 - Posílení dostupnosti primárního datového centra a zálohování 2023

Stručný popis opatření:

Zpětně uplatněné náklady na nákup tří serverů k zajištění HA datového centra, zálohovacího serveru a rozšíření diskového pole z roku 2023

Technický popis realizace opatření:

Dodávka 3 ks serverů ve shodné konfiguraci pro HA Cluster. Dvě CPU pro servery, 2 GHz, Počet jader: 20, 37 MB L3 cache, minimální průměrný výkon 45120 STR: 3200, paměť: 384 GB (12x32GB) PC5-4800, Poptávané HDD: 2x 480GB SSD, 8x 1 GbE Eth. Nezávislý management s podporou na 3 roky. Technická podpora na dva roky.

Dodávka 1 ks zálohovacího serveru, CPU pro servery, 2,1 GHz, Počet jader: 8, 11 MB L3 cache, Minimální průměrný výkon 11300 STR: 1800, paměť: 160 GB (5x32GB)-
Poptávané HDD: 2x 480GB SSD, poptávané HDD: 5x 6 TB SAS 7,2k, 5x 6TB SAS BC
Poptávaný RAID Adapter: 4 GB Cache, zálohovací baterie RAID
Nezávislý management s podporou na 3 roky.

Rozšíření diskového pole
Poptávaný počet SSD a velikost: 2 x 1.92 TB (Read intensive)
2x HPE MSA 1.92TB SAS 12G Read Intensive SFF (2.5in)
Typ HDD: 12 x 2.4 TB, SAS 10K SFF M2
2x 6pck HPE MSA 14.4TB SAS 12G Enterprise 10K SFF (2.5in),
SFP+

Technická podpora všech zařízení na dva roky.

Digitally signed by Ing. Martin Dušek
Date: 2025.02.20 10:57:57 +01'00'