# 1 Implementace správy privilegovaných účtů a auditního přístupu třetích stran (dodavatelů a administrátorů)

V rámci prostředí Krajského úřadu Pardubického kraje (dále jen „KÚPK“) je provozováno velké množství informačních a komunikačních systémů, které jsou tvořeny rozlehlou síťovou infrastrukturou. Jednotlivé informační a komunikační systémy v sobě obsahují privilegované účty, které jsou využívány pro jejich správu, nebo se jedná o servisní účty aplikací nebo systémových služeb. Privilegované účty existují na všech vrstvách ICT – od operačních systémů, databází, komunikačních a bezpečnostních prvků až po uživatelské aplikace. Privilegované účty jsou využívány administrátory, kteří se podílejí na provozu a rozvoji informačních systémů a technologií. Jedná se jak o interní zaměstnance, tak o externí dodavatele. Privilegované účty představují významné bezpečnostní riziko pro každou organizaci, protože:

* umožňují téměř neomezený přístup a manipulaci s informačními aktivy organizace. V případě kompromitace privilegovaného účtu je organizace vystavena velkému riziku neautorizovaného zneužití nebo vyzrazení kritických informačních aktiv,
* privilegované účty jsou v praxi často sdíleny mezi více administrátory, proto je obtížné určit odpovědnost za případné zneužití ze strany interního zaměstnance,
* hesla u privilegovaných účtů administrátorů a servisních účtů služeb a aplikací nejsou obvykle pravidelně měněna a často na ně není aplikována bezpečná politika hesel,
* je obtížné v reálném čase monitorovat nebo aktivně zasahovat do probíhajících relací u privilegovaných účtů v případě podezření na zneužití oprávnění.

Z tohoto důvodu KUPK poptává nástroj pro řízení a správu privilegovaných účtů – tzv. „Privileged Identity Management“ a „Privileged Access Management“ (dále jen „PIM/PAM“), který zajistí jednotnou správu přístupu k privilegovaným účtům a monitorování operací prováděných pod účty s vyšším oprávněním než user/domain user, s vazbou na konkrétního administrátora, který v danou chvíli účet používá. Požadavek řídit privilegované účty vychází rovněž ze zákona č. 181/2014 Sb., zákon o kybernetické bezpečnosti a z normy ISO/IEC 27001.

## Specifikace dílčí dodávky

Pro dodávku PIM/PAM řešení je požadováno, aby se skládala z minimálně následujících fází:

* Analýza,
* Obecné (základní) školení
* Instalace,
* Implementace,
* Testování,
* Dokumentace,
* Zaškolení.

### Analýza

Zhotovitel provede v rámci **opatření 0 (GAP analýza + architektura implementace opatření v rámci výzvy 10)** analýzu prostředí KUPK, koncových zařízení a externích systémů, které se budou do PIM/PAM integrovat a to jak současných, tak budoucí ostatní předměty projektu. Zhotovitel připraví harmonogram projektu, požadavky na zajištění součinnosti, technický popis řešení, testovací scénáře a instalační postup. Dále Zhotovitel připraví návrh integrace PIM/PAM řešení do provozního a bezpečnostního monitoringu stávajícího i nového ze stejného projektu.

### Instalace

* Zhotovitel dopraví dodávku do prostředí KUPK. Veškeré náklady související s dopravou a instalací jdou na vrub Zhotovitele.
* Instalace PIM/PAM bude provedena do vyhrazené infrastruktury Zadavatele.
* Za součást instalace je považována také konfigurace a zprovoznění dodávky v plném rozsahu, včetně součinnosti při konfiguraci sítě a bezpečnostního monitoringu. Dále pak otestování požadovaných funkcionalit.
* Technici Zhotovitele splňují veškeré podmínky dané výrobcem PIM/PAM pro jeho instalaci.
* Popis architektury instalovaného PIM/PAM řešení a popis verzí bude součástí dokumentace.

