Technická specifikace

Správa a monitoring privilegovaných účtů – PIM

OBSAH

Seznam obrázků

Seznam tabulek

1 ÚČEL DOKUMENTU

Tento dokument obsahuje specifikaci řešení a technických požadavků na systém pro správu a monitoring aktivit privilegovaných účtů ICT systémů Ministerstva Zemědělství České republiky. Dokument tvoří přílohu zadávací dokumentace veřejné zakázky „Správa a monitoring privilegovaných účtů - PIM“ a obsahuje představení požadovaného konceptu řešení, základní popis poptávaného řešení a požadavky závazné pro všechny potenciální uchazeče o zajištění realizace zakázky.

2 PŘEHLED ZÁKLADNÍCH POJMŮ

Termín	Význam
AD	Microsoft Active Directory
AK	Aplikační katalog
CAL	Client Access License
DC	Datové centrum
EP	End Point – řízený koncový systém (Win, Linux, DB, Router, SAP …)
DRP	Disaster recovery plan
HA	High Availability – režim vysoké dostupnosti (např. redundance)
HP BAC	HP Business Availability Center – nástroj pro End-to-end monitoring
HW	Hard-Ware
ICT	Informační a komunikační technologie (Information and Communication Technologies)
IDM	Identity Management – správa uživatelských účtů
LDAP	Lightweight Directory Access Protocol
Objednatel/Zadavatel/MZe	Česká republika – Ministerstvo zemědělství
OID	Oracle Internet Directory – LDAP systém od Oraclu, který je implementován v prostředí MZe
OIM	Oracle Identity Manager – IDM systém od Oraclu, který je implementován v prostředí MZe
OS	Operační Systém
OSS	Organizační složka státu – organizace podřízená ministerstvu
PAM	V kontextu Unix/Linux PAM - Pluggable Authentication Modules umožňující např. delegaci autentizace na externí adresář (LDAP/AD) Privileged Account Management - správa privilegovaných identit/účtů
PIM	Privileged Identity Management - správa privilegovaných identit/účtů
Privilegovaný účet	Uživatelský účet informačního systému s širokou nebo neomezenou množinou administrátorských oprávnění, který je zpravidla nepersonalizovaný a může být sdílen mezi vícero uživateli.
PuTTY	Klient protokolů SSH, Telnet, rlogin a holého TCP.
RDP	Remote Desktop Protocol – protokol na přenos vzdálené plochy
RODC	Active Directory Read-Only Domain Controller
SIEM	Security Information and Event Management - správa bezpečnostních informací a událostí
Smlouva	Smlouva o poskytnutí řešení „Správa a monitoring privilegovaných účtů – PIM“
SNMP	Simple Network Management Protocol

SSO	Single sign on - systém jednotného přihlášení
SUR	Aplikace pro správu uživatelů a rolí
SW	Software
TS	Terminálový server
WMI	Windows Management Instrumentation
Zhotovitel, Dodavatel	Subjekt, který je jako Zhotovitel/Dodavatel definován v záhlaví Smlouvy

Tabulka 1 - seznam zkratek a pojmů

3 AKTUÁLNÍ STAV

Informační prostředí MZe je tvořeno velkým množstvím informačních systémů a rozlehlou síťovou infrastrukturou, na kterém je závislý chod celé organizace. Každý z prvků tohoto prostředí obsahuje privilegované účty, které jsou využívány pro jejich administraci, běžnou obsluhu, nebo se jedná o servisní účty použité v rámci integrací. K takovým účtům mají přístup jak zaměstnanci MZe, tak externí dodavatelé, kteří zajišťují provoz a rozvoj IT systémů a služeb MZe.

Současný stav řešení problematiky správy privilegovaných účtů je shrnut v následujících odstavcích:

3.1 Organizační opatření

1. Proces přidělování a manipulace s uživatelskými účty, včetně těch privilegovaných, je organizačně řízen podle vnitřní směrnice.
2. Osoba disponující privilegovaným účtem se musí zavázat k dodržování pravidel informační bezpečnosti (dále jen „prohlášení“). Toto prohlášení jasně definuje způsob manipulace s těmito účty a jejich používání jako například:
    a. Politika hesel – složitost hesla, stáří hesla, unikátnost hesla (stejné heslo není použito pro více účtů).
    b. Účet není dovoleno nikde ukládat pro použití v rámci automatizovaného přihlašování.
3. Tato organizační opatření jsou vynucována pouze na systémech a aplikacích, které umožňují definovat politiku hesel. Kontrola nastavení politiky hesel je však prováděna pouze občasně a nesystematicky.

3.2 Přístup k účtům a jejich evidence

1. Neexistuje centrální evidence všech privilegovaných účtů (jen některých, většinou na úrovni infrastruktury), ani osob, které k nim mají přístup.
2. Některé účty jsou sdíleny mezi více osobami.
3. Záměrem je však, tam kde je to možné, používat osobní účty. V rámci jednotlivých technologií je používán následující přístup:
    a. **Unix/Linux** (HP-UX, RedHat, CentOS) – veškeré účty jsou lokální. Pro administrátory jsou vytvořeny lokální osobní účty. Pro přístup k privilegovaným účtům (root, oracle, …) se používá *sudo*.
    b. **Windows** – většina Windows serverů je zapojena do AD domény MZe. Účty jsou tedy používány převážně osobní doménové. Administrátoři serverů mají své účty přiřazené na jednotlivých serverech do lokální skupiny Administrator (buď napřímo nebo přes doménovou skupinu). Frontend Windows servery (DMZ1) nejsou zapojeny do domény, tudíž správa uživatelů a oprávnění je pouze lokální.
    c. **Network** (routery, switche, firewall, WCF, IPS, IDS, WIFI atd.) – kde je to možné, jsou použity osobní účty administrátorů. Např. Cisco zařízení jsou napojeny na Cisco ACS, který slouží jako centrální autentizační a autorizační bod, na kterém má každý

z uživatelů svůj osobní účet - systémový privilegovaný účet je tedy použit jako záložní varianta pouze v případě výpadku ACS serveru. Pro správu je zpravidla použit buď:

i. Tlustý klient nebo tenký klient.
ii. SSH
iii. Telnet

d. **VMWare** – ESXi servery jsou zapojen do AD domény, používá tedy osobní doménové účty. Systémový účet root je používán výjimečně (např. upgrade). Pro přístup k serveru se používá jak tlustý tak tenký vSphere klient.
e. **Citrix XenApp** – pro autentizaci a autorizaci je použita AD doména. Oprávnění se však řídí z adresáře LDAP, ze kterého jsou synchronizovány do AD. Citrix se používá pro publikaci „tlustých“ aplikací jak pro MZe tak podřízené OSS. Publikováno je interně (do lokální sítě) a také externě prostřednictvím externího portálu.
f. **LDAP** – pro administraci se využívají výhradně osobní účty LDAPu. Výjimku tvoří vytváření skupin, které může být prováděno servisními účty napojených aplikací.
g. **Active Directory a Exchange** – pro administraci se využívají osobní doménové účty. Výjimečně je nutné použít přímo účet doménového administrátora, proto je heslo k tomuto účtu sdíleno v rámci Windows týmu.
h. **SAP** – pro správu účtů je použit SAP Solution Manager. Používány jsou převážně lokální osobní účty.
i. **Databáze** (Oracle, MS SQL, PostgreSQL) – převážně se používají osobní lokální účty. V některých případech se používají servisní administrátorské účty, které jsou sdíleny (jak z nutnosti, tak kvůli usnadnění). Pro přístup k databázi se používají zejména standardní management nástroje: Oracle SQL Developer, Microsoft SQL Management Studio. Běžný je také přístup přímo z napojené aplikace, která v sobě přístupové údaje k databázi uchovává, tudíž je administrátor ani nemusí znát.
j. **Aplikační servery** (WebLogic, JBoss, Tomcat, Oracle AS, GlassFish) – pokud server umožňuje administraci prostřednictvím web GUI, jsou použity lokální sdílené administrátorské účty.

4. Hesla administrátorských účtů jsou po jejich vygenerování a nastavení vytisknuty, vloženy do obálky a založeny ve fyzickém trezoru u bezpečnostního manažera MZe. K heslu mají však přístup také správci příslušných systémů, kteří ho mohou v případě potřeby využívat.
5. Není nijak stanoveno, jak hesla k privilegovaným účtům uchovávat, ani způsob jejich předávání (obzvláště u sdílených účtů).
6. Účty jsou používány v rámci skriptů a integračních komponent informačních systémů, kde mohou být uloženy buď v otevřené formě, nebo v zabezpečeném úložišti.

3.3 Aktivita účtů

1. Aktivita těchto účtů většinou není nijak monitorována, pokud monitorována je, děje se tak zpravidla až na aplikační úrovni a nejednotným způsobem.
2. Logování systémů o aktivitě privilegovaných účtů není standardizováno, tedy není stanoveno, jaké události se mají monitorovat ani jak dlouho se mají uchovávat, či centrálně shromažďovat a vyhodnocovat (SIEM).

