PROVÁDĚCÍ KONCEPT SW ŘEŠENÍ (PK)

projektu
Národní informační systém integrovaného záchranného systému (NIS IZS)

část

F. Bezpečnostní projekt

Dokument obsahuje:	Vymezení rozsahu projektu z hlediska bezpečnosti, specifikaci rizik, zajištění fyzické a komunikační, kybernetické a provozní bezpečnosti a její testování a přehled bezpečnostní dokumentace.
Verze:	6.1
Schválil za Dodavatele:	RNDr. Vladimír Příbramský
Datum aktualizace:	10/10/2014

Registrační číslo projektu CZ.1.06/3.4.00/11.07071

Obsah

1 Metodika

1.1 Předpoklady

V textu je použito označení Dodavatel pro dodavatele projektu NIS IZS jak pro označení Dodavatele v roli dodavatele hotového systému NIS IZS (v rámci projektové fáze). Po uvedení systému NIS IZS do provozu, je použito označení Provozovatel, jakožto subjekt odpovědný za zajištění bezpečnosti v rámci této fáze. Dodavatel popsanými činnostmi v provozní fázi nepřijímá žádné závazky pro dobu, kdy nebude Provozovatelem NIS IZS.

Řešení informační bezpečnosti NIS IZS popsané v tomto dokumentu vychází z následujících předpokladů:

- Předmětem ochrany nejsou data klasifikovaná podle zákona č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.
- Pro komunikaci je použita bezpečná síť ITS.
- Bezpečnostní opatření tvoří provázaný celek. Při změně nebo vynechání jednoho opatření musí být prozkoumán a vyhodnocen vliv změny na celkovou bezpečnost NIS IZS.

1.2 Koncepce informační bezpečnosti NIS IZS

NIS IZS je navržen a budován jako vysoce bezpečný informační a komunikační systém. Technická bezpečnostní opatření jsou navržena s cílem snížit možné riziko zneužití obecně známých slabých míst IT komponent v rámci systému NIS IZS. Důraz je kladen na všechny základní složky bezpečnosti informací:

- **Dostupnost**: informace jsou dostupné v požadovaném čase a na požadovaném místě. V případě NIS IZS se jedná o kritický požadavek.
- **Integrita**: pouze oprávněné subjekty mohou informace vytvářet a měnit.
- **Důvěrnost**: pouze oprávněné subjekty mohou informace číst.
- **Nepopiratelnost**: subjekt, který provedl nějakou operaci s informacemi, se nemůže vzdát odpovědnosti za provedení akce.

2 Řízení rizik NIS IZS

2.1 Identifikace a klasifikace rizik

Následující rizika rozdělená do kategorií jsou uvažována jako základní seznam pro fázi provozu NIS IZS. Systém bude kontinuálně monitorovaný a budou sledována všechna potenciální rizika, která mohou být identifikována i mimo níže uvedený seznam.

2.1.1 Fyzická rizika

a) Ohrožení zařízení NIS IZS přírodními vlivy (záplavy, vítr, sníh, zemětřesení, blesk).
b) Ohrožení zařízení NIS IZS ohněm.
c) Ohrožení zařízení NIS IZS průmyslovými haváriemi.
d) Ohrožení zařízení NIS IZS nevyhovujícími podmínkami pro provoz (teplota, vlhkost, prašnost, stabilita dodávané elektřiny).
e) Krádež zařízení nebo jejich zničení či poškození.
f) Teroristický útok.

2.1.2 Personální rizika

g) Chyba obsluhy: chybné konfigurace hardware nebo software, chybné příkazy administrátorů. Chyby v DNS, směrování, IP adresách.
h) Sociální inženýrství proti osobám podílejícím se na provozu nebo správě NIS IZS s cílem zneužít jejich oprávnění.
i) Provedení neoprávněných činností, zneužití oprávnění ze strany uživatelů nebo správců.

2.1.3 Kybernetická rizika

j) Výskyt škodlivého software, např. viry, spyware, trojské koně, apod. v NIS IZS.
k) Kybernetický útok vedený proti NIS IZS z nějaké vnější sítě (ITS, CMS, KSP) - footprinting, lámání hesel, spouštění kódu.
l) Útok na dostupnost NIS IZS z nějaké vnější sítě (ITS, CMS, KSP).
m) Kybernetický útok vedený proti NIS IZS z vnitřní sítě (NIS) - footprinting, lámání hesel, spouštění kódu.
n) Útok na dostupnost NIS IZS z vnitřní sítě (NIS).
o) Falšování identity uživatele nebo zařízení.

2.1.4 Technická rizika

p) Chyba aplikačního software.
q) Nedostupnost dat potřebných pro fungování aplikací.
r) Použití neověřených dat potřebných pro fungování aplikací.
s) Neoprávněná modifikace nebo smazání dat NIS.
t) Infiltrace komunikace, narušení integrity přenášených dat NIS.
u) Zneužití dat NIS, neoprávněný přístup k datům NIS, neoprávněné kopírování dat NIS.
v) Zachycení komunikace, narušení důvěrnosti přenášených dat NIS.
w) Chyba systémového software.
x) Selhání nebo neúmyslné poškození hardware.
y) Nedostupnost komunikací (počítačové sítě, telefonní síť).
z) Přerušení dodávky elektrické energie.

2.2 Hodnocení rizik

Dodavatel provedl hodnocení rizik, ve kterém vyhodnotil jednotlivá rizika a navrhl opatření na jejich pokrytí, odstranění nebo snížení jejich míry. Opatření tvoří základ tohoto dokumentu a jsou popsána v jeho jednotlivých kapitolách jako požadavky na zajištění bezpečnosti. Hodnocení informačních rizik a návrh protiopatření je klíčovou částí řízení bezpečnosti informačních systémů obecně a tedy i NIS IZS.

Cílem hodnocení rizik je stanovení závažnosti jednotlivých rizik a zajištění, že aktuálně navržená bezpečnostní opatření jsou dostatečná a efektivní.

2.3 Zvládání rizik

Existuje několik metod pro zvládnutí rizika existujícího i po realizaci navržených opatřeni. Tato rizika se nazývají zbytková rizika.

1. Pokrytí rizika, tady snížení jeho míry výběrem takových opatření (dosud nerealizovaných a nenavržených), aby mohlo být zbytkové riziko vyhodnoceno jako akceptovatelné trvale nebo dočasně.
2. Vědomé přijetí (akceptace) rizika se může použít v případě, že se nejedná o vysoké riziko a není vážně ohrožena bezpečnost informačních aktiv a jsou splněny požadavky zadavatele na bezpečnost informací.
3. Přenos rizika lze použít v případě, že je obtížné snížit riziko na přijatelnou úroveň vlastními zdroji. Možnými metodami je pojištění nebo outsourcing.
4. Vyhnutí se riziku znamená jakoukoli akci, při které jsou podmínky provozu informačního nebo komunikačního systému změněny tak, aby výskyt rizika nenastal.

Pro většinu rizik bude navrhnuta opatření, která zajistí požadovanou úroveň bezpečnosti NIS IZS.

Pro pokrytí rizik budou realizována bezpečnostní opatření, která jsou ekonomicky přiměřená a technicky dostupná a která budou mít následující formy:

a) Technická opatření.
b) Personální opatření.
c) Organizační opatření.
d) Bezpečnostní standardy v bezpečnostní politice NIS IZS.
e) Pracovní postupy používané při správě a užívání NIS IZS.