### Implementace

Zhotovitel provede potřebnou konfiguraci PIM/PAM a všech komponent dle této technické specifikace. Implementace bude zahrnovat, zejména:

* nastavení politik pro PIM/PAM,
* nastavení nahrávání privilegovaných relací,
* integrace koncových zařízení, včetně zachování neovlivněného hesla nejvyšší úrovně oprávnění (v obálce do trezoru)
* integrace externích systémů (zejména 2FA, SSO, Service desk, nástroje pro bezpečnostní a provozní monitoring, centrální logování),
* nastavení zálohování, aj.

### Testování

Zhotovitel zajistí řádné otestování řešení PIM/PAM dle navržených testovacích scénářů. Zejména budou provedeny následující testy:

* funkční testy,
* bezpečnostní testy,
* DR testy,
* akceptační testy.

### Dokumentace

Součástí dodávky musí být dokumentace v následujícím rozsahu:

1. Produktová dokumentace ke všem dodávaným modulům PIM/PAM,
2. Popis architektury, instalační a implementační dokumentace a dokumentace k integrovaným systémům v rámci Prováděcí dokumentace
3. Administrátorské a uživatelské příručky, popis konfigurace, instalační procedury, DR řešení,
4. Dokumentace ke všem logům – hlavně popis struktury logů, seznam událostí s jejich významem a vazbou na jednotlivé operace.

Dokumentace uvedená v b) – d) je požadována v českém jazyce. Produktová dokumentace od výrobce je akceptovatelná v anglickém nebo českém jazyce.

Pravidelná aktualizace dokumentace bude prováděna v rámci Služeb servisní podpory a to pravidelně při jakékoliv změně, např. aktualizacích (patchování, upgrade) nabízeného PIM/PAM řešení.

### Školení a zaškolení

* Zajištění školení i zaškolení ICT specialistů proběhne v prostorách KUPK. Konkrétní termíny a místo bude určené KUPK. Školení i zaškolení proběhne v českém jazyce.
* Základní školení pro předem definovaný počet lidí se zaměří na základní seznámení s produktem, jeho instalací, konfigurací a uvedením do provozu. Cílem je porozumění dané technologie objednatelem, srovnání pojmů pro další komunikaci.
* Zaškolení pro architekty a správce tohoto řešení poskytne určeným pracovníkům komplexní informace v takovém rozsahu, aby tito pracovníci dokázali samostatně a dlouhodobě administrovat a provozovat dodané řešení. Součástí zaškolení bude i obnova řešení po havárii.
* Školitel bude disponovat certifikací výrobce dodávané technologie, resp. výrobců všech technologií, ze kterých bude složena dodávka (pokud výrobci takové certifikace vystavují) a bude mít praxi v oboru minimálně 5 let. Certifikát je možno nahradit čestným prohlášením výrobce o způsobilosti daného školitele.
* Školení proběhne před instalací a implementací, součástí zaškolení je i přítomnost při instalaci a implementaci.

Součástí dodávky musí být licence PIM PAM pro uživatele a to v počtu pro 300 uživatelů. Licenčně musí být řešení rozšiřitelné na dvojnásobek bez dalších technických změn.

