Název investora: Správa železnic, státní organizace
adresa včetně PSČ: Dlážděná 1003/7, Praha 1, 110 00
IČ: 70 99 42 34
DIČ: CZ 70994234

ZÁMĚR PROJEKTU

investiční akce: „**Kybernetická bezpečnost Správy železnic**“

1) IDENTIFIKAČNÍ ÚDAJE PROJEKTU:

název projektu: **Kybernetická bezpečnost Správy železnic**

místo realizace (kraj): **Česká republika**

2) NÁVAZNOST NA SCHVÁLENÉ KONCEPCE A PROGRAMY

Udržení provozuschopnosti železniční dopravní cesty je součástí dlouhodobé strategie Ministerstva dopravy, uvedené ve strategických materiálech „Dopravní politika pro období 2014-2020“, která byla schválena usnesením vlády České republiky č. 449 ze dne 12. 6. 2013, a následně v materiálu „Dopravní sektorové strategie, 2. fáze“, který byl schválen usnesením vlády České republiky č. 850 ze dne 13. 11. 2013.

3) POPIS STÁVAJÍCÍHO STAVU A ZDŮVODNĚNÍ NEZBYTNOSTI REALIZACE PROJEKTU

Správa železnic, státní organizace, (dále jen Správa železnic) zajišťuje kromě údržby, oprav a modernizace cca 9,4 tis. km tratí, také jejich vybavení informačními a komunikačními technologiemi v rozsahu 4 tis. km optických tras a téměř 10 tis. aktivních prvků, včetně technologií zajišťujících chod organizace, v důsledku čehož je správcem a provozovatelem prvku kritické informační infrastruktury (KII SŽDC 01), který je dále rozčleněn na patnáct primárních aktiv.

Na zajištění těchto základních potřeb nezbytných pro ekonomiku a bezpečnost ČR vynakládá Správa železnic pravidelně nemalé finanční prostředky. Stále více se uplatňuje potřeba integrovat a centralizovat své informační systémy tak, aby byly schopny vzájemné kooperace, což přináší významný efekt v oblasti provozování informačních a komunikačních technologií, ale také nemalá rizika v podobě možného napadení kybernetickými útoky. Čím vyšší integrace technologií, tím vyšší synergický efekt, ale také tím vyšší zranitelnost celku. Aby mohla Správa železnic úspěšně čelit těmto hrozbám, musí neustále implementovat nová rozsáhlá organizační a technická opatření, směřující proti vektoru možných ohrožení perimetru.

S odkazem na platné ustanovení zákona č. 181/2014 Sb., o kybernetické bezpečnosti (dále jen „ZoKB“) a vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti (dále jen VoKB) byl, v návaznosti na závěry Analýzy (přezkoumání) rizik, která byla realizována na základě interní Metodiky pro identifikaci a hodnocení rizik bezpečnosti informací, zpracován Plán zvládání rizik.

Analýza (přezkoumání) rizik

Analýza (přezkoumání) rizik je realizována s využitím Nástroje pro hodnocení rizik, který zahrnuje katalog hrozeb, zranitelností a dále algoritmy, které umožňují, po expertním doplnění

pravděpodobnosti hrozby, závažnosti zranitelnosti a dopadu na aktivum, výpočet rizika. Dále zpracovává vyhodnocení dalších pohledů a statistické vyhodnocení stanovených rizik, včetně vazby rizik na definovaná opatření.

Během Analýzy (přezkoumání) rizik jsou stanovovány možné kombinace využití zranitelnosti hrozbou, a definováno, zda jsou ve vztahu k důvěrnosti (C), integritě (I) nebo dostupnosti (A) aktiva, a pro každou takovou kombinaci byly stanoveny úrovně dopadu (D) dle stupnice pro hodnocení dopadu. Během iniciální Analýzy (přezkoumání) rizik bylo získáno 1288 kombinací. Každá taková kombinace představuje konkrétní riziko.