4 POŽADOVANÝ STAV A MOTIVACE

Privilegované účty umožňují takřka neomezený přístup ke zdrojům příslušných systémů včetně manipulace s nimi (např. root, Administrator, sys, sa, atp.), proto jsou významným bezpečnostním rizikem. Oprávnění disponovat takovým účtem mají jak interní zaměstnanci, tak externí dodavatelé a takové oprávnění často není nijak evidováno. Znalost přihlašovacích údajů je navíc zpravidla sdílena mezi více uživateli, tudíž odpovědnost za případné zneužití je velice těžko dohledatelná, nebo dokonce není vůbec prokazatelná. Toto riziko se vztahuje na všechny systémy, počínaje operačními systémy, databázemi, síťovými prvky až na komplexní informační systémy distribuované jako produkt, nebo vyvinuté na míru. Ať už přímo nebo nepřímo se tedy problém dotýká všech informačních systémů, včetně systémů potenciálně identifikovaných jako „Významný informační systém“ nebo „Kritická informační infrastruktura“ v rámci zákona č. 181/2014 Sb., zákon o kybernetické bezpečnosti, který vychází z doporučené normy ISO/IEC 27001. Proto je nutné zavést správu přístupu k těmto účtům a monitoring veškeré aktivity účtů s vazbou na konkrétní osobu, která jím právě disponuje.

Řešením správy privilegovaných účtu je nasazení tzv. **Privileged Identity Management** Systému (PIM, nebo také Privileged Account Management – PAM). PIM můžeme rozdělit do následujících tří oblastí, které spolu úzce souvisí:

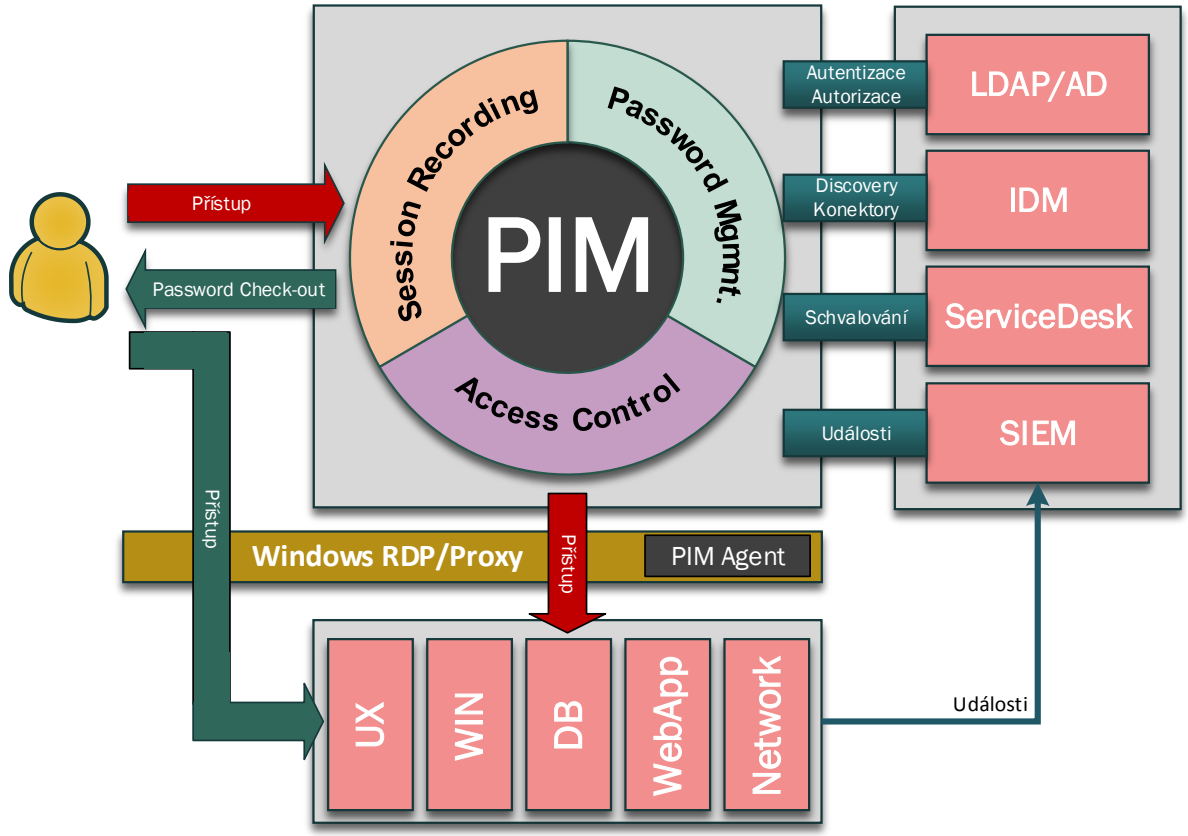
1. **Password Management** – centrální správa privilegovaných účtů se zabezpečeným úložištěm hesel a správou přístupů k těmto účtům.
2. **Session Recording** – zaznamenávání aktivit privilegovaných účtu včetně nahrávek obrazovek a stisků kláves (key-logging).
3. **Access Control** – kontrola přístupu k systému pomocí privilegovaných účtů, zvýšení granularity oprávnění těchto účtů, detekce a ochrana prostředků systému na základě definovaných politik.

Z důvodů urychlení nasazení řešení rizik je požadováno implementovat pouze první dvě oblasti **Session Recording** a **Password Management**, které pokryjí většinu identifikovaných rizik a zároveň umožní naplnit nařízení v rámci návrhu zákona a kybernetické bezpečnost, konkrétně:

Druhá část, HLAVA II – Technická opatření:

- *Nástroj pro ověřování identity uživatelů*
  Stanovení politik hesel, které řeší právě Password Management.
- *Nástroj pro zaznamenávání činností kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a správců*
  Zaznamenávání činnosti privilegovaných účtů, které řeší Session Recording.

Zahrnutí oblasti **Access Controlu** v rámci tohoto projektu není požadováno. Je však vyžadováno, aby nasazované řešení tuto funkcionalitu podporovalo a bylo tak možné celou problematiku pokrýt v rámci jednoho řešení pouze jeho rozšířením.



Obrázek 1 - koncept PIM řešení

5 POPIS POŽADOVANÉHO ŘEŠENÍ

Dodavatel zajistí návrh a dodání PIM řešení, které vyhovuje požadavkům uvedeným v této Technické specifikaci. Jednotlivé oblasti řešení jsou popsány v kapitolách níže.

5.1 Password Management

Jedná se o systém s centrálním vysoce zabezpečeným úložištěm privilegovaných účtů a příslušných hesel spolu s konektory na koncové systémy (EP) s řízenými účty a uživatelským rozhraním, nad kterým je postavena logická vrstva v podobě procesů a politik.

Uživatelé (zaměstnanci/externí dodavatelé) přistupují do systému pomocí uživatelského rozhraní na základě autentizace proti lokálnímu, nebo externímu adresáři (AD/LDAP). Lokální autorizací, nebo autorizací proti stejnému adresáři uživatel získává množinu privilegovaných účtů, kterými může disponovat. Takové účty je možné použít dvěma způsoby:

1. **Heslo** je možné si nechat **zobrazit** na obrazovce a následně použít standardním způsobem.
2. Použít **automatizované přihlášení** (SSO) k systému pomocí privilegovaného účtu bez nutnosti prozrazení hesla. Přihlášení probíhá buďto přímo v prohlížeči prostřednictvím pluginu prohlížeče, který otevře okno s příslušnou klientskou aplikací, bez nutnosti její lokální instalace, nebo je využito lokální klientské aplikace na koncové stanici uživatele, které je heslo předáno pomocí skriptu. Tímto způsobem jsou podporovány běžné protokoly/aplikace:
    - SSH, Telnet;
    - RemoteDesktop;
    - HTTP(s)/Web aplikace;
    - libovolná „tlustá“ klientská aplikace;

    Takový přístup výrazně zvyšuje uživatelský komfort, jelikož uživatelé nejsou nuceni s hesly privilegovaných účtů vůbec pracovat, veškerá akce probíhají automaticky na pozadí (tzv. privileged SSO). Uživatelé si tak např. nemusí pamatovat mnoho dalších hesel, ale využívají jen heslo svého účtu.

Pro zobrazení/použití hesla uživatel spustí akci check-out, při které je za pomoci konektoru heslo změněno, stejně jako po ukončení práce s účtem, kdy je volána akce check-in. Při použití automatizovaného přihlášení dochází k akci check-out/in automaticky. Tímto je zaručena jasná evidence toho, kdo má k jakým účtům přístup a v jaké chvíli je využíval.

Kromě účtů, které má uživatel volně k dispozici, může mít také přiřazeny účty, ke kterým získá přístup až po udání důvodu, nebo po **schválení** jiným uživatelem, nebo skupinou uživatelů. Takový přístup může získat buď na omezenou dobu, nebo na stálo. Schvalovací workflow je možné libovolně strukturovat, nebo je možné využít napojení na externí service desk.