| *Požadavek na funkcionalitu* | *Minimální požadavky* | *Splněno: ANO / NE / Hodnota* |
| --- | --- | --- |
| Bezpečné úložiště - veškeré informace o účtech, heslech, vlastnících, přístupech a veškeré nahrávky a logy budou uložené v centrálním zabezpečeném úložišti, které musí být chráněné alespoň těmito mechanismy" - Firewall nakonfigurovaný tak, aby se systémem mohly komunikovat pouze autorizované komponenty řešení - Restriktivní konfigurace systému - tzv. hardening - Komunikace s dalšími komponenty, externími systémy, nebo uživateli je šifrovaná použitím algoritmů splňující mezinárodní normu FIPS 140-2 - Silný mechanismus řízení přístupů "ACL" - na úrovni bezpečného úložiště a to až na úroveň jednotlivých objektů - Řízení vzdáleného přístupu - Integrace silné autorizace - Ověřování verzí | ANO |  |
| Vysoká dostupnost - Produkční prostředí je nainstalováno v režimu vysoké dostupnosti. Každá komponenta řešení musí obsahovat minimálně dvě samostatné instance v režimech active/active nebo active/passive. Řízení vysoké dostupnosti musí být plně automatické. Řešení, které vyžaduje manuální zásah je nepřípustné a řešení se nesmí spoléhat na zajištění vysoké dostupnosti pomocí virtualizačních funkcí. Bezpečné úložiště musí být instalovatelné na fyzický - nevirtualizovaný - hardware. Ostatní komponenty řešení musí být nainstalované z bezpečnostních a provozních důvodů na jiném systému, než je bezpečné úložiště. | ANO |  |
| Zálohování - Úložiště privilegovaných účtů a jejich přihlašovacích údajů, a nastavení řešení je možné pravidelně zálohovat, aby byla zaručená jeho dostupnost. Zálohy jsou zabezpečené šifrováním proti neoprávněnému přístupu. Je implementovaný proces zajišťující bezpečný přístup k heslům uloženým v systému v případě částečné, nebo úplné nedostupnosti systému. | ANO |  |
| Uživatelské prostředí poskytující funkce uživatelům je přístupné přes webové rozhraní s plnou podporou následujících prohlížečů v OS Windows, Mac, a Linux: Internet Explorer   * Edge * Chrome * Firefox * Safari | ANO |  |
| Auditní záznamy a logy veškerých aktivit v zabezpečeném úložišti jsou chráněné proti změnám a vymazání všemi uživateli (včetně administrátora řešení) | ANO |  |
| Data a objekty jako hesla, SSH klíče, video nahrávky, logy, definice přístupových oprávnění jsou uložené v zabezpečeném úložišti a zašifrované. Přístup k nim má pouze vlastník a jím určené osoby. Administrátor zabezpečeného úložiště ani jiný nepověřený uživatel, nemá práva přístupu ke čtení, používání, modifikace, nebo smazání. | ANO |  |
| Řešení podporuje integraci s LDAP pro správu uživatelů. Nabízené řešení musí podporovat synchronizaci změn a aktualizovat záznamy. Například uživatel přidaný/odebraný ze správy LDAP - řešení automaticky propaguje/odstraní uživatele ze systému správy. | ANO |  |
| Nabízené řešení podporuje dotazy a řízení přístupu k heslům i pro "vnořené" globální skupiny, podporuje komplexní Active Directory infrastruktury - geografické lokality, sofistikované prohledávání LDAP. | ANO |  |
| Autentizace a autorizace uživatelského přístupu k veškerým komponentám je řízená pomocí LDAP, Radius a Active Directory. | ANO |  |
| Pro autentizaci uživatele je možné využít automatické přihlášení (SSO) na základě přihlášení k doméně AD Integrated Windows Authentication. Řešení také podporuje dvoufaktorovou autentizaci PKI, OTP a LDAPS. | ANO |  |
| V rámci řešení jsou definovatelné minimálně tyto role" a) administrátor řešení - může upgradovat systém, přidávat uživatele a řídit povolené objekty b) auditor - má přístup k auditním informacím a nahrávkám c) uživatel - má umožněný přístup k řešení a jeho běžné užívání | ANO |  |