Celkově bylo během Analýzy (přezkoumání) rizik identifikováno 1288 rizik a pro tato rizika byly výpočtem stanoveny hodnoty, podle kterých byla rizika rozdělená do kategorií **Nízká / Střední / Vysoká / Kritická.**

Plán zvládání rizik

Plán zvládání rizik, v aktuálně platné verzi (č. j. 70906/2019-SŽDC-GŘ-O30) navazuje na závěry pravidelné Analýzy (přezkoumání) rizik, jejíž výsledky jsou shrnuty ve Zprávě o hodnocení aktiv a rizik a definuje, případně vymezuje nápravná opatření (projekty) ke zmírnění (mitigaci) rizik identifikovaných a hodnocených během iniciální Analýzy (přezkoumání) rizik (2 rizika Kritická, 61 rizik Vysokých, 517 rizik Středních a 708 Nízkých). Opatření zahrnutá v Plánu zvládání rizik reagují na rizika Kritická, Vysoká a Střední. Zbývající rizika, tj. Nízká, byla Manažerem kybernetické bezpečnosti navržena jako přijatelná a následně došlo ke schválení Výborem pro řízení kybernetické bezpečnosti.

Opatření (projekty) byla navržena ve spolupráci s dalšími Odbory GŘ či organizačními jednotkami Správy železnic a na potřebě jejich realizace, v rozsahu a zaměření definovaném v Plánu zvládání rizik, existuje shoda.

Projekty uvedené v kap. 4.1 – 4.15 jsou součástí Plánu zvládání rizik (č. j. 70906/2019-SŽDC-GŘ-O30), který byl schválen na 6. zasedání Výboru pro řízení kybernetické bezpečnosti 9.12. 2019 a jsou navrženy k realizaci v rámci komplexního programu. Realizace projektů prostřednictvím níže popsaného programu zajistí jejich řádnou koordinaci a návaznost věcnou i časovou.

Současný stav

Správa železnic, v rámci zavádění a následného kontinuálního zlepšování systému řízení bezpečnosti informací, již zavedla a dále rozvíjí organizační opatření dle VoKB (např. řízení aktiv § 4, řízení rizik § 5, organizační bezpečnost § 6, řízení dodavatelů § 8, bezpečnost lidských zdrojů § 9, proces zvládání KBU / KBI § 14).

4) POŽADAVKY NA TECHNICKÉ ŘEŠENÍ

Cílem projektu je realizace technických opatření ve Správě železnic, dle §5 odst. 3 ZoKB.

Důvodem neshodného stavu organizace vůči požadavkům zákona o kybernetické bezpečnosti je právě **velmi rozsáhlá a komplikovaná ICT infrastruktura** a informační prostředí, ve kterém probíhá mnoho změn v úrovních redesignu infrastruktury a informačních systémů, ale také díky komplexnosti takového prostředí velmi vysoké požadavky na investice pro zavedení příslušných technických opatření.

Vzhledem k rozsahu a heterogennosti provozovaných sítí je nezbytné implementovat takové technické prostředky, které svými parametry umožní tyto sítě efektivně chránit a provádět jejich diagnostiku **bez narušení provoz**u technologické části.

Požadavky na legislativu

Požadavky na technické řešení musí být v souladu se ZoKB, v aktuálním znění a navazující VoKB, případně opatření, které ve své působnosti vydává Národní úřad pro kybernetickou a informační bezpečnost.

Přesné stanovení technických požadavků bude provedeno v otevřeném výběrovém řízení s ohledem na zákon č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů. Žádný z požadavků nepodléhá ochraně z hlediska patentu, licence, užitného nebo průmyslového vzoru.

Během roku 2021 dojde k zakoupení a instalaci HW prostředků do datových center interních i těch, která jsou provozována externě. Tento krok, předcházející samotné implementaci jednotlivých technických bezpečnostních opatření, je předpokladem pro jejich provoz v požadovaném výkonnostním rozsahu s cílem plného využití jejich potenciálu zásadně zvýšit ochranu perimetru datové sítě Správy železnic. Pořízení a implentace uvedených technických bezpečnostních opatření, včetně souvisejících SW řešení, bude realizováno během roku 2022.

