Technická specifikace

1 Popis projektu a společná kritéria

Projekt je koncipován jako ucelené řešení kybernetické bezpečnosti Zadavatele, nikoliv jako dodávka technologií. Skládá se z následujících provázaných celků:

- Technologie – souhrn řešení pro jednotlivé oblasti bezpečnosti, jež je tvořena konkrétními produkty s výkonnostními parametry.
- Integrace – způsob kooperace a míra provázanosti technologií tak, aby tvořily funkční celek s maximální přidanou hodnotou pro bezpečnost daného prostředí.
- Automatizace – scénáře pro abstrakci práce s technologiemi formou snadno použitelných předpřipravených akcí pro operátory bez nutnosti manuálního zásahu do konfigurace jednotlivých technologií.

Ke každé technologii bude vypracován Solution Design dokument, který popíše přesné zapojení do stávající infrastruktury, popis systémové konfigurace a provozní konfigurace, včetně integrací a veškeré interoperability s dalšími technologiemi. Nastavení konfigurace a uvedení do ostrého provozu musí být rozplánováno s ohledem na kapacitní možnosti Zadavatele, případně servisní okna daného prostředí dle dopadů na funkcionalitu. Solution Design musí být vzájemně odsouhlasen.

Konfigurační parametry dané definicí procesů a opatření musí být následně aplikovány na všechny technologie v rámci dodávky projektu a dále na existující technologie, které to dovolují (např. komunikační protokoly včetně úrovně zabezpečení, síla hesla, atp.).

Schopnost dané technologie zajistit konzistenci systémové konfigurace a procesovaných dat při zálohování a obnově je společným požadovaným kritériem pro všechny technologie v rámci dodávky.

Nezávisle na interních mechanismech dodávaných technologií musí být všechny napojeny na provozní monitoring skrze standardní otevřené protokoly typu SNMP, zasílat logy skrze Syslog, využívat centrální NTP a DNS službu pro sjednocení času a identifikace zařízení. Všechny technologie využívající certifikáty musí používat PKI definovanou v rámci projektu, přičemž je vyžadován standard TLS 1.2 či vyšší.

Všechny nově pořizované technologie projektu musí být pokryty podporou od výrobce po dobu minimálně 60 měsíců, a to v režimu NBD 5x9; preferovány jsou trvalé (perpetual) licence, v případě, že trvalá licence není k dispozici, pak subscription s plnou funkcionalitou na dobu minimálně 60 měsíců.

2 Část A – Identita a ochrana uživatelů

Tento dílčí celek adresuje systémy potřebné pro práci s identitou uživatelů a ochranu jejich komunikace. IDM systém pomáhá sjednotit identity daného prostředí a poskytuje integrační platformu pro práci s identitami (primárně uživatelskými). AntiSpam ochrana dále pro uživatele zajišťuje odpovídající preprocessing vstupních dat z externích subjektů (email), včetně možnosti interakce formou revize zpráv v karanténě. Další technologie v ostatních částech již neobsahují přímou interakci s uživateli, pokud tito nemají speciálně definovanou roli v rámci IT/bezpečnostních procesů.

2.1. Systém pro správu identit

Cílem IDM (Identity Management) je umožnit automatizovaně spravovat identity (osoby, uživatelské role a oprávnění) ve vybraných hlavních informačních systémech Zadavatele. Cílem je rovněž zavést automatizované nebo samoobslužné procesy pro přidělování oprávnění a zadávání žádostí o oprávnění a přístupů samostatnými koncovými uživateli organizace. V IDM bude možné takovéto požadavky schválit a změny nastavení u identit automatizovaně předat do integrovaných systémů a aplikací.

Systém bude nasazen pro cca 2200 zaměstnanců a 300 externistů.

Přehled klíčových high-level funkcionalit:

- správa životního cyklu uživatelů
- management přístupu k informačním systémům
- řízení a přidělování oprávnění a rolí
- možnost integrace s personálním systémem a dalšími klíčovými systémy Zadavatele
- logování ve všech částech a příslušná auditní stopa
- celkové přehledy nad oprávněními
- schvalovací workflow a notifikace

Systém IDM bude reflektovat veškeré potřebné změny související s životním cyklem identity v prostředí Zadavatele a ve vazbě na všechny informační systémy napojené na IDM, ve kterých bude mít daná identita uživatelské role a oprávnění.

Ve vztahu k napojeným systémům musí IDM zajistit samostatnou a úplnou správu v oblasti identity a uživatelských rolí vůči těmto systémům, včetně skupin uživatelů a systematizovaných míst. Ze strany Zadavatele není rozhodné o kolik politik a konfiguračních operací se na straně informačních systémů jedná, ale je pro něj důležitý výsledek, tedy například správné nastavení uživatelských rolí, zařazení do skupiny a konfigurace oprávnění pro všechny funkcionality Microsoft Active Directory užívané v prostředí Zadavatele. IDM bude autoritativním zdrojem informací o identitách a jejich účtech a přidělených rolích. IDM bude provádět správu automaticky, tak aby byly spravované systémy vždy aktuální.

Poskytnutá licence umožní nasazení a provoz systému bez omezení na počet uživatelů, spravovaných identit a napojených systémů. Nejsou přípustná žádná další omezení omezující obvyklé nasazení a provoz s ohledem na charakter organizace Zadavatele (počet záznamů, velikost databází atd.). Předpokládaný počet uživatelů je do 2000.

1. Systém musí umožnit zvyšování výkonu (zlepšování odezvy) rozložením komponent Systému na více serverů - minimálně oddělení rolí (serverů) uživatelského rozhraní od výkonu integračních a provozních úloh. Data systému budou uchovávána v databázi. Systém bude podporovat režim běhu ve vysoké dostupnosti.
2. Integrovaná správa aplikačních rolí včetně zařazení uživatele do odpovídající role v příslušných IS. V rámci dané role bude možné definovat jemné členění různých významů role. Například roli „editor webu“ bude možné rozšířit o významy odpovídající jednotlivým oddělením, pro které jsou části webu určené. Tyto rozšiřující významy rolí bude možné přímo přiřazovat systematizovaným místům, skupinám, organizačním jednotkám a uživatelům spravovaným v systému.
3. Systém umožní správu zákazových rolí. Zákazová role přiřazená systematizovanému místu, skupině, organizační jednotce nebo přímo uživateli zajistí odebrání této role v synchronizovaných systémech.

4. Systém umožní delegaci aplikačních rolí. Při delegaci jsou aplikační role předány na nového uživatele s možností nastavení do kdy je delegace platná. Následně jsou role vráceny delegujícímu uživateli a odebrány delegovanému.
5. Vestavěná detailní databázová historizace pro evidenci změn identit včetně referenčních objektů a vazeb mezi nimi. Historizace poskytne data v libovolném časovém okamžiku - aktuálním nebo zpětně v minulosti.
6. Podpora intuitivní tvorby pravidel v grafickém prostředí pro automatické vytváření uživatelských účtů, začleňování uživatelů do skupin a přiřazování aplikačních rolí uživatelům na základě kombinace libovolných atributů identity a přidružených referenčních objektů (organizační jednotka, aplikační role, systematizované místo atd.). Provádění vyhodnocení pravidel bude mít stejné vlastnosti jako jiné synchronizační procesy systému. Ruční vs plánované spuštění, historii běhů, simulační režim, atd.
7. Systém bude exportovat auditní logy pro systém typu SIEM ve formátu CSV nebo XML.
8. Systém obsahuje logování min. následujících typů událostí:
   - události systému (aplikační log)
   - změny entit evidovaných systémem a změny konfigurace systému (auditní log)
   - synchronizace s napojenými systémy (synchronizační log)
   - odeslané notifikace a upozornění (notifikační log)
9. Systém bude implementovat princip systemizovaných míst. Umožní systemizaci pracovních míst v souladu se strukturou organizace a bude spravovat jednotlivá systematizovaná místa a sadu oprávnění a rolí pro jednotlivé IS organizace vztažené ke konkrétnímu systemizovanému místu.
10. Systém umožní implementaci procesů a rozhraní, která jsou vyžadována v Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES.
11. Systém bude obsahovat webový portál (dále jen Portál), který bude sloužit jako hlavní rozhraní pro uživatele i správce pro přístup k datům, funkcím, správu a konfiguraci Systému.
12. Správa systému musí být implementována jako webová konzole/aplikace přístupná přes prohlížeče Internet Explorer verze 10 a vyšší a poslední verze prohlížečů Firefox, Chrom. Tato webová konzole musí být přístupná výhradně protokolem HTTPS.
13. Portál bude implementován s responzivním designem (přizpůsobení vzhledu typu zařízení, ze kterého je k portálu přistupováno).
14. Portál bude umožňovat přehlednou správu samostatných identifikovatelných objektů - referenčních objektů, na které se identity mohou odkazovat: min. systematizované místo, organizační jednotka, skupina, aplikace, skupina aplikací, aplikační role, certifikát.
15. Systém umožní přidávání a správu dalších typů referenčních objektů a to i v průběhu správy konkrétní identity s možností okamžitého použití referenčního objektu u spravované identity. Systém bude v modulu správy identit u scénáře správy konkrétní identity implementovat v grafickém rozhraní přímý odkaz (proklik) na referenční objekty, na která se daná identita odkazuje včetně toho, aby administrátor mohl po přechodu na tento odkaz vytvářet a editovat další referenční objekty a následně po vrácení zpět na detail identity je v tomto scénáři přiřadil dané spravované identitě.
16. Systém umožní nastavení samostatných nezávislých administrátorských oprávnění pro správu jednotlivých referenčních objektů.
17. Systém umožní dodatečné rozšiřování identit a referenčních objektů o další atributy a zajistí publikaci těchto nových atributů externím aplikacím prostřednictvím rozhraní webových služeb IDM.

18. Systém bude obsahovat grafické zobrazení identit (uživatelských účtů) ve stromové organizační struktuře. Součástí jednoho pohledu v systému bude zobrazení organizační struktury včetně systematizovaných míst organizace až do úrovně jednotlivých uživatelských účtů (identit). V grafickém zobrazení stromové struktury bude možné vyhledávat jednotlivé identity, systematizovaná místa, organizační jednotky.
19. Portál bude umožňovat vyhledávat i bez diakritiky (např. zadání Novak vyhledává i Novák apod.).
20. Správa uživatelů (identit) bude umožňovat i správu údajů o uživatelských digitálních certifikátech. Data o certifikátech bude možné nahrávat do systému prostřednictvím rozhraní webových služeb. Systém umožní automatické zneplatnění uložených certifikátů po vypršení data platnosti.
21. Systém umožní k jednotlivým účtům (identitám) přikládat obrázky - fotografie.
22. Systém umožní přesun identit mezi jednotlivými organizacemi či jejich odděleními.
23. Systém umožní kopírovaní aplikačních rolí mezi jednotlivými systematizovanými místy.
24. Systém bude obsahovat mechanizmus zabránění hromadným změnám z důvodu případných chybných vstupních dat (např. z personálního systému), aby nedošlo k hromadným nežádoucím změnám (například smazání objektů v Active Directory apod.).
25. Systém bude obsahovat přehled uživatelů aktuálně pracujících s Portálem.
26. Systém umožní sjednocení více uživatelů (identit) do jedné a odpovídající sjednocení spravovaných účtů.
27. Vestavěný export přehledů a seznamů zobrazených na Portále do souborů CSV nebo obdobného strojově zpracovatelného a současně běžně čitelného formátu.
28. Vestavěný editor filtrů pro vyhledávání identit a referenčních identit. Možnost filtrování libovolných atributů identity včetně přidružených referenčních objektů. Možnost uložení filtrů pro opakované použití.
29. Víceúrovňová správa administrátorských oprávnění s možností nastavení oprávnění min. na úrovni organizační jednotky (nebo hlouběji) a detailní přiřazení rolí a oprávnění (např. přiřazení činnostní role, přiřazení aplikační role, editace identity apod.).
30. Systém bude obsahovat editor oprávnění. V rámci editoru bude administrátor definovat oprávnění do Systému a následně tato oprávnění přiřazovat konkrétním uživatelům. Oprávnění bude definováno pro jednotlivé entity a moduly systému (identity, referenční objekty, konfigurace notifikací, konfigurace synchronizací, konfigurace systému, reporty, workflow, správa webových služeb IDM atd.). Dále bude oprávnění u entit (identit a referenčních objektů) definováno až na jejich konkrétní atributy včetně zobrazení / nezobrazení daného atributu, možnosti editace atributu uživatelem, povinnosti atributu, pořadí zobrazení atributů ve formuláři. U jednotlivých entit a modulů bude možnost definovat akce, které může uživatel s entitami v rámci systému provádět.
31. Na úrovní organizační jednotky bude možné pro výběr a přiřazování rolí nastavit sady povolených aplikační rolí, skupiny systematizovaných míst dostupných pro identity z dané organizační jednotky.
32. Systém umožní spravovat licence pro jednotlivé evidované aplikace a přiřazovat je jednotlivým uživatelům (identitám). Pro schvalování přiřazování licencí bude IDM obsahovat workflow platformu s možností vytváření víceúrovňových schvalovacích workflow.
33. Systém bude umožňovat přiřazení rolí konkrétní identitě, systemizovanému místu, skupině a organizační jednotce včetně možnosti nastavení data a času vypršení platnosti přiřazení. Po vypršení platnosti přiřazení systém roli přiřazenému objektu automaticky odebere.

34. Možnost přiřazení identit k systematizovaným místům ve vazbě M:N. Identita může být v systému evidována na více systematizovaných místech a současně na systematizovaném místě může být evidováno více identit.
35. Systém bude zajišťovat zobrazení přidělených rolí a jejich rozšiřujících významům k jednotlivým identitám s rozdělením na role navázané na systematizované místo, role navázané na identitu, role navázané na organizační jednotku, role navázané na skupinu. U identity musí být evidován a v systému souhrnně zobrazen seznam všech rolí včetně informace o tom, odkud uživatel roli zdědil nebo mu byla delegována (z organizační jednotky, systematizovaného místa, skupiny apod.).
36. Systém bude obsahovat správu skupin s možností začleňovat více skupin do sebe, přiřazovat do skupin jednotlivé uživatele i systematizovaná místa.
37. Systém bude obsahovat správu vztahů zastupitelnosti mezi uživateli. Musí umožnit uživatelům, aby v souladu se strukturou organizace mohli uživatelé delegovat v případě potřeby (dovolená, služební cesta) svoje role, nebo jejich část na jiné pověřené osoby a to i v režimu, kdy jeden uživatel může mít pro každou svou činnost nastaveného jiného uživatele jako zástupce.
38. Možnost delegování administrátorských práv.
39. Systém bude obsahovat samoobslužné uživatelské rozhraní pro reset hesla jednotlivých účtů daného uživatele. Zasílání kódů pro reset hesla danému uživateli musí být možno provádět pomocí SMS (tj. v systému musí být možné na SMS bránu či službu napojit). Rozhraní musí umožnit i běžnou změnu hesla (bez resetu).
40. IDM bude obsahovat samoobslužné uživatelské rozhraní pro zadávání žádostí o přidělení jednotlivých aplikačních rolí a členství ve skupinách. Role a skupiny budou kategorizovány a kategoriím bude možné přidělit schvalovací workflow nebo může být žádost vyřízena automaticky bez schválení.
41. Samoobslužné rozhraní umožní na úrovní organizace a organizační jednotky definovat seznam rolí a skupin o které mohou žadatelé požádat.
42. Systém umožní uživatelům individuálně nastavit vlastní zobrazení rozhraní - min. zobrazení / skrytí sloupců u všech seznamů, počet zobrazených záznamů na stránku - vždy pro každý seznam samostatně.
43. Integrované workflow pro řízení životního cyklu změn identit a schvalování změn. Funkční požadavky:
    - Zadávání požadavků uživatelů na změny v přiřazení rolí a skupin ke schválení nadřízeným
    - Možnost sledování stavu svých požadavků uživateli
    - E-mailové upozornění schvalovatele na požadavek ke schválení
    - Přehled úloh ke schválení pro každého schvalovatele
    - Schvalování či zamítnutí požadavků včetně uvedení zdůvodnění
    - Podpora vícekrokového schvalování
    - Podpora schvalování jedním nebo více schvalovateli (skupinou schvalovatelů)
    - Správce IDM může pracovat se všemi úlohami
    - Možnost větvení pro ošetření výjimek vzniklých při schvalování
    - Řešení zastupitelnosti
    - Eskalace - upozornění při překročení termínu splnění
    - Možnost vkládání systémových kroků s voláním webových služeb a spuštěním skriptů
44. Průběh workflow bude možné sledovat v grafické podobě ve formě diagramu, ve kterém bude zřejmý stav probíhajícího workflow. Diagram bude v obvyklém formátu pro zobrazení workflow např. aktivity diagram, BPMN nebo Archimate .