Cílem opatření je zajistit přiměřenou bezpečnost NIS IZS v následujících oblastech:

- Fyzická bezpečnost. Tato opatření zajišťují bezpečné umístění technických prostředků NIS IZS a omezení fyzického přístupu k zařízením NIS IZS. Mezi opatření fyzické bezpečnosti patří i zajištění bezpečných podmínek pro provoz technických zařízení NIS IZS včetně klimatizace, dostatečných prostor, pravidel pro údržbu a kontrolu přístupu k zařízení systému.
- Technická a komunikační bezpečnost. Tato opatření zahrnují implementaci bezpečnostních technologií, které zajistí kontinuální prosazení požadované úrovně bezpečnosti v celém systému po technické stránce. Technická bezpečnostní opatření

vycházejí z bezpečnostních standardů a vynucují jejich dodržování uživateli a správci NIS IZS.

- Kybernetická bezpečnost. Tato opatření zajišťují bezpečnost dat v digitální formě při jejich zpracování, ukládání a přenosech včetně ochrany proti malware, hackerským útokům a jinému zneužití.
- Personální bezpečnost. Tato opatření zajišťují bezpečnost činnosti osob při provozu NIS IZS. Zahrnuje definice postupů pro různé činnosti, obsazování bezpečnostních rolí důvěryhodnými osobami (viz kapitolu „Personální bezpečnost“), povinnosti zachovávat mlčenlivost a bezpečnostní vzdělávání.
- Organizační bezpečnost. Tato opatření zajišťují jasnou definici kompetencí, práv a odpovědností jednotlivých rolí v systému na straně Zadavatele i Dodavatele.

Součástí návrhu řešení NIS IZS je řada bezpečnostních opatření. Během výběru opatření je důležité zvážit náklady na zavedení a provozování opatření ve vztahu k hodnotě chráněných aktiv. Dodavatel navrhne a implementuje taková protiopatření, která splní požadavky na zvládnutí rizik a budou respektovat existující finanční, časová a technická omezení.

V rámci dalších prací budou bezpečnostní požadavky uvedené v dalších kapitolách tohoto dokumentu transformovány do Registru bezpečnostních požadavků a opatření, který bude základním etalonem pro nastavení požadované úrovně bezpečnosti NIS IZS. Registr bude umožnovat sledování naplnění jednotlivých požadavků v průběhu vývoje, implementace i provozu NIS IZS. Registr bezpečnostních požadavků a opatření vytvoří a bude udržovat Dodavatel.

Detailní a kompletní návrh bezpečnostních opatření v registru, včetně plánu jejich implementace bude vytvořen v dalších fázích projektu. Opatření budou vycházet z ISO/IEC 27002, NIST 800-53 a dalších nejlepších praktik. V dalších kapitolách jsou uvedena základní opatření, která musí být realizována, nicméně jejich přesná technická specifikace je závislá mj. na konkrétních technologiích, které při tvorbě tohoto konceptu nejsou známé zcela nebo jsou známé pouze z části.

3 Fyzická bezpečnost

Pojem „fyzická bezpečnost“ je používán ve smyslu zajištění bezpečných podmínek pro provoz technických zařízení. Zahrnuje jak opatření pro omezení fyzického přístupu k zařízením, tak pro zajištění provozních podmínek (teplota, vlhkost atd.) pro zařízení. Toto je ve shodě s terminologií používanou v Zákoně č. 181/2014 Sb., o kybernetické bezpečnosti a s terminologií používanou NBÚ (např. v zákoně č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů).

Dodavatel předpokládá zajištění požární bezpečnosti v prostorách KDC a SKDC, v nichž bude provozována infrastruktura projektu NIS IZS, provozovatelem těchto datových center v souladu se zákonem o požární ochraně č. 133/1985 Sb., vyhlášky o požární prevenci č. 246/2001 Sb. a souvisejících norem v aktuálních zněních.

Opatření na omezení fyzického přístupu k zařízením tvoří základ bezpečnostních opatření. Pokud totiž útočník získá fyzický přístup k některým zařízením, stanou se bezpečnostní opatření proti určitým typům útoků neúčinná.

Běžná zařízení výpočetní techniky potřebují ke své činnosti přiměřené provozní podmínky, zejména určitou teplotu a vlhkost a omezenou prašnost. Pro spolehlivé fungování zařízení je důležité takové prostředí zajistit. Dále tato zařízení potřebují zásobování elektřinou a to v požadované úrovni a kvalitě. Kolísání proudu a napětí ovlivňuje negativně nejen životnost zařízení výpočetní techniky ale i jejich funkce. Správné funkce a prodloužení životnosti zařízení lze také zajistit pravidelnou údržbou podle pokynů výrobce.

3.1 Fyzická bezpečnost datových center NIS IZS

Pro bezpečný provoz infrastruktury NIS IZS v KDC a SKDC navrhujeme jednotné zajištění bezpečnostních opatření pro všechna KDC a SKDC pro provoz infrastruktury projektu tak, aby bylo zabráněno fyzickému poškození, neoprávněné manipulaci či zcizení provozovaných IT zařízení. Doporučujeme zajištění následujících bezpečnostních opatření:

1. DC budou v budovách se řízeným přístupem a evidencí vstupujících osob. Kontrolu a evidenci budou provádět buď pracovníci recepce/vrátnice nebo bude prováděna automaticky pomocí technických zařízení.
2. Pro řízení přístupu do DC a prostor se zařízením NIS IZS jsou vytvořeny postupy a je udržován aktuální seznam pracovníků s oprávněným přístupem k zařízení NIS IZS.
3. Přístup do lokality a budovy DC bude monitorován.
4. V DC bude zajištěna vhodná požární ochrana.
5. DC budou chráněna proti živelným katastrofám.
6. DC nebudou umístěna v blízkosti nebezpečných průmyslových provozů (typu výroby výbušnin a velkých chemických podniků).
7. V budovách s DC nebudou provozy nebo zařízení způsobující vibrace instalovaných zařízení.
8. DC budou umístěna tak, aby nebyla ve zvýšené míře ohrožena pořádáním hromadných akcí (zejména demonstrací a sportovních akcí spojených s vandalismem) v jejich blízkosti.

9. Prostory se zařízeními NIS IZS budou monitorovány a záznamy budou uloženy a archivovány.
10. Prostory se zařízeními NIS IZS nebudou dostupné z veřejně přístupných prostor.
11. Systémy pro podporu zabezpečovacích a přístupových systémů budou umístěny mimo prostory, kde se nachází zařízení NIZ IZS. Přístup k zabezpečovacím a přístupovým systémům bude přísně řízen.
12. Prostory se zařízeními NIS IZS budou vybaveny proti elektromagnetismu a statické elektřině (antistatická podlaha).
13. Zařízení NIS IZS budou v rámci DC umístěna v prostorách oddělených od okolí. Stačí uzamykatelné skříně (rack).
14. Bude zajištěna fyzická ostraha DC. Ostraha DC bude mít povolen přístup do prostor se zařízeními NIS IZS pouze v případě mimořádných událostí a každý vstup ostrahy bude zaprotokolován. Mimořádnými událostmi se zde myslí následující události: požár, zaplavení, vysoká teplota, neoprávněný vstup.
15. Fyzický přístup k zařízením NIS IZS bude monitorován (např. prostřednictvím automatických záznamů otevření racků/skříní nebo organizačním opatřením – klíče k racku budou vydávány pouze oprávněným pracovníkům Dodavatele proti podpisu, případně budou práce na zařízení NIS IZS prováděny pod dohledem ostrahy DC).
16. Provozovatelem budou vytvořeny postupy pro nouzové opravy zařízení a jejich výměnu, či opravu na místě.
17. Bude zajištěn bezpečný přístup k jednotlivým zařízením a budou zajištěny dostatečné servisní prostory kolem nich (min. 0.5m mezi racky).
18. DC budou vybavena elektrickými silovými rozvody dostatečné kapacity a kvality dle specifikace, která bude upřesněna po výběru konkrétních technologií. Budou splněny minimálně následující požadavky:
    a) Elektrické kabely budou buď uloženy ve dvojité podlaze, nebo budou zakryté lištami.
    b) Bude zajištěna kvalita proudu a ochrana před kolísáním napětí. Napájení bude procházet přes záložní zdroj elektřiny, který potřebnou ochranu zajistí.
19. Bude zajištěno bezpečné zásobování všech zařízení NIS IZS v DC elektřinou. DC bude vybaveno UPS a centrálními záložními zdroji podle standardů A Analýzy interoperability základních složek integrovaného záchranného systému.
20. Bude omezen fyzický přístup k datovým rozvodům. Buď budou uloženy do lišt, nebo vedeny pod podlahou nebo pod stropem.