Dodaná řešení musí splnit legislativní normy v rozsahu nezbytně nutném pro zpracovávanou agendu a rozsah a obsah dat. Očekáváme, že dodavatel v rámci analýzy určí přesně rozsah povinnosti z níže uvedených zákonů a norem, které implementovaný systém bude plnit. Jedná se z pohledu IT zejména o tyto zákony a normy:

- zákon o kybernetické bezpečnosti, včetně souvisejících vyhlášek
- požadavky související s normou GDPR platnou od května 2018 pro všechny členské země EU

Dále budou podrobně popsány následující oblasti řešené tímto projektovým záměrem:

4.1. Zavedení systému řízení bezpečnostních událostí a incidentů**.**

4.2. Konsolidace sběru provozních a bezpečnostních logů ze systémů a sítě Správy železnic

4.3. Implementace jednotného způsobu ověřování identit a zařízení v síti Správy železnic

4.4. Optimalizace internetového perimetru a demilitarizované zóny sítě Správy železnic**.**

4.5. Konsolidace a zabezpečení přístupových částí a dynamické správy a evidence adresního prostoru sítě Správy železnic

4.6. Nasazení managementu pro zprávu privilegovaných účtů pro infrastrukturu v prostředí Správy železnic

4.7. Nasazení systému IDM v prostředí Správy železnic

4.8. Implementace vícefaktorové autentizace

4.9. Pořízení a personalizace nosičů certifikátů

4.10. IT Compliance Validation

4.11. Analýza zavedení technických prostředků typu HoneyPot

4.12. Automatizované testování zranitelností

4.13. Zavedení systému prevence úniku dat (DLP)

4.14. Realizace systému zabezpečeného úložiště v prostředí Správy železnic

4.15. Zajištění segmentace interní datové sítě

4.16. Požadavky na inteligentní dopravní systémy

4.1. Zavedení systému řízení bezpečnostních událostí a incidentů

Technické opatření VoKB §14 Zvládání kybernetických bezpečnostních událostí a incidentů, §23 Nástroj pro detekci kybernetických bezpečnostních událostí a §24 Sběr a vyhodnocování kybernetických bezpečnostních událostí.

Cílem řešení je zavést centralizovanou správu kybernetických bezpečnostních událostí a incidentů na základě objektivně měřených a vyhodnocovaných dat o chování systémů a aplikací v rámci infrastruktury Správy železnic a získání širší informace o událostech, incidentech a podkladová data pro následnou korelaci takových informací s dalšími poznatky o stavu okolních systémů.

4.2. Konsolidace sběru provozních a bezpečnostních logů ze systémů a sítě Správy železnic

Technické opatření VoKB §14 Zvládání kybernetických bezpečnostních událostí a incidentů a §22 Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů.

Jedním z požadavků vyplývajících z VoKB §22 je požadavek na sběr informací o provozních a bezpečnostních činnostech a jejich ochranu před neoprávněným přístupem nebo změnou.

V současné době jsou informace o provozních a bezpečnostních událostech (logy) zaznamenávány převážně jen na lokální úrovni, kde není vždy možné zaručit jejich integritu.

Projekt zavede kompletní centrální sběr a uchovávání informací o provozních a bezpečnostních událostech (logů) na jednom místě, řešením zaručujícím jejich integritu i všechny další požadavky kladené výše uvedeným zákonem.

Toho by mělo být dosaženo nasazením centrálního log management řešení a zapojením všech zdrojů logů ze systémů a sítě Správy železnic do tohoto řešení.

4.3. Implementace jednotného způsobu ověřování identit a zařízení v síti Správy železnic

Technické opatření VoKB §19 Nástroj pro ověřování identity uživatelů.