45. Systém zajistí zasílání konfigurovatelných emailových upozornění min. pro následující události: vytvoření a změna identity, referenčního objektu (systematizované místo, organizační jednotka, skupina, aplikace, skupina aplikací, aplikační role atd.), problém při synchronizaci, vypršení hesla v Active Directory, vypršení platnosti certifikátu. Mechanismus správy notifikací včetně náhledu na odeslané notifikace musí být spravován přímo v Portálu systému.
46. Portál bude obsahovat notifikační šablony a notifikace pro upozornění na vypršení hesla v Active Directory a vypršení platnosti certifikátů. Notifikaci lze nastavit na několik dní dopředu před vlastním vypršením hesla nebo certifikátu.
47. Šablony upozornění umožní definovat příjemce, předmět a obsah upozornění. U upozornění vázaného k identitám musí být možné nastavovat různé příjemce pro různé části organizační struktury (např. odbor, oddělení) apod. Šablony musí umožnit vložit do obsahu upozornění libovolný atribut identity a/nebo referenčního objektu.
48. U notifikací ve vazbě na identity a referenční objekty musí být možné konfigurovat nastavení na úroveň jednotlivých atributů. V šabloně musí být možné vybrat libovolné atributy identity a referenčních objektů a následně je vložit a použít v definici textu pro emailové zprávy. Dále musí být možné u notifikací konfigurovat podmínky pro provedení notifikace na základě hodnot jednotlivých libovolných atributů identity a referenčních objektů (například notifikace je generována pouze pro identitu v konkrétních uvedených skupinách, která má uvedenu konkrétní aplikační roli, systematizované místo, atd.). V Portálu musí být možné notifikace aktivovat pro jednotlivé zdrojové systémy, které v IDM změnu identity nebo referenčního objektu provedly.
49. Veškeré změny vyvolané požadavky uživatele a administrátorů/správců IDM budou provedeny transakčně. Budou logovány tak, aby bylo možné zpětně prokázat co, kdo a kdy měnil v identitách a referenčních objektech i v administraci a konfiguraci IDM. Záznam v logu bude obsahovat původní i novou hodnotu.
50. Veškeré požadavky na změny v IDM bude možné zadávat výhradně prostřednictvím Portálu. Není přípustné realizovat požadavky ručními změnami textových souborů jako XML, CSV, atd. z důvodu zajištění úplného logování všech změn jednotlivých konfigurovaných parametrů IDM.
51. IDM umožní export auditního reportu z údajů o identitách uložených v IDM a to i historických. Auditní reporty budou minimálně ve formátu XML nebo CSV a budou obsahovat souhrnné zobrazení daných uživatelů (identit) a jejich rolí v IS napojených na IDM, přiřazených skupin ve vybraném časovém okamžiku od aktuálního času do minulosti.
52. IDM bude obsahovat editor pro vyhledávání identit a referenčních objektů v systému IDM pro vytvoření reportu. Do filtru musí být možné zadat libovolné atributy identity, které jsou v systému IDM evidovány včetně přidružených referenčních objektů.
53. Vestavěné reporty obsahující uživatele s přímo přiřazenými aplikačními rolemi a s aplikačními rolemi delegovanými od jiných uživatelů. Reporty budou exportovatelné do CSV souboru.
54. IDM bude obsahovat možnost generovat do CSV souboru report uživatelů přiřazených aplikačním rolím a možnost nastavení pravidel pro automatické zasílání reportu emailem.
55. IDM bude obsahovat report, který do formátu PDF vygeneruje kartu uživatele obsahující informace o uživateli včetně seznamu rolí, které uživatel má, skupin, certifikátů, atd.
56. Automatické ukládání vygenerovaných reportů s možností pozdějšího zobrazení či stažení.
57. Snadné porovnání změn mezi vygenerovanými reporty stejného typu v prostředí Portálu.
58. Součástí IDM bude centrální dashboard, který bude obsahovat následující údaje:
    - Synchronizační úlohy v chybě
    - Chyby běhu synchronizací
    - Chyby při generování a odesílání notifikací

- Chyby volání metod rozhraní webových služeb IDM (např. pokus o přístup k metodě, na kterou nemá oprávnění)
- Chyby plánovaných úloh (agentů)
- Nově vytvořené poznámky
- Workflow v chybě
- Neúspěšné akce systému v systému IDM

Záznamy v dashboard se budou načítat za počet dnů definovaných v konfiguraci IDM.

59. IDM bude poskytovat rozhraní webových služeb pro napojení dalších systémů s možností konfigurace v Portálu.
60. Webové služby IDM budou definované v rozšířeném standardu WSDL a podporovat protokol SOAP. V rámci povahy předávaných identitních údajů (včetně osobních údajů) je požadováno zajistit maximální zabezpečení a zajištění spolehlivosti volání webových služeb minimálně v rozsahu specifikací WS–Security, WS-SecurityPolicy, WS-ReliableMessaging, WS-AtomicTransactions.
61. Konfigurace webových služeb umožní konfigurovat přístup pro volání jednotlivých vybraných služeb pro každý odpovídající systémový účet samostatně.
62. Volání webových služeb bude logováno na úrovni databáze a bude možné je zobrazit v prostředí Portálu.
63. Rozhraní bude poskytovat minimálně následující služby:
    - Načtení organizační struktury
    - Načtení hierarchie systematizovaných míst
    - Načtení seznamu identit
    - Načtení nadřízené osoby pro daného zaměstnance
    - Načtené seznamu aplikační rolí
    - Načtení seznamu uživatelů dané aplikace
    - Zápis seznamu aplikačních rolí do IDM
    - Zápis certifikátů do IDM
    - Zápis a změna uživatelů a osob
    - Zabezpečená služba pro přihlášení aplikace k IDM
    - Zabezpečená služba pro přihlášení uživatele k IDM
    - Přidání a odebrání uživatele do/z skupiny
    - Přidání a odebrání aplikační role a jejího rozšiřujícího významu na/z uživatele, organizační jednotku, systematizované místo nebo skupinu
    - Přidání a odebrání agendové role na uživatele nebo systematizované místo
64. Ruční i automatické spuštění synchronizací s propojenými systémy.
65. Spuštění synchronizací i v simulačním režimu pro ověření dopadu reálného spuštění bez ovlivnění produkčních dat a napojených systémů. Simulační logy budou zobrazitelné v Portálu.
66. Zobrazení jednotlivých stavů průběhu synchronizace bude k dispozici v přehledné grafické podobě.
67. Pro napojení na jednotlivé systémy a implementaci jejich synchronizací s IDM umožní IDM u každého systému využít více režimů synchronizací (za předpokladu podpory napojovaného systému):
    - Plná synchronizace – prochází všechny objekty v IDM a synchronizuje je s objekty daného systému.
    - Změnová synchronizace – synchronizuje vždy jen změny od poslední spuštěné synchronizace.

- Okamžitá synchronizace konkrétní identity na vyžádání – synchronizuje okamžitě pouze vybranou identitu.
- Rekonciliační synchronizace – synchronizace vytvoří rekonciliační report pro porovnání změn mezi nastavením identit a jejich oprávnění pro daný systém v IDM vs. nastavení identit a oprávnění přímo v připojeném systému.
- Simulační synchronizace – synchronizace vytvoří report očekávaných změn v napojeném systému pro provedení ostré synchronizace. Report změn bude evidován jako pohled nebo přehledná souhrnná tabulka.
- Historie běhu synchronizací – jednotlivé běhy synchronizací budou zaznamenány v databázi a dostupné v Portálu. Historie plné synchronizace bude obsahovat odkazy na objekty, které byly synchronizovány a log, co bylo u těchto objektů změněno v synchronizovaném systému. V případě změnové synchronizace pak bude v historii dále informace o události, která změnovou synchronizaci vyvolala.

68. Vestavěná správa jednotlivých synchronizací včetně nastavení připojení na synchronizované systémy, nastavení plné a změnové synchronizace, počet změn, které je možné zpracovat, závislostí mezi synchronizacemi, nastavení časového intervalu spouštění, nastavení intervalu odstávky. U jednotlivých synchronizací je rovněž požadováno, aby bylo možné vybírat organizace, které se mají z IDM synchronizovat s danými systémy. Správa bude součástí Portálu.
69. V rámci systému bude možné spravovat evidenci aktiv s klasifikací dle zákona o kybernetické bezpečnosti. V systému bude možné spravovat evidenci primárních, podpůrných a technických aktiv. Technická aktiva budou dále rozdělena na datová, softwarová, hardwarová aktiva, informační služby. Jednotlivá aktiva je možné členit do hierarchie aktiv.
70. Minimální rozsah evidovaných dat:
    - Základní údaje:
        - ID Aktiva - identifikátor
        - Název aktiva – označení aktiva
        - Popis aktiva – popis aktiva
        - Typ aktiva – typ aktiva
        - Kategorizace aktiva – kategorizace aktiva
        - Organizace – označení organizace daného aktiva
        - Stav aktiva – stav daného aktiva
        - Kód ISVS – číselný kód přidělený informačnímu systému veřejné správy
        - Datum identifikace aktiva
        - Lokalizace aktiva
        - Vazby na jiná aktiva
    - Analýza rizik:
        - Požadavky na dostupnost aktiva
        - Požadavky na důvěrnost aktiva
        - Požadavky na integritu aktiva
        - Celkové hodnocení aktiva – číselné hodnocení aktiva
        - Popis zabezpečení aktiva – popis způsobu zabezpečení aktiva
        - Frekvence přístupu – hodnota frekvence použití aktiva
        - Nedostupnost – popis hodnocení maximální doby nedostupnosti a definice náhradních postupů v případě nedostupnosti
    - Ochrana v rámci zpracování osobních údajů:
        - Klasifikace – klasifikace osobních údajů
        - Zdroj dat – popis získání osobních údajů

- Aktualizace – popis způsobu aktualizace osobních údajů
- Skartace – popis skartace dat
- Zpracování – popis způsobu zpracování osobních údajů
- Registrace – popis registrace zpracování osobních údajů na Úřad pro ochranu osobních údajů
- Kategorie – kategorie osobních údajů
- Účel zpracování – účel zpracování osobních údajů
- Zpracovatel – informace o zpracovateli osobních údajů
- Příjemce – informaci o příjemci osobních údajů v případě, že jsou předávány
- Legislativa – popis legislativy vztahující se k danému aktivu

- Garanti aktiv:
  - Vlastník – vlastník aktiva
  - Správce aktiva – správce aktiva (například dané aplikace)
  - Zástupce – zástupce správce aktiva
  - Uživatelé – seznam uživatelů daného aktiva. Uživatele bude možné slučovat do rolí a skupin
- Technické údaje (týkající se technických aktiv):
  - Technické prostředky (servery, databáze) – odkaz na technické prostředky, pro provoz a aktiva
- Zálohování – popis způsobu a frekvence zálohování.

71. Systém bude obsahovat správu osob, organizační struktury, rolí. Tuto evidenci bude možné synchronizovat s personálním systémem a navázat na správu aktiv.
72. Systém bude obsahovat funkcionalitu pro generování následujících reportů:
    - Přehled aktiv s možností filtrování a třídění podle všech dostupných polí
    - Karta aktiva se všemi navázanými údaji
    - Zobrazení vazeb mezi aktivy
    - Možnost definice vlastních sestav
    - Přehled žádostí o přidělení aktiva aktivních a dokončených
    - Přehled oprávnění a přístupů k danému aktivu
73. Systém bude obsahovat implementaci následujících workflow:
    - Žádost o přístup k aktivu směrovaná na seznam garantů jako schvalovatele žádosti
    - Periodická revize aktiv jednotlivými garanty
    - Periodická revize stavu evidence garantem z oblasti řízení bezpečnosti
74. Systém bude napojen na systém řízení autentizace uživatelů.
75. Systém umožní dodatečné konfigurační rozšiřování evidence o další atributy.
76. Systém poskytne rozhraní pro pravidelnou synchronizaci softwarových aktiv a jim přidělených uživatelům.
77. Systém bude obsahovat službu autentizace pro napojené systémy formou jednotného webového přihlášení Single Sign On. Systém bude řídit připojení třetích aplikací pro federovanou autentizaci a autorizaci (komunikace mezi poskytovatelem identity (IdP) a poskytovatelem služeb (SeP)) pomocí SAML 2.0 protokolu.
78. Systém zprostředkuje ověření identity vůči externím poskytovatelům identit NIA. Systém bude schopen fungovat v režimu IdP vůči poskytovatelů služeb (SeP). Systém bude dále vystupovat v režimu SeP vůči NIA.
79. Systém zprostředkuje autentizace formou OTP napojením na SMS bránu. Systém rovněž bude obsahovat modul pro zprostředkování autentizace přes DB systém a Active Directory.

80. Systém zajistí dle nastavení parametru v konfigurace platnost tokenu pro přihlášení Single Sign On pro napojené aplikace. Po vypršení tohoto časového intervalu bude nutné se opět autentizovat.
81. Systém obsahuje rozcestník pro výběr vhodného poskytovatele identit a autentizačního prostředku. Pro jednotlivé poskytovatele služeb (SeP) bude možné v platformě konfigurovat seznam povolených poskytovatelů identit (IdP) a úrovně autentizace.
82. Systém využije pro perzistenci dat diskové úložiště a databázový systém.
83. Systém bude pro koncové uživatele obsahovat funkcionalitu pro samoobslužné spárování účtu mezi původním účtem například s autentizací vůči DB a novým účtem využívaným v NIA.
84. Vestavěné obecné skriptovatelné (javascript, groovy) konektory pro správu identit v napojených systémech:
    - konektor pro spouštění CMD a powershell příkazů, SSH
    - konektor pro práci s CSV soubory
    - konektor pro práci s databázemi Microsoft SQL, Oracle
    - konektor pro napojení na SOAP webové služby
    - konektor pro napojení na REST webové služby
85. U jednotlivých konektorů je možné dynamicky měnit transformační logiku pro nutnou komunikaci s danými typy rozhraní.

Implementace

V rámci nasazení je požadováno:

- Předimplementační analýza a vytvoření prováděcího dokumentu, včetně návrhu metodiky:
    - jmenné konvence uživatelských jmen a zajištění jejich unikátnosti (sjednocení loginů)
    - mechanismu práce s hesly (přidělení, změna, samoobslužný reset...)
    - postupy správy uživatelů (zavádění, změny, rušení, nastavování oprávnění...)
    - návrh členění objektů v rámci IDM (osoby, účty, funkce, org. jednotky, skupiny...)
    - definice bezpečnostních zásad a pravidel pro práci s IDM
- Implementace IDM v produkčním prostředí
- Implementace požadovaných funkcionalit IDM
- Integrace na systémy dle požadavků na konektory specifikované v rámci funkčních požadavků
- Úspěšné provedení akceptačních testů
- Předání dokumentace skutečného provedení, databázového modelu a popis všech konektorů včetně vazeb
- Předání Administrátorské příručky
- Předání Uživatelské příručky

Integrace
Výčet aktuálně používaných systémů, které zadavatel plánuje integrovat:

- MS Active Directory
- Microsoft 365
- NIS FONS Akord
- NIS FONS Enterprise
- NIS Medicalc
- Laboratorní IS Envis LIMS
- Laboratovní IS OpenLIMS
- Systém pro správu zdravotnické obrazové dokumentace (PACS)
- Personální IS Avensio
- Lékárenský IS Mediox
- Spisová služba
- Ekonomický IS Helios
- Transfuzní IS Amadeus
- ServiceDesk Alvao

Konektor na Active Directory

IDM musí obsahovat konektor umožňující napojení na Microsoft Active Directory s následující funkcionalitou:

- komplexní správu účtů, kontaktů, certifikátů a skupin (založení, změnu atributů, zrušení, změnu hesla atd.)
- založení domovského adresáře včetně nastavení oprávnění
- správu účtů a jejich certifikátů včetně inicializačního načtení z AD
- správu skupin a členství ve skupinách včetně inicializačního načtení z AD
- správu organizačních jednotek včetně inicializačního načtení z AD

Konsolidace domén MS Active directory

Součástí nasazení systému IDM bude také sjednocení heterogenního prostředí MS Active directory jednotlivých nemocnic do unifikovaného jednotného identitního prostředí.