V případě nouzové situace, kdy je potřeba získat přístup k heslu privilegovaného účtu okamžitě, existuje proces, který takovou akci podporuje, za současného zalogování a odeslání notifikace na určenou kontaktní osobu.

Pro spravované účty jsou definovány **politiky hesel**, které jasně definují složitost hesla a jeho stáří – dle těchto politik jsou generována náhodná hesla, která jsou aktivně propisována do EP pomocí konektorů. V pravidelném intervalu je naplánována kontrola, zda nedošlo ke změně hesla privilegovaného účtu při externím zásahu mimo PIM systém. Detekovaný zásah je aktivně notifikován. Zároveň je plánováno pravidelné **discovery** účtů na EP – zde je vhodná interakce s IDM, aby bylo možné jednoznačně odlišit, zda se jedná o uživatelský účet patřící konkrétní identitě, nebo o sdílený privilegovaný účet. Takové účty jsou reportovány odpovědné osobě, která je na základě definovaného procesu zařadí příslušným uživatelům a nastaví odpovídající politiky.

Kromě přístupu uživatelů k privilegovaným účtům, systém obsluhuje také **přístup aplikací**. Je poskytnut aplikační interface umožňující provést check-out hesla k účtu, čímž poskytuje možnost vyvarovat se použití otevřeného hesla přímo v kódu skriptu/aplikace. Standardně je v rámci řešení password managementu možné integrovat mechanizmus pro získávání hesla přímo do aplikačních serverů, které jej mohou používat k získání přístupu k různým datovým zdrojům (databáze). Tímto jednoduchým mechanizmem je možné zbavit se uložených přístupových údajů bez nutnosti upravovat aplikaci.

5.2 Session Recording

Další důležitou oblastí je detailní audit aktivity privilegovaných účtů. Password Management zajišťuje přehled o přístupu k účtům, nikoliv však přehled aktivit, které jsou s takovým účtem konány. To je zajištěno nahráváním uživatelských relací - snímáním obrazovky a logování uživatelského vstupu (key-logging). Každá akce (stisk klávesy, změna obrazovky apod.) privilegovaného účtu je nahrávána a je jednoznačně přiřazena konkrétní osobě. Nahrávky jsou zabezpečeným způsobem přenášeny do centrálního úložiště, kde jsou dlouhodobě uchovávány. Takové nahrávky jsou klíčovým důkazem, kterým je možné uživateli jednoznačně prokázat veškeré jeho aktivity. Zároveň však mohou obsahovat velice citlivé informace. Proto je nutné dodržovat základní bezpečnostní triádu CIA (confidentiality, integrity, availability):

- **Confidentiality** (důvěrnost) – nahrávky jsou po celou dobu uchovávány v zašifrované podobě - tedy od jejich zaznamenání, až po konečné uložení do centrálního repository a jejich archivace. Dále je zaručeno, že k těmto nahrávkám mohou přistupovat pouze autorizované osoby, aby nemohlo dojít k jejich zneužití. U vysoce citlivých/kritických systémů je možné aplikovat metodu čtyř očí, kdy je k zobrazení záznamu podmíněno schválením další osoby.
- **Integrity** (celistvost) – je nutné zabránit jakékoliv manipulaci s nahrávkami po celou dobu jejich existence, aby nemohlo dojít ke zpochybnění její prokazatelnosti. Toho je možné dosáhnout digitálním podpisem každé z nahrávek.
- **Availability** (dostupnost) – klíčovost těchto nahrávek implikuje nutnost zaručit jejich dostupnost. Nahrávky jsou pravidelně zálohovány, současně je zajištěno, že nemohou být jednoduše odstraněny.

Nahrávky jsou efektivním způsobem zaznamenávány a přenášeny (komprimace, zaznamenávání pouze aktivní relace), aby nedocházelo ke zbytečnému zatěžování prostředků (úložiště, síť).

Aby měl systém nahrávání relací vůbec význam, je nutné zajistit, aby ho nebylo možné jednoduše obejít. Toho je dosaženo následujícími prvky:

1. Uživatelé přistupují k EP výhradně prostřednictvím jednoho, nebo více bodů, na kterých je systém nahrávání provozován.
    - Může se jednat o prvek, který funguje jako **síťová proxy**, tedy je přes něj směrována veškerá síťová komunikace od uživatele k EP, která je zaznamenávána.
    - Další variantou je využití vyhrazených **terminálových serverů** (TS) nebo zařízení, které jsou využívány jako jediný bod zprostředkovávající komunikaci uživatele s EP (dále jen „přístupový bod“). Veškeré aktivity na tomto přístupovém bodě jsou zaznamenávány.
2. Jakýkoliv pokus přihlášení k EP z jiného než vyhrazeného bodu (proxy/přístupový bod) je detekován a buď aktivně přerušen, nebo alespoň notifikován. K tomuto účelu je možné využít systém SIEM.

Síťová pravidla jsou nastavena takovým způsobem, aby byl umožněn přístup výhradně přes tyto kontrolní body, pokud to prostředí podporuje.

Nahrávky obsahují kromě samotných obrazovek a uživatelského vstupu také příslušná **metadata** – např. názvy oken na obrazovce, stisknutá tlačítka, výstup příkazů na obrazovce, otevřené soubory, atp. Všechny tyto údaje jsou **indexovány** tak, aby v nich bylo možné efektivně vyhledávat a z výsledku vyhledání moci přejít rovnou na relevantní místo v nahrávce, bez nutnosti sledovat kompletní záznam.

5.3 Access Control

Tato oblast se zabývá řízením přístupu privilegovaných účtů, tedy kontrolu nad tím, jaké aktivity může jaký uživatel s privilegovaným účtem provádět. Můžeme chápat jako přidání další vrstvy oprávnění na koncovém systému, kde je účet využíván.

Tato funkcionalita není v rámci tohoto projektu vyžadována. Je však vyžadováno, aby nasazované řešení tuto funkcionalitu podporovalo, aby bylo možné celou problematiku pokrýt v rámci jednoho řešení pouze jeho rozšířením.

Access control je tedy určen **sadou politik**, které se skládají z následujících pravidel:

1. Výčet příkazů, které uživatel může/nemůže spouštět.
2. Výčet zdrojů, které uživatel může/nemůže využívat – např. soubory, adresáře.
3. Výčet kanálů, které uživatel může/nemůže využívat pro přístup k systému.
4. Časová okna, definující kdy je možné k systému přistupovat.

Omezení mohou být buď přímo vynucena, nebo pouze auditována, kdy vyhodnocení pravidla v případě porušení může spustit generování události do systému SIEM nebo notifikaci.

Politiky jsou **centrálně** spravovány a je zajištěna jejich distribuce a deployment na koncové systémy a to buď manuální (politiky jsou EP ručně přiřazeny), nebo automatická (na základě typu nebo kategorie EP).

5.4 Integrace

Systém na řešení PIM podporuje následující integrace s ostatními systémy organizace.

5.4.1 LDAP/AD

Adresářová služba LDAP nebo Active Directory je využita jako primární zdroj autentizace a autorizace uživatelů pro všechny jejich aktivity. Autorizace opravňuje uživatele k těmto aktivitám:

1. Aktivity v rámci systému na řízení PIM, tedy příslušnost základních rolí:
    a. **Administrátor** – konfiguruje systém nebo jeho část, může vytvářet/upravovat/odstraňovat objekty systému (kromě odstraňování auditních informací a nahrávek).
    b. **Auditor** – má přístup k auditním informacím a nahrávkám.
    c. **Uživatel** – je mu umožněn přístup k systému PIM a jeho běžné používání.
2. Aktivity spojené s privilegovanými účty:
    a. **Vlastník** – nastavuje, kdo má k účtu přístup, případně schvaluje přístup v rámci workflow, přiřazuje politiky hesel.
    b. **Uživatel** – může účet buď přímo používat, nebo je mu umožněno o přístup k účtu zažádat.

Struktura oprávnění je zpravidla ještě dále členěna, jedná se pouze o základní pohled.

5.4.2 IDM

IDM systém je nepřímo integrován prostřednictvím adresáře LDAP/AD, který je IDM systémem spravován.

Dále je navržena kooperace systému IDM a PIM při discovery účtů na EP, kdy je potřeba zjistit, zda nově nalezený neřízený účet patří identitě (osobě), nebo se jedná o sdílený privilegovaný účet, na základě čehož je účet předán do správy buď IDM nebo PIM systému.

5.4.3 Logování a SIEM Systém

PIM loguje jak veškeré aktivity prováděné administrátory nad řešením, tak i veškeré operace uživatelů používajících PIM. Všechny tyto logované záznamy je možné přenášet, nejlépe real-time, do systému pro bezpečnostní monitoring (SIEM) k jejich vyhodnocení a uložení na centrálním bezpečném místě pro případnou zpětnou analýzu.