4 Technická a komunikační bezpečnost

Opatření zahrnují implementaci bezpečnostních technologií a jejich nastavení, které zajistí kontinuální prosazení požadované úrovně bezpečnosti v celém systému po technické stránce. Technická bezpečnostní opatření vynucují jejich dodržování uživateli a správci NIS IZS.

4.1 Bezpečnost sítí v SKDC a KDC NIS IZS

Pro zajištění bezpečnosti počítačových sítí v jednotlivých SKDC a KDC NIS budou v rámci projektu realizována minimálně následující opatření:

1. Síťová zařízení NIS IZS budou umístěna pouze v chráněných (případně i monitorovaných) prostorech s řízeným přístupem.
2. Pro provoz a správu NIS IZS nebudou využívané bezdrátové sítě Wi-Fi.
3. Bude kontrolováno připojení zařízení k aktivním síťovým prvkům NIS IZS. Nepoužívané porty budou deaktivovány.
4. Bude prováděna autentizace zařízení připojených k aktivním síťovým prvkům NIS IZS, aby bylo zabráněno připojení neautorizovaných zařízení.
5. Logický přístup na administrační rozhraní síťových prvků bude řízen a omezen pouze na oprávněné a jednoznačně identifikovatelné správce systému.
6. U síťových zařízení budou pro privilegované a neprivilegované činnosti používány samostatné účty (oddělený účet pro činnosti vyžadující privilegované oprávnění a pro rutinní servisní činnosti).
7. Vzdálený přístup k síťovým zařízením je omezen pouze na jednoznačně identifikovatelné správce systému.
8. Na síťových zařízeních bude vytvořen pohotovostní účet pro případ obnovy systému v případě havárie (či např. při odchodu všech administrátorů, atd.).

4.2 Bezpečnost propojení mezi komponentami NIS IZS

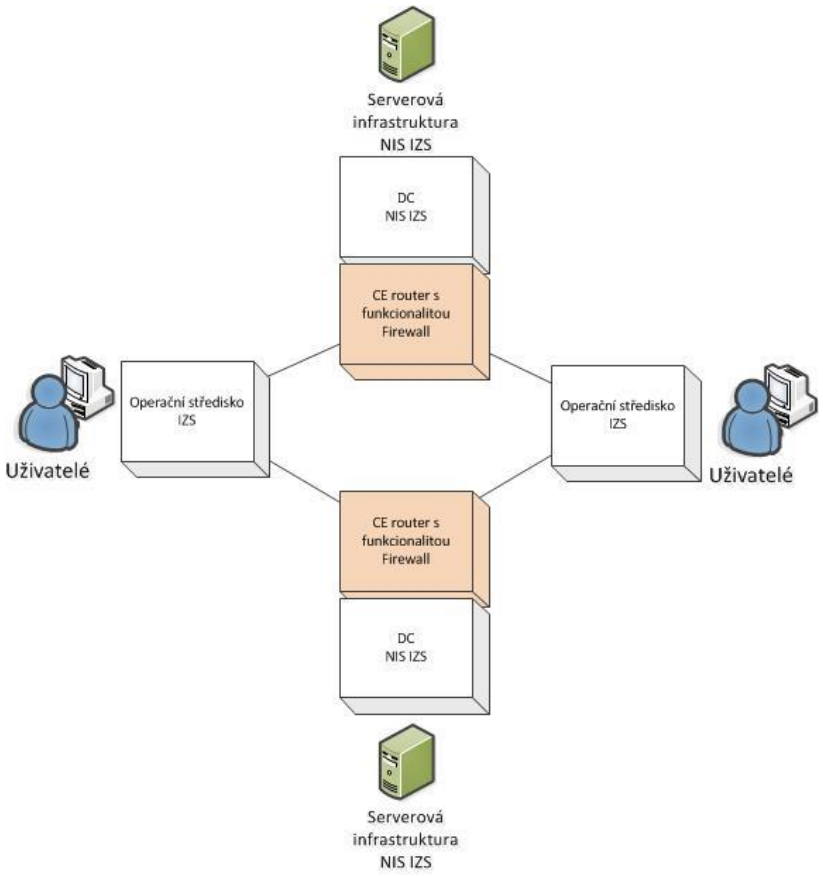
V této kapitole je řešena bezpečnost následujících propojení:

- komunikace operačních středisek NIS s SKDC a KDC NIS,
- komunikace středisek operačního řízení IZS s SKDC a KDC NIS,
- komunikace mezi SKDC a KDC NIS.

4.2.1 Filtrování komunikace v SKDC a KDC NIS

V SKDC a KDC budou umístěny servery a další zařízení potřebná pro provoz NIS (disková pole, zálohovací a archivační zařízení, atd.). Tato zařízení budou plně pod kontrolou Dodavatele a nebudou připojena do žádných dalších sítí. K propojení bude použita zabezpečená síť ITS (viz část C „Síťová infrastruktura“).

Střediska operačního řízení IZS budou oddělena od SKDC a KDC NIS. Toto oddělení bude provedeno **ve všech SKDC a KDC NIS**. Pro filtrování datové komunikace mezi SKDC a KDC NIS a okolím budou využity firewall funkcionality u dodaných CE směrovačů. Viz následující návrh:



Obrázek 1: Komunikace mezi DC

Zajištění Operačních středisek IZS není předmětem dodávky projektu ze strany Dodavatele.

Na CE směrovačích (případně dalších relevantních síťových zařízeních) v KDC a SKDC budou realizována následující bezpečnostní opatření:

1. Síť projektu NIS IZS bude rozdělena pomocí VPN do dvou částí: NIS „backplain“ a NIS „public“.
2. SKDC a KDC projektu bude umístěna v části NIS „backplain“ (tato VPN zajišťuje komunikaci mezi jednotlivými systémy, klienti nebudou mít do VPN NIS “backplain“ přístup)
3. Bude zajištěna komunikace v rámci VPN NIS „backplain“ řízeným prostupem výlučně pro požadované služby.
4. Bude zajištěno vzájemné oddělení a prostupy LAN sítí jednotlivých složek a krajů IZS, což umožní odebírání potřebných služeb bez nutnosti budovat oddělenou LAN pro projekt NIS IZS.
5. Bude oddělena datová síť VPN NIS „backplain“ a VPN NIS „public“ a prostupy mezi nimi budou řízeny pomocí ACL pravidel.
6. Bude zakázána propagace směrovacích informací ostatních subjektů IZS z VPN NIS „public“ do jednotlivých sítí složek IZS.
7. Bude vyžadovaná autentizace pro přístup pracovníků k síťovým zařízením.
8. Budou změněna všechna předdefinovaná hesla na síťových zařízeních. Budou zrušeny a nahrazeny předdefinované účty na síťových zařízeních, pokud to bude možné.