ZoKB v platném znění, prostřednictvím VoKB §19, vyžaduje nasazení systémových prostředků a nástrojů pro ověření identity uživatelů a stavu koncových zařízení.

V souvislosti s tím je nutno implementovat systém autentizace koncových zařízení v technologických sítích (TECHLAN) Správy železnic (kamery, záznamová zařízení, průmyslové síťové komponenty a koncová zařízení informačních systémů pro cestující, IP rozhlasů, dispečerské řídící technologie pro obsluhu napájení od distributora energie a uvnitř Správy železnic, dálkové diagnostiky technologických systémů, vytápění odstavených vagónů,

ohřev výměn a další). Zároveň s tím je nutno ověřovat identitu uživatelů, kteří k těmto zařízením přistupují.

Současný stav technologických sítí (TECHLAN), jejíž součástí je většina kritické informační infrastruktury Správy železnic, neumožňuje autentizaci koncových zařízení jednotlivých provozně technických systémů souvisejících s provozováním železniční dopravní cesty (ŽDC).

Cílem projektu je zajistit možnost ověření identity u rozsáhlého distribuovaného systému a stavu koncových zařízení (min. na úrovni protokolu 802.1x) a zároveň možnost ověření identity uživatelů, přistupujících k těmto technologickým systémům a to na jedné společné platformě.

4.4. Optimalizace internetového perimetru a demilitarizované zóny sítě Správy železnic

Technické opatření VoKB §18 Bezpečnost komunikačních sítí a §23 Detekce kybernetických bezpečnostních událostí.

Přestože bylo řešení síťového perimetru Správy železnic v průběhu doby stále postupně modernizováno a posilováno, poslední zásadní změna, projevující se výrazným zlepšením vlastností a možností, proběhla před několika lety. Od té doby došlo jednak k pokroku v oblasti dostupných technologií a služeb, které je s jejich použitím možné získat a také k významným organizačním změnám.

Navrhované úpravy v oblasti síťového perimetru by tedy měly pro Správu železnic zajistit odpovědně zastávat roli správce kritické infrastruktury. Nové řešení musí disponovat dostatečným výkonem a flexibilitou pro spolehlivý a bezpečný běh provozovaných úloh různých kategorií a nároků.

4.5. Konsolidace a zabezpečení přístupových částí a dynamické správy a evidence adresního prostoru sítě Správy železnic

Technické opatření VoKB §18 Nástroj pro ochranu integrity komunikačních sítí, §20 Řízení přístupových oprávnění a §28 Průmyslové, řídicí a obdobné specifické systémy.

ZoKB v platném znění, prostřednictvím VoKB §18 a §28, vyžaduje nasazení různých systémových prostředků pro zajištění bezpečnosti provozu a dat informačních systémů kritické informační infrastruktury a komunikačních systémů kritické informační infrastruktury a významných informačních systémů.

Aby bylo možná tyto systémy implementovat a efektivně využívat, je nutná určitá předchozí konsolidace a modernizace síťových prostředků, a to zejména v úrovni přístupových (koncových) segmentů sítí Správy železnic.

Současný stav síťové infrastruktury Správy železnic vykazuje v některých koncových segmentech značnou roztříštěnost použitých technologií a HW prostředků, což má za následek např. nemožnost permanentního dálkového dohledu a managementu některých aktivních prvků v síti, nepodporování funkcionalit, protokolů a standardů autentizace a autorizace, nemožnost exportu diagnostických dat, slučování různých a odlišných síťových funkcí na jednom aktivním síťovém prvku, atd. K tomu je třeba přidat riziko plynoucí z nepodporovaných technologií, které již není možno firmwarově upgradovat tak, aby splňovaly aktuální bezpečnostní požadavky.