Do SIEM sytému se rovněž integrují i logy ze systémů a aplikací na EP, aby bylo možné vyhodnotit dodržování pravidel pro přístup daných PIM řešením (např. že uživatelé přistupují k EP přes vyhrazené přístupové řešení a ne napřímo).

5.4.4 Service Desk

Schvalování přístupů k účtům je buď řešeno přímo v systému PIM, nebo je možné využít integrace se Service Desk systémem, na který je schvalování zcela, nebo jen částečně delegováno (např. nutnost zadání čísla schvalovacího ticketu, který je následně ověřen). Stejný způsob schvalování může fungovat také při žádosti o přístup k nahrávkám.

5.5 Rozsah

Dále jsou uvedeny informace k rozsahu analýzy a implementace.

5.5.1 Integrované systémy/aplikace

Cílem bude postupně zahrnout do Session Recordingu a Password Managementu[1] následující systémy a aplikace:

	Systém/Aplikace (typ EP)	Protokol/Rozhraní	Přibližný počet systémů/apl.
1.	Fyzické servery s operačním systémem • Unix/Linux – HP-UX, RedHat, CentOS • Windows (lokální, nebo zapojené do domény)	**SSH – Unix/Linux** **RDP/WMI – Windows**	**100**
2.	Virtuální servery s operačním systémem • Unix/Linux – RedHat, CentOS • Windows (lokální, nebo zapojené do domény)	**SSH – Unix/Linux** **RDP/WMI – Windows** **VMWare**	**250**
3.	Infrastrukturní a bezpečnostní prvky (routery, switche, firewall, WCF, IPS, IDS, WIFI atd.)	**SSH/Telnet,** **HTTP(S) (webové rozhraní)**	**70**
4.	VMware ESXi 5.1.0	**Tlustý klient/web** **vSphere**	**Fyz. serverů: 16** **CPU 12 core: 6** **CPU 8 core: 24** **CPU 6 core: 4** **CPU 4 core: 6**
5.	Citrix XenApp platforma, včetně session recordingu deployovaných aplikací.	**Tlustý klient/web** **ICA**	**2**
6.	LDAP (Oracle Internet Directory)	**LDAP**	**1**
7.	Microsoft Active Directory (přístup k doméně privilegovanými osobními účty nelze omezit, proto bude řešeno monitoringem SIEM systémem)	**LDAP/RDP**	**3**
8.	SAP • SAP Business Warehouse • SAP ERP (systémy R3, AF, EP)	**Tlustý klient/web**	**1**
9.	Databáze (Oracle, MS SQL, PostgreSQL)	**SQL/Tlustý klient** **Oracle** – SQL*Plus, SQL Developer **MS SQL** – SQL Server Management Studio	**15 (instance)**
10.	Aplikační servery s administračním web GUI (JBoss, WebLogic, GlassFish, Oracle AS, Tomcat)	**Webové rozhraní**	**35**

[1] Některé z uvedených aplikací/systémů nebude možné zařadit do plného Password Managementu z důvodu nemožnosti jednoduše měnit hesla k účtům. V takovém případě bude heslo alespoň evidováno a v pravidelném intervalu měněno správcem manuálně.

11.	Ostatní aplikace využívající webové rozhraní nebo tlustého klienta, např.: *SUR, AK, OIM, dohledové systémy, zálohovací systémy, SIEM, ServiceDesk* Některé z těchto aplikací využívají jako úložiště uživatelů LDAP/AD, proto správa hesel k účtům spadá pod správu hesel k LDAP/AD.	**Tlustý klient/web**	**30**
12.	Aplikace/skripty využívající aplikačního rozhraní na získání hesla k účtu prostřednictvím PIM	**Java** **.NET** **Unix/Linux shell script** **Windows batch**	**5**

Tabulka 2 - typy a počty EP

Předpokladem je začlenit produkční prostředí systémů. O integraci testovacích prostředí bude rozhodnuto v rámci interního procesu, v kterém se budou vyhodnocovat převážně kritéria:

- Umožňuje testovací prostředí přístup k ostrým/produkčním datům?
- Jedná se o kritický/významný systém?
- Je uživatelský interface testovacího prostředí publikován do intranetu/internetu?

Z důvodu urychlení nasazení je doporučeno v rámci implementace integrovat pouze část zmíněných systémů/aplikací, další integrace proběhnout následně vlastními silami MZe proškoleným personálem.

5.5.2 Počet uživatelů

Odhadovaný počet uživatelů využívající PIM pro přístup k systémům je následující:

- Celkový počet uživatelů: **260**;
- Maximální počet současně přistupujících uživatelů: **70**;
- Průměrný počet přistupujících uživatelů za den: **70**;
- Průměrná délka uživatelské relace za den: **5 hodin**;

5.5.3 Archivace nahrávek

Nahrávky Session Recordingu je požadováno uchovávat na **5 let** na bezpečném úložišti. Z tohoto úložiště nemusí být nahrávky nutně okamžitě dostupné, je možné využít tzv. cold archive, tedy archivu, ze kterého je nutné před jejich prohlížením nejprve nahrávky přenést na určené místo (vyvolat). Nahrávky, které nejsou starší než **8 měsíců** by měli být dostupné bez nutnosti jejich vyvolávání.

Pro výpočet velikosti úložiště lze použít údaje z odstavce 5.5.2 Počet uživatelů.

5.5.4 Terminálové servery

Pokud řešení bude vyžadovat farmu Windows Terminálových serverů (pro Session Recording), předpokládá se, že bude vystavěna na novém HW, který je poptáván v rámci jiné zakázky na dodávku HW pro securitní řešení. Windows Terminal servery (OS, HW, CAL) **nebudou** požadovány jako součást dodávky.

Síťová pravidla budou nastavena tak, aby z terminálových serverů byly dostupné pouze prvky, ke kterým má být jednotlivému uživateli (skupině) umožněn přístup – více v odstavci 5.5.6 Řízení přístupu k EP.

5.5.5 Prostředí

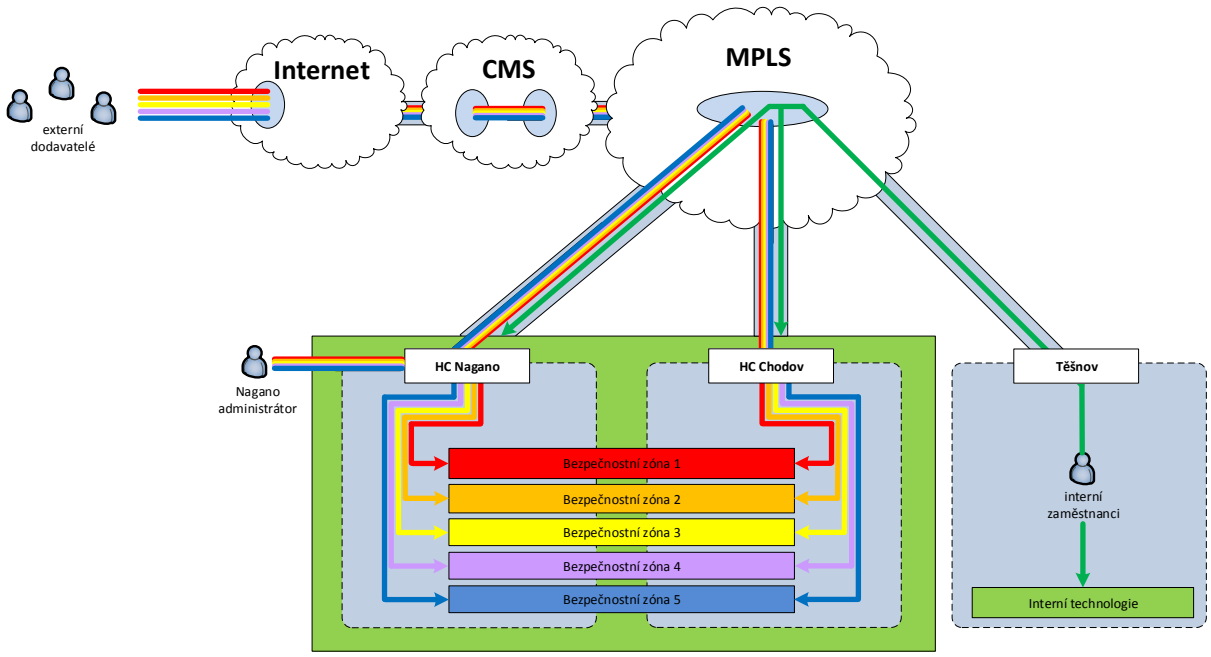
V rámci dodávky je požadována instalace dvou prostředí PIM:

- **Produkční**
- **Vývojové/Testovací**

Vývoj./test. prostředí bude sloužit k testování patchů a nových verzí systému dodaných výrobcem. Zároveň na něm bude probíhat vývoj dalších funkcionalit v rámci rozšiřování systému (konektory, skripty pro automatizované přihlašování, schvalovací WF, integrace, atp.).