9. Bude nastaveno automatické odhlášení uživatele ze síťového zařízení po určité době nečinnosti (max 5 min).
10. Pro přístup ke směrovači a dalším síťovým zařízením budou upřednostňovány šifrované protokoly.
11. Bude použit protokol SNMP nejméně ve verzi SNMPv2.
12. Budou definovány bezpečné NTP servery pro synchronizaci času síťových zařízení.
13. Bude aktivována ochrana proti modifikaci software a konfigurací uložených v síťových zařízeních, pokud je na použitých zařízeních taková ochrana dostupná (jedná se např. o digitální podpisy software, kontrolní součty a podobná opatření).
14. Bude použita ochrana proti resetování hesel na síťových zařízeních, pokud je na použitých typech zařízení taková funkce dostupná.
15. Budou blokovány pakety pokoušející se falšovat totožnost odesilatele (anti-spoofing), pokud je na použitých typech zařízení taková ochrana dostupná.
16. Bude aktivována ochrana proti útokům na úrovni dat, pokud je na použitých typech zařízení taková ochrana dostupná (např. ochrana proti útokům typu buffer overflow).

4.3 Bezpečnost aplikací a systémů NIS IZS

Pro zajištění bezpečnosti poskytovaných služeb NIS IZS budou aplikována následující opatření:

1. Přístup k datům n úrovni databáze bude realizován výhradně skrze ORM (Object-Relationship Mapping) prostředky (např. Hibernate). V případě, že z nějakého důvodu budou některé funkce aplikace vyžadovat přímé dotazování pomocí SQL, budou realizována nápravná opatření (zn. ošetření vstupů), aby se zamezilo útokům tzv. SQL Injection.
2. Bude zajištěna jednoznačná autentizace pro přístup do NIS IZS. Pro přihlašování do subsystémů NIS IZS budou upřednostňovány individuální účty (namísto sdílených), aby byla zajištěna jednoznačná identifikace přistupujícího uživatele. Pracovníci budou používat výhradně individuální účty.
3. Politika hesel do aplikace a subsystémů NIS IZS (např. pro LDAP službu, pro uživatelské PostgreSQL účty, atd.) bude vyžadovat následující politiku hesel:
   a) heslo má délku minimálně 8 znaků,
   b) heslo nemůže být prázdné,
   c) není umožněno tzv. anonymní přihlášení,
   d) bude nastaven kontrolní mechanismus pro zajištění komplexity vytvářených hesel (heslo musí splňovat kombinaci znaků - alespoň 1 velký znak, alespoň 1 malý znak, alespoň 1 číslice),
   e) počet neplatných pokusů o přihlášení do systému 10x.

V případě, že některé budoucí komponenty NIS IZS technicky neumožňují nastavení výše uvedené politiky hesel, bude tato skutečnost zaznamenána a komunikována v rámci předávané bezpečnostní dokumentace (popis bezpečnostní architektury).

1. Bude zajištěna a dodržována koncepce uživatelských rolí v celém systému NIS IZS a na základě této koncepce bude umožněno definovat matici odpovědností a oprávnění (tzv. Segregation of Duties) pro uživatele řešení NIS IZS.
2. Pro administraci aplikačních modulů NIS IZS bude použito webové rozhraní pro administraci. Do webového rozhraní pro administraci NIS IZS budou mít přístup pouze oprávnění uživatelé s rolemi.

3. Pro komunikaci nebudou použity jiné než uvedené komunikační služby (JMS, REST, SOAP, HTTP, HTTPS).
4. Nešifrované HTTP bude použito v rámci interní komunikace uvnitř VPN „backplain“ sítě.
5. Pro komunikaci v rámci webového rozhraní pro administraci bude zajištěno šifrování HTTP (bude použito HTTPS).
6. Bude stanoven seznam ověřených povolených webových prohlížečů pro přístup do webových rozhraní NIS IZS (rozhraní pro administraci).
7. Nebude povoleno přístup na webové rozhraní pro administraci z nepodporovaných platforem OS (např. Windows XP).
8. Na IT komponentách NIS IZS budou aktivovány základní bezpečnostní funkce (dle konkrétní technologie)
9. V rámci komponent systému NIS IZS bude zajištěna integrita transakcí tak, aby bylo možné detekovat a opětovně spustit neúspěšně provedenou dávkovou úlohu či datový transfer (např. pomocí kontrolních součtů, atd.).

4.4 Bezpečnost záložního propojení

Pro případ výpadku ITS doporučuje Dodavatel, aby existovala možnost komunikace mezi operačními středisky a SKDC/KDC NIS přes CMS2. **Zřízení těchto linek není součástí projektu NIS IZS**. V této kapitole jsou uvedeny bezpečnostní požadavky na toto propojení.

Záložní propojení bude realizováno využitím standardních přípojek KIVS. Existuje několik různých situací lišících se místem a rozsahem výpadku ITS:

- výpadek propojení z kraje k SKDC NIS,
- výpadek ITS v rámci kraje,
- výpadek celé ITS.

Základní schéma je popsáno v samostatné kapitole G – Spolehlivost.

4.5 Připojení do Internetu

Operační střediska NIS IZS mohou mít přístup do Internetu. **Zřízení přístupu do Internetu není součástí projektu NIS IZS**. Doporučeným způsobem pro přístup do Internetu (a sTESTA) je využít služeb CMS2. Jednotlivé složky IZS mohou každá za sebe požádat provozovatele CMS2 o zřízení přístupu do Internetu, případně do sTESTA. Půjde o žádost na zřízení standardních služeb CMS2. Zejména o službu „Bezpečné připojení do Internetu“. Tato služba bude nabízet zabezpečené připojení do Internetu.

Poskytovatelem připojení bude provozovatel ITS v roli nekomerčního poskytovatele připojení k CMS2. Jednotlivé složky IZS použijí pro přístup do Internetu jim přidělené datové VPN NIS (technicky jde o VPN sítě ITS).

5 Kybernetická bezpečnost NIS IZS

5.1 Bezpečnostní monitoring NIS IZS

Bezpečnostní monitoring zajistí Provozovatel systému. Bezpečnostní monitoring není předmětem projektové části NIS IZS. Návrh řešení v případě, že Dodavatel NIS IZS bude současně jeho Provozovatelem, je popsán v provozní části zajištění bezpečnosti.

Aby bylo možné požadované události sledovat, budou mít jednotlivé komponenty NIS IZS zapnuté logování a zapnutý auditing. Komponentami NIS IZS jsou zejména aktivní síťové prvky, aplikační servery a související infrastruktura NIS IZS. Tím bude zajištěno, že vzniknou primární data o událostech podstatných z hlediska bezpečnosti přímo u zdroje. Tato data mohou být následně systémem bezpečnostního dohledu centralizována a centrálně vyhodnocována, oznamována (alerty) a prezentována.

Bude nastaveno zaznamenávání vybraných uživatelských a systémových událostí, které mohou mít zásadní vliv při identifikaci a šetření kybernetického bezpečnostního incidentu. Rozsah zaznamenávaných činností bude stanoven na základě analýzy rizik, mj. úspěšné a neúspěšné pokusy o přihlášení uživatele, založení nového uživatele, pozastavení a restart služby, atd.

Logy a záznamy o aktivitách budou bezpečně uloženy a archivovány. Pro vybrané záznamy bude vymezen úložný prostor tak, aby byla umožněna jejich archivace minimálně po dobu 5 let.

5.2 Ochrana proti virům a škodlivému kódu

Koncové stanice (případně také související terminálové servery) nejsou předmětem hybridní varianty dodávky NIS IZS. Nasazení antivirových systémů tedy není předmětem realizace ze strany Dodavatele NIS IZS. Antivirové systémy na serverovou infrastrukturu projektu NIS IZS nebudou implementovány s ohledem na oddělení VPN „public“ a VPN „backplain“ sítě, viz kapitola *Bezpečnost propojení mezi komponentami NIS IZS*.

5.3 Zálohování a archivace

Zálohování je popsáno v kap. 1.4. části A - HW PKv51 a archivace je popsána v kap. 1.3. části A - HW PKv51. Budou naplněny základní bezpečností požadavky na zálohování:

1. Budou vytvořeny zálohy všech klíčových dat.
2. Zálohy dat budou chráněny stejně jako ostrá data
3. Zálohy budou zahrnovat i programové vybavení komponent NIS IZS.

