Sem vložte zadání Vaší práce.

České vysoké učení technické v Praze
Fakulta informačních technologií
Katedra počítačových systémů

Bakalářská práce

Systém pro správu sdílených předdefinovaných administrátorských hesel

Vedoucí práce: Mgr. Monika Součková

20. června 2015

Poděkování

Chtěl bych poděkovat vedoucí práce Mgr. Monice Součkové a jejímu manželovi Ing. Tomášovi Součkovi za nabídku zajímatého tématu a cenné rady, připomínky i trpělivost při jeho vypracovávání. Dále bych chtěl poděkovat všem osloveným technickým konzultantům od srovnávaných produktů, kteří ochotně spolupracovali a poskytli mi informace potřebné k vypracování této práce.

Prohlášení

Prohlašuji, že jsem předloženou práci vypracoval(a) samostatně a že jsem uvedl(a) veškeré použité informační zdroje v souladu s Metodickým pokynem o etické přípravě vysokoškolských závěrečných prací.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona, ve znění pozdějších předpisů. V souladu s ust. § 46 odst. 6 tohoto zákona tímto uděluji nevýhradní oprávnění (licenci) k užití této mojí práce, a to včetně všech počítačových programů, jež jsou její součástí či přílohou, a veškeré jejich dokumentace (dále souhrnně jen „Dílo“), a to všem osobám, které si přejí Dílo užít. Tyto osoby jsou oprávněny Dílo užít jakýmkoli způsobem, který nesnižuje hodnotu Díla, a za jakýmkoli účelem (včetně užití k výdělečným účelům). Toto oprávnění je časově, teritoriálně i množstevně neomezené. Každá osoba, která využije výše uvedenou licenci, se však zavazuje udělit ke každému dílu, které vznikne (byť jen zčásti) na základě Díla, úpravou Díla, spojením Díla s jiným dílem, zařazením Díla do díla souborného či zpracováním Díla (včetně překladu), licenci alespoň ve výše uvedeném rozsahu a zároveň zpřístupnit zdrojový kód takového díla alespoň srovnatelným způsobem a ve srovnatelném rozsahu, jako je zpřístupněn zdrojový kód Díla.

V Praze dne 20. června 2015 .....

Odkaz na tuto práci

Hutr, Marek. *Systém pro správu sdílených předdefinovaných administrátorských hesel*. Bakalářská práce. Praha: České vysoké učení technické v Praze, Fakulta informačních technologií, 2015.

Abstrakt

V současné době je vzhledem k rostoucímu množství hesel ve firmách nutnost používat nástroj na jejich správu. V této práci je představen enterprise správce hesel jako vhodné řešení do kolaborativního prostředí. Na základě analýzy ve firmě DHL International Services jsou pak definovány základní funkční a nefunkční požadavky. Podle těchto požadavků je pak provedena analýza trhu a jsou vybrány produky vhodné ke srovnávání. Dále jsou definována srovnávací kritéria, která tvoří strukturu pro detailní popisy jednotlivých produktů. Výsledkem práce je testování závěrečných produktů, představení vhodného produktu k nasazení a návrh implementace delegačního modelu.

Klíčová slova firemní správa hesel, kolaborativní prostředí, bezpečnost, sdílená hesla, privilegované účty, srovnání produktů

Abstract

Nowadays, due to a growing number of passwords used in enterprises, there is a need to use a tool to manage them. In this thesis, the enterprise password manager is introduced as a suitable solution for a collaborative enviroment. Based on the analysis done in the company DHL International Services, functional and non-functional requirements are defined. According to these requirements

an analysis of the market is done and products suitable for comparsion are picked. Then benchmarks are defined, which form the structure for detailed descriptions of each product. The result of this thesis is a final product testing, an introduction of a product suitable to deploy, and a design implementation of the delegation model.

Keywords enterprise password management, collaborative enviroment, security, shared passwords, privilleged accounts, product comparsion

Obsah

Seznam tabulek

Úvod

V dnešní době informačních technologií roste ve firmách počet systémů a zařízení. K jejich správě je potřeba znalost přístupových údajů pro ověření identity správce. S rostoucím počtem systémů a zařízení tedy roste i počet přístupových údajů k nim. To vede k používání nevhodných metod pro evidenci přístupových údajů, jako je například tabulkový dokument, nebo k rezignování na bezpečnostní standardy a nastavování snadno prolomitelných hesel, nebo například stejného hesla na všechny systémy. K řešení tohoto problému s množstvím hesel, jsou na trhu produkty, které se zabývají správou hesel.

Existují dva typy správců hesel rozdělené podle rozsahu nasazení: osobní a firemní. Zatímco osobní řešení jsou vhodná pro ukládání hesel jednotlivců, firemní řešení umožňují ukládání hesel, jejich následné sdílení skupinám, nebo jednotlivým uživatelům, automatické změny hesel na cílových zařízeních a systémech a to vše na vysokých standardech bezpečnosti. Právě na firemní řešení je tato práce zaměřena.

V této práci se nejprve věnuji popisu problematiky současných nejvíce rozšířeným řešením i jeho nedostatky a konstatuji, že možným řešením je nasazení firemního správce hesel. Dále pak provádím analýzu ve firmě DHL, na základě které stanovuji základní funkční a nefunkční požadavky na hledaný produkt. Podle stanovených základních požadavků hledám vhodné produkty dostupné na trhu a zamítám produkty, které nesplňují stanovená kritéria, nebo jiným způsobem nevyhovují. Následuje definice srovnávacích kritérií pro srovnávání.

Stěžejní částí práce je detailní popis produktů podle kritérií pro srovnávání, na základě dostupných informací na webových stránkách prodejců, z emailové komunikace a telefonátů, nebo účasti na video konferencích.

Praktickým výsledkem z práce je pak porovnání dostupných produktů a doporučení finálního produktu spolu s návrhem možného delegačního modelu do konkrétní situace ve firmě DHL International Services.

Kapitola 1

Cíl práce

Cílem mé práce je navrhnout systém pro správu sdílených administrátorských hesel ve firmě DHL International Services.
Nejprve provedu analýzu aktuální situace ve firmě DHL International Services v oblasti správy hesel a stanovím základní funkční a nefunkční požadavky. Na základě získaných informací provedu analýzu dostupných produktů na trhu a vyberu ty, které splňují stanovené požadavky. Poté nadefinuji objektivně měřitelná srovnávací kritéria, podle kterých vypracuji detailní srovnáí produktů, podle kterého poté vyselektuji produkty vhodné do prostředí DHL International Services a ty otestuji. Podle výsledků z testování vyberu závěrečný produkt, pro který vypracuji doporučení pro instalaci a implementaci delegačního modelu podle rolí v DHL International Services.

Kapitola 2

Popis problematiky

V dnešní době je většina informací ve firmách uchovávána ve složitých softwarových systémech, ke kterým denně přistupují firemní zaměstnanci.
Z průzkumu[1], který v roce 2012 provedlo Norské centrum pro informatiku, vyplynulo, že průměrný zaměstnanec používá ve svém zaměstnání 8,5 hesla. Za uplynulé 3 roky od průzkumu se samozřejmě mnohé změnilo s nástupem SSO technologií, přesto můžeme brát tento údaj za směrodatný.

Tento údaj však platí pro běžné uživatele, pro IT administrátory je toto číslo mnohem větší. Pokusím se to ukázat na extrémním příkladu: systémy pro koncové zaměstnance běží na různém hardwaru a dalších systémech, ke kterým potřebují mít administrátoři přístup. Řekněme, že by každý tento koncový systém běžel na systémovém serveru a ten zase na hardwarovém serveru, ke kterým jsou také přístupové záznamy. Rázem nám naroste průměrný počet hesel na IT administrátora na troj násobek. V průměrné firmě bychom tedy v této extrémní situaci měli počet přístupových údajů pro IT administrátora přibližně 25, které se navíc musí kvůli následování firemních bezpečnostních standardů často měnit.

Zatím jsme se bavili pouze o průměrné firmě, kde je tento počet hesel relativně malý. Pokud se přesuneme do prostředí rozsáhlé firmy, pro které je tato práce cílena, může nám číslo přístupových záznamů pro IT administrátora narůst do řádu stovek až tisíců. Tyto záznamy není možné si pamatovat, je tedy potřeba je nějakým způsobem evidovat a navíc je zde nutnost jejich sdílení mezi skupinou administrátorů.

2.1 Současná řešení

V praxi existují tři varianty, jak IT administrátoři tento problém nejčastěji řeší:

- **Spreadsheet**
  Neboli tabulkový dokument je nejjednodušší řešení, jak uchovávat přístupové záznamy. Jednoduše se vytvoří dokument, kde se nadefinují potřebné sloupce a poté se přidávají a editují záznamy. Spreadsheet může být také online například na cloudovém systému.

- **Firemní intranet**
  Jedná se v podstatě o to samé, jako je spreadsheet. V intranetu (například MS SharePoint) se vytvoří stránka, kde budou mít přístup pouze IT administrátoři a nadefinují se potřebná pole. Pak už se pouze přidávají a editují záznamy.

- **Osobní správce hesel**
  Password manager (správce hesel) je software, nebo služba, co pomáhá uživateli udržovat přehled nad jeho hesly a jinými přístupovými záznamy.[2]

2.2 Nedostatky a problémy současných řešení

Tyto způsoby uchovávání záznamů jsou však pro prostředí rozsáhlé firmy nevhodné z několika důvodů, popíši alespoň ty zásadní.

- **Problémy synchronizace záznamů**
  U všech řešení může nastat situace, že dva administrátoři udělají různé úpravy, oba uloží změny, ale ten, kdo uloží změny jako druhý, přepíše změny toho prvního.

- **Problém zabezpečení záznamů**
  Záznamy ve spreadsheetu i na intranetu jsou většinou někde uloženy v souboru, který není šifrovaný. Kdokoliv se tedy k němu dostane, může číst všechny záznamy. Dalo by se argumentovat tím, že spreadsheet lze zamknout, nicméně například excelový dokument lze snadno odemknout pomocí makra.[3]

- **Problém možnosti odcizení dat**
  Kvůli problémům se zabezpečením si zaměstnanec při svém odchodu z firmy může data odnést a má tak přístup ke všem citlivým informacím.

- **Problém s efektivitou**
  Ve všech řešeních je náročné seskupovat záznamy například podle typu a efektivně v nich hledat.

- **Problém s kontrolou aktivit**
  U všech řešení není možné evidovat, kdo kdy k jakému záznamu přistupoval a jaké dělal úpravy.

- **Problém s rozdělením rolí**
  U těchto řešení lze jen velice těžko nadefinovat, který uživatel bude mít k jakému záznamu přístup, a tak mají většinou přístup všichni ke všemu, což je neakceptovatelné z pohledu rozdělení rolí a odpovědností ve firmě.