Všechny změny v rámci PIM řešení, zejména upgrade, bezpečnostní záplaty, nové funkcionality a další nové verze PIM řešení nebo jeho částí, musí být řádně otestovány Dodavatelem případně výrobcem ještě před nasazením do produkčního prostředí Objednatele. Tato povinnost se vztahuje na již otestované a předané produkční prostředí. V rámci Implementace se prostředí až do jeho akceptace považuje za testovací.

5.5.6 Řízení přístupu k EP



Obrázek 2 - schéma přístupů k EP

Infrastruktura MZe se skládá ze dvou geograficky oddělených datových center, která jsou hostována v HC Nagano a HC Chodov a vlastní infrastruktury v lokalitě Těšnov. Tyto tři lokality jsou připojeny do společné MPLS sítě, která je přes CMS připojena do Internetu. V datových centrech v Naganu a

Chodově jsou umístěny EP, které jsou spravovány externími dodavateli ze sítě Internet nebo lokálně v rámci hostingového centra. Zároveň k těmto EP přistupují i interní pracovníci z lokality Těšnov.

Komunikační schéma na obrázku znázorňuje požadovaný cílový stav, který musí být řešením PIM zajištěn. Řešení PIM musí umožňovat řídit a monitorovat přístup:

- externích dodavatelů přistupujících z Internetu k EP hostovaným v HC Nagano a HC Chodov;
- administrátorů připojených v rámci HC Nagano a přistupujících k EP v HC Nagano a HC Chodov;
- interních zaměstnanců MZe přistupujících ze sítě v lokalitě Těšnov k EP hostovaným v HC Nagano a HC Chodov a technologiím provozovaných v lokalitě Těšnov;

Jednotlivé EP v datových centrech Nagano a Chodov přísluší do jedné z pěti bezpečnostních úrovní označených jako „Bezpečnostní zóna 1-5“. Řešení PIM musí externím dodavatelům a administrátorům připojeným v HC Nagano umožňovat přístup pouze a jen k EP umístěných v Bezpečnostních zónách, do kterých má přihlášený uživatel oprávnění. K EP umístěným v Bezpečnostních zónách, ke kterým přihlášený uživatel oprávnění nemá, nesmí PIM řešení umožňovat žádný přístup a tyto EP pro takového uživatele nesmí být nijak dostupné. Pro interní uživatele musí PIM řešení umožnovat řídit přístup k jednotlivým EP v datových centrech a lokalitě Těšnov, od PIM řešení však již není vyžadována komunikační nedostupnost EP, pro který přihlášený uživatel nemá oprávnění. Všechny relace externích dodavatelů, administrátorů v HC Nagano a interních uživatelů řízené pomocí PIM řešení musí být nahrávány.

Jelikož je zajištění přístupu k EP v datových centrech kritické pro zajištění funkčnosti služeb poskytovaných MZe, je nutné, aby řešení PIM splňovalo jak výkonnostní požadavky, tak i požadavek na vysokou dostupnost a to jak pro externí dodavatele (řádově desítky přistupujících uživatelů), Nagano administrátory (jednotky přistupujících uživatelů), tak i interní uživatele (jednoty přistupujících uživatelů).

6 PŘEHLED POŽADAVKŮ

Objednatel v rámci výběrového řízení požaduje zajištění kompletní dodávky řešení PIM, které vyhovuje požadavkům uvedeným v této Technické specifikaci.

6.1 Funkční požadavky

V jednotlivých níže uvedených tabulkách Přehledu funkčních požadavků jsou uvedeny požadavky na funkcionalitu řešení PIM. Pokud je v Přehledu funkčních požadavků některý požadavek označen jako povinný, nebude řešení, které takovému požadavku nevyhovuje, akceptováno a nabídka takové uchazeče bude vyřazena. Ostatní funkční požadavky uvedené v tabulce Přehled funkčních požadavků jsou volitelné a budou předmětem hodnocení.

Bude-li uchazečem předkládaný Návrh technického řešení splňovat konkrétní volitelný funkční požadavek, bude mu přiděleno bodové hodnocení stanovené zadavatelem ve vztahu k takovému funkčnímu požadavku. Nebude-li uchazečem předložený Návrh technického řešení příslušný volitelný funkční požadavek splňovat, obdrží uchazeč v jeho rámci 0 bodů.

Ve sloupci „Odkaz do NTŘ“ uvedeném v tabulce Přehled funkčních požadavků uchazeč vyplní stránku a kapitolu předkládaného Návrhu technického řešení, z něhož bude zřejmé, zda jsou naplněny stanovené funkční požadavky. Návrh technického řešení bude popisovat způsob naplnění požadavků, případně bude obsahovat odkaz na příslušnou část dokumentace výrobce, ve které bude konkrétní požadavek popsaný a z popisu bude zřejmé, že nabízené řešení tento požadavek splňuje.

6.1.1 Základní vlastnosti a obecné požadavky

	Popis	Povinné	Váha	Odkaz do NTŘ
A.1.	Všechny komponenty systému (PIM řešení) jsou dostupné v českém nebo anglickém jazyce.	**ANO**	-	**[doplní uchazeč]**
A.2.	Zařízení musí být určené pro český trh (potvrzeno prohlášením výrobce). Prodávající zajistí v souvislosti s poskytováním záručního servisu registraci kupujícího v příslušné databázi výrobce zboží tak, aby byl kupující oprávněn k technické podpoře v České republice přímo ze strany tohoto výrobce či jeho servisních partnerů.	**ANO**	-	**[doplní uchazeč]**
A.3.	Uživatelské rozhraní poskytující základní funkce je přístupné přes webové rozhraní s podporou prohlížeče: • Internet Explorer 10 a novější	**ANO**	-	**[doplní uchazeč]**
A.4.	Systém podporuje instalaci v režimu vysoké dostupnosti.	**ANO**	-	**[doplní uchazeč]**
A.5.	Autentizace uživatelského přístupu ke všem komponentám je řízena adresářem LDAP, nebo Active Directory.	**ANO**	-	**[doplní uchazeč]**
A.6.	Autorizace uživatelského přístupu ke všem	**NE**	**4**	**[doplní uchazeč]**

	komponentám je řízena adresářem LDAP, nebo Active Directory.			
A.7.	K autentizaci je využit stávající SSO provider (Forgerock OpenAM), nebo automatické přihlášení na základě přihlášení k AD doméně (Integrated Windows Authentication)	**NE**	**3**	**[doplní uchazeč]**
A.8.	PIM řešení musí logovat auditní záznamy o všech administrátorských a uživatelských aktivitách. Minimálně se musí logovat následující typy událostí vykonaných v PIM: • úspěšné a neúspěšné (pokus o) přihlášení a odhlášení • konfigurační změny (musí být zřejmé, kdo udělal jakou konfigurační změnu) • check-in/check-out hesla • přístup k nahrané session	**ANO**	**-**	**[doplní uchazeč]**
A.9.	Řešení PIM musí být integrovatelné se SIEM řešením HP ArcSight, které je provozováno v prostředí MZe. Musí tak být možné do SIEM HP ArcSight přenášet logované auditní záznamy, nejlépe v reálném čase, jednou z následujících metod: • Syslog • SNMP TRAP • Textový soubor • JDBC • Microsoft Event Log	**ANO**	**-**	**[doplní uchazeč]**
A.10.	V systému je možné generovat reporty ve formátech PDF, excel, popřípadě dalších. Následující reporty jsou k dispozici: • Seznam uživatelů a jejich oprávnění, včetně výpisu účtů, které mají k dispozici • Seznam všech spravovaných účtů, včetně přiřazených politik hesel a výčtu uživatelů, kteří mají k danému účtu přístup • Seznam aktivit nad účty – check out/in, přidělení účtu, atp.	**ANO**	**-**	**[doplní uchazeč]**
A.11.	Reporty je možné naplánovat k pravidelnému odesílání na email, nebo k ukládání do složky.	**NE**	**3**	**[doplní uchazeč]**
A.12.	Je umožněno vytvářet nové reporty a libovolně je editovat.	**NE**	**3**	**[doplní uchazeč]**
A.13.	Systém umožňuje definovat emailové notifikace na základě vybraných událostí.	**NE**	**2**	**[doplní uchazeč]**
A.14.	Minimální zatížení sdílených prostředků, tedy: • Integrovaných systémů/aplikací (řízené EP) • Síťové infrastruktury (např. při přenosu nahrávek)	**ANO**	**-**	**[doplní uchazeč]**