| Řešení musí logovat auditní záznamy o administrátorských a uživatelských aktivitách. Minimálně musí logovat následující typy událostí vykonaných v rozhraní aplikace: • úspěšné a neúspěšné (pokusy o) přihlášení a odhlášení • konfigurační změny (musí být zřejmé, kdo provedl jakou konfigurační změnu)  • získání hesla  • přístup k nahrané session | ANO |  |
| Řešení podporuje zasílání notifikací pomocí emailu pro definované události a to minimálně při následujících akcích: • Přístup a ukončení práce v systému • Změny v systému • Použití hesla • Požadavek na heslo a schválení požadavku | ANO |  |
| Řešení disponuje vlastními předdefinovanými reporty o aktivitách uživatelů a auditech používání spravovaných přihlašovacích údajů. Podporuje plánování automatického generování těchto reportů: • Oprávnění uživatelů • Veškeré aktivity uživatelů • Přehled privilegovaných účtů  • Přehled spravovaných aplikací • Přehled zadaných/schválených požadavků   * Přehled provedených změn na konkrétním systému * Přehled činností konkrétního uživatele | ANO |  |
| Řešení je možné integrovat s externím ticketovacím systémem a zároveň má integrovaný vlastní interní ticketing systém pro schvalování požadavků na přístup k objektům (privilegované účty, záznamy, logy). | ANO |  |
| Řešení je napojeno na dodávaný centrální logovací systém, který je také součástí tohoto projektua přenáší data v reálném čase a v těchto formátech: • Syslog • SNMP Trap • Textový soubor • JDBC  • CEF nebo LEEF • Microsoft Event Log | ANO |  |
| Řešení PAM umožňuje komplexní centrální evidenci a správu privilegovaných osobních, sdílených, servisních a aplikačních účtů | ANO |  |
| Řešení PAM umožňuje definovat, kterým uživatelům mají být k dispozici jaké privilegované účty, na kterých systémech, jakým způsobem se mají uživatelé k vybraným privilegovaným účtům moci připojit. | ANO |  |
| Uživatel se do systému autentikuje přes webové rozhraní a po přihlášení je uživateli zobrazen seznam jenom těch privilegovaných účtů, ke kterým má přidělený přístup. Veškeré ostatní privilegované účty zůstávají v systému pro uživatele skryté a nedostupné. | ANO |  |
| Řešení umožňuje správu neomezeného počtu privilegovaných účtů na neomezeném počtu zařízení. | ANO |  |
| Řešení PAM se připojuje k spravovaným systémům a umožňuje změnu hesel privilegovaných účtů na koncových systémech bez instalace agenta atp. Připojení probíhá tak, aby minimálně zatěžovalo spravovaný systém a je možné plánovat čas připojení. | ANO |  |
| Řešení PAM umožňuje také evidovat hesla pro nespravované privilegované účty. Změna hesel u takových účtů se provádí manuálně. | ANO |  |
| Řešení PAM podporuje proces pro automatické vyhledávání 'discovery' nespravovaných účtů na cílových systémech. Takovéto účty jsou v rámci navrhovaného procesu zařazeny do systému řízení PAM. Výsledky Discovery jsou zaznamenány a jsou dostupné v přehledném a interaktivním zobrazení. | ANO |  |
| Řešení PAM umožňuje automaticky vyhledávat a přidávat nové privilegované účty do správy PAM. Řešení dle charakteristiky privilegovaného účtu automaticky přiřazuje definovanou bezpečnostní politiku. | ANO |  |
| Vlastnosti hesel - Řešení PAM umožňuje definovat vlastnosti hesel pro jednotlivé privilegované účty, nebo skupiny privilegovaných účtů: • nastavení komplexnosti hesel - počet znaků a podpora různých znakových sad a kombinace znaků • periodicita výměny hesla na cílových systémech • věk hesla • unikátnost hesla v definovaném počtu posledních výměn a pro veškeré spravované privilegované účty, nebo skupiny | ANO |  |
| **Výměny hesel** - Řešení musí poskytovat možnost změny jednoho nebo skupiny hesel:  • Automaticky, když je stáří hesla větší než... • Manuálně uživatelem - pro vybrané účty nebo skupiny účtů • Automaticky, když heslo není synchronizované (heslo v bezpečném úložišti nesouhlasí s heslem na spravovaném systému) | ANO |  |