6 Testování bezpečnosti NIS IZS

Před zahájením provozu NIS IZS budou provedeny sady bezpečnostních testů, které mají za úkol prověřit integritu tohoto systému. Pro provádění testů budou stanoveny a naplněny následující požadavky:

1. Bude provedeno nezávislé ověření bezpečnosti NIS IZS třetí stranou.
2. Testy budou zahrnovat testování bezpečnostních funkcí.
3. Budou stanoveny testy, data potřebná pro testy a odhadnuty výsledky testů.
4. Závěry testů budou rozděleny podle závažnosti.
5. Testování bude prováděno podle sady standardních bezpečnostních testů.
6. Testy budou sestaveny mj. na základě znalosti slabin systému.

6.1 Testování bezpečnosti aplikací a služeb

Preventivním prostředkem pro zajištění bezpečnosti aplikací vyvíjených vlastními silami Dodavatele, bude statické testování kódu. Vyvíjené programy i programy přebírané z externích zdrojů ve zdrojovém tvaru budou testovány analyzátory zdrojových kódů s cílem odhalit případné zranitelnosti v programech a odstranit je před nasazením aplikací do provozu. Týká se služeb a aplikací:

- Centrální GIS
- Krajské GIS
- Centrální IPL
- Krajské IPL
- Webové rozhraní pro administraci NIS IZS

Bezpečnostní testy proto budou mít zejména charakter ověření autentizace a autorizace k systému tak, aby nemohlo dojít ke zneužití údajů ze strany pracovníků Zadavatele.

Statické testování aplikací bude doplněno dynamickým testováním, které bude primárně orientováno na odolnost vůči chybám ve vstupních datech.

Dodavatel provede statické i dynamické testování před nasazením aplikací do provozu. Dynamické testování provede na produkčním prostředí (ale před nasazením aplikací do provozu).

Před uvedením webového rozhraní pro administraci do produkčního provozu bude tato webová aplikace otestována vůči technickým zranitelnostem podle referenčního modelu OWASP.

7 Bezpečnostní dokumentace NIS IZS

Součástí předání hotového systému NIS IZS bude bezpečnostní dokumentace projektu, která bude obsahovat popis bezpečnostní architektury NIS IZS a bude zahrnovat následující položky:

- Přehled technických bezpečnostních opatření pro jednotlivé typy IT aktiv projektu a vazby mezi nimi.
- Seznam bezpečnostních technologií zajištěných pro projekt.
- Seznam technologických účtů na systémech a hesel k nim (pro dodané bezpečnostní technologie).

8 Zajištění provozní bezpečnosti

Provozní bezpečnost je a bude Dodavatelem řešena ve fázi přípravy NIS IZS pro provoz a v provozu v době, kdy Dodavatel bude ustanoven Provozovatelem NIS IZS. Opatření uvedená v následujícím textu představují rámcový návrh zajištění informační bezpečnosti při uvedení systému NIS IZS do provozu.

Dodavatel chápe informační bezpečnost NIS IZS jako proces. V etapě přípravy a realizace budou navržena a implementována určitá bezpečnostní opatření.

Během provozu bude Provozovatel identifikovat případné nové hrozby ohrožující systém a případné nové zranitelnosti systému a navrhne a realizuje **preventivní opatření** proti novým hrozbám a bude odstraňovat nové zranitelnosti**.**

Provozovatel bude činnost systému kontinuálně a v reálném čase monitorovat, mj. s cílem **detekovat** případná **narušení bezpečnosti**. Pokud se taková narušení vyskytnou, přijme **nápravná opatření a navrhne zvýšení bezpečnosti systému**.

Při řízení informační bezpečnosti NIS IZS bude Provozovatel dodržovat následující principy:

- Bezpečnost je založena na zvládání rizik, tj. na identifikaci rizik a realizaci odpovídajících opatření proti nim.
- Jsou definovány a personálně obsazeny bezpečnostní role pro provoz a správu NIS IZS a vymezeny povinnosti osob, které budou jednotlivé role vykonávat.
- Je kontinuálně a v reálném čase monitorována bezpečnost provozu NIS IZS. Jsou definovány postupy pro vyšetřování bezpečnostních událostí a incidentů a zajištěny mechanismy pro přijetí nápravných opatření.
- Je zajištěna kontinuita činností NIS IZS při narušení systému, zejména pak výskytu následujících situací: při výpadcích jednotlivých zařízení potřebných pro provoz NIS IZS a při výpadcích jednotlivých SKDC a KDC NIS IZS.
- Ze strany Zadavatele, Provozovatele, případně subdodavatelů, jsou respektovány specifické bezpečnostní požadavky kladené na NIS IZS.
- Existuje a v průběhu provozu systému Provozovatel udržuje plán bezpečnostního rozvoje NIS IZS pokrývající realizaci bezpečnostních opatření, která vyplývají z vyhodnocení incidentů, ze změn v charakteristice a hodnotách rizik a z návrhů na zvýšení bezpečnosti systému a jeho prostředí.

8.1 Fyzická bezpečnost zařízení NIS IZS

V rámci provozu bude fyzická bezpečnost řízena také na úrovni IT zařízení systému NIS IZS (vztahuje se na všechna zařízení NIS IZS nezávisle na jejich umístění). Provozovatel realizuje v této oblasti následující opatření:

1. Všechna zařízení NIS IZS budou provozována a udržována v souladu s doporučením výrobce. Veškeré opravy a servisní zásahy budou provádět pouze oprávněné osoby s potřebnou kvalifikací. Veškeré opravy a servisní zásahy budou prováděny pouze se souhlasem Provozovatele a za dozoru jeho zástupce nebo osoby pověřené Provozovatelem.

2. Budou vytvořeny postupy pro nouzové opravy zařízení a jejich výměnu, či opravu na místě. Opravy budou realizovány důvěryhodnými pracovníky s oprávněným přístupem.
3. Bude zajištěno bezpečné vymazání/přepsání obsahu paměťových médií používaných pro NIS IZS v případě jejich likvidace nebo zaslání do opravy.
4. Transport zařízení NIS IZS do opravy mimo lokalitu DC bude prováděn bezpečným způsobem, který zajistí Provozovatel. Provozovatelem budou vytvořeny postupy pro transport.
5. Je stále udržován aktuální seznam technického vybavení a jsou prováděny pravidelné kontroly souladu.

8.2 Bezpečnost sítí v SKDC a KDC NIS IZS

Pro zajištění bezpečnosti počítačových sítí v jednotlivých SKDC a KDC NIS IZS budou v rámci provozu realizována Provozovatelem minimálně následující opatření:

1. Konfigurační nastavení síťových zařízení budou pravidelně zálohována alespoň jednou týdně a také vždy před každou změnou konfigurace síťového zařízení.
2. Na CE směrovačích v KDC a SKDC realizuje Provozovatel následující bezpečnostní opatření:
   - Vypracuje postup pro rychlé a jednoduché zablokování jednotlivých VPN na síťových zařízeních.
   - Bude provádět pravidelné aplikace bezpečnostních aktualizací software síťová zařízení.
   - Nepovolí logický přístup na síťová zařízení jakýchkoli osob mimo správců síťových zařízení a to ani pro read-only přístup.
3. K síťovým zařízením se bude Provozovatel připojovat pouze z autorizovaných, zabezpečených a dohledovaných zařízení.

8.3 Bezpečnost připojení cizích zařízení k NIS IZS

Připojení cizích zařízení do sítě NIS IZS (jiných než dodaných v rámci dodávky NIS IZS nebo vymezených Provozovatelem systému) není doporučeno, pouze s výjimkou pro přístup k záznamům o provozu síťových zařízení za následujících podmínek:

- Na žádost příslušné složky IZS v určité lokalitě bude definován port na přepínači, ke kterému bude možné připojit zařízení spravované příslušnou složkou.
- Na tento port bude směrovač posílat část informací o síťovém provozu.
- Pro předávání informací budou použity standardní protokoly syslog a SNMP traps. Zprávy syslog budou omezeny podle typu (facility) a závažnosti (severity). Posílat se budou pouze takové zprávy, které mají význam z hlediska řešení problémů na úrovni kraje. Obdobně budou omezeny SNMP traps.