Předmětem tohoto projektu je postupná konsolidace síťových aktivních prvků na vrstvách L3 a L2 v sítích Správy železnic v takovém rozsahu, aby splňovaly parametry bezpečnosti, správy a managementu, zajištění dostupnosti služeb a zejména implementaci a provoz systémů a prostředků požadovaných VoKB. To zahrnuje zejména výměnu, nebo doplnění switchů v nejnižších úrovních sítí, kde jsou dosud provozovány nepodporované a nedohledovatelné typy HUBů a switchů, prvky bez technické podpory a tam kde jeden aktivní prvek bez redundance plnící více různých síťových funkcí.

4.6. Nasazení managementu pro zprávu privilegovaných účtů pro infrastrukturu v prostředí Správy železnic

Technické opatření VoKB §12 Řízení přístupu a §20 Nástroj pro řízení přístupových oprávnění.

Cílem projektu je správa a zabezpečení přístupů privilegovaných uživatelů k administrovaným systémům. Naprostá většina kybernetických útoků na systémy státní a veřejné správy, ale i na komerční společnosti, byla a je vedena přes privilegované účty. Ať už se jedná o sofistikovaný dlouhotrvající externí útok typu APT, či o zneužití privilegovaného účtu ze strany zaměstnance či zaměstnance dodavatele IT služeb, vždy se jedná o významné ohrožení daného subjektu. Informační prostředí Správy železnic je tvořeno velkým množstvím informačních systémů a rozlehlou síťovou infrastrukturou, na které je chod celé organizace závislý. Každý z prvků tohoto prostředí obsahuje privilegované účty, které jsou využívány pro jejich administraci, běžnou obsluhu, nebo se jedná o servisní účty použité v rámci integrací.

K takovým účtům mají přístup jak zaměstnanci Správy železnic, tak externí dodavatelé, kteří zajišťují provoz a rozvoj IT systémů a služeb Správy železnic.

4.7. Nasazení systému IDM v prostředí Správy železnic

Technické opatření VoKB §19 Nástroj pro ověřování identity uživatelů a §20 Řízení přístupových oprávnění.

Cílem tohoto projektu je především získat nástroj na správu identit, řízení přístupových oprávnění a jejich kontrolu v organizaci, napojení na personální systém (HR) a otestování v ostrém provozu na sadě informačních systémů. Následným krokem je pak postupné zapojování všech aktiv organizace do tohoto systému.

Implementace systému IDM a napojení všech aktiv v organizaci je chápáno jako dlouhodobá koncepce řízení identit, přístupových oprávnění, jejich kontroly a zvýšení zabezpečení přístupů k aktivům organizace. S ohledem na velikost organizace a velkému množství aktiv, nelze pojmout celé spektrum v jednom projektu, protože z pohledu naší organizace systém IDM nemá řídit pouze informační systém spadající do kritické infrastruktury, ale veškerá aktiva, ke kterým je potřeba přístupy řídit. Tato aktiva tak obsahují jednak informační systémy kritické infrastruktury, ostatní informační systémy, systémy pro kontrolu přístupů do zabezpečených lokalit a ostatních prostor organizace.

4.8. Implementace vícefaktorové autentizace

Technické opatření VoKB §19 Nástroj pro ověřování identity uživatelů, §25 Aplikační bezpečnost a §26 Kryptografické prostředky.

Cílem tohoto projektu je především zavedení prostředků pro ověřování autenticity požadavků oprávněných osob s užitím vícefaktorové autentizace v prostředí informačních systémů a infastruktury Správy železnic, napojení na systém IDM a otestování v ostrém provozu na sadě informačních systémů. Následným krokem je pak postupné zapojování všech aktiv organizace do tohoto systému.

Plánované řešení umožní užívání prostředků pro zajištění práce s kryptografickými prostředky na bázi asymetrické kryptografie a infrastruktury veřejných klíčů, včetně správy kryptografického materiálu, tak také potřeby v oblasti správy a podpory prostředků pro tvorbu a ověřování elektronických pečetí, elektronických podpisů a důvěryhodných časových razítek, a to jak v rozsahu vlastní báze prostředků zajištění důvěry, tak i v rozsahu prostředků pro zajištění důvěry třetích stran.