| Přístup k privilegovaným účtům - Řešení PAM umožňuje definovat vlastnosti přístupů k přihlašovacím údajům pro jednotlivé privilegované účty a pro skupiny privilegovaných účtů: • Přístup bez omezení - uživatel si může heslo zobrazit, zkopírovat a přímo se transparentně připojit k cílovému systému s využitím privilegovaného účtu • Dvojí kontrola - heslo nebo připojení je uživateli poskytnuto až po schválení přístupu schvalovatelem. Pro přístup k heslu se vytvoří žádost, generuje se automaticky emailová notifikace pro schvalovatele, nebo skupině schvalovatelů, kteří musí přístup/y schválit • Exkluzivní přístup: umožňuje využít privilegovaný účet pouze jedinou osobou v jeden čas - ostatní užívatelé nemají možnost přístupu k heslu  • Jednorázový přístup (one time password): po využití hesla řešení PAM vymění heslo privilegovanému účtu | ANO |  |
| Ověření správnosti hesel - Řešení PAM pro jednotlivé privilegované účty, nebo skupiny privilegovaných účtů ověřuje shodu hesla uloženého v bezpečném úložišti a na spravovaném systému (může být například změněno lokálně administrátorem): • Systém je sám schopný ověřit, jestli je heslo uložené v bezpečném úložišti stejné jako na koncovém systému • V případě, že je heslo na koncovém systému jiné, než v bezpečném úložišti, musí být řešení schopné danou událost zalogovat, vytvořit notifikaci a zajistit automatickou výměnu hesla za nové • Generuje report se všemi účty, kde jsou hesla jiná na spravovaných systémech a v bezpečném úložišti | ANO |  |
| Historie hesel - Řešení zaznamenává a uchovává historii hesel (například poslední tři hesla, nebo podle časového období) a umožňuje jednoduchý přístup k historii přes webové rozhraní. | ANO |  |
| Systém podporuje Single Sign On (SSO) pro privilegované účty, tedy možnost automaticky se přihlásit ke koncovému systému prostřednictvím privilegovaného účtu bez nutnosti zadávání hesla. Podporované jsou minimálně následující aplikace/protokoly:  • Windows RDP  • SSH (např. PuTTY) • HTTP(s)/Web aplikace  • Libovolný "tlustý klient pro aplikace instalované ve Windows prostředí | ANO |  |
| Během SSO je heslo automaticky zadané do aplikace na pozadí bez možnosti jeho odhalení. | ANO |  |
| Existuje mechanismus zajišťující bezpečný přístup k heslům uloženým v systému i v případě jeho částečné, nebo úplné nedostupnosti. | ANO |  |
| **Operační systémy** - Systém řízení privilegovaných účtů musí umožňovat měnit hesla, bez instalace agenta na koncový bod, pro privilegované účty v následujících Operačních systémech: - Microsoft a) Windows desktopové systémy od verze Windows 7 a vyšší b) Microsoft Windows serverové systémy Windows Server 2008 a vyšší c) podporované je řízení lokálních a doménových účtů prostřednictvím protokolů WMI, SSH, remote PowerShell - Linux - Red Hat, Ubuntu, Fedora, CentOS, Novell SUSE, Debian  - BSD  - VMware - ESX, ESXi Server - Apple - OS X - Citrix – XenServers  - Cisco – všechny OS - EMC - Unix d) Včetně systémů dodávaných v rámci plnění | ANO |  |
| **Adresářové služby** - Systém řízení privilegovaných účtů musí umožňovat bezagentsky řídit hesla pro privilegované účty v následujících Adresářových službách: - Microsoft Active Directory, Azure Active Directory | ANO |  |
| **Microsoft Windows Aplikace** - Systém řízení privilegovaných účtů musí umožňovat řídit a měnit hesla pro privilegované účty v následujících Windows aplikacích bez nutnosti instalace agenta na koncový bod: - Windows Services - Windows Scheduled Tasks - IIS Application Pool - IIS Directory Security - Windows Registry COM+ - Cluster Service   * SharePoint | ANO |  |