2.3 Vhodné řešení použitím enterprise nástroje

Jak lze vidět, žádné z nejčastěji používaných řešení na evidenci hesel není vhodné do prostředí firmy, kde mezi sebou potřebují IT administrátoři přístupové údaje navzájem sdílet. Navíc je problém v tom, že zmíněné tři nástroje existují pouze jako databáze přístupových údajů. V této práci se však zabýváme systémem, který by nejen řešil všechny běžné problémy s evidencí zmíněné v předchozí podkapitole, ale hledáme systém, který by umožňoval i samotnou správu hesel. Pod správou mám na mysli to, že bude na základě buď to automatických, nebo uživatelem spuštěných operací sám měnit, nebo resetovat hesla na cílových zařízeních a systémech, a následovat tak firemní bezpečnostní standardy například na dobu platnosti, nebo složitost hesla.
Z těchto důvodů se v této práci věnuji nástrojům na správu a sdílení hesel pro firemní (enterprise) prostředí, které řeší všechny popsané problémy a nabízí i správu hesel. Specifikace základních funkčních a nefunkčních požadavků (konkretizovaných pro tuto práci) na tyto nástroje jsou vypsány ve 4. kapitole. Detailní popis konkrétních vlastností je vypsán 6. v kapitole.

Kapitola 3

Analýza situace ve firmě DHL International Services

3.1 Současná situace

Tým spravuje řádově tisíce serverů (z 95% HP s iLO kartami).
Pro správu přístupových záznamů k iLO kartám serveru slouží in-house systém, který umožňuje zobrazení hesla k iLO kartě konkrétního serveru, případné jeho uložení do clip-boardu a změnu hesla na nové, náhodně generované. Tyto kroky jsou spolu s uživatelským ID logovány v audit logu systému. Zabezpečení tohoto systému spočívá v tom, že aplikace je spouštěna z Citrix XenApp[4] a tím pádem se její kód nedostává přímo k uživateli do počítače a nemůže být tak odnesena mimo firemní prostředí. Přístup do Citrix XenApp je přes firemní LDAP (konkrétně Microsoft Active Directory). Samotná aplikace získává data přímým spojením s MS SQL databází, které je šifrované symetrickou šifrou.
Mimo hesel k iLO kartám používá tým nespočet přístupových hesel na lokální administrátorské účty serverů. Ať už se jedná o Windows, nebo UNIX servery. Tyto hesla jsou týmu k dispozici na v podobě databázového souboru pro aplikaci KeePass[5], který je uložen lokálně na počítačích zaměstnanců, nebo na síťovém disku, díky tomu může pochopitelně kterýkoliv zaměstnanec odnést mimo firmu, použití hesel a změna hesel není jakkoliv logována a mohou se vyskytovat problémy se synchronizací databáze. (Jak je popsáno v oddílu 2.2.)

3.2 Ideální situace

Implementace Enteprise produktu, který bude schopný spravovat přístupové údaje k HP iLO kartám, lokálním administrátorským účtům Windows a UNIX serverů a ty pak poskytovat uživatelům podle organizačních skupin oprávnění. Systém bude také umět resetovat hesla k těmto koncovým zařízením a veškeré aktivity bude zaznamenávat do audit logu. Postupné rušení in-house systému na přístup k přístupům na HP iLO karty a zrušení volně dostupné KeePass databáze.
Systém bude splňovat Server – Klient architekturu s velkým důrazem na zabezpečením raw dat. (Tedy například i zvážení možnosti distribuované databáze)
Bylo by dobré, kdyby byl systém otevřený pro plug-iny, aby bylo možné škálovat systém pro různá další cílová zařízení (do budoucna například IBM IMM karty, v současné době již HP BladeSystem)
Bylo by dobré, kdyby měl systém otevřené API a propojil se s dalšími nástroji - například automatická změna účtu při přechodu serveru do Produkce.

Kapitola 4

Základní požadavky na hledaný produkt

Tato kapitola obsahuje výčet a popis funkčních a nefunkčních požadavků na firemní správce hesel v kontextu firmy DHL International Services. Vzhledem k tomu, že se jedná o firemní produkt, nikdy nebudou snadno definovatelné všeobecné funkční, ani nefunkční požadavky, protože ty se budou firmu od firmy lišit.

4.1 Funkční požadavky

Funkční požadavky představují základní předmět systému a jsou měřeny konkrétními prostředky, jako jsou například hodnoty dat, logika a algoritmy rozhodování. Funkční požadavky specifikují, co má produkt dělat.[6]

- **Správa privilegovaných přístupových údajů**
  Hlavním funkčním požadavkem je, aby produkt umožňoval základní operace s privilegovanými přístupovými údaji (obvykle dvojice uživatelské ID a heslo) k cílovým systémům/zařízením, včetně informacích o nich (název, popis, typ, IP adresa).
  Za základní operace považujeme operace zápisu nového záznamu, čtení záznamu, změna záznamu a odstranění záznamu.

- **Změna hesel na cílových zařízeních/systémech**
  Nejprve je však nutné zmínit rozdíl mezi pojmy změna a reset hesla: **Změna hesla** je operace, kterou může provést pouze entita znající heslo. V kontrastu k tomu **reset hesla** je operace, kterou může udělat entita neznající heslo, které chce změnit, musí k tomu ovšem mít jiná oprávnění.

Uživatel musí být schopný změnit, nebo resetovat heslo na následujících cílových systémech/zařízení.
MS Windows – lokální administrátorské účty: „Všechny Microsoft Windows systémy mají lokální administrátorský účet, obvykle nazývaný „Administrator“. Tento účet má privilegovaný (super-uživatelský) přístup.“[7]
Linux – root uživatelé: „Root je uživatelské jméno, nebo účet, který má defaultně přístup ke všem příkazům a souborům na Linuxu, nebo jiném operačním systému Unixového typu.“[8]
HP iLO card (HP Integrity Integrated Lights-Out) – Integrovaný systém v serverovém HW od výrobce HP pro vzdálenou správu serverů přes LAN rozhraní pomocí textového CLI, nebo webového GUI. iLO karta umožňuje například: monitorování stavu a statusu serveru, konzoli virtuálního sériového portu, správu a regulaci napájení a další. Toto rozhraní je dostupné i v případě, kdy server není zapnutý.[9]
HP BladeSystem – architektura pro servery, datová úložiště a síťové prvky určená pro firemní nasazení od 100 do více než 1000 serverů, která seskupuje více IT komponent do jednoho optimalizovaného celku.[10] HP BladeSystem je spravován pomocí HP OneView, který monitoruje všechna zařízení připojená do BladeSystemu a umožňuje jejich automatickou údržbu. [11]
IBM IMM (Integrated Management Module) – Jak již název napovídá, jedná se o integrovaný modul pro vzdálenou správu HW serveru. Jeho součástí je analytický nástroj na predikci selhání, správu a dohled nad napájením, hardwarem a operačním systémem, a další funkce.[12]

- **Automatická rotace hesel a následování firemních politik**
  Potřebujeme, aby produkt uměl automaticky měnit hesla na spravovaných cílových zařízeních/systémech a zároveň aby automaticky měněná hesla splňovala firemní politiky na délku a složitost, tedy generátor náhodných hesel musí být schopen na tyto požadavky reagovat.

- **Audit log**
  Je dokument, do kterého se ukládají záznamy o všech aktivitách všech uživatelů spolu s jejich uživatelským ID a časovým údajem, kdy byla aktivita vykonána.

4.2 Nefunkční požadavky

Nefunkční požadavky představují vlastnosti v oblasti chování, které musí mít stanovené funkce jako například výkonnost, uživatelnost atd. Nefunkčním požadavkům lze přiřadit konkrétní metodu měření. Nefunkční požadavky specifikují, jaké vlastnosti má produkt mít.[6]

- **Enterprise Archutektura**
  (podniková architektura) je způsob proměny firemní vize a strategie do efektivní změny vytvořením, komunikací a zlepšením klíčových požadavků, principů a modelů, které budou popisovat firemní budoucnost a umožní její následné zlepšování. Do enterprise architektury patří lidé, procesy, informace a technologie, které firma využívá, jejich vzájemné vazby a vazby k externím prostředím. Enterprise architektura nabízí celostní řešení, které se zaměřuje na firemní výzvy a podporuje prostředky potřebné k jeho implementaci.[13]
  Je vždy založena na **klient–server architektuře** – typ dvouvrstvé architektury popisující distribuované systémy, které zahrnují samostatného klienta a server systému propojené sítí. Nejjednodušší formou tohoto modelu je serverová aplikace, ke které přímo přistupuje více klientů.[14]

- **Vysoké bezpečnostní standardy**
  Předpokládáme-li enterprise architekturu, tak bude jako vysoký bezpečnostní standard stačit, když budou záznamy uložené v databázi a šifrovány 256bit AES šifrou, která byla v roce 2001 schválena Americkým Národním Institutem Standartů a Technologií (NIST) jako vhodná k zabezpečení citlivých elektronických dat.[15]
  I přesto, že by se někomu povedlo provést kopii databáze a tu ukrást, bylo by prakticky nemožné 256bit AES šifru prolomit. Vzhledem k tomu, že jediný možný způsob jak je možné šifru prolomit je útok hrubou silou, následující příklad ukazuje jak dlouho by to trvalo: Předpokládejme, že každá osoba na Zemi vlastní 10 počítačů. Na Zemi žije 7 miliard lidí. Každý z těchto počítačů může otestovat 1 bilion kombinací klíčů za vteřinu. V průměru se podaří prolomit klíč po vyzkoušení 50 % možností. V tomto případě by celá populace Země mohla prolomit jeden klíč za 77 000 000 000 000 000 000 000 000 let. (zdroj: Jak bezpečná je AES šifra proti útoku hrubou silou?[16])

Kapitola 5

Analýza trhu

Jako další krok jsem provedl analýzu všech produktů na trhu zabývajících se správou hesel pro firemní prostředí. Bohužel jsem většinu z nalezených produktů musel zamítnout pro nesplnění základních požadavků zmíněných v předchozí kapitole. Bylo by zajímavé se v jiné práci věnovat zpracování podrobné rešerše této oblasti softwaru a zjistit nakolik jsou tyto produkty vhodné pro firemní prostředí. Produkty vhodné ke srovnávání vypisuji ve druhé části této kapitoly.

5.1 Zamítnuté produkty

Celý seznam zamítnutých produktů spolu s odkazy na jejich stránky je vzhledem k rozsahu přiložen k práci jako příloha B.
Většinu z dostupných produktů na trhu jsem zamítl kvůli nesplnění požadavku na automatickou rotaci hesel, nebo správu HP iLO karet. Nicméně je zde několik málo programů, které stojí za zmínku.

Enterprise Password Vault[17] od firmy CyberArk Software - Tento produkt splňuje všechny naše požadavky, ale bohužel jsem se hned ze začátku setkal s arogancí obchodních zástupců a tím pádem jsem nezařadil produkt mezi vhodné ke srovnání kvůli tomu, že by i následná komunikace mohla být složitá.
Něco obdobného se mi stalo u produktu Fischer Identity[18] od firmy Fischer International, který také splňuje všechny naše požadavky, ale bohužel jsem nedostal ani jednu odpověď na mé emaily.
Oproti tomu PasswordState7[19] od firmy ClickStudios Pty Ltd. jsem musel zamítnout, protože mi v únoru 2015 napsali, že momentálně nepodporují požadovaný HW. V polovině května téhož roku mi pak poslali email, že nakoupili různé HW zařízení a implementovali do produktu jejich podporu, takže nyní již splňují naše požadavky. I přes to jsem je bohužel již do srovnání nestihl zahrnout.

5.2 Produkty vhodné ke srovnávání

K dalšímu srovnávání jsem vybral následující produkty, které splňovaly všechny požadavky z předchozí kapitoly.