4.9. Pořízení a personalizace nosičů certifikátů

Technické opatření VoKB §19 Nástroj pro ověřování identity uživatelů, §25 Aplikační bezpečnost a §26 Kryptografické prostředky.

Cílem tohoto projektu je především získat a ustavit bázi pro správu prostředků PKI a vícefaktorové autentizace a bázi ověřovacích předmětů a prostředků.

Plánované řešení uspokojí jak potřebu užívání prostředků pro zajištění práce s kryptografickými prostředky na bázi asymetrické kryptografie a infrastruktury veřejných klíčů, včetně správy kryptografického materiálu, tak také potřeby v oblasti správy a podpory prostředků pro tvorbu a ověřování elektronických pečetí, elektronických podpisů a důvěryhodných časových razítek, a to jak v rozsahu vlastní báze prostředků zajištění důvěry, tak i v rozsahu prostředků pro zajištění důvěry třetích stran.

4.10. IT Compliance Validation

Technické opatření VoKB §3 Systém řízení bezpečnosti informací, §16 Audit kybernetické bezpečnosti a §21 Nástroj pro ochranu před škodlivým kódem.

V současnosti nemá organizace žádný nástroj nebo systém, který by na základě definovaných bezpečnostních standardů konfigurací příslušných podpůrných technických aktiv dokázal detekovat míru shody nebo neshody těchto aktiv s příslušnou vzorovou předdefinovaných konfigurací.

Implementace nástroje pro detekci a vyhodnocování požadavků na technickou shodu bezpečnostních opatření IT Compliance Validation v rámci ochrany podpůrných aktiv.

Systém bude monitorovat a vyhodnocovat míru technické shody na bezpečnostní požadavky podpůrných aktiv v sítích organizace a dále detekovat anomálie údržby a aktivit na provedení shody.

Nástroj bude zjišťovat atributy připojených podpůrných aktiv v síťové infrastruktuře zadavatele, bude je porovnávat s požadavky na vlastnosti aktuálních konfigurací, verzí a nastavení aktiv oproti přednastaveným bezpečnostním zásadám, platným pro dané typy aktiv nebo provozních celků a monitorovat změny a aktivity v rozsahu uvedených atributů aktiv a dokumentovat je.

Pro naplnění tohoto technického bezpečnostního opatření je nezbytné zavést interní pravidla pro pravidelné testování zranitelnosti aplikací. Tyto testy zranitelnosti musí být provedeny včetně odborného vyhodnocení a návrhu opatření k ošetření zjištěných zranitelností a problémů, které v tomto případě je nezbytné a není možné ho provést interními kapacitami. Nejdříve je nezbytné provést iniciační testy zranitelnosti ke zjištění základní úrovně. Následně pak opakované, pravidelné testy zranitelnosti v intervalech stanovených interními pravidly.

Pro zajištění tohoto technického bezpečnostního opatření implementován integrovaný systém umožňující identifikaci a zaznamenání technického a konfiguračního stavu technických aktiv v sítích a IT systémech zadavatele a porovnání získaných informací s požadovaným konfiguračním, resp. technickým stavem technických aktiv.

Systém je nezbytný pro nasazení systémů typu Security Information & Event Management a jejich informační podporu o stavu technických aktiv v systémech.

Systémy pro automatické zaznamenávání a porovnání shody informační systémy se schopností identifikovat stav aktiv v kybernetickém prostředí, jejichž účelem je zjistit objektivní technický stav aktiv.

4.11. Analýza zavedení technických prostředků typu HoneyPot

Technické opatření VoKB §23 Nástroj pro detekci kybernetických bezpečnostních událostí a §24 Sběr a vyhodnocování kybernetických bezpečnostních událostí.

Pro zajištění tohoto technického bezpečnostního opatření implementovat integrovaný systém umožňující simulaci provozního prostředí pro záchyt a identifikaci činnosti malware a dalších kybernetických útoků, poskytující dostatek informaci pro zaznamenávání a analýzy jejich činnosti a účinku v rozsahu určených simulovaných prvků infrastruktury a systémů včetně archivace po určené doby.