A.15.	Vzájemná komunikace mezi komponentami PIM řešení (např. replikace konfigurace, databáze, přenos souborů nebo nahrávek uživatelských sezení, synchronizace, apod.) je úsporná z pohledu nároku na kapacitu přenosových cest mezi komponentami řešení PIM	**ANO**	-	**[doplní uchazeč]**
A.16.	Systém využívá kryptografické mechanizmy, které jsou v souladu s mezinárodně uznávaným standardem FIPS 140-2. V případě hardwarových bezpečnostních prvků je podmínkou splnění standardu FIPS 140-2 stupně minimálně 2.	**ANO**	-	**[doplní uchazeč]**
A.17.	Systém umožňuje rozšíření o modul na řízení přístupu (Access Control), tedy omezení oprávnění privilegovaných účtů dle definovaných politik na operačních systémech Unix/Linux a Windows (např. náhrada za sudo).	**ANO**	-	**[doplní uchazeč]**
A.18.	V rámci PIM řešení jsou definovány alespoň tyto následující uživatelské role: a. **Administrátor** – konfiguruje systém nebo jeho část, může vytvářet/upravovat/odstraňovat objekty systému (kromě odstraňování auditních informací a nahrávek). b. **Auditor** – má přístup k auditním informacím a nahrávkám. c. **Uživatel** – je mu umožněn přístup k systému PIM a jeho běžné používání.	**ANO**	-	**[doplní uchazeč]**
A.19.	Přístup k řízeným EP je uživatelům umožněn pouze v rámci zóny, v které daný EP náleží. Přístup k ostatním zónám, není uživateli prostřednictvím PIM řešení vůbec umožněn. (např. přístup prostřednictvím RDP a několika Windows Terminálů, kde každý je v jiném síťovém segmentu) Členství EP v zónách definuje Zadavatel.	**ANO**	-	**[doplní uchazeč]**

Tabulka 3 - Základní funkční požadavky

6.1.2 Session Recording

	Popis	Povinné	Váha	Odkaz do NTŘ
B.1.	Systém podporuje záznam videa s aktivitou účtu s jednoznačnou vazbou na osobu, které ji vykonává.	**ANO**	-	**[doplní uchazeč]**
B.2.	V rámci nahrávky jsou zaznamenávány uživatelské vstupy (key-logging) a výstupy na obrazovku.	**ANO**	-	**[doplní uchazeč]**
B.3.	V rámci nahrávky jsou ukládány následující strukturovaná metadata: • Stisknuté klávesy	**ANO**	-	**[doplní uchazeč]**

	• Názvy oken spuštěných aplikací V obsahu metadat je možné vyhledávat dle zadaného řetězce.			
B.4.	V rámci nahrávky jsou ukládány následující strukturovaná metadata: • Výstupy na obrazovku V obsahu metadat je možné vyhledávat dle zadaného řetězce.	**NE**	**3**	**[doplní uchazeč]**
B.5.	Nahrávky jsou zabezpečeně přenášeny do centrálního repository. Po celou dobu jejich existence je zaručen pouze autorizovaný přístup.	**ANO**	**-**	**[doplní uchazeč]**
B.6.	Přístup k nahrávkám je řízen členstvím uživatele ve skupině/roli.	**NE**	**3**	**[doplní uchazeč]**
B.7.	Uživatelé jsou upozorněni na skutečnost, že jejich aktivita je nahrávána.	**ANO**	**-**	**[doplní uchazeč]**
B.8.	Nahrávky je možné exportovat do samostatného souboru, který lze přehrát bez nutnosti připojení (offline).	**ANO**	**-**	**[doplní uchazeč]**
B.9.	Pro přístup k nahrávkám je možné vynutit metodu čtyř očí, tedy nutnost autorizace přístupu k nahrávce další osobou.	**NE**	**1**	**[doplní uchazeč]**
B.10.	Systém podporuje integraci se Service Deskem – HP Service Manager • Přístup k nahrávce je povolen až na základě existence schváleného servisního ticketu.	**NE**	**1**	**[doplní uchazeč]**
B.11.	Systém podporuje integraci se Service Deskem – HP Service Manager • Před samotnou inicializací nahrávaného spojení je vynuceno zadání čísla schváleného servisního ticketu. Číslo servisního ticketu je dostupné v rámci metadat uložených k nahrávce	**NE**	**4**	**[doplní uchazeč]**
B.12.	Systém umožňuje vynutit udání důvodu přístupu k EP před zahájením nahrávaného spojení. Text důvodu je dostupný v rámci metadat uložených k nahrávce. Forma zadání důvodu je: • Volné textové pole	**NE**	**4**	**[doplní uchazeč]**
B.13.	Systém umožňuje vynutit udání důvodu přístupu k EP před zahájením nahrávaného spojení. Text důvodu je dostupný v rámci metadat uložených k nahrávce. Forma zadání důvodu je: • Volba položky číselníku	**NE**	**4**	**[doplní uchazeč]**
B.14.	Systém zaručuje, že není možné nahrávky jednoduše odstranit ani upravit, aby nemohla být zpochybněna jejich průkaznost.	**ANO**	**-**	**[doplní uchazeč]**
B.15.	Repository s nahrávkami je možné pravidelně	**ANO**	**-**	**[doplní uchazeč]**

	zálohovat tak, aby byla zaručena jeho dostupnost. Zálohy jsou dostatečně zabezpečeny proti neoprávněnému přístupu (např. jsou zašifrovány).			
B.16.	Nahrávky jsou efektivním způsobem zaznamenávány a přenášeny (komprimace, zaznamenávání pouze aktivní relace), aby nedocházelo ke zbytečnému zatěžování prostředků (úložiště, síť).	**ANO**	**-**	**[doplní uchazeč]**
B.17.	Relace je možné sledovat v živém režimu, pokud právě probíhají. Relaci je možné během sledování kdykoliv přerušit.	**NE**	**4**	**[doplní uchazeč]**
B.18.	Je podporováno nahrávání SSH a RDP relace.	**ANO**	**-**	**[doplní uchazeč]**
B.19.	Je podporováno nahrávání Citrix session (protokol ICA).	**NE**	**5**	**[doplní uchazeč]**
B.20.	Je podporováno nahrávání následujících protokolů/relací: • Telnet • VNC • HTTP • HTTPS • Xserver • VMware hypervizor • MSSQL DB • Oracle DB	**NE**	**5**	**[doplní uchazeč]**
B.21.	Řešení PIM nemá zaznamenatelný vliv na odezvy činností realizovaných v rámci probíhající uživatelské relace.	**ANO**	**-**	**[doplní uchazeč]**

Tabulka 4 - Požadavky na Session Recording

6.1.3 Password Management

	Popis	Povinné	Váha	Odkaz do NTŘ
C.1.	Repository privilegovaných uživatelů s hesly je šifrována a dostatečně chráněna před všemi hrozbami, které by ji mohly kompromitovat nebo poškodit.	**ANO**	**-**	**[doplní uchazeč]**
C.2.	Repository privilegovaných uživatelů s hesly je možné pravidelně zálohovat tak, aby byla zaručena jeho dostupnost. Zálohy jsou dostatečně zabezpečeny proti neoprávněnému přístupu (např. jsou zašifrovány).	**ANO**	**-**	**[doplní uchazeč]**
C.3.	Existuje mechanismus zajišťující bezpečný přístup k heslům uložených v systému i v případě jeho částečné nebo úplné nedostupnosti.	**ANO**	**-**	**[doplní uchazeč]**
C.4.	Systém umožňuje vzdáleně měnit hesla k účtům na řízeném EP. Změna hesla bude poskytnuta v rámci následujících akcí na řízeném účtu:	**ANO**	**-**	**[doplní uchazeč]**

	• Reset hesla • „Check-out“ hesla (změna hesla a následné poskytnutí hesla uživateli spolu s označením účtu jako používaného daným uživatelem) • „Check-in“ hesla (změna hesla a odznačení účtu)			
C.5.	Systém podporuje funkci vzdálené změny hesla na následujících typech EP: • Microsoft Windows Server 2012 • Microsoft Windows Server 2008 R2 • Red Hat Enterprise Linux 6 (64-bit) • HP-UX 11i v3 • Oracle RAC database 11g • Microsoft SQL Server 2008 R2 SP1 • Microsoft ActiveDirectory	**ANO**	**-**	**[doplní uchazeč]**
C.6.	Systém umožňuje evidovat hesla k účtům neřízených EP. Změna hesel u těchto účtů je prováděna manuálně.	**ANO**	**-**	**[doplní uchazeč]**
C.7.	Systém umožňuje označit řízené účty jako exkluzivní. Takové účty může v jednu chvíli používat (prostřednictvím funkce check-out/in a SSO) maximálně jeden uživatel.	**ANO**	**-**	**[doplní uchazeč]**
C.8.	Řešení PIM je schopné spravovat EP přes přenosové cesty se sníženou propustností (WAN, DSL, apod.)	**ANO**	**-**	**[doplní uchazeč]**
C.9.	Systém umožňuje definovat různé politiky hesel definující: • Složitost hesla (délka, sady znaků) • Stáří hesla • Opakovatelnost hesla Politiky je možné přiřazovat účtům jednotlivě nebo skupinově. Politiky jsou vynucovány během generování nových hesel, nebo při ručních změnách hesel z PIM systému.	**ANO**	**-**	**[doplní uchazeč]**
C.10.	Systém automaticky provede změnu hesla na EP, pokud vypršela jeho platnost dle stáří, které je definované v přiřazené politice.	**NE**	**2**	**[doplní uchazeč]**
C.11.	Systém v pravidelném intervalu kontroluje, zda heslo na EP odpovídá tomu evidovanému v PIM systému. V případě rozdílu je odeslána notifikace.	**NE**	**4**	**[doplní uchazeč]**
C.12.	Přístup k účtům a jejich heslům je definován buď na úrovni účtu, nebo skupiny účtů.	**ANO**	**-**	**[doplní uchazeč]**