- **Device42**[20] od společnosti Device42, Inc.
- **Enterprise Random Password Manager**[21] od od společnosti Lieberman Software
- **Password Manager Pro**[22] od společnosti ZohoCorporation
- **PowerBroker Password Safe**[23] od společnosti BeyondTrust, Inc.
- **Privileged Access Manager**[24] od společnosti Hitachi ID Systems, Inc.
- **Privileged Password Manager**[25] od společnosti Dell, Inc.
- **Secret Server**[26] od společnosti Thyotic

Kapitola 6

Srovnávací kritéria

Předtím, než začnu porovnávat jednotlivé produkty, je třeba specifikovat, které konkrétní ověřitelné oblasti budu sledovat. V této kapitole je výčet srovnávacích kritérií a specifikace konkrétních údajů, které budu zjišťovat pro srovnávání produktů.

6.1 Modelová situace

Pro některá srovnávací kritéria je důležité uvést konkrétní prostředí, do kterého bude produkt nasazen. Pro tyto případy definujeme modelovou situaci, která je srovnatelná, nikoliv však identická s prostředím firmy DHL International Services.
V našem modelovém prostředí tedy budeme mít:

Cílové systémy
- 6 000 serverů, z toho 5 500 Windows - lokální administrátoři a 500 Linux - root uživatelé

Cílová zařízení
- 3 000 HP iLO karet
- 100 HP BladeEnclosures

Uživatelé
- 150 uživatelů s různými rolemi a právy

Samotný server by pak měl fungovat v HA nasazení na Windows serveru.

6.2 Výčet srovnávacích kritérií

Možnosti práce se záznamy

- **Automatické změny hesel**
  Je základním funkčním požadavkem. Zjišťuji, jakým způsobem je v rámci produktu vykonávána. Například periodická automatická změna ve stanovený termín, nebo po ukončení uživatelské relace například vrácením hesla po dokončení práce na cílovém zařízení/systému.

- **Ověření platnosti hesla**
  Zjišťuji, zda umí produkt kontrolu shody hesel na cílovém zařízení/systému s heslem uloženým v databázi?

- **Složitost hesla**
  Zjišťuji, zda produkt umožňuje nastavení vlastních politik na složitost hesla.

- **Historie hesel**
  Je pro náš případ důležitá hlavně pro IBM IMM karty, protože hesla na těchto kartách nejdou resetovat pomocí aplikace běžící na systému. Reset hesla je možný pouze pomocí hardwarového jumperu, což je velmi nepraktické a může trvat dlouho, než se povolaná osoba dostane k serveru (který může být i v jiném státě, nebo na jiném kontinentě). Pokud heslo na cílovém systému a v databázi nebude souhlasit, můžeme zkusit poslední známé funkční heslo.

- **Import záznamů**
  Ve firmě je již nasazen systém, který spravuje hesla k některým cílovým zařízením/systémům. Bylo by tedy vhodné, aby bylo možné databázi z tohoto systému migrovat do systému nového.

- **Kategorie a vyhledávání**
  Při velkém počtu záznamů v systému je důležité, aby je bylo možné efektivně spravovat a efektivně v nich vyhledávat.

- **Report o stáří hesel**
  Obsahuje produkt report, který by ukazoval, která hesla nebyla dlouho změněna?

Podporované systémy a zařízení

V této sekci zjišťuji, jakým způsobem probíhá správa konkrétních cílových zařízení a systémů. Je důležité rozlišit termíny reset a změna hesla pro Windows lokální administrátory. Při změně hesla se nepřeruší provázanost hesla na uživatelské certifikáty, které mohou být využity softwarem třetí strany.
Dále je důležité rozlišit pojem reset a změna hesla u IBM IMM karet, kde je

možná pouhá změna. Pokud nevíme heslo, je možné ho resetovat pouze hardwarově. (viz sekce historie hesel v předchozí sekci)

- Změna/reset HP iLO karet a HP BladeSystem
- Změna hesla IBM IMM karet
- Změna hesla lokálního administrátora Windows
- Změna/reset hesla root účtu na Linuxu

API
(Application Programming Inteface) je jazyk a formát zpráv používaný aplikací ke komunikaci s operačním systémem, nějakým jiným programem, nebo komunikačním protokolem. API jsou implementovány sepsáním funkčních volání v programu, které poskytuje propojení s požadovaným procesem ke spuštění.[27] Budu zjišťovat informace o tom, zda produkt má otevřené API a co vše je možné skrze něj udělat.

Doporučené systémové a hardwarové požadavky

- **Plně podporované databázové a operační systémy**
  Systémy, pro které prodejce zaručuje přímou podporu a pro které je produkt certifikovaný. Není neobvyklé, že některé softwarové společnosti si zakládají na tom, že hned nepodporují nejnovější operační systémy, ale na druhou pokud poslední plně podporovaný systém je Windows 2000 Server, je otázka, zda můžeme očekávat splnění standardů současné bezpečnosti a kompatibility.
- **Požadavky na software**
  Jaký další software je potřeba pro chod systému.
- **Optimální hardwarové nároky pro modelovou situaci**
  Tato informace je však spíše pro porovnání hardwarové náročnosti, zadavatelská firma má specifické požadavky na vlastní servery, které by měly nadmíru splňovat jakékoliv požadavky.
- **Možnosti nasazení**
  Různí prodejci poskytují různé možnosti nasazení: virtual appliance (operační systém a aplikace dodávaná na předinstalované image pro virtuální prostředí jako například VMVare[28], nebo VirtualBox[29])[30], hardware appliance (zařízení, které je určeno pro konkrétní funkci na rozdíl od univerzálního PC. HW je dodáván s předinstalovanou aplikací)[31] a software appliance (samotný SW).

Vzhledem k tomu, že zadavatel se snaží vyhýbat se virtuálním serverům a má vysoké požadavky na hardware, je pro nás tento údaj důležitý.

- **Integrace AD**
  AD (Active Directory) je úložiště informací o objektech, které jsou v síti, jako například uživatelé, skupiny počítačů, tiskáren, aplikací a souborů. Výchozí schéma podporuje množství atributů pro každou třídu objektů uložených v AD.[32]
  Zjišťuji využití informací o uživatelích, skupinách a počítačích z firemního AD. V ideálním případě využití již definovaných politik na hesla v rámci AD.

Zabezpečení

- **Zabezpečení aplikace a komunikace klient-server**
  Detailní popis zabezpečení komunikace mezi klientem a serverem a aplikace samotné.

- **Zabezpečení úložiště dat**
  Jinými slovy: jak těžké je dostat se k fyzickým datům a rozšifrovat informace v nich skryté.

- **TPM čipy / USB tokeny**
  TPM (Trusted Platform Module) chip je čip sloužící k uložení šifrovacího klíče, který je na základní desce většiny počítačů z vyšších tříd.[33] Zjišťuji podporu TPM čipů, nebo USB tokenů pro uložení šifrovacího klíče, kterým jsou šifrována databázová data. Je to další krok zabezpečení, který slouží k případům, kdy někdo provede kopii databáze. Případně zjišťuji podporu modulů pro HW šifrování.

- **Zamezení zobrazení hesla uživateli**
  Dalším prvkem v zabezpečení je zamezení zobrazení hesla uživateli, kdy produkt uživateli heslo vůbec nezobrazí a přímo ho připojí ke kýženému cílovému zařízení.

- **Garance aktualizací**
  Zjišťuji jakým způsobem a jak často probíhají aktualizace. Pro hardended řešení také zjišťuji, jestli prodejce garantuje aktualizace těchto zařízení.

- **Certifikace a testy bezpečnosti**
  Je pochopitelné, že firma nebude vždy chtít sdílet veškeré informace o zabezpečení svého produktu. Proto zjišťuji, jestli je produkt certifikovaný pro vysoké standardy bezpečnosti, nebo jestli prošel nějakým testováním.

- **Nahrávání relace**
  Dalším bezpečnostním prvkem, který většina produktů nabízí je takzvané nahrávání relací (session recording). Zjišťuji jak tato funkce funguje u jednotlivých produktů a kolik místa na disku nahrávky zabírají.

- **Autentizace pomocí přístupových údajů do AD**
  Je možné použít pro přihlášení do programu údaje z firemního AD?

- **Audit log**
  Záznam detailních informací o tom kdo, kdy přistupoval k jakému účtu/heslu.

- **ACL**
  (Access control list) je sada oprávnění, která jsou připojená k objektu. Tato sada upřesňuje, které subjeky mají právo přistupovat k objektu a které operace na něm mohou vykonávat.[34]
  Zjišťuji, jestli je možné nastavit ACL pro každý záznam jednotlivě a podle skupin. V rozsáhlé firmě se očekává, že ne všichni budou mít přístup ke všem záznamům.

- **RBAC**
  (Role-based access control) je metoda řízení přístupů, která je založena na uživatelově roli v rámci firmy. RBAC je způsob zabezbpeční, protože umožňuje uživatelům přistupovat pouze k informacím a procesům, které potřebují k jejich práci, zatímco jim zabraňují přistupovat k informacím, které pro ně nejsou relevantní. Role zaměstnance určuje, aby se zaměstnanec nižší úrovně nedostal k citlivým informacím z vyšší úrovně.[35]
  Zjišťuji, jestli je v systému zaveden RBAC model, pomocí kterého například lze modelovat proces requestor/approver, kdy uživatel s rolí requestora (žadatele) si vyžádá přístup k nějakému účtu/heslu a může do něj přistoupit až tehdy, kdy mu approver (schvalovatel) schválí jeho žádost.[36]

Řešení krizové situace

- **Nouzový přístup**
  Známý také jako „Break the glass“, nebo „Unlimited admin“. Jak první výraz demonstruje, jedná se o situaci obdobnou rozbití sklíčka u požárního hlásiče. Jde o přístup do aplikace s právy na všechno, který se využívá v krizové situaci (například při kolapsu sítě).

- **Možnost HA setupu**
  zjišťuji možnost HA setupu a způsob zabezpečení komunikace mezi jednotlivými instancemi.

- **Záloha databáze**
  Zjišťuji jaké je řešení zálohy databáze produktů. Záznamy v ní se totiž

každou chvíli mění, takže například denní záloha je při obnovení prakticky nepoužitelná.

Cena pro modelovou situaci
Zjišťuji informace o tom, na základě čeho probíhá licencování a jaké modely licencování firma nabízí. Dále je důležité zjistit, zda firma nabízí podporu a kolik tato podpora stojí.
Veškeré finanční nabídky jsou vypracované pro modelovou situaci z této kapitoly.

Hodnocení komunikace
Hodnocení komunikace je důležitý aspekt, pokud firma nekomunikuje s potencionálním zákazníkem, nebo veřejností, nemusí být uspokojivá ani následná podpora.

Kapitola 7

Popisy srovnávaných produktů

7.1 Device42

Možnosti práce se záznamy

- **Automatické změny hesel**
  Samotný produkt nenabízí automatickou změnu hesel, ale pomocí integrace s AD je možné změnu Windows uživatelských hesel vynutit. Změny ostatních přístupových údajů je možné automaticky měnit pouze pomocí externích skriptů.

- **Ověření platnosti hesla**
  Není implementováno v produktu, lze docílit přes API a externí skripty.

- **Složitost hesla**
  Je možné vynunit pouze u Windows uživatelských účtů na základě politik hesel v AD.

- **Historie hesel**
  Ano, vždy.

- **Import záznamů**
  Možný přes nahrání .xls, nebo .csv souboru, nebo pomocí API.