Dodavatel je povinen v rámci dodávky realizovat minimálně následující činnosti (případně další dle svých znalostí a zkušeností):

1) Analytická část konsolidace

a) Analýza a popis aktuálního stavu AD
- Zmapování současných adresářových, autentizačních a identitních služeb a jejich vazeb v jednotlivých subjektech
- Analýza uživatelských účtů, skupin a řízení uživatelských identit
- Analýza a popis základních síťových a serverových služeb a požadavků na jejich funkcionalitu
- Posouzení síťové topologie, vzájemného propojení dotčených subjektů z hlediska požadavků AD
- Zmapování požadavků na správu AD prostředí
- Analýza současných infrastrukturních zdrojů z hlediska AD
- Analýza současných ICT personálních zdrojů z hlediska potřeb pro realizaci změny a následné provozování AD
- Analýza stavu koncových stanic
- Zmapování aplikací využívajících AD autentizaci
- Zmapování nároků na licenční pokrytí

b) Analýza a popis aktuálního stavu emailových služeb
- Zmapování současných emailových služeb a jejich vazeb v jednotlivých subjektech
- Zjištění kvantitativních údajů (velikosti schránek, počty, obsazené místo)
- Individuální a skupinové mailboxy, aliasy, distribuční listy
- Analýza mail flow, využité protokoly, způsob ověřování uživatelů
- Analýza zabezpečení mailů
- Analýza klientského prostředí
- Zmapování nároků na licenční pokrytí
- Zmapování nároků na výpočetní zdroje

c) Rekapitulace - zhodnocení stávajícího stavu

2) Návrhová část konsolidace
a) Definice cílů konsolidace
b) Návrh cílového stavu, architektura
- Architektura a technický popis struktury AD – fyzický a logický model, včetně vazby na MS Entra ID
    (1) Fyzická infrastruktura
        (a) Doménové řadiče
        (b) Sites
        (c) Subnety
        (d) Rozmístění FSMO rolí
        (e) Konektivita
        (f) Vazba na DNS
    (2) Logická struktura
        (a) Organizační jednotky
        (b) Účty uživatelů, počítačů, serverů, skupin
        (c) GPO, logon skripty

(d) Atributy uživatelských účtů
(e)

(3) Bezpečnost

(a) Bezpečnostní politiky
(b) Certifikáty
(c) Kerberos protokol
(d) Audit policy
(e) Politiky hesel a zabezpečení

- Architektura a technický popis poštovních služeb, včetně vazby na M365 cloud
- Strategie nasazení v dotčených subjektech
- Stanovení kapacitních nároků na serverový fyzický resp. virtuální hardware a případné posílení či úpravu komunikační síťové infrastruktury
- Organizační pohled – popis organizačních změn (pokud budou třeba) v implementačních/konsolidačních fázích a při běžném provozu; odhady a zdůvodnění potřebných interních/externích zdrojů
- Rámcový harmonogram a návrh etapizace konsolidace AD a poštovních služeb, včetně popisu očekávaných výstupů jednotlivých navrhovaných etap
- Odhad kapacit potřebných lidských zdrojů, a to jak interních, tak externích členěných dle jednotlivých etap a fází implementace
- Požadovaná součinnost na straně Zadavatele
- Návrh a popis projektové metodiky pro vlastní realizaci implementačního projektu.

3) Realizace konsolidace domén
- Realizace infrastrukturní části AD
  i) Instalace a konfigurace DC
  ii) Security hardening AD prostředí
  iii) Zavedení Active Directory Administrative Tier modelu (správa/delegování administrativních oprávnění)
  iv) Propojení stávajících AD struktur (vztahy důvěryhodnosti, SID filtering)
  v) Síťové služby - integrace na stávající prostředí (DNS, NTP, DHCP)
  vi) Model řízení přístupu ke zdrojům
  vii) Model řízení uživatelských účtů a skupin
  viii) GPO model
- Integrace na MS Entra ID
  ix) Instalace a konfigurace konektoru MS Entra ID Connect
  x) Synchronizace identit on-premise AD a cloud
  xi) Parametrizace
- Integrace poštovního systému, přizpůsobení mail flow
  xii) Konfigurace virtuálních složek
  xiii) Úprava send a receive konektorů pro SMTP bránu
  xiv) Nastavení RBAC a write scope dle administračních OU
  xv) Nastavení SPF, DKIM, DMARC a DANE
  xvi) Případná konfigurace federace na ADFS
  xvii) Nastavení bezpečnostních bran a prvků
- Instalace a customizace nástrojů, skriptů a podpůrných služeb pro provedení migrace AD a poštovních systémů
- Provedení migrace AD v jednotlivých subjektech:
  i) příprava, testování, řešení dopadů

ii) Příprava a migrace dat ze stávající adresářové služby (účty, skupiny a další objekty) včetně transformace jejich názvů do harmonizovaného tvaru dle jmenných konvencí centrální domény
iii) Požadovaný postup migrace pro koncové stanice
(1) Pilotní migrace na stanovené množině koncových stanic a uživatelů, odladění migračních nástrojů, ověření funkčnosti účtů, stanic, pošty a klientského prostředí
(2) Předání nástrojů a zaškolení lokální správy IT pro provádění dávkové migrace dalších koncových stanic vlastními administrátory
(3) Dodavatel bude poskytovat podporu během migrace koncových stanic, bude odstraňovat případné nestandardní stavy a poskytovat konzultace

- Provedení migrace mailových schránek ze stávajícího do nového systému v jednotlivých subjektech
  i) Konfigurace úložiště mailových zpráv
  ii) Provedení transportu mailových dat
  iii) Integrace mailového klienta na nové mailové řešení
  iv) Případná rekonfigurace mobilních klientů na nové mailové řešení
- Konfigurace centrálních prvků zabezpečení mailového systému a mailové hygieny
- Provedení dokumentace nastavených hodnot
- Základní zaškolení administrátorů

Konektor na ostatní systémy z výčtu

IDM musí obsahovat konektor umožňující napojení s následující funkcionalitou:

- inicializační načtení dat
- správu lokálních identit
- správu oprávnění pro jednotlivé uživatele na moduly IS (správa konfiguračních skupin)

2.2. Systém certifikačních autorit, autentizace certifikátem (PKI)

Je požadováno vybudování interní certifikační autority PKI (Public Key Infrastructure – architektura veřejných klíčů), která bude ve správě Zadavatele. Zaměstnanci se tak budou moci jednoznačně a bezpečně identifikovat například při přístupu do sítě nebo do významných aplikací.

Záměrem je doplnit do infrastruktury bezpečnostní vrstvu vybudovanou na bázi PKI. Implementace PKI by měla doplnit bezpečnostní funkce, jako jsou například zabezpečení komunikace (SSL apod.) nebo autentizace serverů vůči počítačům a uživatelům. Část PKI je určena pro vydávání uživatelských certifikátů na čipové karty a následné zavedení dvoufaktorové autentizace jako náhrady autentizace jménem/heslem.

Pro implementaci PKI je požadována technologie, která je nativně podporována v prostředí Active Directory - certifikační služba na platformě MS Windows Server.

V rámci dodávky bude v prostředí vybudována hierarchie certifikačních autorit. Vybudované certifikační autority budou podřízeny pod jedinou kořenovou CA, a to:

- autorita pro vydávání uživatelských certifikátů
- autorita pro vydávání certifikátů serverů, počítačů a prvkům infrastruktury

Všechny vydávající CA budou mít vydán certifikát z kořenové CA, která bude offline a bude chráněna prostředky na úrovni fyzické bezpečnosti. K certifikačním autoritám bude existovat provozní i bezpečnostní dokumentace.

Provozní a bezpečnostní koncept PKI Zadavatele
Požaduje se zpracování dokumentu cílového konceptu PKI v prostředí Zadavatele. V rámci konceptu budou navrženy jednotlivé aspekty PKI:

- hierarchie CA
- infrastruktura PKI
- bezpečností perimetry a jejich separace
- vlastnosti a parametry jednotlivých CA
- bezpečnostní koncept PKI, role, oprávnění, ochrana aktiv
- typy vydávaných certifikátů a vlastnosti příslušných šablon certifikátů
- parametry certifikačních autorit (1 CA kořenová, 1 CA pro vydávání uživatelských certifikátů a 1 CA pro vydávání certifikátů pro počítače, servery, infrastrukturu)
- definice distribučních bodů CRL a certifikátu CA
- návrh konceptu zálohování CA

Koncept PKI bude v souladu s bezpečnostními politikami Zadavatele. Podle navrženého konceptu PKI budou následně implementovány PKI subsystémy do prostředí Zadavatele.

2.3. Pokročilá AntiSpam ochrana

Nasazení systému zajišťujícího kontrolu proti spamu, virům a malware u emailů, které projdou přes emailový server. Dále budou propuštěny pouze emaily, které budou splňovat nastavená kritéria. Systém na bázi integrace SaaS služby integrované s M365 prostředím. Licenční model dle počtu chráněných uživatelů.

Architektura řešení
SaaS řešení integrované do M365 prostředí. Předpokladem je zařazení ochrany za standardní bezpečnostní mechanismy poskytované v rámci MS 365 platformy. Řešení nesmí vyžadovat pro svůj běh dedikované HW požadavky na on premise síti dodavatele ani v cloudu.

Licenční pokrytí
Dodávka musí poskytnout SW licence dle uvedené výkonnostní specifikace , a to v počtech uvedených v příloze č. 1 – Krycí list této zadávací dokumentace.

Minimální požadavky

- Řešení musí být nabízené formou SaaS služby bez nutností změny stávajícího MX záznamu
- Řešení musí být integrované do O365 pomocí cloudového API
- Řešení musí podporovat integraci s následujícími službami: O365 Mail, O365 OneDrive, O365 SharePoint, MS teams
- Řešení musí fungovat v Inline módu s možností zachycení phishing/malware emailu předtím než dorazí do inboxu uživatele
- Řešení musí kontrolovat i odchozí maily
- Onboarding musí proběhnout bez nutnosti manuální konfigurace O365, pouze udělením oprávnění při onboardingu
- Rešení musí obsahovat ochranu proti známému i neznámému malware v příloze mailu
- Rešení musí obsahovat ochranu proti známému i neznámému

- Řešení musí obsahovat prevenci spamu
- Řešení musí obsahovat DLP
- Řešení musí detekovat používání ShadowIT software/služeb (software v organizaci, který není oficiálně podporovaný IT oddělením organizace)
- Přílohy mailů musí být kontrolované formou sandboxingu pro detekci zero-day hrozeb s možností CDR (content disarm and reconstruction)
- Podpora URL emulace - možnost bezpečného zobrazení náhledu obsahu webové stránky na kterou URL odkazuje v administrátorské konzoli
- Možnost tvorby politiky s granularitou na jednotlivé uživatele a na Azure AD skupiny
- Možnost pokročilého vyhledávání hrozeb a tvorba vlastních dotazů
- Možnost použít předpřipravené dotazy v politice
- Možnost nahrazování URL odkazu v těle mailu i v příloze s možností následné kontroly zda a který uživatel na odkaz klikl
- Vyhodnocování reputace URL odkazu v těle mailu i v příloze
- Detekce impersonifikace, kdy se odesílatel mailu vydává za osobu v organizaci, která je cílem mailu. Řízení impersonifikace na základě Azure AD skupin.
- Detekce šifrovaných příloh s možností pozdržení přílohy a automatického vyžádání hesla od uživatele k dešifrování souboru a následnému skenování na přítomnost malware
- Detekce resetu hesla uživatele
- Detekce, že uživatel odesílá malware
- Detekce, že uživatel vytvořil pravidlo pro smazání všech příchozích mailů
- Detekce, že se uživatel přihlásil poprvé z nové země (geo detekce)
- Detekce, že uživatel přeposílá všechny příchozí maily do externí/soukromé schránky
- Detekce, že se uživatel přihlásil poprvé z netradiční země (např. Honduras atd.)
- Detekce, že uživatel používá zranitelný prohlížeč
- Možnost definování Allow a Block listů pro URL, typy souborů v příloze a ochraně proti phishingu
- Možnost mailové karantény
- Možnost sledování SLA pro požadavky uživatelů na uvolnění z karantény
- Možnost archivace mailů až na 10 let
- Možnost auditního logu se záznamem pro přístup administrátora k hlavičce nebo tělu/obsahu mailu
- Možnost vyčlenit specifickou admin roli pro přístup k tělu/obsahu mailu
- Možnost zobrazení O365 BCL a SCL skóre mailu v logu, nebo reportu

3 Část B – Systémy pro ochranu infrastruktury a zařízení

Část B obsahuje systémy a technologie potřebné pro zabezpečení infrastruktury a dat, která jsou v ní procesována. Požadovaná řešení jsou určena na ochranu IT a OT prostředí, zejména před hrozbou malware, která je takto vyhodnocována a eliminována na několika úrovních. Jakožto technologický celek daných parametrů zajišťuje potřebnou interoperabilitu a zejména možnost okamžité automatizované reakce na rizika a konkrétní incidenty. Bez této provázanosti nelze eliminovat rizika dostatečně rychle a není možné zamezit efektivně horizontálnímu šíření hrozeb.

3.1. Zabezpečení proti škodlivému kódu a analýza aktivit na koncových stanicích a serverech

Zadavatel požaduje nástroj pro ochranu před škodlivým kódem na koncových stanicích s možností reakce na bezpečnostní incidenty (Endpoint Detection & Response – EDR nebo eXtended Detection & Response – XDR). Je vyžadováno, aby se řešení sestávalo z jednoho agenta na koncových systémech a centrální správy s jednou webovou konzolí pro kompletní správu. Agent nesmí vyžadovat konektivitu do cloudu nebo centrální správy pro poskytování ochrany před škodlivým kódem.

Dodávané řešení Endpoint Detection & Response musí splňovat alespoň následující funkce a parametry.

Licenční pokrytí

1. Zajištění licenčního pokrytí všech systémů uvažovaných v projektu dle specifikace v příloze č. 1 – krycí list.
2. Všechny níže uvedené funkce jsou součástí dodávané licence.
3. Retence dat alespoň 90 dní pro detekované bezpečnostní incidenty a události a 60 dní pro telemetrická data.

Architektura řešení

1. Centrální správa řešení musí být provozována v síti Zadavatele nebo jako SaaS cloudové řešení. V případě cloudového řešení je nutné, aby data byla uložena a zpracovávána na serverech v EU.
2. V případě on-premise varianty centrální správy musí být podporován provoz na virtualizační platformě.
3. Zadavatel preferuje v případě on-premise řešení provoz centrální správy dodané jako kompletní virtuální appliance.
4. Řešení nevyžaduje pro ukládání dat externí databázi (v opačném případě je nutné do ceny řešení promítnout i cenu na pořízení a provoz takové databáze).
5. Agent musí podporovat následující operační systémy:
    a. Windows 10, 11 a případné novější verze
    b. Windows Server 2012 R2, 2016, 2019, 2022 a případné novější verze
    c. Linux distribuce RHEL (7, 8, 9), CentOS (7) a Rocky Linux (8, 9) a případné novější verze
6. Běžný provoz agenta nesmí mít dopad na výkon koncové stanice (předpokládá se maximálně 3 % CPU, 200 MB RAM).
7. Instalace ani aktualizace agenta nesmí vyžadovat restart koncového systému.