Systém je nezbytný pro nasazení systémů typu Security Information & Event Management a jejich informační podporu o probíhajících závadných aktivitách v systémech.

Honeypot (neboli „hrnec medu“) jsou specializované informační systémy se schopností simulace provozního prostředí, jejichž účelem je přitahovat potenciální útočníky a zaznamenat jejich činnost. Honeypoty jsou užívány zejména pro včasné detekování malwaru a následnou analýzu jeho chování. Malwary stále mění svoji strategii útoku a různými způsoby se skrývají a vyhýbají nalezení. Z těchto důvodů je nutno malware nějak nalákat a poté analyzovat jeho chování – takto získané informace se mohou použít pro aktualizování antivirových systémů.

Honeypoty detekují činnost neoprávněných zdrojů přicházejících do systému. Tato detekce je po odhalení útočníka plně automatická. Automaticky se sbírají data o činnosti potenciálního útočníka. Detekce buď vyloučí, že se jednalo o útočníka, nebo to potvrdí. Je to rychlejší, než kdyby se sbírala data z funkčního napadeného systému. Honeypoty se někdy sdružují do sítě, tzv. honeynetu. V těchto sítích jsou sdílena data o malwarech a jejich trendech. Nejčastěji jsou to způsoby šíření, užité algoritmy v malwaru, atd.

4.12. Automatizované testování zranitelností

Technické opatření VoKB §5 Řízení rizik, §10 Řízení provozu a komunikací, §11 Řízení změn.

Zajištění automatizovaného testování zranitelností podpůrných technických aktiv zajišťujících provoz primárních aktiv, automatická identifikace zranitelných míst ICT Infrastruktury, provádění automatických akcí k eliminaci identifikovaných zranitelností.

4.13.Zavedení systému prevence úniku dat (DLP)

Technické opatření VoKB §18 Bezpečnost komunikačních sítí a §23 Nástroj pro detekci kybernetických bezpečnostních událostí, nařízení Evropského parlamentu a Rady (EU) č. 2016/679 ze dne 27.dubna 2016 (dále jen GDPR) a Zákona č. 110/2019 Sb. o zpracování osobních údajů.

Zavedení organizačních a technických opatření (tj. automatické klasifikace dat / informací a zavedení potřebných nástrojů) k monitorování způsobů šíření informací a provádění automatických akcí (zaslání informace, odejmutí oprávnění, zastavení datového přenosu, apod.).

4.14.Realizace systému zabezpečeného úložiště v prostředí Správy železnic

Technické opatření VoKB §18 Bezpečnost komunikačních sítí, §19 Správa a ověřování identit, §20 Řízení přístupových oprávnění, §26 Kryptografické prostředky a §27 Nástroje pro zajištění vysoké úrovně dostupnosti.

Cílem centralizovaného zabezpečeného úložiště je zajistit potřebnou kapacitu pro bezpečnou správu, ukládání a archivaci dat pro vybrané aplikace organizace a dále průmyslové a řídící technologie tak, aby byla zajištěna odpovídající kybernetická bezpečnost na fyzické i logické úrovni s řízením přístupových oprávnění.

Úroveň fyzické ochrany aktiv bude zajištěna přímo v návrhu využitím technologií geografických clusterů a replikací dat mezi fyzicky oddělenými lokalitami.
Centralizované zabezpečené úložiště bude přímo součástí bezpečnostní architektury pro zajišťování úrovně dostupnosti. Logická ochrana aktiv bude spočívat v návrhu vysoké dostupnosti a odolnosti proti výpadku technických aktiv až na úroveň zotavení z katastrofy lokálního významu. Data budou ukládána dle definovaných bezpečnostních klasifikací, obsahu a dále podle četnosti použití do příslušných tříd (storage tiering).