- **Kategorie a vyhledávání**
  Záznamy se dají přidávat do kategorií a organizačních skupin. Následné vyhledávání nad těmito kategoriemi a organizačními skupinami je možné.

- **Report o stáří hesel**
  V produktu je robustní nástroj na tvorbu reportů. Pomocí filtrů v něm můžeme nastavit, které konkrétní informace nás zajímají, tedy i report o stáří hesel.

Podporované systémy a zařízení

- **Změna/reset HP iLO karet a HP BladeSystem**
  Produkt umožňuje správu hesel pomocí svého API. Ať už se tedy připojujeme ke koncovému zařízení přes IPMI, SSH, nebo jiným způsobem, vždy je možné vytáhnout ze systému aktuální heslo a provést změnu. Systém sám o sobě tuto změnu neumí automaticky provést.

- **Změna hesla IBM IMM karet**
  Stejným způsobem, jako u HP iLO karet, opět není možná automatická změna hesla.

- **Změna hesla lokálního administrátora Windows**
  Změna možná není, pouze reset. Není možnost provádět reset automaticky.

- **Změna/reset hesla root účtu na Linuxu**
  Možné pomocí SSH skriptu, opět není možná automatická změna.

API
Rozsáhlé API. Podpora Restful API jako způsob zadávání, editace a přístupu k datům. Jsou také dostupné Python skripty pro integrace s vlastními systémy.

Doporučené systémové a hardwarové požadavky

- **Plně podporované databázové a operační systémy**
  Produkt je dodáván jako virtual appliance a není zde volba operačního systému, jako databázový systém je použit PostgreSQL, který je přístupný pouze uvnitř virtual appliance.

- **Požadavky na software**
  Uživatelé přistupují k systému přes webového klienta. Potřebují tedy prohlížeč podporující HTML5 (tedy IE 9+, nebo aktuální verzi Firefoxu, Safari, Opery, nebo Chrome).

- **Optimální hardwarové nároky pro modelovou situaci**
  Virtual appliance využívá 1 vCPU, 1GB RAM a 8GB HDD, při této konfiguraci nejsou známy žádné problémy z pohledu škálovatelnosti. Systém je využíván v největších světových data centrech, kde je pod správou tisíce koncových zařízení.

- **Možnosti nasazení**
  Pouze virtual appliance.

- **Integrace AD**
  Možnost importování uživatelů, včetně organizačních skupin a počítačů.

Zabezpečení

- **Zabezpečení aplikace a komunikace klient-server**
  Připojení k serveru přes HTTPS.
- **Zabezpečení úložiště dat**
  Výrobce má aplikované bezpečnostní mechanismy, které znemožňují přístup dovnitř virtual appliance. Hesla jsou šifrována 256 bit AES šifrou s uživatelem definovanou solí a samotné soubory databáze jsou opět šifrovány 256 bit AES šifrou.
- **TPM čipy / USB tokeny**
  Nejsou podporovány.
- **Zamezení zobrazení hesla uživateli**
  Uživatel si může heslo vždy zobrazit, nebo si ho zkopírovat do clipboardu, možnost zamezení zobrazení hesla a navázání přímého spojení k cílovému zařízení není možný.
- **Garance aktualizací**
  Device42 uvádí, že vždy záplatují své systémy, když se vyskytne nějaká bezpečnostní hrozba. Aktualizace produktu pak můžeme ručně spustit kdykoliv se nám to hodí.
- **Certifikace a testy bezpečnosti**
  Firma žádné certifikáty o bezpečnosti nemá, pouze se odvolává na to, že má hodně státních klientů a korporátních klientů jako je Apple Inc. a Cisco Systems Inc., pro které je bezpečnost velmi důležitá.
- **Nahrávání relace**
  Nahrávání relací není součástí produktu.
- **Autentizace pomocí přístupových údajů do AD**
  Ano.
- **Audit log**
  Produkt obsahuje rozsáhlý audit log pro každou akci provedenou uživatelem.
- **ACL**
  Pro každý záznam je možné zvolit, který uživatel, nebo skupina si ho může zobrazit, nebo editovat. Také je možno tyto práva nastavit na úrovni organizačních skupin, ze kterého ho pak záznamy zdědí.
- **RBAC**
  Podpora RBAC na úrovni uživatelů, nebo skupin. Správa uživatelů probíhá pomocí skupin práv, které jsou některé již vytvořené, ale je možné si vytvořit vlastní.

Řešení krizové situace

- **Nouzový přístup**
  Není implementován.
- **Možnost HA setupu**
  Není možná.
- **Záloha databáze**
  Je implementována přímo v aplikaci, administrátor jí může naplánovat několikrát za den, nebo přímo spustit pomocí tlačítka v administraci.

Cena pro modelovou situaci
Licencování probíhá podle počtu zařízení (koncových uzlů) a počtu IP adres, které jsou produktem spravovány. Pro náš model se hodí licence pro 5 001 -– 10 000 serverů a 50 001 -– 100 000 IP adres, která stojí $14 999 ročně.

Hodnocení komunikace
Komunikace probíhala v pořádku, všechny dotazy byly zodpovězeny do 24 hodin.

7.2 Enterprise Random Password Manager

Možnosti práce se záznamy

- **Automatické změny hesel**
  Poté co uživatel oznámí, že heslo vrátil, nebo mu skončí výpůjčka je heslo změněno. Možnost plánovaných změn hesla.
- **Ověření platnosti hesla**
  Ano, výsledky jsou volitelně zasílány emailem.
- **Složitost hesla**
  Podpora nastavení „Fine Grained Password Policy“[37], nebo je možné paralelně využívat jiné politiky hesel pro jednotlivé záznamy. Systém také podporuje vlastní DLL pro politiky hesel.
- **Historie hesel**
  Produkt ukládá všechny předchozí hesla s časovým údajem o změně.
- **Import záznamů**
  Je možný import záznamů pomocí SQL dotazu, nebo importu souboru se záznamy.
- **Kategorie a vyhledávání**
  Možnost definování různých „Management Sets“, do kterých se můžou přiřazovat cílové systémy. Jeden cílový systém může být v několika „Management Sets“ pokud je potřeba.

- **Report o stáří hesel**
  Součástí produktu jsou reporty, včetně reportu na stáří hesel. Je zde i možnost tvorby vlastních reportů pomocí SQL příkazů.

Podporované systémy a zařízení

- **Změna/reset HP iLO karet a HP BladeSystem**
  Produkt umí nejen resetovat hesla, ale také zjistit stav cílového zařízení (Check Host System Status), vypnout a zapnout systém a Power Cycle Host System. HP iLO karty a HP Blade Enclosures jsou spravovány přes IPMI protokol. Pro správu těchto zařízení jsou však podporovány i SSH skripty.

- **Změna hesla IBM IMM karet**
  Ano, přes SSH spojení. Je zde možnost ověření identity pomocí standardního přihlášení (uživatelské ID a heslo), nebo pomocí SSH klíče. Možnost přidání kontroly hesla.

- **Změna hesla lokálního administrátora Windows**
  Změna i reset hesla lokálního administrátorského účtu na Windows je možná jak na Serverech, tak na Desktopech.

- **Změna/reset hesla root účtu na Linuxu**
  Ano pomocí SSH spojení s pomocí XML souboru, kde je uložena souslednost příkazů a očekávaných odpovědí vedoucích ke změně hesla. Je zde opět možnost ověření identity pomocí standardního přihlášení (uživatelské ID a heslo), nebo pomocí SSH klíče.

API
Přes API je možné udělat vše, co umí samotný produkt. API je dostupné přes Webovou službu, Java klienta, Powershell, nebo přes SDK.

Doporučené systémové a hardwarové požadavky

- **Plně podporované databázové a operační systémy**
  Plně podporované OS pro server jsou: Windows Server 2012 R2/2012/2008 R2. Pro klientské stanice jsou to Windows 7 Professional a vyšší, vždy však pouze 64 bit verze.
  Plně podporované databázové systémy jsou MS SQL Server 2008 Express a vyšší až po verzi 2014. Dále produkt plně podporuje Oracle Database 11g R1, nebo R2 (32 bit i 64 bit verze).

- **Požadavky na software**
  Klienti i server musí mít nainstalovaný .NET Framework v3.5 SP1, nebo vyšší.

Pro každý cílový systém, který vyžaduje aplikaci, musí být na klientském počítači nainstalovaná tato aplikace. Například pokud chce klient přistupovat do SAPu, musím mít nainstalovaný SAP klient.

- **Optimální hardwarové nároky pro modelovou situaci**
  Pro chod produktu je třeba dedikovat tyto prostředky nad rámec hardwarových požadavků na OS:
  - 2 GB RAM pro ERPM aplikaci, 4GB+ RAM pro databázi, 512 MB RAM pro .NET Frameworky
  - alespoň 4GB na hard disku pro lokální soubory logů, 500MB pro prázdnou databázi
  - Více jádrový procesor. Pro naší modelovou situaci je doporučeno používat Zone Processor, což je plánovací služba, která využívá lokálních stanic místech, kde se nacházejí cílové systémy a úlohy správy tak neběží všechny na centrálním serveru. Pro snížení síťové komunikace se zpět posílají pouze SQL

- **Možnosti nasazení**
  Software appliance

- **Integrace AD**
  Do produktu je možno importovat nejen uživatele a systémy spravované AD, ale je zde podpora i pro extrakci politiky hesel z AD, která se ověří v průběhu transakce.

Zabezpečení

- **Zabezpečení aplikace a komunikace klient-server**
  Veškerá komunikace mezi komponenty produktu může být zabezpečena povolením SSL/TLS spojení. Hesla nejsou nikdy odesílána v plaintextu, vždy jsou odesílána jako ciphertext, dešifrována na koncovém zařízení.

- **Zabezpečení úložiště dat**
  Hesla jsou uložena v databázi, která může být šifrována jak softwarově, tak hardwarově. Defaultně je zvoleno softwarové AES šifrování s 256 bit klíčem.

- **TPM čipy / USB tokeny**
  Hashovací klíč k databázi může být uložený na HSM zařízení, které musí mít PKCS#11 rozhraní.

- **Zamezení zobrazení hesla uživateli**
  Je možné nezobrazovat heslo uživateli a rovnou ho spojit s aplikacemi běžícími na Terminálovém serveru, nebo na Citrix XENAPP.

- **Garance aktualizací**
  Aktualizace musí být manuálně staženy ze serveru a také manuálně nainstalovány.

- **Certifikace a testy bezpečnosti**
  Produkt splňuje všechny standardy podle směrnice ISO 27001. Produkt je běžně testován na zabezpečení soukromou firmou z USA.

- **Nahrávání relace**
  Nahrávání relací je součástí produktu, velikost záleží na rozlišení a barevném módu. Navíc je zde možnost propojení produktu s produkty na nahrávání relací ObserveIT, Balabit a Wallix.

- **Autentizace pomocí přístupových údajů do AD**
  Ano, nebo také LDAP a Radius, nebo také možnost vícefaktorové autentizace (například více AD, LDAPů, Radiusů paralelně).

- **Audit log** - Ano

- **ACL**
  V produktu je možné definovat ACL pro záznamy a skupiny.

- **RBAC**
  Podpora rolí na management konzoli serveru i ve webové aplikaci.

Řešení krizové situace

- **Nouzový přístup**
  Podpora režimu Break-The-Glass, kdy má pověřená osoba přístup ke všem záznamům.

- **Možnost HA setupu** - HA setup je podporován.