Ochrana proti škodlivému kódu

1. Řešení nesmí spoléhat primárně na signaturní detekci nebo reputační engine.
2. Řešení musí umět detekovat pokročilé hrozby, alespoň:
    - souborový malware
    - fileless útoky
    - neznámý malware
    - exploity
    - ransomware
    - cryptominer malware
    - škodlivé skripty
    - lateral movement
    - pokusy o exploitaci zranitelností
    - pokusy o zajištění persistence

- pokusy o neoprávněnou eskalaci privilegií
- známé ransomwarové techniky (například mazání shadow copies)

3. Výše uvedené musí dokázat agent detekovat i bez nutnosti konektivity do cloudu nebo centrální správy.
4. Detekci malware musí řešení umožňovat ve dvou fázích, jak před samotným spuštěním (pre-execution), tak i za běhu (run-time).
5. Řešení musí umožňovat automatizovanou reakci na detekované hrozby, alespoň:
   - notifikace o detekované hrozbě uživateli i administrátorovi řešení
   - vynucené ukončení škodlivého/podezřelého procesu
   - přesunutí škodlivých/podezřelých souborů do karantény
   - odpojení napadené stanice od sítě a zachování komunikace pouze s centrální správou
   - kompletní remediace útočníkových aktivit (vynucené ukončení procesů, smazání zdrojových souborů útočníkových aktivit, obnovení konfigurace OS do původního stavu)
   - možnost automatické obnovy souborů v případě ransomware incidentu
6. Řešení musí umožňovat provést jakoukoliv z výše uvedených aktivit také manuálně z centrální správy.
7. Agent na koncových systémech musí být schopen detekovat a zabránit pokusům o jeho vypnutí, poškození nebo jakoukoliv manipulaci s jeho soubory.
8. Odinstalace nebo vypnutí agenta musí být umožněna pouze po zadání hesla. Zadavatel požaduje možnost specifického hesla pro každého nainstalovaného agenta. Řešení musí podporovat funkci hromadné odinstalace za využití jednotného hesla, kterou ale je nutné nejprve zapnout.
9. Systém musí umožnit vytváření politik s možností výběru detekčních enginů/modulů.
10. Zadavatel požaduje možnost manuální i automatické analýzy v sandboxovém prostředí. Tato funkcionalita může být nabídnuta i jako add-on licence.

Další požadované funkce agenta

1. Agent musí poskytovat vlastní lokální firewall nebo umožňovat správu nativního OS firewallu (pro všechny platformy – Windows, Linux, macOS). V případě vlastního řešení pro lokální firewall je požadována podpora FQDN, IP, CIDR.
2. Agent musí poskytovat možnost spravovat připojitelná zařízení (device control modul) alespoň pro USB rozhraní.
3. Agent musí poskytovat informace o instalovaných aplikacích na koncovém systému v rozsahu alespoň:
   - název aplikace
   - vydavatel / výrobce
   - verze aplikace
   - datum instalace

EDR funkce

1. Telemetrická data musí být dostupná po dobu alespoň 30 dní s možností rozšíření až na 1 rok.
2. Agent v rámci telemetrických dat musí umožňovat sbírat informace v rozsahu alespoň:
   - vytvoření procesu
   - vytvoření, smazání, modifikace a přejmenování souboru
   - URL, DNS, IP adresa síťové komunikace
   - informace o přihlášení a odhlášení uživatele
   - aktivity v rámci registrů – vytvoření, smazání a modifikace klíče a vytvoření, smazání a modifikace hodnoty

- vytvoření a spuštění nové plánované úlohy
- logování příkazů zadávaných v CLI ručně nebo skriptem
- načtení DLL knihovny

3. Řešení musí umět korelovat alespoň výše uvedené spolu související události a pro takové související události umožňovat jejich vyčítání (například pomocí unikátního ID) i pro události, které nebyly detekované jako podezřelé nebo škodlivé.
4. Řešení musí umožňovat v rámci investigace incidentu zobrazení tzv. process tree a časové osy událostí.
5. Řešení musí podporovat tvorbu vlastních detekčních / alert pravidel na základě alespoň níže uvedených parametrů:
   - vytvoření definovaného procesu
   - vytvoření definovaného souboru
   - komunikace na definovanou doménu
6. Řešení na základě výše uvedených vlastních detekčních pravidel dokáže kromě hlášení detekce aktivity také preventovat (terminace procesu, blokace spuštění procesu).
7. Řešení musí umožňovat alespoň následující manuální response aktivity:
   - zobrazení zprávy uživateli
   - stažení libovolných souborů z koncové stanice pro účely detailní analýzy
   - nahrání skriptů na koncovou stanici a jejich vzdálené spuštění
   - vzdálené terminálové připojení k stanici
8. Výše uvedené terminálové připojení ke stanici musí být plně auditováno (který uživatel se připojoval, na jakou stanici, jaké aktivity prováděl).
9. Zadavatel požaduje možnost vzdáleně se připojit k terminálové relaci pouze uživatelům s příslušným oprávněním.

Automatizace

1. Řešení musí umožnit automatizaci incident response playbooků alespoň v rozsahu:
   - síťová izolace zařízení v případě definovaného incidentu (např. kritická závažnost, ransomware, lateral movement a podobně)
   - přiřazení striktnějších prevenčních politik v případě detekovaného incidentu
   - automatické získání škodlivého souboru z infikovaného zařízení v případě detekovaného incidentu (aby nedošlo k jeho smazání dříve, než dojde k manuální analýze SOC analytikem)
   - zaslání podezřelého souboru do sandboxu v případě detekovaného incidentu souvisejícím se spustitelným souborem, jehož reputace není známá

Kvalita detekce a úroveň visibility

1. Za rozhodující faktor se považuje hodnocení z MITRE ATT&CK Evaluations 2023 (5. kolo s označením Turla, poslední zveřejněné v době vytváření technické specifikace):
   - řešení musí úspěšně detekovat (kategorie Technique, Tactic, General) alespoň 80% technik (substeps) v scénáři Carbon a Snake na Windows a zároveň na Linux platformě
   - řešení musí úspěšně zablokovat alespoň 80 % testovacích scénářů v testech Protections

Centrální správa

1. Centrální správa musí umožňovat hierarchické dělení zařízení do skupin.
2. Řešení musí umožňovat snadné a efektivní nastavení výjimek na definované skupiny zařízení. Je požadováno, aby vybrané zařízení mohlo být členem více skupin.
3. Řešení pro aplikaci výjimek nesmí vyžadovat restart zařízení.

4. Zadavatel požaduje, aby bylo možné vynutit vícefaktorovou autentizaci do centrální správy alespoň pomocí TOTP.
5. Řešení musí umožňovat zasílat alespoň následující notifikace pomocí SMTP:
   - detekce podezřelého nebo škodlivého incidentu / události
   - vypnutí agenta
   - odinstalace agenta
   - otevření terminálového remote shell spojení
   - provedení síťové karantény zařízení
   - odebrání zařízení ze síťové karantény
6. Řešení poskytuje detailní auditování uživatelských aktivit.
7. Řešení musí poskytovat alespoň následující typy reportů:
   - management report s počtem detekovaných hrozeb, stavem mitigace a změnou oproti předchozímu období / reportu, počtem instalovaných agentů
   - přehled hrozeb, typ hrozby, způsob detekce, způsob mitigace, datum a čas detekce, infikované systémy, verdikt analytika (true vs false positive) a stav incidentu
   - seznam všech agentů se zobrazením alespoň IP adresy, OS, skupiny, verze agenta, poslední konektivity do centrální správy

Integrace

1. Řešení musí disponovat rozhraním REST API pro integraci s interními systémy zákazníka.
2. Řešení musí být schopno integrace na tiketovací systémy.
3. Řešení musí být schopno integrace na systémy sbírající a korelující logy.
4. Řešení umožňuje integraci na Threat Intelligence služby za účelem ověřování vůči aktuálním reputačním databázím (minimálně IP adresy a hashe).

Implementace

V rámci implementace je požadováno:

1. Vytvoření dokumentu Solution Design s popisem architektury, jednotlivých komponent, návrhu hromadného rolloutu, akceptačních testů, pilotního testování.
2. Instalace centrální správy a hardening serverových komponent (OS, webový server, databáze) v případně on-premise varianty. Zprovoznění centrální správy v případě cloudové varianty.
3. Konfigurace centrální správy, vytvoření uživatelů a skupin, nastavení SMTP reportingu, vytvoření nebo úprava dashboardů po domluvě s administrátory Zadavatele. Volitelně nastavení SSO.
4. Nastavení skupin zařízení, konfigurace politik, známých výjimek.
5. Instalace na pilotní vzorek zařízení, vyladění politik a vytvoření potřebných výjimek na 3rd party software.
6. Podpora během hromadného rolloutu.
7. Vytvoření provozní dokumentace – popis běžných operativních aktivit, upgradu agentů a komponent, instalace a odinstalace (manuální i hromadné), troubleshooting.
8. Vytvoření uživatelské dokumentace.
9. Realizace akceptačních testů.
10. Školení pro administrátory řešení.

3.2. Systém pro ochranu před moderním malwarem a Zero-day útoky

Řešení pro ochranu uživatelského provozu a eliminaci hrozeb pomocí emulace pro potenciálně rizikové soubory. Ochrana bude vynucena pro veškerý mailový provoz, selektivně pro webový provoz a pro průběžnou kontrolu dokumentů na sdílených uložištích. Přípustné je pouze řešení ve formě dedikovaných appliance, tak aby data nebyla zasílána mimo infrastrukturu provozovatele. Každá appliance musí být schopna pokrýt následující výkonnostní parametry a jejich umístění bude v nezávislých lokalitách pro georedundanci.

Sandbox appliance zpracovává dokumenty poskytnuté firewall řešením a není zapojena inline v cestě datového toku infrastruktury. Appliance musí být schopna provádět kontrolu souborů zaslaných přes API rozhraní.

1. Minimální propustnost 1200 souborů za hodinu.
2. Licence potřebné pro kontrolu Windows systémů v počtu odpovídajícím maximálnímu počtu virtuálních instancí dané appliance musí být součástí dodávky.
3. Minimálně 2x napájecí hot-swap zdroj.
4. Možnost stažení reportu ke každému podezřelému souboru s popisem jeho analýzy.
5. Všechny dokumenty musí být emulovány výhradně lokálně.
6. Hodnota BTU menší než 1650.
7. Podpora ICAP protokolu.
8. Možnost využití otevřeného API pro kontrolu zaslaných dokumentů.
9. Dodávka včetně příslušenství pro montáž do racku.

Integrace

Události ze sandbox appliance musí být korelovány v jednotném managementu společně s firewall řešením, které tuto integraci zajišťuje. K sandbox řešení se může připojit paralelně několik instancí firewallu a využívat výkon dle aktuálních realtime provozních požadavků bez nutnosti rekonfigurace.

3.3. Systém pro ochranu klinické přístrojové techniky

Systém musí provádět pasivní (tj. bez explicitní komunikace směrem ke koncovým zařízením) detekci klinické přístrojové techniky a dalších IoT technologií. Takto vytváří evidenci a díky široké databázi a schopnosti rozpoznání jednotlivých technologií vytváří také kategorizaci do logických celků. Součástí řešení je také vizualizace komunikační matice, rozpoznání zranitelností a granulární nastavení risk skóre zařízení dle nalezených parametrů. Systém musí poskytovat informace a reporty o používaní zdravotnické techniky, a to nejen dobu po kterou je zařízení online, ale i počet a případně typ zákroku na zařízeních zobrazovací techniky propojených přes DICOM standard.

Dodávané řešení zabezpečení zdravotnických zařízení musí splňovat alespoň následující funkce a parametry.

Licenční pokrytí

Systém musí být poskytnut formou virtuálního zařízení do virtualizovaného prostředí. Požadována je licence do prostředí obsahujícího 950 zdravotnických prostředků bez omezení počtu koncových IoT zařízení.

Primární funkcionality systému

Automatický discovery engine – systém eviduje a rozpozná přístrojovou techniku, vytvoří katalog zařízení pro asset management, tj. vytváří pro dané prostředí CMDB, která může být pro následné procesy primární, či podpůrná pro validaci existující CMDB.

Kategorizace zařízení – nalezená zařízení jsou rozčleněna do logických skupin, ke kterým lze následně přistupovat v rámci nastavení dalších systémů jako k objektům, bez nutnosti vytvářet pravidla pro každé zařízení zvlášť. Tento mechanizmus musí zajistit odpovídající škálovatelnost řešení bez nutnosti vykonávat atomické operace nad jednotlivými zařízeními manuálně.

Vyhodnocení zranitelnosti – díky schopnosti rozpoznat aktuální verzi systému/firmware nalezeného zařízení a propojení na databázi zranitelností systém reportuje riziková zařízení. Výrobce systému musí být v alianci s výrobci přístrojové techniky a zohlednit reálné bezpečnostní riziko daných zařízení, nikoliv odhadované riziko na základě generických hodnocení o použitém OS, či SW. Tento postup zajišťuje snížení false positive a tím nutné operativy na adekvátní mez. Systém musí v této souvislosti pracovat se vstupy MDS2 standardu.

Monitoring provozu – vytvoření komunikační mapy pro ověření validity provozu a zejména reporting podezřelé a závadné komunikace. Systém musí být schopen zobrazit také servisní přístupy pro jednotlivá zařízení v rámci mapy komunikační matice. Požadována je nativní integrace se systémem pro správu a monitoring servisních přístupů, tj. možné rozšíření o tuto funkcionalitu od stejného výrobce.

Indikátory kompromitace pro dané prostředí – specifické indikátory kompromitace pro nemocniční prostředí pomohou odhalit potenciální incident v preinfekční i postinfekční fázi díky nativní IDS funkcionalitě, jejíž výstupy jsou součástí management rozhraní a obohacují informační profil jednotlivých zařízení přístrojové techniky.

Integrace se síťovými a bezpečnostními prvky – je požadována automatizace s bezpečnostními prvky tak, aby bezpečnostní politika z pohledu síťových prostupů či potřebné izolace infikovaných zařízení zajistila okamžitou reakci bez nutnosti manuální rekonfigurace správcem řešení. To obsahuje zejména výměnu informací o objektech v reálném čase a schopnost práce se skupinami zařízení dle navržených bezpečnostních profilů a politik. Konkrétní automatizační scénáře budou definovány v Solution Design dokumentu.

Utilizace přístrojové techniky – vytváření statistiky pro reálnou utilizaci zobrazovacích zařízení a infuzních pump tak aby mohla být v přehledné formě reportována v manažerském přehledu. Integrací s PACS/DICOM zároveň poskytne statistiky typu zobrazovacích záznamů, včetně statistik segmentů.

Standardizace výstupů bezpečnostních událostí – podpora klasifikace a vizualizace atomických událostí ve frameworku MITRE ATT&CK ICS, tj. včetně rozšíření o ICS kategorie.

Vzhledem k nutnosti automatizovat bezpečnostní procesy pro schopnost okamžité reakce je nutné zajistit interoperabilitu požadovaného systému s dalšími existujícími či plánovanými systémy v rámci infrastruktury. Požadovaný systém v sobě kombinuje bezpečnostní mechanismy a naplňuje související procesy ISO 27001 standardu (change management, patch management, incident management). Primární oblastí z pohledu síťové architektury je OT, resp. IoT část prostředí, která je v současné době definována separátním IP rozsahem a oddělena na úrovni VLAN segmentů. Dále je požadována podpora pro pxGrid – schopnost pracovat s SGT tagy pro bezpečnostní skupiny.

Integrace a nativní kompatibilita

Integrace je požadována pro následující okruhy řešení. Kompatibilita musí být zajištěna pro všechny relevantní komponenty tohoto projektu. Integrace na stávající řešení je nutná pro WiFi profiling, Skenner zranitelností a bezpečnostní brány. Dále je požadována integrace s produkty výrobců, které jsou v infrastruktuře již provozovány:

- VMware vCenter
- DHCP integrace – požaduje se integrace na Microsoft DHCP Server.
- NAC integrace - požaduje se přímá integrace na systém pro řízení přístupu na síti Aruba ClearPass Policy Manager
- Syslog - řešení musí být schopno integrace se systémy SIEM pomocí syslog protokolu
- SNMP – vyčítaní dat ze zařízení pomocí SNMP protokolu
- LDAP – Active Directory
- Next generation firewall - Fortinet, Check Point
- Vulnerability management - Tenable Nessus, Tenable.sc
- Patch management - MS WSUS, MS SCCM
- Netflow – Aruba switche
- Síťový management - Aruba AirWave, Aruba Central
- Integrace na zdravotnické prostředky: DICOM/PACS, Alaris infuzní pumpy, Philips Focal Point

Dále řešení musí podporovat integrace na:

- EDR – řešení dodávané v části Zabezpečení proti škodlivému kódu a analýza aktivit na koncových stanicích a serverech
- REST API - řešení musí disponovat rozhraním REST API pro integraci s interními systémy zákazníka
- Řešení musí být schopno integrace se systémy SIEM, a využívat SNMP pro čtení dat ze síťových zařízení.