8.4 Bezpečnost připojení vlastních zařízení k NIS IZS

Systém bude schopen ověřit pomocí Network Access Control, případně odpovídající funkcionality na síťovém prvku (typicky na přepínači), zda má připojené síťové zařízení právo připojit se k síti NIS IZS.

Připojení neschváleného zařízení k NIS IZS bude kvalifikováno jako závažný bezpečnostní incident a proto budou realizována bezpečnosti opatření proti připojování neschválených

zařízení k NIS IZS. Může se jednat buď o pokus připojit neschválené zařízení k nějakému nevyužitému portu aktivního síťového prvku, nebo o pokus o nahrazení schváleného zařízení neschváleným zařízením, nebo o pokus vydávat neschválené zařízení za schválené.

8.5 Řízení privilegovaného přístupu k systému

Přístup administrátorů a správců systému NIS IZS bude řízen. Budou vytvořeny postupy pro získání, využívání a odebrání privilegovaného přístupu k systému. Budou naplněny minimálně následující bezpečnostní požadavky:

1. Privilegovaný přístup k NIS ISZ budou mít jen odpovědní administrátoři.
2. Pravomoci jednotlivých administrátorů budou odděleny podle SoD (Segregation of Duties, oddělení odpovědností).
3. Budou prováděny kontroly, že práva přidělená pracovníkům nejsou v rozporu s bezpečnostní politikou a odpovídají jejich pracovní náplni.
4. Budou rušena přístupová práva pracovníkům měnícím pozici nebo opouštějícím organizaci.
5. Bude vedena kompletní evidence administrátorů a přidělených privilegií.
6. Kopie hesel účtů systémových správců budou pro případ pohotovosti bezpečně uloženy v sejfu (případně šifrovaném archivu) a budou vypracovány postupy pro vyzvednutí kopií těchto hesel.
7. Použití privilegovaných účtů administrátorů bude minimální a účty nebudou používány k běžné práci v systému.
8. Administrátoři a správci NIS IZS budou používat vždy 2 oddělené uživatelské účty: běžný uživatelský účet pro rutinní činnosti, administrátorský účet pro cílené administrativní zásahy do konfigurace. Tímto opatřením bude omezeno riziko šíření virové nákazy např. při otevírání nedůvěryhodných příloh e-mailu, atd.

8.6 Řízení změn v systému

Pro bezpečné řízení změn v rámci NIS IZS po jeho uvedení do provozu budou aplikována následující opatření:

1. Všechny změny v systému budou řízeny předem připraveným procesem.
2. Všechny změny budou před realizací schváleny oprávněným pracovníkem, dokumentovány a předem otestovány v testovacím prostředí, že změny nemají vliv na bezpečnost řešení.
3. Budou identifikovány všechny komponenty a oblasti, které změna ovlivní.
4. Budou předem určeny osoby/role, které jsou odpovědné za změny.
5. Změny s vlivem na bezpečnostní požadavky budou schvalovány vlastníkem aktiva systému, kterého se změna dotkne.
6. Změny budou v rámci možností realizovány v časech s nejnižší úrovní provozu.
7. Provozovatel nebude žádné aktualizace standardního software aplikovat na serverech a zařízeních automaticky, ale půjde vždy o manuální a kontrolovaný zásah.
8. Při aplikaci opravných balíčků bude Provozovatel dodržovat zásady (s výjimkou situací, kdy nutnost aplikace balíčků bude kritická, např. kvůli vysokému ohrožení NIS IZS existující zranitelností):
   a) Centrální systémy NIS IZS budou umístěny ve třech různých SKDC. Dodavatel aplikuje balíčky nejprve v jednom vybraném datovém centru (např. DC3) a teprve po tomto vyzkoušení v DC3 postupně s časovým odstupem na stejná zařízení v DC1 a DC2. Odstup bude zvolen podle typu zařízení, typu opravy a míře ohrožení existující zranitelnosti.
   b) Pro zařízení, která jsou v jedné lokalitě zdvojena, Provozovatel aplikuje balíčky postupně vždy nejprve na jedno a potom na druhé zařízení, pokud bude tento postup technicky možný. Odstup bude zvolen podle typu zařízení, typu opravy a míře ohrožení existující zranitelnosti.
   c) Dodavatel aplikuje najednou omezenou množinu oprav, aby byla usnadněna analýza případných problémů.
9. Pro řešení problémových stavů bude Provozovatel používat některý z následujících postupů, nebo jejich kombinace.
   a) Návrat k předcházející verzi software (tj. odstranění balíčku).
   b) Aktivace jiného zařízení jako náhrady.
   c) Omezení funkcionality zařízení, pokud se omezení nevztahuje na kritické funkce zařízení.
10. Všechny nouzové změny budou zaznamenány v registru změn a budou následně detailně zdůvodněny.
11. V pravidelných intervalech je prováděna kontrola registru změn pro zajištění, aby všechny žádosti o změnu byly řádně dokumentovány.

8.7 Správa systému

Pro bezpečnou správu systému (HW i SW) budou aplikována následující opatření:

1. Správu NIS IZS bude provádět pouze autorizovaný personál Provozovatele.
2. Bude vedena evidence všech prací při správě NIS IZS. Všechny práce v rámci správy systému budou zdokumentovány.
3. Během provádění správy NIS IZS je uživatelům umožněno používání systému.
4. Plánované údržby nebudou zasahovat do ostrého provozu NIS IZS.
5. Fyzický i logický přístup pracovníků provádějících správu NIS IZS bude řízen, dokumentován a kontrolován. Budou vypracovány postupy pro řízení přístupu.
6. Nepoužívané zařízení v rámci NIS IZS bude fyzicky chráněno (bezpečně uskladněno v prostorách k tomu vymezených).

8.8 Řízení kontinuity a obnova po havárii

Detailní požadavky a technický návrh řešení pro oblast BCM a DRP jsou uvedeny v kapitole *G. Spolehlivost* tohoto prováděcího konceptu. Z pohledu bezpečnosti budou Provozovatelem naplněny minimálně následující požadavky:

1. Pro NIS IZS budou vytvořeny plány kontinuity systému a postupy obnovení činností. Budou vypracovány plány krizového řízení.
2. Strategie řízení kontinuity činností bude vytvořena na základě analýzy dopadů a hodnocení rizik. Jsou identifikována rizika, která mohou způsobit narušení chodu organizace
3. Plány a postupy budou identifikovat zapojení jednotlivých osob a jejich odpovědností. Budou dokumentovány role a odpovědnosti osob a týmů mající pravomoci během a po incidentu.
4. Postupy a plány budou přezkoumávány a aktualizovány při významných změnách v procesech nebo technologií NIS IZS a vždy, když se odhalí nedostatky.
5. Všechny nouzové postupy a procesy budou dokumentovány, aby mohly být později vyhodnoceny.
6. Všichni pracovníci Zadavatele i Provozovatele budou seznámeni s postupy a procesy pro případ stavu nouze a budou pravidelně školeni v oblastech BCM a DRP.
7. Opatření BCM a DRP budou přezkoumávána pomocí procesů testování, auditu i sebehodnocení, aby bylo zajištěno, že jsou přiměřená, vhodná a účinná.

8.9 Bezpečnostní monitoring NIS IZS

Bezpečnostní monitoring zajistí Provozovatel systému. Bezpečnostní monitoring splní následující požadavky.