- **Záloha databáze**
  Je v režii zákazníka. Je doporučené zálohovat databázi častěji, než jsou intervaly plánovaných změn hesel.

Cena pro modelovou situaci
Financování je zřejmé z tabulky 7.1 .

Hodnocení komunikace
Komunikace s firmou byla problematická. Informace mi sdělili, ale se značným zpožděním, protože komunikovat se studentem pro ně není prioritou, navíc nakonec mi řekli, že se mnou již komunikovat nebudou. Jsem ovšem přesvědčen, že pokud bych byl potencionálním klientem, tak by komunikace probíhala bez problémů. Obchodní zástupce produkt a problematiku identit velmi dobře znal.

Název	Cena za 1 kus	Počet kusů	Celkem
Core ERPM Engine	$ 25 000	1	$ 25 000
ERPM Engine HA/DR	$ 5000	1	$ 5 000
Server Licenses (cena při koupi 5000+ kusů)	$ 50	6000	$ 300 000
Workstation Licenses (cena při koupi 3000+ kusů)	$ 6	3150	$ 18 900
Celkem:	$ 25 000	1	$ 348 900

Tabulka 7.1: Složení ceny - Enterprise Random Password Manager

7.3 Password Manager Pro

Možnosti práce se záznamy

- **Automatické změny hesel**
  Je možné používat tzv. „One Time Password“ funkci, díky které je heslo automaticky resetováno po vypršení zápůjčky definované časovým rámcem. Automatický periodický reset hesel možný.
- **Ověření platnosti hesla**
  Produkt automaticky kontroluje, jestli se hesla na zařízení a v databázi shodují, případné rozdílnosti ukazuje jako varování ve webové aplikaci.
- **Složitost hesla**
  Je zde možnost vytváření různých politik pro rozdílné typy zařízení a jejich následné vynucení.
- **Historie hesel**
  Do historie hesel se ukládají veškerá hesla nehledě na to, jestli proběhla změna úspěšně, nebo ne.
- **Import záznamů**
  Import záznamů je možný přes .csv, nebo .txt soubor.
- **Kategorie a vyhledávání**
  Kategorie se tvoří poskytnutím kritérií, díky kterým se může nový záznam automaticky zařadit do již existující kategorie. Kritéria mohou být také na základě uživatelem definovaných polí u záznamů a hodnot uložených v těchto polích. Samozřejmostí je i následné vyhledávání a filtrování pomocí kategorií.
- **Report o stáří hesel**
  Produkt nabízí mnoho reportů včetně reportů dle ISO 27001 standardu[38] včetně reportu o stáří hesel.

Podporované systémy a zařízení

- **Změna/reset HP iLO karet a HP BladeSystem**
  Produkt se připojí cílovému zařízení přes SSH a spustí příslušný CLI příkaz ke změně hesla. Pomocí produktu lze konfigurovat port, protokol a účet kterým bude heslo změněno.

- **Změna hesla IBM IMM karet**
  Postup je stejný jako u HP iLO karet, produkt má nástroj na ověřování shody hesel na zařízení s hesly uloženými v databázi.

- **Změna hesla lokálního administrátora Windows**
  Změna není možná, heslo je resetováno pomocí doménového administrátora.

- **Změna/reset hesla root účtu na Linuxu**
  Změna hesla je prováděna pomocí SSH.

API

Skrze RestAPI je možné automaticky vytvářet nové záznamy, nebo mazat současné, získávat informace o záznamech (včetně hesla), měnit hesla u záznamů, vznést žádost na heslo a následně si vyzvednout heslo schválené administrátorem, schválit, nebo zamítnout žádost na heslo a vytvořit nového uživatele.

Doporučené systémové a hardwarové požadavky

- **Plně podporované databázové a operační systémy**
  OS Linux: Ubuntu 9.x a vyšší, CentOS 4.4. a vyšší, Red Hat Linux 9.0, Red Hat Enterprise Linux 5.3, 5.4, 5.5
  OS Windows: Windows Server 2008/2008R2/2012/2012R2, Windows Vista/7/8
  Databáze: PostgreSQL 9.2.1 je svázán s produktem, navíc podpora MySQL a MS SQL Server 2005 a vyšší včetně MS SQL Server 2014.

- **Požadavky na software**
  Na straně serveru je instalace soběstačná (obsahuje vlastní webový i databázový server). Na straně klienta je nutný HTML prohlížeč (IE7 a vyšší/Chrome/Firefox).

- **Optimální hardwarové nároky pro modelovou situaci**
  Intel Core2Duo, 4GB RAM, 20GB HDD

- **Možnosti nasazení**
  Software appliance.

- **Integrace AD**
  Importování uživatelů, skupin a počítačů. Počítače budou automaticky

přidány spolu s příslušnými lokálními administrátorskými účty. Politiky hesel je třeba zadat manuálně.

Zabezpečení

- **Zabezpečení aplikace a komunikace klient-server**
  Komunikace mezi klientem a serverem je pomocí šifrovaného HTTPS spojení, komunikace mezi primárním a sekundárním serverem při HA řešení je taktéž šifrovaná.

- **Zabezpečení úložiště dat**
  Data v databázi jsou šifrována nejprve 256 bit AES šifrou na při poslání dat do databáze a samotná databáze je pak šifrovaná 256 bit AES šifrou v MSSQL nebo PostgreSQL databázích, ale pouze se 128 bit AES šifrou pro MySQL databáze.

- **TPM čipy / USB tokeny**
  USB médium s hashem musí být zapojeno pouze při startu aplikace. Poté může být odpojeno a schováno do trezoru.

- **Zamezení zobrazení hesla uživateli**
  Heslo je defaultně skryto, je zde možnost nezobrazovat uživatelům heslo vůbec a rovnou ho spojit přes RDP/CLI ke koncovému zařízení.

- **Garance aktualizací**
  Firma poskytuje časté aktualizace včetně aktualizací komponent využitých v řešení (webový a databázový server). Běžně bývá jedna větší aktualizace verze produktu za čtvrtletí. Na webu je přehled všech aktualizací.

- **Certifikace a testy bezpečnosti**
  Firma nemá žádný certifikát o bezpečnosti, ale na serveru seibert-media.net jsou výsledky testu na průnik.[39]

- **Nahrávání relace**
  V produktu je implementován nástroj na nahrávání relací. RDP připojení se nahrávají jako video a CLI relace se ukládají celé jako text. Pro RDP relace má velikost přibližně 1MB za minutu.

- **Autentizace pomocí přístupových údajů do AD**
  Ano je podporována autentizace pomocí AD přístupových úzajů, ale také jiné LDAPy, SmartCard, Radius a SAML SSO. Navíc je zde možnost dvou faktorové autentizace pomocí telefonu, emailu, nebo Google Autenticator.

- **Audit log**
  V produktu je Audit sekce, kde jsou logovány veškeré aktivity produktu i uživatelů. Tyto aktivity jsou zaznamenávány a je zde možnost nastavení upozornění v reálném čase na jakoukoliv podezřelou aktivitu uživatelů.

- **ACL**
  Ano.

- **RBAC**
  Defaultně jsou v produktu předdefinované rozdílné uživatelské role s odlišnými úrovněmi pravomocí.

Řešení krizové situace

- **Nouzový přístup**
  V produktu je role super administrátora.

- **Možnost HA setupu**
  S jednou licencí je možné mít dva aplikační a databázové servery. Obě databáze budou propojeny kvůli replikaci. Replikace dat probíhá přes zabezpečený, šifrovaný kanál.

- **Záloha databáze**
  V produktu jsou dvě možnosti:

  - Live backup – kdykoliv se cokoliv změní v databázi, změna se propíše do Slave databáze.
  - Scheduled backup – plánovaný backup v intervalu 1 až 28 dní.

Cena pro modelovou situaci
Prodejce nabízí dvojí možnost licencování. Vždy je však licencováno podle administrátorů, kteří budou přistupovat do programu.

1. **Trvalý licenční model**:
   Jednorázový poplatek za instalaci: $ 29 988.
   Roční poplatek za údržbu a podporu: $ 5 998.

2. **Model ročního předplatného**: Ročně se platí poplatek, který zahrnuje podporu a licenční poplatek na jeden rok: $ 11 995.

Hodnocení komunikace
Komunikace byla bezproblémová, firma odpovídala a předávala si dotazy mezi obchodním oddřením a oddělením technické podpory a vývoje, aby byli schopni co nejlépe odpovědět. Mají také velmi kvalitní materiály na webu, ze kterých jde vyčíst mnoho informací, poskytli mi také veškeré manuály.

7.4 Password Safe

Možnosti práce se záznamy

- **Automatické změny hesel**
  Ano, na základě vrácení hesla (zaškrtnutím checkboxu, nebo vypršením času výpůjčky), nebo periodicky.
- **Ověření platnosti hesla**
  Ano. Navíc na cílových zařízeních, které to podporují je navíc servisní účet. Ten je pouze v databázi produktu a pomocí něj se ověřuje platnost hesel a v případně neshody je automaticky resetuje.
- **Složitost hesla**
  U produktu je možnost nastavení vlastních politik na složitost hesel.
- **Historie hesel**
  Historii hesel produkt neuchovává.
- **Import záznamů**
  Import záznamů je možný pomocí .csv souboru.
- **Kategorie a vyhledávání**
  V systému jsou takzvané „SmartGroups“, které může uživatel tvořit na základě kritérií jako je například operační systém na cílovém zařízení, typ cílového zařízení a další. Nad těmito skupinami se dá následně vyhledávat.
- **Report o stáří hesel**
  V systému je reportovací nástroj, včetně reportu o stáří hesel.

Podporované systémy a zařízení

- **Změna/reset HP iLO karet a HP BladeSystem**
  Produkt spustí agenta, který se připojí k cílovému zařízení přes SSH spojení a provede sérii příkazů vedoucí ke změně hesla.
- **Změna hesla IBM IMM karet**
  Pro každé zařízení, ke kterému se dá připojit přes SSH, je možné vytvořit šablonu připojení a změny hesla pomocí průvodce, který je součástí produktu.
- **Změna hesla lokálního administrátora Windows**
  Možný pouze reset. Na počítačích se vytváří lokální účet, pomocí kterého se kontrolují hesla, která v databázi již jsou a případně se pomocí něj resetují další lokální účty.

- **Změna/reset hesla root účtu na Linuxu**
  Podporován, změna probíhá přes SSH skript.

API
API je dostupné jako verze REST compilant API přes HTTP. Je možné se pomocí něj přihlásit/odhlásit z produktu, zažádat si o heslo, získat heslo v roli žadatele. A v roli schvalovatele naopak zamítnout, nebo potvrdit žádost o heslo.

Doporučené systémové a hardwarové požadavky

- **Plně podporované databázové a operační systémy**
  Microsoft Windows Server 2008 R2
  Microsoft SQL Server 2008 Standard a vyšší
- **Požadavky na software**
  Na straně klienta je nutný HTML prohlížeč (IE7 a vyšší/Chrome/Firefox).
- **Optimální hardwarové nároky pro modelovou situaci**
  Bohužel nejsou schopni upřesnit.
- **Možnosti nasazení**
  Prodejce doporučuje hardended virtual appliance, ale poskytuje také software appliance.
- **Integrace AD**
  Integrace s AD nabízí import uživatelů a jejich členství ve skupinách do systému.