Implementace

1. **Technologie** – nástroj pro identifikaci a hodnocení zdravotnických prostředků a dalších aktiv Zadavatele, který je tvořen konkrétním produktem s výkonnostními parametry, kdy součástí je dodání, implementace, optimalizace nástroje a předání do správy Zadavateli.
2. **Integrace** – napojení a integrace technologie na současné provozní a bezpečnostní technologie Zadavatele tak, aby tvořily funkční celek s maximální přidanou hodnotou pro kybernetickou bezpečnost Zadavatele.
3. **Dokumentace** – zpracování provozní a bezpečností dokumentace, DRP, Exit strategie.
4. **Školení –** seznámení vybraných zaměstnanců zadavatele s obsluhou a správou technologie.

3.4. Interní firewall pro mikrosegmentaci

Doplnění škálovatelné platformy o aditivní výkon potřebný k interní segmentaci. Specifikované řešení bude sloužit pro mikrosegmentaci interních subnetů v uživatelské a datacentrové části infrastruktury. Díky možnosti sdílení výkonu škálovatelné platformy pro virtuální firewally je možno tento výkon pružně doplnit o další prostředky z již existujících HW appliance v rámci clusteru. Primární konektivita FW řešení je napojena na orchestrační prvky, které disponují potřebnými 100G rozhraními.

Jedná se o appliance ve vysoké dostupnosti, přičemž každá z nich musí splňovat následující výkonnostní parametry.

1. Firewall výkon dle RFC 3511, 2544, 2647, 1242 nejméně 80Gbps
2. IPS propustnost nejméně 25Gbps
3. Alespoň 3 virtuální systémy
4. LOM/iLO/DRAC či adekvátní karta pro lights out management
5. Redundantní zdroje napájení

6. Příslušenství pro montáž do racku
7. Propojovací kabeláž pro zapojení do škálovatelné platformy

Licenční pokrytí

Požadovaná licence obsahuje moduly pro virtuální patching (IPS), aplikační ochranu, zero-day hrozby, detekci botnetů, možnost integrace s Active Directory.

Integrace

Řešení musí podporovat dynamické seznamy objektů z komponent, které definují virtuální koncová zařízení a uživatele, nejméně z prostředí Microsoft AD a VMware tak, aby tyto objekty mohly být využity pro tvorbu bezpečnostních politik bez nutnosti manuální rekonfigurace pravidel při změně jednotlivých položek dynamického objektu.

Dále je požadována integrace na Nástroj pro zabezpečení zdravotnických zařízení a to minimálně v rozsahu:

- Automatické generování firewallové politiky na základě vlastností zařízení
- Detekce připojených zdravotnických zařízení a jejich export do objektů firewallu

Výstupy pro log management a další platformy řídící dohled a bezpečnostní korelace musí být ve formátu Syslog.

Automatizační procesy jež jsou požadovány a budou součástí Solution Designu musí zahrnovat změny bezpečnostní politiky firewallu formou změn bez nutnosti manuálního zásahu správce. Řešení musí být takto konfigurovatelné i přes API rozhraní. Minimální množina automatizačních postupů pro firewall:

- změna filtračních pravidel reflektujících riziko koncového zařízení či síťového segmentu (zablokování, restrikce na administrátorský prostup, povolení do původního stavu)
- konfigurace IPS profilu
- založení VPN prostupu či jeho zablokování
- nastavení nového uživatele pro SSL VPN či jeho zrušení
- schopnost záchytu síťové komunikace ve formě PCAP pro požadované rozhraní
- odpojení síťových rozhraní či skupin rozhraní při kritickém scénáři

Implementace

Nasazení firewallu předpokládá mezi segmentovou ochranu infrastruktury včetně všech definovaných ochran uživatelského provozu, oddělení IT a OT infrastruktury, případně využití aplikačních ochran pro další segmenty v rámci interní infrastruktury, a to zejména technologií datových center.

- Analýza segmentů/VLAN a návrh úpravy počtu segmentů, změn adresace atp.
- Definice segmentů, které musejí být vzájemně separovány na úrovni L4 či L7
- Přesun L3 interface z centrálního přepínače na segmentační firewall
- Definice propoje mezi centrálním přepínačem a firewallem, úprava trunk konfigurace
- Konfigurace FW politik pro jednotlivé segmenty dle profilingu komunikace
- Testy definované komunikace a ověření funkcionality propojů
- DR testy výpadků propojů a boxů v rámci řešení

3.5. Webový aplikační firewall

WAF řešení pro kontrolu provozu jednotlivých aplikací s možností průběžné úpravy kontrolovaných dat dle požadavků. Je požadováno řešení, které podporuje plnohodnotnou georedundanci, přičemž každá HW appliance musí splňovat následující požadavky.

Licenční pokrytí

Dodávka musí poskytnout HW a SW licence dle uvedené výkonnostní specifikace .

Obecné požadavky na jedno zařízení

1. Propustnost zařízení alespoň 20Gbps/L4, 13Gps/L7
2. Počet HTTP požadavků 800k za sekundu
3. Počet nových L4 spojení 170k za sekundu
4. Počet současných L4 spojení 19M
5. Počet SSL transakcí za sekundu 7K (RSA 2K klíče)
6. Počet SSL transakcí za sekundu 5K (ECDHE-ECDSA P-256)
7. Propustnost SSL spojení (Bulk Encryption) 8Gbps
8. 4 x 10G/1G RJ45
9. 4 x 25G/10G/1G SFP+/SFP28/SFP
10. Redundantní zdroj napájení
11. L4-L7 loadbalancing
12. Web aplikační firewall
13. Dedikovaný port pro management
14. Plnohodnotná Full Proxy architektura
15. Podpora NAT/SNAT/PAT
16. Podpora IPv6, IPv4/IPv6 gateway
17. Podpora IPSEC IKE v2
18. Podpora redundance dvou a více zařízení v režimech Active-Active/Active-Standby/N+1 s možností automatické i manuální synchronizacie konfigurace
19. Správa přes GUI (může být dodáno i jako samostatné virtuální zařízení) a plnohodnotné CLI (SSH přístup s možností ověření uživatele heslem nebo certifikátem/klíčem) proti externím službám (např. RADIUS/TACACS+, LDAP, AD, atd.)
20. Možnost přidat vlastní funkce pomocí skriptování – umožnění plnohodnotné manipulace a správy veškerého aplikačního provozu s cílem zachytit, zkontrolovat, transformovat a nasměrovat příchozí nebo odchozí provoz pomocí skriptovacího jazyka
21. Podpora RBAC – různé uživatelské role
22. Podpora tvorby heterogenního clusteru (různé HW platformy, nebo kombinace SW edice a HW platformy)
23. Podpora filtrování paketů
24. Podpora QoS, rate-limiting
25. TCP optimalizace síťových flows např. při přístupu k aplikaci z mobilních sítí pomocí výrobcem dodaných, nebo vlastních TCP profilů
26. Ukončení šifrovaného provozu SSL TLS 1.2, TLS 1.3
27. Dvoucestná SSL autentizace – serverový, klientský certifikát
28. Podpora SSL certifikátů s elektronickým podpisem dle standardu SHA-2 s podporou TLS
29. Podpora ECC a RSA certifikátů
30. Podpora vysokorychlostního granulárního logování / logování per aplikace na externí logovací systém
31. Podpora otevřeného API pro konfiguraci a automatizaci nástroji třetích stran
32. Podpora SW utilit na troubleshooting např. tcpdump
33. Zajištění “session persistence” na základě IP adresy, HTTP cookie, HTTP host

34. Podpora různých typů health monitoringu – ICMP, HTTP/HTTPS, TCP/UDP
35. Možnost kontinuálního monitorování nejen cílových serverů, ale i všech souvisejících aplikačních komponent
36. Možnost kombinace (AND/OR) více metod monitoringu (např., ICMP, HTTP, TCP port)
37. Možnost definování intervalu pro monitorování (samostatný interval pro oba stavy UP/DOWN)
38. Vložení/přepsání cookie
39. Vložení/přepsání HTTP hlavičky
40. Modifikace URL
41. Možnost vložit zdrojovou IP do L7 hlavičky (XFF)
42. Možnost vložit klientský certifikát do hlavičky
43. Modifikace HTTP/HTML obsahu
44. Použití existující aplikační cookie k zajištění persistence spojení na daný server
45. Možnost směrovat požadavky z určitého subnetu jen na určité servery
46. Možnost mít v poolu nadefinované hot-standby servery ve skupinách s různou prioritou
47. Podpora cachování a komprese HTTP per služba
48. Podpora HTTP/2 směrem k uživateli i k serveru
49. Webový aplikační firewall musí zajistit ochranu proti TOP 10 zranitelnostem dle metodiky OWASP dle https://owasp.org/www-project-top-ten/ včetně podpory pro AJAX/JSON XML/SOAP
50. Webový aplikační firewall s implementovaným negativním i pozitivním bezpečnostním modelem
51. Řešení musí podporovat logování přístupů k webovým službám
52. Základní aplikační firewall pro protokoly FTP a SMTP
53. Možnost konfigurace webového aplikačního firewallu za využití učícího se módu
54. Automatické nahrávání a aplikování nových signatur od výrobce
55. Možnost vytvoření bezpečnostních politik způsobem hierarchie nadřízené a podřízené politiky
56. Validace aplikačních flow pro webové aplikace
57. Ochrana přihlašovací stránky proti bruteforce attack
58. Podpora CAPTCHA (generování a ověření)
59. Detekce aktivity klávesnice a myši (rozlišení člověk/robot)
60. Možnost propojení WAF s externím skenerem zranitelností webových aplikací pro automatickou tvorbu/úpravu bezpečnostních pravidel (Tenable SC)
61. Ochrana proti Session Hijackingu pomocí jednoznačné identifikace PC/prohlížeče uživatele (fingerprint) a v případě vyhodnocení rizika vynucení CAPTCHA
62. Podpora standardu PCI DSS - možnost vytváření PCI reportů
63. Podpora maskování/odstranění citlivých informací jako např. čísla kreditních karet (možnost definovat pravidla pomocí RegEx) z odpovědi serveru
64. Filtrování WebSocket provozu
65. Podpora externí antivirové kontroly pomocí ICAP
66. DoS a DDoS detekce a ochrana na L7
67. Ochrana proti DDoS pomocí detekce stresu chráněné aplikace – zpoždění odpovědi a behaviorální analýza s následným omezením počtu requestů, Captcha, TCP reset a podobně
68. Rozpoznání legitimního provozu na silně vytížených URL, odlišení od DoS nebo DDoS útoku a tím zamezení blokování legitimních uživatelů
69. Automatické nebo ruční „blacklistování“ IP adres, které se opakovaně snaží překonat zabezpečení, nebo se vyznačují vysokou mírou nežádoucího provozu
70. Podpora nastavení konkrétních bezpečnostních politik podle IP adresy, doménového jména a URI
71. Podpora reportingu per HTTP request/response
72. Blokování útočníků podle geolokace
73. Automatické odlišení skutečných uživatelů od botnetů na základě signatur
74. Kategorizace botnetů do skupin (validní/nežádoucí)

75. Ochrana proti automatizovanému provozu/útokům (botnet) nejen pomocí signatur, ale také pomocí aktivní detekce zda se jedná o browser vs. Bot pomocí tzv. „challenge“, neboli úkolů, díky kterým WAF identifikuje Bot vs Uživatel pro případ kdy Bot umí simulovat chování skutečného prohlížeče a zamezení propuštění takové komunikace na aplikační server
76. Průběžná analýza stresu aplikace, analýza nestandardního chování tzv. behaviorální analýzy a zpřesnění ochrany aplikace pomocí vytváření a uplatňování dynamických signatur. WAF mapuje a zaznamenává standardní chování uživatelů v rámci aplikace. V případě zjištění odchylky se dynamicky vygeneruje signatura založená na těchto odchylkách, která jednoznačně identifikuje zdroje škodlivého provozu, který může být zablokován nebo zpomalen
77. Podpora importu „Swagger souboru“ pro definici bezpečnostní politiky pro ochranu API

Integrace

Propojení se SIEM platformou ve formě zasílání logů dle definované granularity. Automatická kontrola a nastavení politik přes automatizační nástroj / API.

Implementace

Zadavatelem jsou dále požadované implementační práce v minimálním rozsahu:

- Fyzická montáž zařízení
- Konfigurace síťového prostředí (VLAN, IP, routing)
- Nastavení parametrů HA
- Základní konfigurace virtuálních serverů (až 50)
- Nastavení profilů
- Terminace SSL
- Nastavení loadbalancingu
- Případné komprese a cacheování
    - K sestavení pokročilejších kontrol modulem WAF musí být využito Learning módu, až 20 aplikací
    - Základní vytvoření bezpečnostních politik
- Konfigurace základních parametrů negativního bezpečnostního modelu dle využitých platforem
- Základní konfigurace pozitivního modelu a aplikace nastavení na filetypes a URI metacharter validation
    - Konfigurace anomaly detection
    - Konfigurace/import WSDL schémat
    - Nastavení parametrů learning módu (po uplynutí 1 měsíce aktivního learning módu)
    - Vyhodnocení událostí a incidentů learning módu
- Úprava hodnot learning módu
- Úprava blocking settings pro jednotlivé položky
- Zapnutí blocking módu
- Připojení k autentizačním prvkům a nastavení SSO
- Nastavení ochrany proti volumetrickým útokům DDoS
- Nastavení ochrany proti bruteforce
- Napojeni na SIEM řešení a provozní monitoring

4 Část C – Opatření a nástroje pro ochranu klíčových systémů

Část č. 3 obsahuje systémy a služby směřující k posílení zabezpečení klíčových systémů formou zvýšení odolnosti, posílení komunikačních standardů a unifikace přístupu k těmto klíčovým systémům. Klíčovým systémem se rozumí nejen systémy v rámci dodávky tohoto VŘ, ale vybrané systémy ve stávající IT i OT infrastruktuře (servery, aplikace atp.).

4.1. Nástroj pro detekci zranitelnosti a hardeningové politiky

Zadavatel požaduje nástroj pro detekci a řízení zranitelností v síti, který musí umožňovat pravidelné automatizované skenování sítě (serverů a koncových stanic, databází, síťových prvků, aplikačních a webových serverů apod.) a poskytovat nástroje pro analýzu zranitelností (využití různých typů náhledů, možnost použití filtrů atd.). Dále musí nástroj disponovat funkcemi pro řízení zranitelností, jako je možnost akceptace výjimek, integrace na ticketovací systém, možnost reportingu za využití předdefinovaných šablon a v neposlední řadě možnost vytvoření vlastního reportu dle potřeb Zadavatele (custom report).

Řešení bude provozováno v síti, kde není centrální bod, ze kterého by byla vidět celá síť, proto je nutné, aby řešení umožňovalo instalaci více distribuovaných skenerů. Dále je požadováno, aby bylo možné specifikovat parametry skenování tak, aby nedošlo k zatížení sítě nebo v opačném případě, aby byla snížena doba skenování na minimum.

Zadavatel dále požaduje, aby dodané řešení disponovalo funkcí pro specifikaci nejkritičtějších zranitelností na základě více parametrů, díky které bude možné identifikovat zranitelnosti, které je nutné odstranit v první řadě bez ohledu na proces patch managementu.

Dodané řešení musí pokrýt minimálně 750 aktiv a musí mít následující funkce a parametry:

Architektura řešení

- Cloud – preferuje se provozování centrální správy v cloudovém prostředí.
- Skenery dodány formou virtuální appliance. V opačném případě je požadováno, aby skener mohl běžet na aktuálním operačním systému RHEL, Ubuntu nebo Rocky Linux.
- Možnost distribuovaného nasazení skenovacích agentů do podsítí Zadavatele s napojením na centrální správu.
- Možnost skenování ze skenovacích agentů umístěných v externí síti (internetu).
- Možnost specifikace výkonnostních parametrů jednotlivých skenů, aby nedošlo k přetížení sítě, v opačném případě aby bylo využito maximálního potenciálů síťových prvků a sken trval kratší dobu.