1. Hlášení o výskytu bezpečnostních událostí v reálném čase.
2. Možnost vyhodnocování údajů o provozu NIS IZS od všech komponent. To znamená, že produkt bude umět přijímat a zpracovávat data v těch formátech, ve kterých je produkují jednotlivé systémy a zařízení NIS IZS. Bude podporovat sběr dat pomocí standardních protokolů, které se pro tento účel používají (zejména syslog, SNMP, netflow, a WMI).
3. Vyhodnocování bezpečnostních událostí za zvolené období.
4. Vytváření standardních a příležitostných reportů.

Bude vytvořen registr bezpečnostních metrik a pravidel, na jehož základě budou vyhodnocovány události a budou nastaveny postupy pro řešení alertů a incidentů. Množina událostí, o kterých bude systém informovat pomocí alertů v reálném čase, bude minimálně zahrnovat následující bezpečnostní události:

1. Pokus o útok proti NIS IZS. Jde o události zaznamenané aktivními síťovými prvky, servery a aplikací v tom rozsahu, v jakém jsou tyto komponenty schopné útoky detekovat. Zahrnuje pokusy o (D)DOS útok, výskyt malware, výskyt nebezpečných anomálií v síťových protokolech použitých pro komunikaci mezi prvky NIS IZS.
2. Pokus o neoprávněné připojení zařízení do sítě NIS IZS. Půjde o detekci připojení zařízení k aktivním síťovým prvkům, které jsou součástí infrastruktury NIS IZS. Nepoužívané porty aktivních prvků budou deaktivovány. Aktivní síťové prvky budou nakonfigurovány tak, aby hlásily změnu stavu jakéhokoli portu „down“ –> „up“ i opačně. Bezpečnostní dohledový systém bude vyhodnocovat, zda jde o zapnutí zařízení na povoleném portu, nebo o připojení zařízení k portu, který by neměl být aktivní.
3. Změny přiřazení hardwarových adres síťových karet a jejich logických adres zařízení, která jsou součástí NIS IZS. Bude detekována změna přiřazení IP adres a MAC adres. Změna jejich přiřazení signalizuje, že buď LAN rozhraní nějakého zařízení byla DHCP serverem přiřazena nová adresa, nebo v zařízení byla vyměněna LAN karta, nebo že se někdo pokouší falšovat svoji totožnost. Předpokládá se, že IP adresy budou zařízením NIS IZS přidělovány staticky. V případě virtuálního prostředí dochází v některých případech k přirozené změně MAC adres virtuálních serverů, např. v případě migrace virtuálního serveru mezi fyzickými servery. Tyto situace budou ze sledování vyloučeny, aby nedocházelo k výskytu „false positive“ hlášení.
4. Pokus o změnu času některého zařízení NIS IZS. Jakýkoli pokus o změnu času zařízení NIS IZS může signalizovat pokus o narušení bezpečnosti NIS IZS. Správné nastavení času je podstatné při analýze bezpečnostních událostí, při některých metodách autentizace (certifikáty a bezpečnostní kalkulátory) a z hlediska důvěryhodnosti systémových a auditních záznamů.
5. Neúspěšný pokus o přístup k aktivnímu síťovému prvku NIS IZS. Jde o pokus o přihlášení, při kterém byl překročen maximální počet povolených neúspěšných pokusů.
6. Pokus o manipulaci s lokálním uživatelským účtem, nebo lokální uživatelskou skupinou na serveru NIS IZS. Týká se vytvoření, zrušení a změny účtu nebo skupiny. Jde o událost, ať byla operace úspěšná nebo ne a ať se jednalo o oprávněnou nebo neoprávněnou operaci. Předpokládá se, že lokální účty budou sloužit téměř výhradně pro servisní účely. Budou vytvořeny při instalaci NIS IZS a jejich změna bude výjimečná.
7. Neočekávaná aktivita pracovních stanic spojená s monitorováním prostředí, pokusy o distribuci malware nebo s únikem dat. Základní informace pro tuto analýzu je export netflow dat ze směrovačů.

Aby bylo možné požadované události sledovat, předpokládá se, že budou mít jednotlivé komponenty NIS IZS zapnuté logování a zapnutý auditing (viz návrh bezpečnosti NIS IZS v projektové fázi). Tím bude zajištěno, že vzniknou primární data o událostech podstatných z hlediska bezpečnosti přímo u zdroje. Tato data budou systémem bezpečnostního dohledu centralizována a centrálně vyhodnocována, oznamována (alerty) a prezentována.

Systém bezpečnostního dohledu (SIEM) bude upozorňovat na výskyt bezpečnostních událostí v reálném čase. Bude umožněno okamžité vyhodnocení událostí. Součástí bude uchování a

archivace bezpečnostních záznamů pro potřeby dodatečných analýz a vyšetřování. Provozovatel bude tato data pravidelně vyhodnocovat a na základě vyhodnocení bude případně přijímat dodatečná bezpečnostní opatření a kontrolovat účinnost existujících opatření.

Systém bezpečnostního dohledu (SIEM) a systém pro zaznamenávání systémových událostí (log management) bude naplňovat minimálně následující požadavky:

1. Rozsah zaznamenávaných dat (logů) bude nastavitelný a budou zaznamenány všechny informace o události dle registru metrik a pravidel.
2. Logy a záznamy budou bezpečně uloženy a archivovány. Vybrané záznamy budou archivovány minimálně po dobu 5 let.
3. Nearchivované logy a záznamy budou bezpečně ničeny v rámci předem ustaveného procesu.
4. Řízení přístupu k logům a záznamům bude přísně řízen. Viz kapitola Řízení privilegovaného přístupu k systému.
5. Všechny zaznamenávané události budou auditovatelné v souladu s registrem bezpečnostních metrik a pravidel. SIEM bude poskytovat nástroje pro práci s logy a záznamy. Prací je myšlené vyhledávání, filtrování, zobrazení detailu o auditním záznamu apod. Budou existovat prostředky pro analýzu logů a záznamů, které umožňují exportování do databázových a textových formátů.
6. V registru metrik a pravidel budou definovány události, které budou eskalovány dále k řešení v rámci procesu řízení incidentů. Budou vyšetřovány všechny podezřelé incidenty a zjištěné pokusy o narušení bezpečnosti.

8.10 Analýza technických zranitelností

Bude zajištěn proces pro řízení technických zranitelností, který zajistí, že každá identifikovaná zranitelnosti bude řádně řešena. Systém pro analýzu technických zranitelností (angl.. Vulnerability scanner) bude naplňovat minimálně následující požadavky:

1. Systém pro analýzu technických zranitelností bude napojen na všechna zařízení NIS IZS, aby se zjistilo, že nově se objevující zranitelná místa a slabiny v systému budou včas identifikovány a řešeny.
2. Analýzy technických zranitelností budou realizovány v pravidelných intervalech.
3. Bude kontrolována konfigurace síťových a systémových technických zranitelností, zda neobsahuje zranitelná místa.
4. Databáze známých zranitelností bude pravidelně aktualizována v minimálních intervalech dle možností dané technologie.
5. Pro řízení a správu technických zranitelností budou určeny role a odpovědnosti.

8.11 Zálohování a archivace

Zálohování je popsáno v kap. 1.4. části A - HW PKv51 a archivace v kap. 1.3. části A - HW PKv51. V rámci provozu budou naplněny základní bezpečností požadavky na provádění záloh:

1. Dodavatelem budou vytvořeny postupy pro zálohování, archivaci a skartaci dat.
2. Zálohy dat budou chráněny stejně jako ostrá data
3. Bude udržována více než jedna generace záloh.
4. Budou pravidelně testovány postupy zálohování a obnovování záloh.
5. Zálohy budou zahrnovat i programové vybavení všech aplikací.

8.12 Personální a organizační bezpečnost

Bude zajištěna jasná definice kompetencí, práv a odpovědností jednotlivých rolí v systému na straně Zadavatele i Provozovatele. Obsazení všech rolí bude dokumentováno a udržováno aktuální.