Zabezpečení

- **Zabezpečení aplikace a komunikace klient-server**
  Komunikace je přes HTTP/TLS spojení. Přímé SSH/RDP spojení klienta s cílovým systémem je navíc zabezpečeno přes proxy.
- **Zabezpečení úložiště dat**
  Hesla jsou ukládána do databáze zašifrovaná 256 bit AES šifrou. Pro hardended appliance ať už virtual, nebo hardware zaručuje prodejce vysoký standard zabezpečení. Pokud však zákazník nevyužije hardended řešení, poskytne prodejce rady, jak zařízení co nejlépe zabezpečit.
- **TPM čipy / USB tokeny**
  Momentálně nejsou podporovány.
- **Zamezení zobrazení hesla uživateli**
  Je zde možnost uživateli heslo vůbec nezobrazovat a přímo ho připojit k cílovému systému/zařízení. Zabezpečení tohoto spojení je popsáno výše.

- **Garance aktualizací**
  Všechy appliance se připojují k PowerBroker aktualizačnímu serveru, který je automaticky aktualizuje a záplatuje.
- **Certifikace a testy bezpečnosti**
  Produkt žádné nemá.
- **Autentizace pomocí přístupových údajů do AD**
  Ano.
- **Audit log**
  Systém obsahuje rozsáhlý audit log toho kdo, kdy a k čemu přistoupil.
- **ACL**
  Možnost nastavení ACL pro každý záznam.
- **RBAC**
  Systém podporuje model Requestor/Approver.[36]

Řešení krizové situace

- **Nouzový přístup**
  Existuje model, kdy je v produktu účet super administrátora, který má extrémně dlouhé heslo, které je uloženo v reálném sejfu a používá se v krizových situacích.
- **Možnost HA setupu**
  Ano, podpora různých schémat: aktivní-pasivní instance, aktivní-aktivní instance a aktivní- více aktivních instancí.
- **Záloha databáze**
  Virtual i hardware appliance mají vestavěné záložní funkce. Pokud klient využívá software appliance, tak mu poradí jak nastavit zálohování.

Cena pro modelovou situaci
Nepodařilo se mi získat.

Hodnocení komunikace
Nejdříve firma komunikovala celkem dobře. Na webové prezentaci mi představili produkt a ukázali mi demo produktu. Když jsem však pak chtěl vědět detailnější informace, zjišťovali tyto informace z centrály z USA a komunikace vázla. Cenovou nabídku jsem nedostal za celou dobu vůbec.

7.5 Privileged Access Manager

Možnosti práce se záznamy

- **Automatické změny hesel**
  Heslo se automaticky mění na novou hodnotu pokaždé, když uživatel skončí svojí relaci s oním heslem. Uživatelské relace mohou být nastaveny na časové omezení, po kterém systém uživatele vyhodí a změní heslo. Navíc je možnost plánovaných změn hesel (například v první den v měsíci).

- **Ověření platnosti hesla**
  Produkt může kontrolovat platnost hesel v databázi, pokud zjistí neshodu, resetuje na známou hodnotu a emailem upozorní na kolizi.

- **Složitost hesla**
  Každý spravovaný systém může mít svou vlastní politiku na složitost hesla.

- **Historie hesel**
  Všechna stará hesla jsou uložená v databázi a přístupná podle ACL.

- **Import záznamů**
  Import je možná .csv souborem, nebo vlastním importním SQL příkazem.

- **Kategorie a vyhledávání**
  Kategorie se v tomto produktu nazývají Managed Systém Policies (dále MSP). MSP jsou pojmenovány a obsahují systémy včetně privilegovaných účtů k nim. Systémy k nim mohou být přiřazeny explicitně „přiřaď SYSTEM123 k MSP1“ nebo implicitně pomocí výrazu „Všechny systémy Linuxového typu na 10.0.1.0/24 k MSP2“. Výrazy mohou být založeny na operačním systému, IP adrese, MAC adrese, názvu systému, nebo jiných metadat. MSP jsou konfigurovány operačními a přístupovými pravidly jako například: která hesla kterého účtu náhodně měnit na přidruženém systému, jak často měnit hesla, jakou nastavit politiku heslům, jakým prostředkem se může uživatel k zařízení připojit, nebo jestli může být uživateli zobrazeno heslo,... Když je cílové zařízení asociováno k nějaké MSP, je nad nimi možno vyhledávat a filtrovat.

- **Report o stáří hesel**
  V systému je přes 150 reportů, které by měli uspokojit všechny myslitelné scénáře reportování (včetně stáří hesel). Mohou být zobrazeny v systému, odeslány emailem jako pdf, csv nebo html příloha, nebo uloženy k uživateli nebo na síť.

Podporované systémy a zařízení

- **Změna/reset HP iLO karet a HP BladeSystem**
  Je využitý vlastní SSH agent, k němu je dodávaný konfigurační soubor, který je přímo nastaven pro HP iLO karty (s názvem agtxml-hpilo.cfg). Reset HP BladeSystem je prováděn stejným způsobem jako u iLO karet, pouze s jiným konfiguračním souborem.

- **Změna hesla IBM IMM karet**
  Prováděna stejným způsobem jako u HP iLO karet, s jiným konfiguračním souborem. Je zde možnost přidání ověření změny hesla a případného vrácení původního hesla.

- **Změna hesla lokálního administrátora Windows**
  Hesla k windows administrátorům jsou vždy resetována pomocí administrátora.

- **Změna/reset hesla root účtu na Linuxu**
  Root účty jsou obsluhovány vlastním SSH agentem.

API
API umožňuje prozrazování přístupových údajů přímo za běhu aplikace, zabraňuje tím ponechávání hesla v plaintextu. Systém tyto hesla, která jsou využívána k síťovým službám (DB, FTP, web, atd.), často mění. API je přístupné jako SOAP web service přes HTTPS.

Doporučené systémové a hardwarové požadavky

- **Plně podporované databázové a operační systémy**
  OS: Microsoft Windows Server 2012, 2012R2, 2008 a 2008R2
  DB: MS SQL 2008 a vyšší, Oracle 11g

- **Požadavky na software**
  Na straně serveru:

  - Microsoft IIs webový server

  Na straně klienta:

  - Webový prohlížeč podporující HTML5 (například: IE 9+, Firefox, nebo Chrome)
  - Klientské aplikace pro které produkt spravuje hesla (například pro připojení k SAPu je potřeba SAP klient)

- **Optimální hardwarové nároky pro modelovou situaci**
  Intel Xeon, 16GB RAM, 500GB konfigurované jako RAID, alespoň 1 Gigabit Ethernet NIC.
- **Možnosti nasazení**
  Virtual appliance i software appliance
- **Integrace AD**
  Integrace s AD je na více úrovních: Integrace je využívána k přidání uživatelů, jejich členství ve skupinách a informacích o nich do systému. Přidání zařízení spravovaných AD a následné nabídnutí správci systému, jestli tyto zařízení mají být systémem spravovány. Převedení správy hesel pro privilegované účty z domény (doménoví administrátoři, služby, atd.) pod systém a následná kontrola přístupu k nim.

Zabezpečení

- **Zabezpečení aplikace a komunikace klient-server**
  Komunikace mezi serverem a klientem a i mezi serverem a cílovými systémy je plně šifrovaná nativními protokoly.
- **Zabezpečení úložiště dat**
  Hitachi ID poskytuje zákazníkům informace k tomu, jak zabezpečit server, na kterém běží Hitachi ID software. Databáze je šifrována pomocí 256 bit AES šifry.
- **TPM čipy / USB tokeny**
  Jsou podporovány.
- **Zamezení zobrazení hesla uživateli**
  Hesla jsou defaultně skryta a až na výjimečné případy se doporučuje heslo vůbec uživateli neukazovat a rovnou ho připojit přes RDP, PuTTY, nebo další klienty.
- **Garance aktualizací**
  Pravidelně vychází nové verze produktu.
- **Certifikace a testy bezpečnosti**
  Common Criteria Certification (EAL-2). Četné množství organizací provádělo průnikové testy, všechny byly bez úspěchu.
- **Nahrávání relace**
  V produktu je zaveden robustní nástroj na nahrávání relací. U připojení ke vzdálené ploše se nahrává video záznam z relace, při připojení k terminálu se snímá celá uživatelova plocha a vstupy z klávesnice. Volitelně u obou připojení lze nahrávat i například záznam z web kamery počítače nebo například copy buffer.

- **Autentizace pomocí přístupových údajů do AD**
  Ano, je zde také možnost předání hesla k účtu z AD do produktu přes Kerberos autentizaci.

- **Audit log**
  Systém loguje všechny kroky, které uživatel podnikne, včetně pokusů k přístupu k cílovým zařízením ke kterým nemá práva a dokonce i vše co uživatel vyhledával.

- **ACL**
  Systém kontroluje, co všechno uživatel může vidět a dělat pomocí ACL. ACL mohou být přiřazeny explicitně k uživatelům, nebo implicitně přiřazeny uživatelům podle členství ve skupinách v AD. V systému jsou 3 skupiny ACL práv: První definuje to, co může uživatel dělat v rámci produktu samotného, druhá definuje, co může uživatel upravit na svém profilu a na profilech ostatních uživatelů a třetí definuje ke kterým systémům a spravovaným účtům má uživatel přístup.

- **RBAC**
  Produkt umožňuje tvorbu rolí a jejich následné přiřazování uživatelům a následné využití těchto rolí k přístupu k různým prvkům v systému. Firemní pravidla (jako například Segragation of Duties) mezi různými uživateli také pomocí rolí a skupin.

Řešení krizové situace

- **Nouzový přístup**
  Tato funkcionalita je možná, ale zákazník musí nadefinovat, ke kterým záznamům bude při tomto scénáři přístup a zda musí někdo aktivaci tohoto scénáře schválit.

- **Možnost HA setupu**
  Ano, produkt podporuje load balancing (vyvažování zátěže) a replikaci dat mezi více fyzických serverů. Jakákoliv aktualizovaná data jsou automaticky replikovaná v reálném čase přes šifrované spojení do všech ostatních instancí.

- **Záloha databáze**
  Vzhledem k tomu, že hesla se mění každou minutou, tak není v produktu implementována žádná funkce, která by se o backup přímo starala. Zálohu databáze je možné nakonfigurovat přes standardní SQL procedury na SQL serveru.

Cena pro modelovou situaci
Produkt je licencován podle toho, kolik je jím spravováno záznamů. Za každý tento záznam se platí jedna tzv. HiDS Privileged Access Manager Systém

Licene (my jich máme dohromady 9 100). Navíc se platí ještě jedna licence za serverovou část produktu tzv. HiDS Privileged Access Manager Vault, tu máme jednu. **Katalogove ceny v EUR jsou**:

- 1x Licence HiDS Privileged Access Manager Vault = 44 925 EUR (Support na 12 měsíců pro tuto licenci = 4 717 EUR)
- 1x Licence HiDS Privileged Access Manager System License = 30,24 EUR (Support na 12 měsíců pro tuto licenci = 3,12 EUR)

Celková katalogová cena je tedy jednorázově 320 109 EUR a 33 109 EUR za každý rok podpory. Z těchto katalogových cen pak budou nabídnuty projektové ceny.

Hodnocení komunikace
Veškerá komunikace byla nadmíru v pořádku, zprostředkována přes českého zástupce jiného oddělení firmy Hitachi. Nicméně všechny dotazy byly zodpovězeny do 1, maximálně 2 dnů. Přes sjednanou webovou konferenci mi byl produkt představen přímo týmem z Kanady, kde je ústředí firmy.