Centrální správa

- Podpora zabezpečeného přístupu do management konzole pomocí využití protokolu HTTPS ze standardních webových prohlížečů.
- Možnost řízení přístupu podle sledovaných systémů (např. administrátoři z jedné pobočky nebudou mít přístup k systémům z druhé pobočky).
- Možnost řízení přístupu uživatelů dle předdefinovaných rolí.
- Automatické aktualizace databáze zranitelností minimálně na denní bázi.
- Centrální správa musí disponovat přehledovou obrazovkou, kterou si může uživatel přizpůsobit. V rámci přizpůsobení je požadováno alespoň:
    - možnost zobrazit nejzranitelnější systémy v síti
    - zobrazení nejčetnějších zranitelností v síti

- zobrazení nejprioritnějších zranitelností (dle exploitace, závažnosti, CVSS…)

Seznam skenovaných aktiv

- Možnost rychlé identifikace technických aktiv za využití discovery skenování.
- Možnost kategorizace aktiv na základě operačního systému, IP adres a dalších atributů.
- Možnost dynamické kategorizace aktiv na základě počtu zranitelností, typu zranitelností, přítomnosti konkrétní zranitelnosti a dalších atributů.
- Možnost tagování na základě dynamických pravidel i manuálního přiřazování statických tagů.

Skenování zranitelností

- Řešení musí umožňovat detekci zranitelností minimálně na těchto typech systémů:
  - koncové stanice
  - souborové servery, aplikační servery, webové servery
  - databázové systémy
  - síťové prvky
  - webové aplikace
- Možnost definovat šablony skenů pro jednoduché vytváření více stejných skenů pro různé systémy.
- Možnost definovat skenovaný systém pomocí statické a dynamické kategorizace aktiv.
- Skenování za pomoci časového harmonogramu.
- Řešení musí umožňovat tři typy skenů:
  - autentizovaný sken za využití privilegovaného účtu
  - síťový port sken
  - sken pomocí agenta instalovaného na cílovém zařízení
- Možnost autentizovaného skenu:
  - OS Microsoft Windows
  - OS Linux
  - databáze (alespoň MySQL a MSSQL)
  - pomocí SSH
- Řešení musí obsahovat předdefinované šablony pro jednoduché spuštění skenů zranitelností bez nutnosti složité konfigurace.
- Možnost definovat vlastní sken bez nutnosti využít předdefinované šablony.

Kontrola souladu s bezpečnostní politikou

- Řešení musí být schopno zkontrolovat konfiguraci skenovaného systému vůči standardizovaným bezpečnostním politikám (např. CIS).
- Řešení musí umožňovat kontrolu konfigurace vůči vlastním bezpečnostním politikám Zadavatele.

Vyhodnocení výsledků

- Řešení musí umožňovat analýzu detekovaných zranitelností a poskytovat minimálně následující informace o zranitelnosti:
  - IP adresa a DNS systému, na němž byla zranitelnost detekována
  - operační systém systému, na němž byla zranitelnost detekována
  - závažnost zranitelnosti
  - CVE zranitelnosti
  - CVSSv3 skóre
  - CVSSv3 vektor
  - datum zveřejnění zranitelnosti

    - datum první identifikace v síti Zadavatele
    - datum poslední identifikace v síti Zadavatele
    - datum zveřejnění záplaty (v případě, že byla zveřejněna)
    - možnost exploitace a náročnost exploitace
    - popis zranitelnosti
    - návod na odstranění zranitelnosti
- Řešení musí umožnit filtrovat zranitelnosti dle výše uvedených parametrů.
- Řešení musí poskytovat obrazovku s přehledem:
    - všech detekovaných zranitelností
    - zranitelností detekovaných konkrétním skenováním
    - zranitelných systémů specifikovaných IP adresou nebo DNS názvem s počtem zranitelností jednotlivých závažností
    - zranitelností seskupených dle portu
- Řešení musí být schopno oddělit zranitelnosti od položek konfigurace, které nejsou ve shodě s bezpečnostní politikou.
- Řešení musí umožnit vytvoření výjimky pro konkrétní zranitelnost případně snížení její závažnosti.
- Řešení musí umožňovat integraci na ticketovací systémy.
- Řešení musí poskytovat funkci pro specifikaci nejkritičtějších zranitelností na základě minimálně těchto parametrů:
    - dopad na důvěrnost, integritu, dostupnost
    - možnost exploitace
    - stáří zranitelnosti
    - informace z Threat Intelligence o zneužívání dané zranitelnosti

Reporting

- Řešení musí poskytovat reporting ve formátu HTML, PDF a CSV.
- Možnost využít předdefinovaných šablon.
- Možnost vytvoření vlastního reportu bez využití šablon.
- Řešení musí umožňovat vytvořit vlastní report s možností filtrování zranitelností dle parametrů uvedených v prvním bodě kapitoly „Vyhodnocení výsledků“.
- Řešení musí umožňovat přidání vlastních komponent do reportu (tabulky, grafy, texty), aby si mohl Zadavatel přizpůsobit reporty svým požadavkům a vytvářet reporty pro různé úrovně managementu.
- Možnost automatického reportování po vykonání skenu a odeslání na specifikované emailové adresy.
- Možnost pravidelného reportování za pomoci časového harmonogramu.

Integrace

- Řešení musí být schopno integrace na systém SIEM.
- Řešení musí být schopno integrace na systém správy privilegovaných účtů za účelem poskytnutí přihlašovacích údajů pro autentizované skeny.
- Řešení musí být schopno integrace na service desk systém.
- Řešení musí disponovat rozhraním API pro integraci s interními systémy zákazníka.

Hardeningové politiky

V rámci projektu je požadováno vytvoření návrhu interního standardu hardeningu pro provozované technologie uvedené níže. Návrh interního standardu bude založen na běžně užívaném profesionálním

standardu CIS přizpůsobeném konkrétním provozním podmínkám s ohledem na akceptovaný práh rizika.

Provozované platformy:

- Windows 10, 11
- Windows Server 2016, 2019, 2022
- Red Hat Enterprise Linux, CentOS, Rocky Linux
- Vmware vCenter, esxi
- Check Point NGFW

Na základě schválených návrhů interních hardeningových standardů dojde k vytvoření/úpravě politik pro kontrolu konfigurace dodaných řešení tak, aby byly rozsahem v souladu s vytvořeným návrhem.

Implementace

V rámci implementace je požadováno:

1. Vytvoření dokumentu Solution Design s popisem architektury, jednotlivých komponent, návrhu hromadného rolloutu agentů (bude-li použito), akceptačních testů, pilotního testování.
2. Návrh politiky pro řízení zranitelností a pravidelný patch management. Konzultace se Zadavatelem a finalizace politiky.
3. Instalace centrální správy a hardening serverových komponent (OS, webový server, databáze).
4. Instalace dalších komponent (například skenery nebo další potřebné servery), hardening.
5. Konfigurace centrální správy, vytvoření uživatelů a skupin, nastavení SMTP reportingu, vytvoření nebo úprava dashboardů po domluvě s administrátory Zadavatele. Volitelně nastavení SSO.
6. Vytvoření skenovacích úloh (host discovery, privilegovaný i neprivilegovaný sken zranitelností), otestování funkčnosti na pilotním vzorku, vyladění autentizace v rámci privilegovaných skenů.
7. Instalace agentů na pilotní vzorek a otestování skenů zranitelností (bude-li použito).
8. Podpora během hromadného rolloutu.
9. Vytvoření až pěti reportů dle požadavků Zadavatele.
10. Vytvoření provozní dokumentace – popis běžných operativních aktivit, upgradu agentů a komponent, instalace a odinstalace (manuální i hromadné), troubleshooting.
11. Vytvoření hardeningových standardů a na jejich základě úprava skenovacích šablon.
12. Vytvoření konfiguračních skenů dle výše uvedených šablon a otestování jejich funkčnosti.
13. Realizace akceptačních testů.
14. Školení pro administrátory řešení.

4.2. Systém pro správu a monitoring administrátorských přístupů

Nasazení systému, který zajistí správu privilegovaných účtů a monitoring privilegovaných relací. Tento systém zajistí logování všech relací, logování aktivit administrátorů, možnost dohledání zadaných a vykonávaných příkazů a možnost pozastavit, uzamknout nebo terminovat relaci. Dodávané řešení pro správu privilegovaných uživatelských účtů musí splňovat alespoň následující funkce a parametry.

Součástí licence je i řešení redundance všech komponent a taktéž geo-redundance (alespoň active-passive) s dodatečnou místní redundancí v sekundární geolokaci. Množství licencí lze v budoucnu dále rozšiřovat dle aktuálních potřeb aditivně, tj. bez nutnosti zpětného odkupu původního balíku a jeho náhrady. Zadavatel vyžaduje on-premise řešení a neumožňuje alternativu umístěnou v cloud prostředí. Součástí nabízeného řešení musí být i licence MS CAL, pokud je řešení potřebuje k naplnění jakéhokoliv z uvedených bodů v této definici.

Architektura řešení

Veškeré komponenty řešení musí splňovat nároky na vysoké zabezpečení a automaticky vynucovat tzv. hardening. Úložiště dat, kde jsou uloženy jednotlivé účty, přihlašovací údaje, nahrávky relací a auditní záznamy musí být vysoce zabezpečeno dle požadavků. Řešení bude dodáno na dvou virtuálních appliance, které jsou out-of-the-box dodány jako uzavřená hardenovaná platforma obsahující všechny licence na provoz řešení, existující v produktové řadě výrobce s produktovým číslem a jsou výrobcem zabezpečeny proti hrozbám hardeningem. Update OS na vyšší verzi musí být realizován výměnou appliance. Úprava systému/instalace aplikací na úrovni operačního systému není možná. Zadavatel požaduje autonomní řízení aktualizací OS a samotného SW pomocí výrobcem dodávaných balíčků skrze administrační rozhraní dodávané výrobcem. Je požadována nezávislost na místním repozitáři aktualizací.

Řešení musí být nasazeno ve vysoké dostupnosti pro zajištění High Availability, minimálně v režimu Active-Passive, Disaster Recovery a zálohování řešeno tak, aby citlivá data byla stále vysoce zabezpečená a dostupná pouze vlastníkům dat. Disaster recovery a HA proces musí být plně automatický.

Systém musí umožňovat až 8 otevřených spojení na jednoho administrátora. Systém musí umožňovat alespoň 250 RDP paralelních spojení a 450 SSH paralelních spojení.

Řešení musí umožňovat bezpečné zálohování dat systému – zálohy musí být šifrované a přístup k zálohovaným datům je umožněn pouze pomocí zabezpečených postupů, které zajišťují integritu zálohovaných dat. Řešení musí poskytovat automatický hardening úložiště dat, který bude nezávislý na zásahu správců systémů a bude minimalizovat možnou lidskou chybu. Řešení musí být v navrhované konfiguraci stabilní a je možné ho ověřit dle odkazovaných referencí.

Řešení musí pokrývat tzv. "break glass" scénáře s postupy, jak jednat v situacích s fatálním dopadem na PAM systém. Součástí dodávky bude rámcový popis pro řešení disaster recovery a break-glass scénářů, který bude detailně rozpracován při analýze.

Veškeré komponenty systému musí podporovat SNMP monitoring, tak aby bylo možné monitorovat dostupnost. Požadován je monitoring vytížení CPU, využití disků a paměti.

Řešení musí být dimenzované tak, aby umožňovalo uložit minimálně 29 000 hesel a uchovávalo nahrávky relací minimálně po dobu 365 dní.

Obecné požadavky

Řešení poskytne nástroj pro správu privilegovaných účtů, řízení přístupu k těmto účtům a monitoring veškerých aktivit privilegovaných účtů. Uživatelské přístupy budou řízeny bezpečnostní politikou, ve které má vybraný uživatel práva přístupu pouze k definovaným účtům a systémům. Účty a systémy, ke kterým nemá práva přístupu, nejsou pro uživatele viditelné.

Systém musí plně podporovat oddělení přístupových oprávnění. Uživatelé/skupiny uživatelů mají přístup pouze k vybraným účtům, systémům, auditním záznamům, konfiguraci atp. Řešení podporuje minimálně následující role:

- Žadatel
- Schvalovatel
- Auditor
- Administrátor systému

Řešení umožní víceúrovňové schvalování správcovských přístupů k cílovým systémům – přístupy lze omezit dle vybraného účtu, nebo na daný časový úsek. Schvalování přístupu lze vynutit odděleně pro přístup k přihlašovacím údajům privilegovaného účtu, nebo pro připojení na koncový systém. O nových žádostech, schválení a zamítnutí budou uživatelé upozornění emailem, vytvořením ticketu v helpdesk systému, nebo jinou metodou schválenou v rámci Solution Design dokumentu.

Řešení zaručí vysokou bezpečnost přenášených a uložených informací (confidentiality, integrity, availability). Uložené informace, včetně nahrávek a spravovaným přihlašovacích údajů, jsou uloženy v jedné centrální zabezpečené databázi dle požadavků. Řešení musí umožňovat omezení práv správce systému tak, aby neměl sám přístup k uloženým přihlašovacím údajům, logům, nebo nahrávkám bez autorizace vlastníků dat. Systém musí být certifikovaný bezpečnostním standardem Common Criteria.

Správa řešení bude umožněna pomocí jednotné centrální správy. Přístup k uživatelskému rozhraní přes webový portál s možností ověření přes LDAP/MS Active Directory a druhým faktorem (minimálně PKI karty, RSA ID, Radius server).

Řešení bude možné spravovat a konfigurovat také pomocí Rest API a to minimálně pro vytváření a editace uživatelů a účtů, nastavení oprávnění, system health monitoring, schvalování požadavků, autentizaci, změny přihlašovacích údajů, terminace spojení atp.

Řešení musí umožňovat integraci s ticketovacími nástroji třetích stran – žádost o schválení přístupu, přístup na základě existujícího tiketu, atp.

Řešení nabídne plnou integraci s Microsoft Active Directory na úrovni informací o uživatelích, příslušnosti ke skupinám a informace o emailech. Integrace musí umožňovat mapování rolí v PAM řešení v návaznosti na skupiny v AD.

Nástroj umožní vynutit silnou autentizaci uživatelů pro přístup k uloženým údajům i pro bezpečné vzdálené připojení. Silnou autentizací je míněna minimálně možnost kombinace jméno/heslo + druhý faktor (RADIUS, PKI, certifikát, atp ...). Řešení umožní integraci s MFA nástroji třetích stran.

Řešení musí splňovat standard FIPS 140-2 a šifrovací algoritmy minimálně na úrovni AES-256 a RSA-2048. Řešení umožní společnostem splnit compliance požadavky pro ZKB, GDPR, PCI-DSS, SOX, HIPAA.

Řešení musí poskytovat zabezpečení přístupu k veřejným webovým aplikacím pomocí SSO portálu. Pro autentizaci k SSO portálu se použije jméno+heslo a vynucení vícefaktorového ověření. Systém musí podporovat minimálně následující integrace:

- NTLM
- Basic auth
- SAML
- Uživatelské heslo

Management hesel

Řešení umožní vyhledávat privilegované účty v operačních systémech Windows, Unix, Linux a Mac OS / LDAP, Active Directory, databázích a síťových zařízeních a přidat je (manuálně i automaticky) do systému řízení přístupu dle bezpečnostní politiky. Dále řešení dokáže určit o jaký typ účtů se jedná (běžný uživatel vs. Administrátor/root). Vyhledávání účtů nevyužívá instalaci agentů na koncová zařízení. Systém umožní vyhledávání v on-premise i cloud prostředí (např. AWS).

Řešení umožní automatickou výměnu hesel a SSH klíčů privilegovaných účtů po ukončení relace (jednorázové heslo), nebo v pravidelných intervalech dle bezpečnostní politiky. Rotaci hesla/SSH klíče lze vynutit i uživatelem. Hesla a SSH klíče se vyměňují bez nutnosti využití agenta.

Řešení musí v pravidelných intervalech kontrolovat shodu uloženého hesla v systému řízení přístupů a na cílovém bodu. V případě neshody vynutí synchronizaci, nebo zašle upozornění správci.

Systém umožní vyhledat účty v MS Windows prostředí a jejich návaznost na další služby/aplikace (services, scheduled tasks, IIS pool, COM+ object, atd.). Při přidávání účtů na návaznosti upozorňuje, nebo automaticky integruje do systému. Při vynucení změny hesla je heslo propsáno i do návazných služeb.

Systém umožní pravidelné vyhledávání účtů, které nejsou řešením spravovány, ale jsou používány pro přístupy na koncové systémy. Systém takové účty dokáže vyhledat, upozornit na jejich použití a případně automaticky zařadit do správy. Řešení zároveň umožňuje detekci nespravovaných účtů a automatické uložení a vynucení změny hesla.

Řešení musí umožňovat možnost úpravy systému password management, tak aby bylo možné integrovat další systémy Zadavatele. Úpravy je možné provádět pomocí nástroje dodávaného výrobcem a případně úpravou konfiguračních souborů.