C.13.	Uživatel má k dispozici účty buď na přímé použití, nebo je má k dispozici na podání žádosti. Žádost o přístup k účtu musí schválit jiný uživatel nebo skupina uživatelů. Schvalovatel je jasně definován v kontextu konkrétního účtu nebo skupiny účtů.	**ANO**	**-**	**[doplní uchazeč]**
C.14.	Uživateli je umožněno požádat o přístup k účtu jen na omezenou dobu (interval od-do).	**ANO**	**-**	**[doplní uchazeč]**
C.15.	Je navržen a implementován proces pro nouzový přístup k účtu bez potřebného schválení. Při spuštění takového procesu je současně vytvořen záznam o této události a je odeslána notifikace na určenou kontaktní osobu/osoby.	**NE**	**5**	**[doplní uchazeč]**
C.16.	Systém poskytuje, prostřednictvím API, bezpečný přístup k heslům privilegovaných účtů pro aplikace/skripty na základě nastavených oprávnění (pro eliminaci otevřených hesel v kódech a konfiguračních souborech). S API je možné komunikovat z následujících programovacích jazyků: • Java • .NET • Unix/Linux shell script • Windows batch	**ANO**	**-**	**[doplní uchazeč]**
C.17.	Řešení PIM musí podporovat použití spravovaného hesla účtu pro plánovanou úlohu (Scheduled Task) v OS Windows.	**ANO**	**-**	**[doplní uchazeč]**
C.18.	Systém podporuje proces pro automatické discovery neřízených účtu na EP. Takové účty jsou v rámci navrženého procesu zařazeny do systému řízení PIM, nebo označeny jako výjimky, na které není již dále upozorňováno. Výsledek discovery je zaznamenán a je dostupný v podobě reportu, který může být naplánován k automatickému odesílání emailem.	**NE**	**5**	**[doplní uchazeč]**
C.19.	Systém podporuje SSO pro privilegované účty, tedy možnost se automaticky přihlásit ke koncovému systému prostřednictvím privilegovaného účtu bez nutnosti zadávání hesla. Podporovány jsou minimálně následující aplikace/protokoly: • Windows RDP • SSH (např. PuTTY)	**ANO**	**-**	**[doplní uchazeč]**
C.20.	Další podporované aplikace/protokoly pro SSO jsou: • HTTP(s)/Web aplikace • Libovolná „tlustá“ klientská aplikace	**NE**	**5**	**[doplní uchazeč]**
C.21.	Během SSO je heslo automaticky zadáno na	**NE**	**5**	**[doplní uchazeč]**

	pozadí bez možnosti jeho odhalení.			

Tabulka 5 - Požadavky na Password Management

6.2 Analýza

Dodavatel v rámci dodávky provede nejprve analýzu nezbytnou pro instalaci a konfiguraci komponent PIM řešení, integraci všech typů EP (viz. 5.5.1 Integrované systémy/aplikace) a připraví technický popis řešení, instalační postup, detailní časový harmonogram a definuje nároky na součinnost. Na základě požadavků na PIM řešení Dodavatel připraví návrh testovacích scénářů, pokrývajících testování všech funkčních rysů implementovaného řešení, včetně testování vybraných výkonových parametrů a výpadků jednotlivých komponent. Dále Dodavatel připraví návrh integrace PIM řešení do provozního a bezpečnostního (SIEM) monitoring systému Objednatele.

Všechny požadované výstupy z etapy Analýza budou Objednateli předloženy k odsouhlasení. Objednatel prostuduje předložené výstupy a bez zbytečného odkladu posoudí, zda navrhované řešení splňuje všechny požadované vlastnosti dané touto Technickou specifikací. Pokud Objednatel shledá nesoulad nebo nejasnosti navrhovaného řešení oproti této Technické specifikaci, požádá Dodavatele o nápravu. Teprve po akceptaci bez výhrad všech požadovaných výstupů Objednatelem je etapa Analýza považována za ukončenou a Dodavatel tak může pokračovat v realizaci dodávky následnou etapou Instalace v souladu s odsouhlasenými výstupy z etapy Analýza. Akceptační řízení bude probíhat dle parametrů uvedených v čl. 4 Smlouvy, nedohodnou-li se smluvní strany jinak.

6.3 Instalace

Instalace řešení PIM bude provedena do vyhrazené bezpečnostní infrastruktury Objednatele, která je založena na virtuální platformě VMware a je distribuována přes obě datová centra (geocluster DC Nagano a DC Chodov) a lokalitu Těšnov. V případě nemožnosti instalace do virtuálního prostředí, zajistí Dodavatel fyzické umístění a instalaci všech HW komponent řešení do místa určení v prostředí Objednatele jako součást dodávky PIM řešení. SW prostředky dodané v rámci řešení PIM budou instalovány v poslední verzi dostupné v době plnění. Dodavatel dále zajistí nasazení a aktivaci všech licencí a licenčních klíčů. Architektura instalovaného PIM řešení, včetně identifikace komponent, přehledu instalovaných verzí a použitých licencí a licenčních klíčů bude součástí instalační dokumentace.

6.4 Implementace

V rámci fáze implementace bude Dodavatelem zajištěna konfigurace PIM řešení tak, aby řešení vyhovovalo požadavkům uvedeným v Technické specifikaci.

Jako součást dodávky bude provedeno:

- Konfigurace komponent PIM řešení;
- Navržení a nasazení mechanizmu vynucování a kontroly přístupu k EP výhradně přes nahrávaný kanál;
- Integrace následujících EP:

Název systému	Počet	Přístup/Aplikace

1.	Red Hat Enterprise Linux 6 (64-bit)	1	SSH
2.	HP-UX 11i v3	1	SSH
3.	Microsoft Windows Server 2012 (64-bit)	1	WMI/RDP
4.	Microsoft Windows Server 2008 R2 (64-bit)	1	WMI/RDP
5.	Firewall Fortinet FortiGate	1	SSH/Web
6.	Switch HP 7500 (SSH)	1	SSH
7.	Switch Cisco Catalyst 4500 (Telnet)	1	Telnet
8.	Oracle RAC database 11g (11.2.0.3)	1	SQL
9.	Microsoft SQL Server 2008 R2 SP1	1	SQL
10.	Microsoft ActiveDirectory	1	RDP/LDAP(s)
11.	LDAP (Oracle Internet Directory)	1	LDAP(s)
12.	VMWare ESXi 5.1.0	1	vSphere
13.	Webová aplikace – vyplyne z analýzy	2	Web
14.	SAP – vyplyne z analýzy	1	Web/SAP klient
15.	Aplikace/systémy podporované PIM řešením, které vyplynou z analýzy	2	

Tabulka 6 - Seznam EP k integraci v rámci implementace

- Vytvoření politik v souladu s bezpečnostní politikou Objednatele;
- Vytvoření schvalovacího procesu pro žádost o privilegovaný přístup;
- Vytvoření procesu pro nouzový přístup k EP v případě celkového nebo částečného výpadku PIM řešení;
- Integraci PIM řešení do provozního a bezpečnostního monitoringu provede Objednatel za součinnosti Dodavatele;
- Nastavení zálohování konfigurace a dat PIM řešení;
- Provedení vlastních funkčních testů;

6.5 Akceptační testy

V rámci analytické fáze budou Dodavatelem navrhnuty testovací scénáře, které budou pokrývat následující oblasti a parametry řešení:

- Funkční testy

Funkční testy ověří, že implementované PIM řešení poskytuje bezchybně všechny požadované funkcionality uvedené v Technické specifikaci, včetně řádně integrace se systémy Objednatele (SIEM, SSO, apod.).

- Zátěžové testy

Jejich úkolem je ověřit, že implementované komponenty jsou schopny obsloužit požadovaný maximální počet současně přistupujících uživatelů bez výrazného dopadu na kvalitu a odezvu řešení.

- Bezpečnostní testy

Úlohou bezpečnostních testů je ověřit, že jsou všechny komponenty zabezpečeny dle požadavků definovaných v Technické specifikaci, např. je zabezpečený přístup k úložišti účtů a hesel, přístup

k nahrávkám mají pouze autorizované osoby a jejich přístup je logován, zálohy konfigurace a dat jsou řádně zabezpečeny, uživatelé mají přístup pouze do přidělených bezpečnostních segmentů, apod.

- Testy zajištění kontinuity (DRP testy)

Úlohou testů je ověřit dostupnost PIM řešení v případě výpadku jednotlivých funkčních komponent a ověřit funkčnost nouzového přístupu na EP a k databázi hesel v případě nedostupnosti PIM řešení.