7.6 Privileged Password Manager

Možnosti práce se záznamy

- **Automatické změny hesel**
  Uživatel si může vyžádat heslo vždy na určený časový rámec a po skončení tohoto rámce se heslo změní. Lze též nastavit plánované změny hesel.
- **Ověření platnosti hesla**
  Ano, je zde možnost nastavení pravidelných kontrol na hesla, kdy produkt zkontroluje, jestli se hesla z cílového zařízení/systému a z databáze shodují a v případě rozdílu je produkt resetuje. (je-li to možné)
- **Složitost hesla**
  Produkt podporuje nastavení politik na složitost hesla, tyto politiky se však nedají importovat a musí se v produktu nastavit ručně. Poté se dají přiřazovat k záznamům a skupinám.
- **Historie hesel**
  Historie všech hesel může být uchovávána.
- **Import záznamů**
  Je možný přes .csv, nebo .xls soubor.

- **Kategorie a vyhledávání**
  Záznamy mohou být slučovány do skupin s možností vyhledávání a filtrování pro jednotlivé skupiny/uživatele.

- **Report o stáří hesel**
  Možnost různých reportů, obzvláště reportů zaměřených na hesla. Report o stáří hesel je součástí produktu.

Podporované systémy a zařízení

- **Změna/reset HP iLO karet a HP BladeSystem**
  Možná změna hesla přes SSH skript.

- **Změna hesla IBM IMM karet**
  Stejně jako HP zařízení změna hesla možná přes SSH skript.

- **Změna hesla lokálního administrátora Windows**
  Produkt podporuje i reset i změnu hesla. Defaultně je prováděn reset, pokud je však u Windows záznamu příznak, že je třeba heslo změnit, produkt použije stávající heslo ke kýžené změně.

- **Změna/reset hesla root účtu na Linuxu**
  Ano pomocí SSH skriptu.

API

Produkt disponuje s CLI a API přístupným z C++, Java, .NET a Perl. Připojení je přes SSH s DSS výměnou klíče. Podpora přístupu na základě rolí pro CLI a API. U uživatelů je pak třeba nastavit, který bude přístupný pro CLI a API, je možné přidat uživatele, kteří budou mít přístup pouze přes API a CLI. Defaultně lze skrze API a CLI zažádat o přístup k heslu, ale s administrátorskými právy mohou tyto žádosti i schvalovat a vykonávat administrativní úkoly jako například editaci záznamů, spouštění resetů hesel, přidávání a mazání záznamů.

Doporučené systémové a hardwarové požadavky

- **Plně podporované databázové a operační systémy**
  Produkt je dodáván na hardended Microsoft Windows Server 2008R2 s hardended MS SQL Server 2008R2.

- **Požadavky na software**
  Uživatelé přistupují k produktu přes webového klienta. Potřebují tedy prohlížeč podporující HTML5 (tedy IE 9+, nebo aktuální verzi Firefoxu, Safari, Opery, nebo Chrome).

- **Optimální hardwarové nároky pro modelovou situaci**
  Produkt je dodávaný jako hardware appliance, konfigurace se bude lišit podle toho, jestli bude vyžadováno HA, nebo DR.

- **Možnosti nasazení**
  Pouze hardended hardware appliance.

- **Integrace AD**
  Integrace s AD umožňuje import uživatelů a systémů (počítačů) a jejich provázání k příslušným šablonám. Produkt však neimportuje skupiny, ty je možné importovat pomocí dávkového souboru, nikoliv však pomocí integrace s AD.

Zabezpečení

- **Zabezpečení aplikace a komunikace klient-server**
  Spojení klient server je přes HTTPS.

- **Zabezpečení úložiště dat**
  Hardended stroj se šifrovaným diskem (Bitlocker), databáze je šifrovaná 256 bit AES šifrou.

- **TPM čipy / USB tokeny**
  Produkt nepodporuje.

- **Zamezení zobrazení hesla uživateli**
  Heslo je defaultně skryto, produkt nabízí navázání relace přímo přes RDP/SSH klienta, tím pádem nemusí být heslo zobrazeno vůbec.

- **Garance aktualizací**
  Aktualizace si nejprve každý zákazník vyzkouší na testovacím rozhraní (které je součástí každé instalace) a teprve když je otestovaná funkčnost s konkrétní instalací je možné nasadit aktualizace do produkce. Každá instalace má vestavěnou možnost pro zálohování a obnovení celkového produktu.

- **Certifikace a testy bezpečnosti**
  ISO 27001 certifikace.[38]

- **Nahrávání relace**
  Nahrávání relací je do vlastního formátu, který je kompresován tak, že hodina záznamu zabírá přibližně 10MB místa na disku.

- **Autentizace pomocí přístupových údajů do AD**
  Je možná.

- **Audit log**
  Kompletní audit log je součástí produktu.

- **ACL**
  Je možné nakonfigurovat při individuálním nastavování produktu.

- **RBAC**
  V produktu není implementovaný přímo RBAC model, ale spíše model který se stará o kontrolu přístupu (uživatel, uživatel nebo povolení, členství ve skupině, povolení). Tento model je granuálnější a dá se pomocí něj dosáhnout use casů, které RBAC model plně nepokývá. (Práva pomocí uživatelů, skupin, kolekcí, atd. . .)

Řešení krizové situace

- **Nouzový přístup**
  V produktu jsou i uživatelé, kteří mají speciální práva. Musí sice projít procesem vyžádání hesla, ale tato žádost bude automaticky schválena a zaznamenána v logu. Tento přístup bude označen pro reportování.

- **Možnost HA setupu**
  Více souběžně běžících instancí produktu může být nasazeno k dosažení HA.

- **Záloha databáze**
  V produktu je zabudovaná backup-restore procedura, která zazálohuje všechna nastavení, záznamy, politiky atd.. Avšak musí být spuštěna, není zde automatická záloha.

Cena pro modelovou situaci
Složení ceny pro tento produkt je složitější, protože zahrnuje i hardware, na kterém server poběží, dále pak hardware pro distribuci zátěže, licenci jádra programu, licenci správce relací a licenci pro správce identit. Detailněji popisuje tabulka 7.2 .

Hodnocení komunikace
Zprvu se zdálo, že Dell vůbec nekomunikuje, pouze jeho systém na podporu poslal potvrzení přijetí dotazů. Asi 3 týdny poté mi volal zástupce české pobočky, že jeho kolegům z USA neodpovídám, jestli mám další dotazy. Z nějakého důvodu se ztrácely emaily. Od té doby jsem komunikoval přes českého zástupce a komunikace byla bez problému. Prodejce navíc na svých webových stránkách nabízí možnost RDP připojení na terminál, kde je plná verze produktu k vyzkoušení.

Popis produktu	**Cena(EUR)**
Standard Appliance HW	7 190,40
Distributed Processing Appliance HW	7 454,00
Privileged Password Management Lincense + 24/7 Maintenance	83 400,00
Privileged Session Management License +24/7 Maintenance	34 400,00
Privilege Account Management Module License +24/7 Maintanance	24 044,00
Celkem	**156 488,40**

Tabulka 7.2: Složení ceny - Privileged Password Manager

7.7 Secret Server

Možnosti práce se záznamy

- **Automatické změny hesel**
  Je možná změna hesla po ukončení RDP relace, kdy uživatel zaškrtne pomocí check boxu konec své aktivity, nebo automatická periodická změna hesla.

- **Ověření platnosti hesla**
  V produktu je takzvaná heartbeat funkce, která ověřuje, zda jsou záznamy v databázi validní.

- **Složitost hesla**
  Lze nastavit.

- **Historie hesel**
  Produkt defaultně uchovává historii hesel.

- **Import záznamů**
  Import záznamů je možný přes .csv, nebo .xml soubor.

- **Kategorie a vyhledávání**
  Ano, navíc produkt nabízí možnost tzv. oblíbených záznamů, které se pak zobrazují na úvodní stránce.

- **Report o stáří hesel**
  Produkt obsahuje report o stáří hesel a také nástroj na tvorbu vlastních reportů a jejich následné sdílení s dalšími uživateli.

Podporované systémy a zařízení

- **Změna/reset HP iLO karet a HP BladeSystem**
  Reset je prováděn pomocí SSH skriptu. Out-of-box podpora pouze pro HP iLO 2,3 a 4, ale pro všechny BladeSystemy.

- **Změna hesla IBM IMM karet**
  Změnu hesla je možno provést pomocí SSH skriptu.

- **Změna hesla lokálního administrátora Windows**
  Možný je pouze reset.

- **Změna/reset hesla root účtu na Linuxu**
  Změna hesla pomocí SSH skriptu.

API
API je přístupné jako webová služba, přes kterou se lze přihlásit k produktu, vyhledávat v záznamech, ukládat nové záznamy a označovat záznamy jako oblíbené.

Doporučené systémové a hardwarové požadavky

- **Plně podporované databázové a operační systémy**
  OS: Od verze 8.8 končí podpora Windows Server 2008, dále bude podporovaný pouze Windows Server 2008Rx/2012/2012R2.
  DB: Microsoft SQL Server 2005/2008/2008 R2/2012/2014

- **Požadavky na software**
  Na straně serveru:
  - Microsoft Internet Information Services 7, nebo 8
  - Microsoft .NET Framework 4.5.2

  Na straně klienta:
  - nutný pouze HTML prohlížeč (IE7 a vyšší/Chrome/Firefox)

- **Optimální hardwarové nároky pro modelovou situaci**
  Čtyř jádrový 2GHz procesor, 8GB RAM, 2GB místa na disku pro databázi plus 10MB za 1uživatele za rok a 500 MB pro webový server. Tyto požadavky nezahrnují prostor na nahrávání relací.

- **Možnosti nasazení**
  Software appliance.

- **Integrace AD**
  Z AD lze importovat pouze uživatele a jejich členství ve skupinách. Počítače už nikoliv.

Zabezpečení

- **Zabezpečení aplikace a komunikace klient-server**
  Komunikace mezi klientem a serverem je šifrovaná pomocí SSL, komunikace mezi databází a serverovou aplikací může být také šifrovaná pomocí SSL, to však není nutné, protože data jsou šifrována pomocí 256 bit AES šifry hned v aplikaci.

- **Zabezpečení úložiště dat**
  Zabezpečení úložiště dat je v režii zákazníka, prodejce však poskytuje manuál k tomu, jak nejlépe zabezpečit server, kde produkt běží.

- **TPM čipy / USB tokeny**
  Podpora HSM zařízení, tato možnost je však zpoplatněna.

- **Zamezení zobrazení hesla uživateli**
  Možnost přímého připojení uživatele k cílovému zařízení bez zobrazení hesla.

- **Garance aktualizací**
  Aktualizování serveru a produktu je zodpovědnost zákazníka. Aktualizace vycházejí pravidelně, všechny jsou zaznamenány v release notes na webových stránkách.

- **Certifikace a testy bezpečnosti**
  Produkt nemá žádné certifikace na bezpečnost, je však používán vojenskými, vládními, akademickými, bankovními a soukromými organizacemi po celém světě. (jmenovitě jsem ovšem žádné nezískal) Firma tvrdí, že zabezpečení je proces, nikoliv produkt, proto poskytuje svým zákazníkům rady jak svojí instalaci produktu zabezpečit a je schopná reagovat na klientské požadavky.