Řízení privilegovaných relací

Nabízené řešení musí obsahovat Privileged Session management minimálně pro RDP a SSH spojení navázaná z administrátorské stanice bez nutnosti instalace agenta na stanici administrátora nebo na cílové aktivum.

Správcovský přístup na cílový systém bude zprostředkován pomocí tzv. terminal/proxy serveru prostřednictvím zvoleného komunikačního protokolu, aplikace a příslušného privilegovaného účtu tak, aby koncový uživatel neměl přístup k přihlašovacím údajům. Izolace přístupu je možná až na úroveň aplikace (typu webový prohlížeč s konkrétní URL, MMC konzole s vybraným snap-in, konkrétní aplikace...např. MS SQL Management Studio, WinSCP, atp.), kdy uživatel nemá možnost přistupovat k jiným službám či aplikacím v rámci dané relace. Po ukončení aplikace se uzavře spojení celé relace. Vzdálené připojení k relaci lze navázat jak přes vlastní GUI dodaného řešení, tak i pomocí standardních protokolů RDP a SSH a standardních klientů typu putty a remote desktop manager. U všech možností připojení ke vzdálené relaci musí být podporováno vynucení silné autentizace (minimálně integrace s LDAP a RADIUS).

Správcovský přístup prostřednictvím SSH protokolu se bude provádět přes SSH Proxy, kde bude uživatel ověřen svými přihlašovacími údaji (je možné spárovat s MS Active Directory) a bude připojen zvoleným privilegovaným účtem na cílový systém bez zadávání hesla a dle bezpečnostní politiky. Pro připojení pomocí SSH Proxy je vyžadována podpora silné autentizace (minimálně integrace s LDAP, RADIUS, či autentizace pomocí SSH klíče).

Řešení musí umožňovat monitoring a nahrávání celé relace a aktivit privilegovaných účtů v komprimovaném video formátu s možností kontextového vyhledávání, bez nutnosti instalace permanentních agentů na koncový systém nebo na stanici administrátora. V nahrávkách je možné zpětně vyhledávat v záznamu ve formě metadat – minimálně u RDP spuštěné aplikace a události, u SSH relací jednotlivé příkazy, u Webových aplikací click na jednotlivé odkazy, u jiných typů relací alespoň stisky kláves. Pro přehrávání nahrávek není potřeba instalace nástrojů třetích stran (flash, java, codec, atp...) a je dostupné z GUI dodávaného řešení.

Řešení nabídne možnost uživatelům s konkrétním oprávněním (Auditor) manuální nahlížení do probíhajících relací a jejich případné pozastavení, zamknutí a terminaci potenciálně nebezpečných RDP a SSH relací, s možností jejich následného odemčení.

Řešení nabídne možnost automatického pozastavení, zamknutí a terminace potenciálně nebezpečných SSH relací a reporting nad těmito potenciálně nebezpečnými relacemi.

Sledování "živých" relací je také možné pomocí prohlížeče a protokolu HTTPS.

Systém umožní autorizovanému personálu centrálně vyhledávat v nahrávkách podle data, uživatele a spuštěného příkazu.

Součástí řešení nebo pomocí integrace na SIEM nebo SOAR musí být možnost provádět průběžnou analýzu využívání privilegovaných účtů a následnou detekci potenciálně škodlivého chování – uživatel se připojuje z nestandardní IP, uživatel se připojuje na systémy, na které běžně nemá přístup, uživatel používá privilegovaný přístupy v nestandardní časy, atp.

Nahrávky musí být zaznamenávány efektivním způsobem (např. s využitím komprimace, zaznamenávání pouze aktivní relace). Řešení které zaznamenává celou nahrávku není z kapacitních důvodů připuštěno. Maximální povolená velikost SSH/RDP nahrávek za 1min je 20 MiB.

Bezpečný vzdálený přístup

Řešení umožní okamžité zavedení nových uživatelů do systému. Správce řešení může přes webové rozhraní vytvořit uživatele, přiřadit mu oprávnění s jakými privilegovanými účty může disponovat a pro jaké časového období. Řešení následně zašle email novému uživateli a umožní mu bezpečné vzdálené připojení k PAM řešení.

Před bezpečným vzdáleným připojením uživatele k řešení PAM je uživatel ověřen pomocí druhého faktoru.

Řešení musí obsahovat nativní TOTP (Time-based one-time password) nástroj, pro silnou autentizaci přistupujících uživatelů k řešení. Nástroj musí generovat QR kódy pro rychlé zavedení silného ověření pro uživatele. Souběžně toto nativní řešení musí podporovat autentizační mechanizmy min. typu Microsoft Authenticator, Google Authenticator.

Spojení mezi externím uživatelem a řešením PAM musí být plně šifrované. Není umožněno přímé spojení mezi stanicí uživatele a cílovým systémem – je využit princip tzv. „jump/proxy serveru“.

Nástroj musí při žádosti o přístup automaticky vyhodnocovat kontextová data založená na konkrétním dni, datu, času a geolokaci žadatale o přístup ještě před schválením/odmítnutím daného přístupu. Tento proces musí být plně automatický.

Základní řešení PAM nesmí vyžadovat instalaci agenta na stanice uživatelů a na cílové systémy. Uživatelům je umožněno bezpečně přistupovat pomocí webového prohlížeče do řešení PAM.

Audit a reporting

Systém musí umožňovat audit jednotlivých akcí uživatelů s privilegovanými účty – zobrazení hesla, změny uložených údajů, vytvoření relace.

Řešení musí umožňovat vygenerování reportu veškerých aktivit administrátora řešení.

V nabízeném řešení musí být k dispozici minimálně následující předdefinované typy reportů:

- report uživatelů a jejich oprávnění, včetně výpisu účtů, které mají k dispozici
- report všech spravovaných účtů, včetně přiřazených politik hesel a výčtu uživatelů, kteří mají k danému účtu přístup
- report o současných i historických změnách hesel napříč prostředím
- report aktivit nad účty (check out/in, přidělení účtu atp.)

- report software, který je instalovaný na koncových privilegovaných aktivech a otevřené porty na daném aktivu včetně vizuální prezentace

Řešení umožní nastavení přístupu k reportům pouze pro vybrané uživatele.

Pro zabezpečení přístupu k archivovaným relacím systém nesmí umožnit uživatelům / správcům exportovat nahrávky do jiného video formátu, ani externě nakládat s nahrávkami a mít tak citlivé nahrávky plně pod kontrolou po celou dobu jejich existence.

Auditní záznamy a logy veškerých aktivit v zabezpečeném úložišti musí být chráněné proti změnám a smazání všemi uživateli (včetně všech administrátorských rolí řešení), a to minimálně po dobu 30 dní. Auditní záznamy musí být bezpečně uloženy v zašifrované podobě, tak aby k nim měl přístup pouze oprávněný uživatel.

Řešení umožní nahlížení do historie snapshotů a stavu jednotlivých aktiv v síti, v návaznosti na automatické skenování. Tyto snapshoty musí reportovat historii změn, a to minimálně privilegovaných účtů, sdílených účtů, servisních účtů, instalovaného SW a otevřených portů.

Systém umožní monitoring jednotlivých komponent pomocí RestAPI – integrace s monitoring systémy Zadavatele.

Integrace a Podporované platformy

Výrobce musí poskytovat veřejně seznam integrovaných řešení na úrovni Password Management, Remote Session Management, SIEM, atp.

Nabízený systém musí obsahovat API pro automatizaci a integraci třetích stran a mít jej plně zalicencované. Řešení musí umožnit integraci s nástroji typu Vulnerability Management, nebo RPA pro automatické a bezpečné předávání dat pomocí API rozhraní.

Řešení musí podporovat integraci s nástroji třetích stran pro vynucení vícefaktorové autentizace. Minimálně na úrovní LDAP/S, RADIUS, PKI, RSA.

Systém musí umožňovat integraci s nástroji SIEM pro přenos logovaných auditních záznamů a to v reálném čase pomocí Syslog.

Systém musí umožňovat integraci s nástroji HSM – uložení šifrovacích klíčů k databázi řešení.

Systém musí nativně podporovat řízení hesel a bezpečné přístupy minimálně na systémech:

- Windows 10, 11
- Windows Server 2008, 2012, 2016, 2019, 2022
- Active Directory,
- HP iLO, Dell DRAC, IBM,
- Windows Services, Windows Scheduled Tasks, IIS Application Pool, Windows Registry COM+,
- VMWare
- Red Hat, Unix, Debian
- MS SQL, MySQL, PostreSQL, Oracle,
- Fortinet ,Checkpoint
- Cisco, F5, HP,
- Office 365, Microsoft Azure Application Keys.

Pro další systémy pak musí disponovat možností definovat password management modul.

Nativní integrace klientských aplikací: Microsoft Management Studio, WinSCP, Putty, VNC. Po integraci budou mít administrátoři dostupné jejich viditelné servery v nativních výše zmíněných aplikacích a při přístupu přes tyto aplikace budou zachovány všechny funkcionality PAM (automatické vydání hesla, nahrávání přístupu, rotace hesel a SSH klíčů) a nemusí využívat webové prostředí nástroje, nebo tlustého klienta.

Implementace

V rámci implementace je požadováno:

1. Vytvoření dokumentu Solution Design s popisem architektury, jednotlivých komponent, návrhu hromadného rolloutu agentů (bude-li použito), akceptačních testů, pilotního testování.
2. Návrh politiky způsobu řízení privilegovaných účtů. Konzultace se Zadavatelem a finalizace politiky.
3. Instalace centrální správy.
4. Instalace dalších komponent (například skenery nebo další potřebné servery).
5. Konfigurace centrální správy, vytvoření uživatelů a skupin, nastavení SMTP reportingu, vytvoření nebo úprava dashboardů po domluvě s administrátory Zadavatele. Volitelně nastavení SSO.
6. Vytvoření skenovacích úloh (host Discovery a privilegovaných účtů, otestování funkčnosti na pilotním vzorku, vyladění autentizace v rámci privilegovaných skenů.
7. Načítaní všech privilegovaných účtů a zařízení na platformách Windows, Linux, databáze, síťová zařízení, bezpečnostní technologie a automatizace vyhledávání zařízení / účtů a jejich automatické členění do skupin dle sítí a účelu zařízení / účtů.
8. Nastavení skupin a oprávnění uživatelů a administrátorů PAM, nastavení a přiřazení přístupových politik skupinám uživatelů, nastavení politik hesel podle skupin zařízení.
9. Automatizované navázání administrátorských účtů z domény k administraci jednotlivých skupin zařízení.
10. Automatizované navázání osobních administrátorských účtů z domény a ze zařízení běžným účtům administrátorů tak, aby každý administrátor používal jen svůj osobní privilegovaný účet a neviděl v žádném případě jiné osobní administrátorské účty.
11. Přiřazení automaticky vytvářených skupin účtů skupinám uživatelů.
12. Spuštění automatické rotace řízených účtů.
13. Zajištění automatického reportování změny hesel a aktivit s účty.
14. Vytvoření provozní dokumentace – popis běžných operativních aktivit, upgradu agentů a komponent, instalace a odinstalace (manuální i hromadné), troubleshooting.
15. Realizace akceptačních testů.
16. Školení pro administrátory řešení.

4.3. Systém pro vzdálený privilegovaný přístup

Účelem této části je vybudovat řešení, které dokáže vzdálený privilegovaný přístup administrátorů a externistů sjednotit. Tím bude efektivně vyloučen přístup pomocí rizikových technologií (vypublikované RDP, TeamViewer a další) a zároveň redukován tzv. Attack Surface. Řešení musí vzdáleným administrátorům a externistům poskytovat přístup do interní sítě na privilegované účty pomocí vypublikované webové konzole, v rámci které je možné vybrat, na jaké systémy a pomocí jakého privilegovaného účtu se může vzdálený administrátor / externista připojit. Takové řešení

nezbytně předpokládá vysoce zabezpečenou hardwarovou nebo virtuální appliance na okraji perimetru sítě s vypublikovanou webovou konzolí do internetu.

Do tohoto systému budou zařazeny všechny privilegované účty, které mohou být vzdálenými administrátory nebo externisty využívány. Pomocí takto spravovaných účtů bude možné se připojit na cílové systémy v interní síti žadatele.

Řešení bude dle předem nastavených politik automaticky měnit heslo k privilegovanému účtu. Administrátor nebo externista, který bude vzdáleně k privilegovanému účtu přistupovat, tak nemusí (a nebude) znát heslo k tomuto účtu, využije přímého připojení, které zprostředkuje implementované řešení.

Všechna privilegovaná spojení budou nástrojem monitorována tak, aby byla aktivita privilegovaných účtů zaznamenána.

Předpokládá se přímá integrace na část technické specifikace Systém pro správu a monitoring administrátorských přístupů.

Součástí licence je i řešení redundance všech komponent a taktéž geo-redundance (alespoň active-passive) s dodatečnou místní redundancí v sekundární geolokaci. Množství licencí lze v budoucnu dále rozšiřovat dle aktuálních potřeb aditivně, tj. bez nutnosti zpětného odkupu původního balíku a jeho náhrady. Zadavatel vyžaduje on-premise řešení a neumožňuje alternativu umístěnou v cloud prostředí. Součástí nabízeného řešení musí být i licence MS CAL, pokud je řešení potřebuje k naplnění jakéhokoliv z uvedených bodů v této definici.

Obecné požadavky

Řešení musí být dodáno jako uzavřený hardenovaný systém bez možností přístupu do OS, databáze a instalovaných aplikací. Tento systém musí být nasazený on-premise, s podporou vysoké dostupnosti HA Active-Passive. Zajištění HA vysoké dostupnosti nesmí být závislé na HA vysoké dostupnosti části řešení pro přístup interních uživatelů. A v případě jedné části musí být dostupná část druhá.

Řešení musí být navrženo tak, aby používalo pouze dedikovaný protokol a pomocí něj se dostávalo na koncová aktiva. Současně řešení musí umožnit přístup i k systémům, které nejsou přímo připojeny k internetu. Takové připojení musí mít podporu šifrování alespoň AES 256 a poslední verze TLS a být pravidelně testováno na zranitelnosti nezávislými třetími stranami.

Řešení musí umožnit uživatelům pracovat s řešením bez nutnosti instalace jakýchkoli softwarových komponent na jejich pracovní stanice. Před navázáním spojení musí být řešení schopno omezit přístup na základě rozsahu IP adres. Souběžně řešení musí poskytovat nativní TOTP pro rychlé přidání nového dodavatele a podporovat silnou autentizaci pomocí čipových karet, TouchID a SSO + Windows a Google authenticator.

Řešení musí podporovat metodiku řízení přístupu založenou na rolích (role based access control) na specifické systémy, stejně jako u interních uživatelů. Správci systému mohou definovat detailní parametry relace, jako jsou konkrétní časové rámce přístupu, požadované počty schválení a konkrétní povolené funkce přístupu (používání/zákaz konkrétních příkazů a spouštění aplikací).

Řešení umožní detekci a blokování aktivit, které vedou ke zcizení přihlašovacích údajů uživatelů na koncových bodech. Systém poskytne zabezpečení minimálně na úrovni ochrany Windows credentials (SAM, LSASS, LSA, NTDS.dit atd.), přihlašovacích údajů uložených v cache prohlížečů (IE, Edge, Chrome, Firefox), přihlašovacích údajů uložených v různých nástrojích pro vzdálenou správu (WinSCP, VNC, Putty) a dalších standardních nástrojích (Git, Total Commander).

Řešení musí umožňovat řídit, které aplikace může operátor v rámci relace používat a které ne. Tyto politiky lze navázat na konkrétní koncové body a na nich vynucovat specifická pravidla, která obsahují blacklist nebo whitelist aplikací ne/spustitelných v relaci. Současně poskytovat nastavení a následné automatické filtrování příkazů v rámci relace. Jakékoliv použití těchto zakázaných příkazů bude zablokováno a automaticky ukončí relaci.

Řešení musí umožňovat připojení aplikací třetích stran ke spravovaným koncovým bodům.

Řešení musí umožňovat připojení k web-based admin konzolím.

Řešení musí umožnit operátorům odesílat příkazy do cílového koncového bodu.

Řešení musí umožňovat připojení ke vzdáleným systémům mimo interní síť (perimetr) bez nutnosti použití sítě VPN.

Řešení musí umožňovat interaktivní sdílení a ovládání obrazovky koncového zařízení, včetně mobilních zařízení a PC.