Testování bude provedeno Objednatelem za součinnosti Dodavatele. Dodavatel k realizaci testů zajistí:

- Nástroje a komponenty potřebné pro testování;
- Přípravu návrhu testování a hodnotících kritérií;
- Přípravu testovacích scénářů;
- Přípravu prostředí a testovacích dat (v součinnosti s Objednatelem);
- Testovací protokoly s výstupy testů;
- Seznam defektů a způsob a harmonogram jejich odstranění;

Akceptační testy jsou ukončeny nahlášením výsledku a předáním seznamu nalezených vad. Po odstranění podstatných vad budou akceptační testy celé opakovány a ověří tak kvalitu předávaného PIM řešení. U ostatních vad se provedou akceptační testy s ohledem na ověření řešení pouze příslušné vady.

Podstatné vady jsou vady, které způsobují tak závažné problémy, že Objednatel nemůže produkt nebo jeho klíčovou část používat či ovládat.

6.6 Dokumentace

Dokumentace dodaná v rámci řešení bude obsahovat jak originální dokumentaci dodávanou výrobcem PIM řešení, tak i dokumenty popisující nasazení PIM řešení v prostředí Objednatele.

Oficiální dokumentace výrobce produktu k PIM řešení bude předána v elektronické podobě (formát PDF nebo MS Word) a bude provedena v českém, nebo anglickém jazyce. Dokumentace od výrobce musí pokrývat minimálně následující oblasti:

- popis architektury;
- instalace řešení;
- administrace řešení;
- uživatelská příručka;

Dokumentace popisující nasazení PIM řešení v prostředí Objednatele musí být předána v elektronické podobě ve formátu MS Word a bude provedena v českém jazyce. Minimální požadavky na rozsah a obsah dodávané dokumentace je následující:

- Instalační dokumentace
    - Popis architektury;
    - Komunikační matice komponent;
    - Instalované verze;
    - Licence;

  - Instalační postup;
- Implementační dokumentace
  - Popis nastavení komponent PIM řešení;
  - Popis způsobu integrace (jednotlivých typů EP, AD, LDAP);
  - Popis konfigurace zálohování PIM řešení;
- Uživatelská příručka
  - Popis uživatelského rozhraní PIM řešení z pohledu uživatele;
  - Popis uživatelských postupů při práci PIM řešením;
- Administrátorská příručka
  - Popis uživatelského rozhraní PIM řešení z pohledu administrátora;
  - Popis základních úkonů nutných pro údržbu PIM řešení a standardní profylaktické testy;
- Zajištění kontinuity provozu
  - Popis postupu obnovy ze zálohy;
  - Doporučení pro archivaci (nahrané uživatelské relace a související data);
  - Popis postupu v případě havárie jednotlivých komponent včetně postupu obnovy do provozního stavu;
  - Popis postupu nouzového přístupu k EP v případě nedostupnosti/omezené funkčnosti PIM řešení;

6.7 Školení

Dodavatel zajistí proškolení minimálně 3 osob Objednatele na úrovni administrace řešení v rozsahu umožňujícím provádět:

- Běžný rutinní provoz a údržbu dodávaného PIM řešení, včetně provedení příslušných konfiguračních změn;
- Řešení obvyklých problémů;
- Správu uživatelských oprávnění;
- Integraci EP;
- Analýzu zaznamenaných uživatelských relací;
- Monitoring stavu zařízení;
- Zálohování a obnovu konfigurace a dat;
- Tvorbu pohledů a reportů;

6.8 Podpora

Dodavatel ručí za to, že PIM řešení bude funkční a použitelné v prostředí Objednatele a bude odpovídat požadavkům Objednatele uvedených v Technické specifikaci a vlastnostem deklarovaným v dokumentaci dodané Dodavatelem. Služby poskytované Dodavatelem musí vyhovovat technickým specifikacím a požadavkům výrobce.

Podpora PIM řešení zahrnuje:

- Odstraňování vad programových prostředků PIM řešení;
- V případě dodání HW odstranění vad technických prostředků;

- Poskytování aktualizací programových prostředků (nové verze, opravné verze, bezpečnostní záplaty, apod.);
- Pomoc při řešení provozních problémů;
- Podpora při implementaci aktualizací programových prostředků;

Podpora bude poskytována dle parametrů definovaných ve Specifikaci katalogových listů viz Příloha č.2 Smlouvy a bude probíhat v českém jazyce, nedohodnou-li se pověřené osoby smluvních stran v konkrétním případě jinak.

Odstraňování vad technických prostředků bude Dodavatelem prováděno výměnným způsobem na místě s tím, že náhradní díl nebo zařízení musí být nové a bezvadné a musí být doručeny do místa provádění opravy.

6.9 Platformy

Pokud to bude PIM řešením podporováno, bude instalováno do virtuální VMware infrastruktury Objednatele. Součástí nabídky tak musí být:

- specifikace počtu požadovaných virtuálních serverů a jejich parametrů s ohledem na dostatečnou výkonnost řešení a současnou adekvátnost parametrů;
- požadavek na geografické umístění virtuálních serverů v rámci infrastruktury Objednatele s ohledem na zajištění dostupnosti a rozložení předpokládaných uživatelských relací (viz 5.5.6 Řízení přístupu k EP);
- specifikace požadavků na parametry komunikačních tras a síťových prostupů mezi jednotlivými komponentami řešení PIM;

Pokud není možné řešení PIM či jeho komponentu/komponenty provozovat ve virtuálním prostředí, budou součástí nabídky i HW prostředky, které však musí být vybaveny přípojkami pro minimálně dva nezávislé přívody napájení a předozadní větrání.

Veškeré dodané komponenty (SW, HW) budou instalovány v konfiguraci podporované výrobcem/výrobci, v konfiguraci zaručující vzájemnou kompatibilitu všech komponent a dostatečně výkonnostně nadimenzované s ohledem na parametry požadované od PIM řešení.

Řešení PIM musí být v souladu s interní směrnici Objednatele „Definice závazné architektury a požadavků pro vývoj a zabezpečení provozu registrů a klíčových aplikací MZe“ (interní směrnice není přílohou zadání, bude Dodavateli k dispozici v rámci projektu - výňatek s přehledem preferovaných technologií je uveden níže).

Důvodem tohoto požadavku je zajištění kompatibility se stávající infrastrukturou Zadavatele a zároveň možnost využití stávajících mechanizmů (HW/SW nástroje, personál, servisní smlouvy) pro správu a monitoring dodaných komponent řešení a jednotného přístupu, bez potřeby dalších investic na straně Zadavatele.

Výjimku tvoří řešení, které budou dodány ve formě tzv. „appliance“, tedy řešení, kdy již samotným výrobce nabízí a dodává PIM řešení či některou z jeho komponent jako společný celek softwarových a hardwarového prostředku.

Níže je vykopírován přehled platforem ze zmíněné směrnice:

- Síťové technologie
  - WAN, LAN, HW balancery – technologie Cisco, HP, F5;
  - Firewally, SSL akcelerátory – technologie Cisco, Citrix, HP, F5;
  - SAN prvky – technologie Cisco, HP, Brocade;
- Databázové systémy
  - RedHat Linux Enterprise rel. 6 a vyšší + Oracle 11g rel. 2 a vyšší;
  - Microsoft SQL server verze 2008 a vyšší (pouze pro technologické platformy neumožňující využití Oracle DB);
- Serverové operační systémy
  - Windows server 2012 R2 a vyšší;
  - Red Hat Enterprise Linux AS release 6 a vyšší (64 bit);
- Technologie pro poštovní služby a autentizaci
  - Aplikační autentizace – LDAP Oracle Internet Directory 10g rel. 2 a vyšší;
  - Poštovní služby – MS Exchange 2013 nebo vyšší;
  - Doménová autentizace a autentizace desktopových aplikací Microsoft v prostředí MZe – MS Active Directory;
- Virtualizační technologie
  - VMware ESX 5.0 a vyšší;
- Aplikační servery
  - Oracle WebLogic Server 11g rel. 1 a vyšší (64 bit) – má vlastní webserver;
  - Microsoft .NET (dot NET) – produkty v rámci MS Internet Information Server 7.0;
  - JBoss – IIS 7.0 a vyšší (win) nebo Apache (linux);
- Prezentační vrstva
  - Microsoft Internet Explorer verze 10.0 a vyšší.

V případě, že zadávací podmínky této Veřejné zakázky obsahují požadavky nebo odkazy na obchodní firmy, názvy nebo jména a příjmení, specifická označení zboží a služeb, které platí pro určitou osobu, popřípadě její organizační složku za příznačné, nebo patenty, ochranné známky nebo označení původu, umožňuje Zadavatel výslovně pro plnění Veřejné zakázky použití i jiných, kvalitativně a technicky obdobných řešení, která naplní Zadavatelem požadovanou funkcionalitu (byť jiným způsobem).