| **Aplikace** - Systém řízení privilegovaných účtů musí umožňovat řídit a měnit hesla pro privilegované účty v následujících Aplikacích bez nutnosti instalace agenta na koncový bod: - SAP Application Server - IBM Websphere, Tivoli Storage Manager - BEA Weblogic - JBOSS - Oracle Application ERP, PeopleSoft, GridControl, Application Server - Tomcat - HP desktop BIOS passwords - Cisco Call Manager   * Apache, nginx * Včetně aplikací dodávaných v rámci plnění | ANO |  |
| **Databázové systémy** - Systém řízení privilegovaných účtů musí umožňovat řídit a měnit hesla pro privilegované účty v následujících Databázových systémech bez nutnosti instalace agenta na koncový bod: : - Oracle - Microsoft SQL Server - IBM DB 2 a Informix - Sybase Database, IQ - MySQL  - FireBird  - PostgreSQL - Všechny ODBC kompatibilní databáze a hesla uložená v tabulkách | ANO |  |
| **SAAS a Webové stránky** - Systém řízení privilegovaných účtů musí umožňovat řídit a měnit hesla pro privilegované účty v následujících SaaS službách a webových stránkách bez nutnosti instalace agenta na koncový bod: - Amazon Web Services - Microsoft Azure - Microsoft Office365 - Facebook - Google Gmail - Linkedin - Twitter - Pinterest  - SalesForce | ANO |  |
| **Bezpečnostní systémy** - Systém řízení privilegovaných účtů musí umožňovat řídit a měnit hesla pro privilegované účty v následujících Bezpečnostních systémech bez nutnosti instalace agenta na koncový bod: - Checkpoint Firewall, SPLAT, Provider, GAIA - Cisco PIX, ASA, IronPort, ISE - Juniper Netscreen - Fortinet FortiGate, FortiManager - BlueCoat Proxy SG, CAS, MAA - Palo Alto Panorama - IBM DataPower - SourceFire 3D - TippingPoint IPS, SMS - WatchGuard Firebox - Intel Security/McAfee ePolicy Orchestrator - Symantec Messaging Gateway - Safenet Luna HSM  - SEP manager | ANO |  |
| **Síťové zařízení** - Systém řízení privilegovaných účtů musí umožňovat řídit a měnit hesla pro privilegované účty v následujících Síťových zařízení bez nutnosti instalace agenta na koncový bod: - Cisco Router, ACS, Switch Catalyst, Nexus Switch, JMC, Wireless LAN Controller, WAAS, ONS - Juniper (JUNOS) - Nortel - Alcatel - F5 BigIP - HP ProCurve - 3com - Enterasys - Aruba - BlueCoat - Brocade  - Avaya - Radware | ANO |  |
| Automatické řízení privilegovaných účtů v těchto systémech musí být dodáno v rámci implementace a podporováno po dobu platnosti zakoupené licence řešení | ANO |  |
| Podporuje detekci SSH klíčů a mapování vztahů veřejného a soukromého SSH klíče používaného pro přihlášení k systémům. | ANO |  |
| Řešení podporuje reporting o stavu klíče, jako je jeho platnost, délka klíče apod. Zároveň identifikuje nesoulad s politikou. | ANO |  |
| Řešení musí bezpečně uchovávat SSH klíče v centrálním zabezpečeném úložišti a zároveň kontrolovat a řídit přístupy k těmto klíčům. | ANO |  |
| Řešení musí podporovat automatickou výměnu klíčů. Podporuje také rotaci páru SSH klíčů (výměnu privátního a veřejného klíče na cílovém zařízení). | ANO |  |
| Řešení musí spravovat a chránit SSH klíče, které jsou používané aplikacemi pro autentizaci. | ANO |  |
| Řešení umí posílat notifikace při použití vybraného SSH klíče. | ANO |  |
| Řešení zabezpečuje správu SSH klíčů a je integrováno do stejné infrastruktury jako zabezpečení privilegovaných účtů a hesel. | ANO |  |
| Nástroj umožňuje nahrávání privilegovaných relací v rámci celého počtu licencí. Minimálně ve formě:  a) textové relace (např. SSH, telnet)  b) relace prostřednictvím vzdálené plochy (např. RDP, VNC) | ANO |  |
| Nástroj umožňuje vyhledávat v nahraných relacích dle zadaných slov. | ANO |  |
| Nástroj umožňuje během privilegovaného přístupu oddělit prostředí klienta od cílového systému, pro zvýšení zabezpečení a minimalizaci rizika nákazy. Stejně tak je možné znemožnit kopírování informací a dat z cílového systému na klienta. | ANO |  |
| Nástroj umožňuje monitorovat aktivní relace jinou osobou, např. bezpečnostními správci, auditory apod. Včetně možnosti do aktivní relace zasáhnout. | ANO |  |