Řešení musí umožňovat přístup ke spravovaným koncovým bodům ze zařízení se systémem Windows, Linux, Mac, iOS a Android.

Řešení musí podporovat připojení k Point-of-Sale (POS) zařízením skrze nativní protokoly RDP, SSH, VNC.

Řešení musí obsahovat samostatný portál pro registraci dodavatele, který umožní požádat o přístup k cílovým zařízením. Administrátoři mohou umožnit uživatelům dodavatele požádat o přístup nebo se zaregistrovat prostřednictvím přizpůsobitelné stránky portálu. Administrátoři mohou vytvářet a přizpůsobovat jednotlivé portálové stránky pro konkrétní dodavatele a umožnit tak uživatelům registrovat se k přístupu, který potřebují a kdy ho potřebují. Dodavatelský portál lze omezit na konkrétní e-mailové domény, nebo na stávající síťová omezení pro skupinu dodavatelů. Samostatná registrace uživatelů dodavatele prostřednictvím portálu dodavatele vždy vyžaduje schválení vytvoření uživatele definovaným administrátorem (správcem) dané skupiny dodavatelů.

Řešení musí upozornit na vypršení platnosti účtu dodavatele. Uživatelé dodavatelů mohou být automaticky upozorněni na blížící se datum vypršení platnosti dodavatele či účtu. Správce nebo uživatel s rolí dohlížející na skupinu dodavatelů může prodloužit datum vypršení platnosti uživatele dodavatele před vypršením platnosti jeho účtu. Kromě toho mohou správci/uživatelé znovu aktivovat uživatele dodavatele, jejichž platnost vypršela.

Řešení musí poskytovat samoobslužnou funkci obnovy hesla pro uživatele dodavatele. Uživatelé dodavatelů mohou obdržet vygenerovaný odkaz z řešení pro obnovení hesla. Každý, kdo může spravovat stránku uživatele dodavatele, může kliknout na tlačítko E-mailový odkaz pro obnovení hesla.

Řešení musí poskytovat uživatelům dodavatele přístup skrze webového klienta, mobilního klienta (iOS, Android), nebo nativního desktopového tlustého klienta s podporou operačních systémů: Mac, Windows, Linux (Debian, Redhat).

Řešení musí umožnit uživateli zobrazit a ovládat obrazovku koncového bodu. Současně řešení umožní uživateli souběžné připojení na více systémů z jedné konzole a práci s více monitory, které jsou zobrazené v rámci jedné relace.

Řešení musí umožnit uživatelům přenášet soubory do/z cílového koncového systému. Veškerá tato aktivita musí být nahrána a logována. Současně musí být v řešení nastavitelné bezpečnostní politiky, jaké soubory je a není možné přenášet.

Řešení musí nabízet zabezpečený chat mezi uživateli v rámci relací a veškerá komunikace skrze tento chat musí být ukládána uvnitř nabízeného řešení. Chat musí být dostupný jak při přístupu z webové konzole, tak i přes desktopovou konzoli a tlustého klienta. Současně řešení umožní spolupráci napříč jednotlivými týmy a uživateli, sdílet relace s ostatními uživateli systému a poskytovat funkcionalitu spolupráce více administrátorů na jedné souběžné relaci.

Řešení musí nabízet uživatelům systémové informace typu poslední restart, protokol událostí, nainstalované programy, běžící služby apod.). Současně nabídne uživatelům možnost provádět systémové úlohy mimo sdílení obrazovky (přenos souborů, regedit, reboot, apod.).

Řešení musí umožnit přístup ke Command Shell koncového bodu.

Řešení poskytne uživatelům způsob centrálního ukládání běžně používaných skriptů a následně jejich zvolení a použití v relaci pouze na klik, bez nutnosti psaní daného skriptu.

Dodavatelé standardně pracují pod nejnižší mírou potřebného oprávnění (princip least privilege) a v případě potřeby řešení musí umožňovat eskalaci oprávnění v rámci relace. Žádost o navýšení oprávnění musí být zaznamenána systémem a schválena pouze konkrétní osobou/skupinou s daným oprávněním.

Řešení musí uživatelům umožnit restartovat koncový systém v rámci relace a automaticky jej znovu připojit, jakmile je koncový systém opět online.

5 Část D – Systémy pro sběr a vyhodnocování událostí

5.1. Systém pro vyhodnocování a korelaci logů

Zadavatel požaduje navrhnout, dodat a implementovat centrální úložiště pro sběr a analýzu logů s možností následné analýzy a řešení bezpečnostních událostí/incidentů z kritických systémů a aplikací. Dodávané řešení pro sběr a korelaci událostí a logů - log management musí splňovat alespoň následující funkce a parametry.

Licenční pokrytí

Řešení musí být schopno sběru logů v průměru až 5000 událostí/s, licence není limitována počtem a ani velikostí uložených dat. Pokud jsou v nabízeném řešení zahrnuty jakékoliv licence, jejich legální používání nesmí být časově omezeno. Nabízené řešení tedy musí být plně funkční i po uplynutí doby placené podpory.

Obecné parametry

Systém musí mít umožnit shromažďování bezpečnostních údajů, analýzu údajů, podávání zpráv, detekci incidentů, poloautomatickou a automatickou reakci v souladu s příslušnými předpisy. Musí být zajištěna redundance systému formou active-active, s podporou horizontálního a vertikálního rozšíření. Možnost používání a správy systému je požadována v jedné centrální konzoli dostupné v prohlížeči přes HTTPS protokol.

Nabízený systém musí mít pokročilé funkce obohacování dat, reporting, možnost analýzy událostí, spuštění alarmu, správu událostí, detekci hrozeb, nastavitelné korelace událostí, včetně nastavení reakce na incidenty.

Pořadavky na funkcionalitu:

- Schopnost shromažďovat data paralelně z více různých segmentů sítě současně a možnost správy v jednom centrálním prostředí.
- Podpora sběru dat pomocí protokolů SYSLOG, SSH, SMB, API, FLOW, SFTP, WMI.
- Možnost sbírat data přímo z tabulek v databázích Microsoft SQL, ORACLE a MY SQL.
- Schopnost shromažďovat data zapsaná databázemi Microsoft SQL a ORACLE do datových struktur operačních systémů Windows a Linux.
- Možnost integrace s aplikacemi MS Office 365, MS Azure a shromažďování dat prostřednictvím API rozhraní.
- Systém musí obsahovat vhodné nástroje pro budoucí integrace s dalšími řešeními třetích stran a IoT zařízení.
- Systém musí vést auditní záznamy o všech operacích a umožnit pro tyto záznamy vyhledávání.
- Systém musí v centrální konzoli umožnit náhled na všechny logovací zdroje v rámci jednoho uceleného přehledu.
- Možnost zahrnout či vyloučit určitá pole ze shromážděných nezpracovaných údajů.
- Možnost provádět sběr dat bez agenta, s agentem a možnost využití agentů třetích stran s globální platností.
- Během procesu sběru dat musí být odděleně zaznamenávány samotné vytvořené údaje, čas jejich přijetí a čas jejich vytvoření. Dotazování a vykazování musí být možné provádět také dle času vytvoření dat.
- Systém musí disponovat nástrojem pro vývoj vlastního modulu pro konzumaci událostí. Pro tvorbu modulů je vyžadována podpora minimálně formátů CEF, Key-value, JSON.
- Vizualizace dat musí podporovat zobrazení všech shromážděných dat a všech jejich parametrů.
- Nabízený software musí být začleněn do systému "Geo Location", který dokáže zobrazovat informace o zemi / poloze na základě IP v internetových datových záznamech a neustále tyto informace aktualizovat a tyto informace dokáže zobrazovat ve svých zprávách.
- Systém musí být schopen prezentovat záznamy včetně informace o geolokaci IP adres obsažených v záznamech. Informace o zemi/poloze musí být dynamicky aktualizovány.
- Schopnost automaticky obohatit data shromážděná ze zdrojů o hodnoty patřičných atributů MS LDAP.
- Schopnost obohatit data z různých zdrojů pomocí funkce modifikátoru.
- Schopnost obohatit údaje shromážděné ze zdrojů o údaje z globálních a místních zpravodajských služeb o kybernetických hrozbách.
- Schopnost určit specifickou politiku správy dat pro každý integrovaný zdroj protokolů.
- Podpora filtrování, slučování a mapování stejných údajů během sběru dat.
- Schopnost vyhledávání podle všech parametrů datových formátů.
- Možnost ukládání dotazů pro následné použití.
- Podpora pokročilého vyhledávacího jazyka, který dokáže vyhledávat v aktuálních datech. Pomocí tohoto vyhledávacího jazyka lze pro všechny parametry datových formátů nebo jejich hodnoty použít logické výrazy (AND, OR, NOT, atd.). Schopnost vyhledávat pomocí seskupování v rámci určitých hodnot, udávání rozsahů v číselných hodnotách, rozsahů v hodnotách IP.
- Podpora fulltextového vyhledávání.
- Schopnost provádět analýzu jednoho či více záznamů v rámci výsledků odpovídajících kritériím vyhledávání.
- Podpora funkce následného vyhledávání pro hlubší analýzu (Drill Down).

- Podpora automatické analýzy časového rozložení dat.
- Schopnost navigace uživatelských kroků při filtrování výsledků v rámci procesu vytváření analýzy.
- Schopnost zobrazení a analýzy tzv. RAW dat (neupraveného záznamu).
- Schopnost vytvářet reporty odpovídající obecným IT standardům (ISO 27001, PCI, SOX, KVKK, GLBA).
- Možnost sledovat parametry monitorovaného systému prostřednictvím navrženého náhledu (např. procesor, paměť, kapacita disku).
- Schopnost generovat reporty ve formátech PDF, XLS, HTML. Systém musí umožňovat uložení nastavení reportu pro další použití.
- Možnost limitovat rozsah vyhledávaných dat a definovat určité období pro vyhledávání dat.
- Možnost využít průvodce pro snadnou přípravu reportu.
- Možnost určit, který obsah se v sestavě reportu zobrazí a možnost přidávat a odebírat sloupce.
- Schopnost provádět matematické a statistické výpočty na základě aktuálních dat. Schopnost provádět výpočty, jako jsou seskupení hodnot, součty číselných údajů, časové rozložení hodnot, počet jedinečných hodnot. Např: Výpočet šířky pásma využívané IP adresou, počet spojení, která navazuje, různé porty, které používá, a počet různých IP adres, ke kterým přistupuje.
- Schopnost vytváření individuálních návrhů monitorovacích obrazovek kombinací požadovaných zpráv a ukládání návrhů pro další použití.
- Všichni uživatelé musí mít oprávnění k přístupu k jednotlivým nabídkám funkcionalit a modulům.
- Možnost nabízet uživatelům autorizaci založenou na zdrojích záznamů.
- Podpora řízení přístupu na základě rolí (RBAC) pro uživatelské účty. Všechny moduly systému a funkce v něm musí být autorizovány na základě uživatelů.
- Správce musí mít možnost definovat neomezené oprávnění na základě rolí pro uživatele, kteří mají být v navrhovaném systému oprávněni.
- Možnost provádět autorizaci musí mít pouze správci se speciálním oprávněním.
- Systém musí být integrován s řešením MS Active Directory pro autentizaci přístupu.
- V případech, kdy je třeba provést operace s komprimovanými daty, se uživateli automaticky zobrazí příslušný záznam bez jakéhokoli provozního zatížení.
- Data uložená v souborovém systému musí disponovat verifikačním mechanizmem zabraňujícím neoprávněnou modifikaci (např. podpis digitálním certifikátem s časovým razítkem).

Implementace

- Způsob sběru dat z jednotlivých zdrojů bude součástí předimplementační analýzy a bude popsán v Solution Design dokumentu.
- Podpora shromažďování dat ze zdroje dat (se známým datovým formátem), který není v navrhovaném systémovém standardu a nepodporuje jej. Potřebné postupy (příprava zásuvných modulů apod.), aby shromážděná data měla smysl, provede ZHOTOVITEL bezplatně před zahájením přejímacích prací.
- Vytvoření modulů pro nepodporované zdroje dat v rámci implementace zajistí Dodavetel. Nutnou podmínkou je poskytnutí formátu dat ze strany Zadavatele.
- Dodavatel v rámci implementačních prací připraví také všechny náhledy na zdroje dat, které budou součástí implementace. Maximální počet požadovaných předkonfigurovaných reportů v rámci implementace je 20.

6 Podmínky technické podpory (SLA) a rozvoje řešení

Tento požadavek je součástí Servisu Díla. Dodavatel se zavazuje poskytovat Zadavateli služby v režimu 24x7 v minimálním rozsahu:

- telefonická hot-line podpora pro okamžitou komunikaci 24h denně
- diagnostika a odstraňování poruch systému
- profylaxe - preventivní prohlídka systému
- kontrola stavu nainstalovaných updatů a hotfixů
- kontrola a analýza chybových logů systémového SW, stejně tak aplikačního programového vybavení
- kontrola vytíženosti systémových zdrojů
- sběr zpětné vazby od administrátorů systému

Dodavatel se zavazuje Zadavateli, že jakékoliv vady plnění Servisu díla či jeho části, které vzniknou v době trvání záruky budou odstraněny na náklady Dodavatele. Dodavatel garantuje Zadavateli čas pro odezvu a čas pro vyřešení provozního incidentu, a to pro jednotlivé kategorie provozních incidentů následovně:

Kategorie incident	Doba odezvy (IRT)	Doba vyřešení (TRT)
Kritický - v případě kritické chyby	60 minut	2 hodiny
Vysoký – v případě závažné chyby	60 minut	8 hodin
Střední – v případě běžné chyby	1 den	3 dny
Nízký – v případě minoritní chyby	3 dny	Best effort

Podpora je poskytovaná v českém jazyce ve formě Helpdesk podpory a v případě kritického incidentu telefonické podpory. Jednotlivé úkony/akce dle specifikace podpory jsou definovány následovně.

Doba odezvy (IRT)

Je definovaná jako časový interval měřený od doby, kdy Zadavatel ohlásil incident do Helpdeskové aplikace poskytovatele nebo telefonicky s následným zadáním do Helpdeskové aplikace po dobu, kdy je zpětně kontaktovaný poskytovatelem nebo je incident přijat do řešení. Doba odezvy může být také označována jako reakční doba.

Doba vyřešení (TRT)

Je definovaná jako časový interval měřený od doby, kdy Zadavatel ohlásil incident do Helpdeskové aplikace poskytovatele nebo telefonicky s následným zadáním do Helpdeskové aplikaci po dobu, kdy poskytovatel vyřešil popsaný incident. Měření SLA pro TRT neběží v době, kdy je ticket předán zpět na Zadavatele k doplnění informací podstatných k vyřešení incidentu a také v době, kdy je incident předán na podporu výrobce.

Priority

Zaručená doba odezvy na vzniklé incidenty se dělí dle jejich priority. Priorita je dána kritičností vzniklého incidentu v návaznosti na požadovanou funkčnost produktu:

- Kritická chyba – Nefunkčnost způsobená dodanou technologií, Nefunkčnost/nedostupnost řešení
- Závažná chyba – Nefunkčnost některé z komponent, která nedovoluje vykonávat požadovanou činnost. Vážné chyby řešení ovlivňující provoz Zadavatele.
- Běžná chyba – Nefunkčnost některé z komponent, která nemá přímý dopad na dostupnost Zadavatele, vážné konfigurační chyby.
- Minoritní chyba – Chyby v konfiguraci, Chyby řešení neovlivňující provoz Zadavatele, Nefunkčnost komponent minoritního charakteru.

Dodání workaroundu znamená předání opravy či náhradního postupu snižujícího závažnost nebo dopady Incidentu. V případě dodání workaroundu se zastaví měření Doby vyřešení.

V rámci části služby rozvoje je požadován rozvoj a údržba díla, tedy činnosti, které nejsou součástí SLA podpory. Cena za Služby rozvoje je automaticky vypočtena jakou součin práce Ceny za jeden člověkoden (MD) práce (implementace) bez DPH a předpokládaného Počtu člověkodní rozsahu 180 MD za období 5 let. Předpokládaný počet člověkodní (MD) je stanoven pouze pro účely hodnocení nabídek v zadávacím řízení. Zadavatel není povinen předpokládaný počet člověkodní (MD) služeb rozvoje vyčerpat, zároveň je oprávněn jej v případě potřeby překročit.