Důležitým prvkem pro zajištění bezpečného provozu NIS IZS je dostatek kvalifikovaného a důvěryhodného personálu. Existují osoby, které budou mít fyzický přístup k zařízením NIS IZS, a osoby, které budou mít privilegovaný (ve smyslu vysokých oprávnění) logický přístup k zařízením NIS IZS.

Dodavatel si je vědom rizik spojených s fyzickým přístupem a logickým privilegovaným přístupem osob k zařízením NIS IZS a věnuje proto pozornost výběru osob na příslušné pozice. Nábor pracovníků se řídí interními pravidly Provozovatele. Na všech pozicích je požadován čistý trestní rejstřík a na výše uvedené pozice je požadována odpovídající kvalifikace, provádí se kontrola životopisu a zjišťují reference. S pracovníky je uzavírána dohoda o mlčenlivosti.

Provozovatel zajistí obsazení rolí správců NIS (role viz část „I - Školení“) kvalifikovanými a důvěryhodnými osobami. Jde o osoby, které provádějí administraci, monitoring, dohledování a podporu 1. a 2. úrovně celého systému NIS IZS.

8.13 Personální bezpečnost

V rámci personální bezpečnosti budou naplněny minimálně následující požadavky:

1. Pro správu systému bude vytvořen dedikovaný tým po celou dobu využití systému.
2. Bude připraveno úvodní školení pro pracovníky pracující s informacemi a daty NIS IZS.
3. Budou stanoveny postihy, které hrozí zaměstnancům při zanedbání bezpečnostních požadavků.
4. Všechny osoby se vztahem k NIS IZS musí podepsat závazek o zachování mlčenlivosti, pokud pro ně požadavek mlčelivosti nevyplývá přímo ze zákona nebo z pracovně právního vztahu.
5. Bude stanovena strategie bezpečnostního vzdělávání a školení pro práci s NIS IZS (pro pracovníky Provozovatele i Zadavatele).
6. Bude provedeno školení všech pracovníků pro práci s NIS IZS, které bude přizpůsobeno roli, odpovědnostem a schopnostem dotyčné osoby.
7. Je vytvořena a udržována evidence zaměstnanců, kteří se zúčastnili školení pro práci s NIS IZS.

8.14 Organizace bezpečnosti

Bezpečnost NIS IZS bude organizačně řízena ze strany Provozovatele tak, aby byla vždy a za všech okolností zajištěna požadovaná úroveň bezpečnosti systému. Budou naplněny minimálně následující požadavky:

1. Za bezpečnostní činnosti v rámci NIS IZS budou stanoveny konkrétní role a odpovědnosti
2. Budou určeni pracovníci odpovědní za přezkoumání/audit stavu bezpečnosti NIS IZS.
3. Pracovníci, kteří se budou podílet na zajištění provozu NIS IZS, mají odpovídající vzdělání a praxi.

4. Provozovatel organizuje interní školení zaměstnanců v informační bezpečnosti a podle potřeby vysílá pracovníky na školení a kursy.

8.15 Řízení bezpečnostních incidentů

V provozu budou ustaveny postupy pro řízení bezpečnostních incidentů, které budou naplňovat minimálně následující požadavky:

1. Budou vytvořeny a zavedeny postupy pro řízení bezpečnostních incidentů, včetně schéma pro hlášení incidentů a podezření.
2. Budou vypracovány pracovní postupy pro řešení incidentů.
3. Incidenty budou hlášeny schváleným způsobem. Všechny slabiny bezpečnosti budou bez prodlení ohlašovány.
4. Bezpečnostní incidenty budou zaznamenány v souladu se zavedenými postupy pro hlášení incidentů.
5. Uživatelé NIS IZS nebudou sami odstraňovat vzniklé problémy, pokud k tomu nebudou odpovědnou osobou přímo vyzváni.
6. Budou shromažďovány důkazy na podporu odpovědných kroků proti osobám či organizacím.
7. Budou vyšetřovány všechny podezřelé incidenty a zjištěné pokusy o narušení bezpečnosti.
8. Vyšetřování bude prováděno odpovědnými pracovníky Dodavatele v rozsahu jeho kompetence. Zadavatel poskytne při vyšetřování bezpečnostních incidentů požadovanou součinnost.
9. Po skončení vyšetřování bude vypracovávána zpráva pro vedení Zadavatele i Provozovatele, která bude popisovat příčiny, škody a provedené nápravné činnosti.

8.16 Testování bezpečnosti NIS IZS

V průběhu používání systému NIS IZS budou v pravidelných intervalech prováděny sady bezpečnostních testů. Pro provádění testů budou stanoveny a naplněny následující požadavky:

1. Budou vytvořeny plány bezpečnostního testování NIS IZS v provozu a bude definována sada bezpečnostních testů.
2. Pro testování bezpečnosti NIS IZS jsou vytvořena akceptační kritéria.
3. Budou stanoveny výkonnostní a kapacitní požadavky na bezpečnost systému.
4. Testy budou zahrnovat testování bezpečnostních funkcí.
5. Budou stanoveny testy, data potřebná pro testy a odhadnuty výsledky testů.
6. Závěry testů budou rozděleny podle závažnosti.
7. Testování bude prováděno podle sady standardních bezpečnostních testů.
8. Testy budou sestaveny mj. na základě znalosti slabin systému.
9. Bezpečnostní testy budou kontrolovat prosazení bezpečnostních požadavků podle akceptačních kritérií.
10. Bude prováděna kontinuální kontrola, zda jsou v systému aktivovány bezpečnostní funkce stanovené systémovou bezpečnostní politikou NIS IZS.

8.17 Kontroly souladu

Předpokládá se, že systém NIS IZS bude procházet pravidelnými technickými i netechnickými audity a kontrolami, jejímž sponzorem může být Zadavatel, Provozovatel či třetí strana. Audity budou naplňovat následující požadavky:

a) Bezpečnostní audity jsou prováděny podle předem schváleného plánu, který je revidován minimálně jednou ročně.
b) Výsledky bezpečnostního auditu jsou předkládány vedení Zadavatele i Provozovatele.
c) Budou prováděny pravidelné i namátkové kontroly souladu faktického nastavení s bezpečnostními předpisy.
d) Budou explicitně určeny a zdokumentovány veškeré požadavky odpovídající zákonům, nařízením a smlouvám a tyto jsou pravidelně kontrolovány (včetně nově přijatých zákonů).
e) Bude pravidelně prováděn audit nainstalovaného programového vybavení na zařízeních NIS IZS a jsou realizována nápravná opatření v případě auditních nálezů. Budou implementována řešení zajišťující nepřekročení limitu stanoveného licencí.
f) Budou udržovány registry/seznamy všech aktiv/zařízení NIS IZS a je pravidelně prováděn soulad reálného stavu systému s registry.

8.18 Bezpečnostní dokumentace pro provoz

Pro NIS IZS bude vytvořena provozní bezpečnostní dokumentace, která bude zahrnovat všechny bezpečnostní požadavky na vývoj a provoz systému, včetně přesných určení rolí a odpovědností. Základní struktura bezpečnostní dokumentace NIS IZS bude následující:

1. Systémová bezpečnostní politika NIS IZS
2. Bezpečnostní směrnice/Administrátorský manuál NIS IZS
3. Bezpečnostní směrnice/Uživatelský manuál NIS IZS
4. Směrnice pro řízení bezpečnostních incidentů NIS IZS
5. Plány kontinuity a obnovy NIS IZS
6. Metodika pro identifikaci a hodnocení aktiv
7. Plán zvládání rizik a kybernetických bezpečnostních incidentů
8. Přehled právních a jiných závazných předpisů

9 Přílohy

9.1 Seznam obrázků