Retence dat a management bude probíhat na základě nastavených pravidel. Data budou migrována s veškerými atributy včetně šifrování mezi lokalitami tak, aby bylo dosaženo jejich bezpečné uložení v centrální lokalitě, ale i v lokalitách, kde budou potřebná. Centrální lokalita bude zajišťovat ukládání a archivaci a zpětnou obnovu na vyžádání. Dále bude zajišťovat obnovitelnost všech uložených dat dle nastavených retenčních pravidel.

Výsledkem bude vznik sofistikovaného systému řízení dat s nastavitelnou úrovní zabezpečení do úrovně „kritické“, vyžadující šifrování dat. Dojde tak k eliminaci případné ztráty aktiv v podobě náhodného, úmyslného smazání či modifikaci dat. Omezený přístup k datům zajistí oprávněné užívání těchto aktiv a eliminuje případná zneužití neoprávněným přístupem.

Centralizované zabezpečené úložiště bude pro aplikace organizace a dále průmyslové a řídící technologie zajišťovat ukládání veškerých dat, které poskytne potřebnou podporu tak, aby

nedocházelo ke zneužití, neautorizované změně, duplikaci nebo nežádoucí modifikaci dat (viz GDPR security by design), proto bude úložiště vybaveno kryptografickými prostředky a algoritmy v souladu s požadavky VoKB.

4.15. Zajištění segmentace interní datové sítě

Technické opatření VoKB §18 Nástroj pro ochranu integrity komunikačních sítí a §28 Průmyslové, řídicí a obdobné specifické systémy.

Zavedení dodatečné bezpečnostní vrstvy umožňující izolaci potenciálního útočníka a zamezení šíření škodlivého kódu z jednoho již napadeného segmentu do dalších částí sítí.

Oddělení datového toku uživatelských zařízení od další ICT Infrastruktury, informačních systémů a prvků kritické informační infrastruktury.

Definování segmentů interní datové sítě a rozdělení jednotlivých systémů a koncových zařízení do těchto segmentů.

Implementace technického řešení k oddělení jednotlivých segmentů interní datové sítě s využitím VLAN, oddělením směrovacích tabulek, pomocí interních FW, apod.

4.16. Požadavky na inteligentní dopravní systémy

Soubory navrhovaných opatření nejsou samy o sobě inteligentními dopravními systémy, nicméně významně interagují do způsobu zajištěni informační a kybernetické bezpečnosti prostředí potřebného pro takové systémy, do jejich infrastruktury a mezivrstevní aplikační podpory a rozhraní integrace. Zajištění atributů informační a kybernetické bezpečnosti pro inteligentní dopravní systémy jako bezesporu klíčové vlastnosti prostředí je podmínkou nutnou pro vlastní bezpečnost a provozuschopnost takových systémů a v předpokladech jejich integrace s okolím se samozřejmě opírá o premisy řádného plnění standardů bezpečnosti, pro jejichž naplnění jsou navrhované soubory opatření klíčové. S ohledem na dynamiku vývoje potřeb a možných aplikací takových opatření informační a kybernetické bezpečnosti je na místě připomenout, že, předkládaný projektový záměr kalkuluje s potřebou flexibility opatření, a to i směrem k inteligentním dopravním systémům, opírá se o nejlepší dostupné praxe v aplikaci takových opatření a striktně předpokládá realizaci opatření, vykazujících nejvyšší možnou míru integrační otevřenosti a využitelnosti na základě průmyslových standardů pro obor informační a kybernetické bezpečnosti. V uvedeném ohledu projektový záměr nejen, že pokrývá potřeby vyplývající z legální obligace SŽ aplikovat taková opatření jak dle národní, tak i evropské legislativy, ale nahlíženo i soubory požadavku připravovaných norem ISO pro oblast ITS a jejich vazbou a prolínáním na požadavky existujících norem ISO pro oblast informační a kybernetické bezpečnosti logicky podporuje společný základ bezpečného a funkčního prostředí i pro inteligentní dopravními systémy, a to hospodárnou a účelnou cestou.