- **Nahrávání relace**
  Nahrávání relací je součástí produktu. Při rozlišení 1024 x 768px bude podle aktivity uživatele velikost záznamu mezi 0,1mbit/s a 1mbit/s. Navíc administrátoři produktu mohou nahlížet v živém náhledu na relace spuštěné přímo přes správce relací z produktu a případně spojení vzdáleně ukončit.

- **Autentizace pomocí přístupových údajů do AD**
  Ano.

- **Audit log**
  Možné nahlížet buď to podle záznamu, nebo podle uživatele.

- **ACL**
  Ano na úrovni záznamů i složek.

- **RBAC**
  Ano.

Řešení krizové situace

- **Nouzový přístup**
  Role zvaná ultimate admin je v produktu, lze nastavit, aby při použití této role přišlo emailové upozornění, veškeré akce ultimate administrátora jsou vedené v audit logu. Lze také nastavit, aby použití této role museli schválit dva další uživatelé.

- **Možnost HA setupu**
  HA setup není podporován. Aplikace se vždy připojuje pouze k jedné databázi a není přípustná ani distribuovaná databáze, nebo třeba režim, kdy by se pouze četlo z replikované databáze.

- **Záloha databáze**
  V produktu je několik řešení na disaster recovery záloh jak pro aplikační, tak pro databázovou část.

Cena pro modelovou situaci
Produkt je licencovaný na základě funkcionalit, které zákazník vyžaduje a počtu přistupujících uživatelů. Pro naší modelovou situaci by stačila professional licence. Rozdíly a výpis funkcionalit pro jednotlivé licence lze vyčíst na stránkách produktu. Tabulka cen jednotlivých edicí produktu pro 150 uživatelů je v tabulce 7.3 .

Název edice	**Přibližná cena**
Professional	15 000 USD
Enterprise	60 000 USD
Enterprise Plus	120 000 USD

Tabulka 7.3: Ceny různch edic - Secret Server

Volitelně pak 22 % z fixní části licence za technickou podporu a aktualizace na jeden rok.

Hodnocení komunikace
Komunikace probíhala v pořádku. Trvalo delší dobu (řádově dny), když jsem se ptal na složitější technické záležitosti, které nelze vyčíst ze stránek produktu a místo vyžadovaného popisu technologií se pouze vrátila odpověď ano/ne, a to i při urgenci o detailní popis.

Kapitola 8

Shrnutí

V této kapitole je zobrazen přehled shrnutí zjištěných informací o produktech v podobě tabulek. Nicméně údaje, které se nedají zjednodušit na pouhé „ANO/NE“, zde nejsou uvedeny. První tabulka je přehled finanční náročnosti produktů pro modelovou situaci8.1, druhá přehled možností práce se záznamy a podporovaných zařízení/systémů 8.2, a třetí přehled možností zabezbpečení a řešení krizových situací 8.3.

Název produktu	Cena
Device 42	$ 14 999*
Enterprise Random Password Manager	$ 348 900
Password Manager Pro	$ 29 988
Password Safe	Nepodařilo se získat
Privileged Acess Manager	$ 355 737**
Privileged Password Manager	$ 173 905**
Secret Server	$ 15 000
*) Cena na jeden rok *) Ceny byly přepočteny z EUR dne 30. 4. 2015 podle kurzu ČNB a zaokrouhleny nahoru, aby neobsahovaly desetinná čísla.	

Tabulka 8.1: Srovnání finanční náročnosti produktů

	Device 42	Enterprise Random Password Manager	Password Manager Pro	Password Safe	Privileged Access Manager	Privileged Password Manager	Secret Server
Automatické změny hesel		*	*	*	*	*	*
Ověření platnosti hesla		*	*	*	*	*	*
Složitost hesla		*	*	*	*	*	*
Historie hesel	*	*	*		*	*	*
Import záznamů	*	*	*	*	*	*	*
Kategorie a vyhledávání	*	*	*	*	*	*	*
Report o stáří hesel	*	*	*	*	*	*	*
Reset hesla HP iLO / HP Blade Enclosure		*	*	*	*	*	*
Změna hesla IBM IMM		*	*	*	*	*	*
Reset hesla Windows lokálního administrátora		*	*	*	*	*	*
Změna hesla Windows lokálního administrátora		*				*	
Změna hesla root účtu na Linux stroji		*	*	*	*	*	*

Tabulka 8.2: Srovnání možností práce se záznamy

	Device 42	Enterprise Random Password Manager	Password Manager Pro	Password Safe	Privileged Access Manager	Privileged Password Manager	Secret Server
TPM/USB pro HW šifrování		*			*		*
TPM/USB pro uložení hashe		*	*		*		*
Zamezení zobrazení hesla uživateli		*	*	*	*	*	*
Nahrávání relace		*	*	*	*	*	*
Autentizace pomocí přístupových údajů do AD	*	*	*	*	*	*	*
Audit log	*	*	*	*	*	*	*
ACL	*	*	*	*	*	*	*
RBAC	*	*	*	*	*		*
Nouzový přístup		*	*	*	*	*	*
Možnost HA setupu		*	*	*	*	*	
Záloha databáze	*	*		*		*	*

Tabulka 8.3: Srovnání zabezpečení a možností řešení krizových situací

Kapitola 9

Eliminace nevyhovujících produktů

Jak lze vyčíst z tabulek z minulé kapitoly, funkce všech popisovaných produktů jsou více méně stejné, přesto ne všechny produkty jsou vhodným řešením pro náš případ.
V této kapitole se budu věnovat produktům, které nejsou vhodné pro závěrečné testování. Popíšu důvody, proč nevyhovují, a zároveň vypíchnu jejich silné stránky, které by mohly být pro jiné prostředí rozhodujícím parametrem, proč právě ten produkt zvolit.

9.1 Device42

Tento produkt nesplňuje základní funkční požadavky, neumožňuje totiž automatickou změnu hesel u zařízení, které spravuje, přesto, že mi to obchodní zástupce firmy zprvu sliboval. Dále je dodáván pouze jako virtual appliance, což je pro firmu DHL International Services nepřípustné.
Při důkladnějším zjišťování se ukázalo, že tato funkcionalita je dostupná pouze přes API pomocí externích skriptů, které si však musí zákazník vytvořit sám. To je však způsobeno tím, že produkt není primárně správcem hesel, ale správa hesel je pouze jednou z jeho součástí a není tolik vyvinutá. Tento produkt nabízí užitečné nástroje pro centralizovanou organizaci a dokumentaci serverů a data center.
Mezi další funkce mimo správy hesel například patří:

- **Data Center Management** - sada nástrojů na tvorbu diagramů na rozmístění racků a jejich obsahu v serverovnách, diagramy patch panelů, detailní informace o zařízeních (IP adresy, CPU, HDD, HW komponenty, URL zařízení, atd. . .), nástroj pro monitorování spotřeby a teploty jednotlivých zařízení a další.

- **Správce IP adres** – detailní rozpis IPv4 & IPv6 adres, rozsahy IP sítí a subnetů, nástroj pro automatické přiřazování IP adres novým zařízením a třeba také integrace s DNS servery.
- **Device Discovery** – odhalování zařízení v místní síti, které ještě nejsou pod správou systému, hledání virtuálních serverů a hledání síťových prvků.
- A další, které lze nalézt na stránkách produktu.

9.2 Privileged Password Manager

Hlavním důvodem pro zamítnutí tohoto produktu je, že je dodávaný pouze jako hardended hardware appliance, což je pro DHL International Services neakceptovatelné. Mají specifické požadavky na hardware, které by Dell nemusel být schopný splnit. Další důvod k zamítnutí je, že se jedná o produkt, který je z porovnávaných produktů nejdražší, což je samozřejmě dáno tím, že se nekupuje pouze software řešení, ale i hardware. Posledním důvodem zamítnutí je, že u takto nákladného produktu bychom očekávali i podporu šifrování na hardwarové úrovni pomocí TPM čipu, obzvláště když se jedná i o hardwarové řešení.
Nicméně to, že pro náš příklad je toto nevyhovující parametr neznamená, že to je mínus produktu. Pro jinou firmu, která má například rámcovou smlouvu se společností Dell, může být toto důvod proč si tento produkt zakoupit. Hardended hardware zařízení má výhodu v tom, že přichází od dodavatele optimalizované na co největší výkon, spolehlivost a kompatibilitu. Navíc do něj poskytovatel má největší možnost implementovat nejlepší praktiky zabezpečení a nemusí zveřejňovat své know-how. Výhodou tedy je, že produkt přijde z větší části již nastavený a na zákazníkovi zbývá jen dokončit individuální konfigurace (například integraci s LDAP, uživatelské účty a role) a pak přidávat spravované systémy.
Tento produkt také jako jeden z mála umí i změnu hesla Windows administrátorského účtu a tím tak zachovává provázanost administrátorských hesel s běžícími aplikacemi, které ho využívají.
Další výhodou je škálovatelnost produktu. Produkt je součástí takzvaného Indentity Manageru od Dellu, který ulehčuje IT administrátorům automatizací některých rutinních procesů, jako je například vytváření a rušení přístupových údajů do různých systémů, nebo třeba obnovu hesel zablokovaných účtů pomocí takzvaného „self service“. Tyto další moduly se však musí dokoupit.

9.3 Password Safe

Hlavním důvodem zamítnutí Password Safe byla špatná komunikace s obchodním zástupcem pro Evropu. Až do konce pracování na mé bakalářské práci jsem nedostal finanční nabídku na produkt i přesto, že mi byla mnohokrát slíbena. Dále byl problém se získáváním odpovědí. Složitější dotazy museli zástupci zjišťovat z centrály z USA a to trvalo někdy i dva týdny. Když jsem vyžádal kontakt na centrálu, nebo na osoby, které by mi mohly lépe odpovědět, nedostalo se mi odpovědi. Nemůžeme proto očekávat, že by podpora po zakoupení produktu fungovala bez problémů.
Silnou stránkou je možnost uchovávání SSH klíčů a autentizace pomocí nich. Další silnou stránkou jsou auditorské moduly pro AD (upozornění na vznik bezpečnostních děr, logování změn kdo kdy co udělal), Exchange(logování a reportování o všech změnách Exchange Server konfigurace, skupin, politik schránek, změn práv, atd.), File System (monitorování změn na důležitých prostředcích a změn bezpečnostních zásad) a SQL Server (upozornění na nevhodná/kritická nastavení, sledování změn v reálném čase).
A v neposlední řadě je velmi zajímavá vlastnost „Active Directory Bridging“, což je služba, která centralizuje autentizaci pro Unix, Linux a Mac prostředí prostřednictvím Kerberos Autentizace z AD a Single Sign-On možností do těchto platforem. Díky tomu mohou uživatelé přistupovat do Unix, Linux a Mac systémů pomocí jejich přihlašovacích údajů z AD. Navíc pokud uživatel přechází mezi systémy, nemusí znovu zadávat své přihlašovací údaje. Dále také tato vlastnost umožňuje rozšíření Group Policy na platformy, které nejsou typu Windows, čímž je možné zajistit jistou míru konzistentní nastavení v heterogenním prostředí.

9.4 Enterprise Random Passwrod Manager

Tento produkt vyhovuje všem kritériím, která zadavatel měl a byl by vhodný k dalšímu testování a srovnávání a původně jsem ho také měl zařazený mezi finalisty. Nicméně situace se změnila kvůli tomu, že zástupce firmy Lieberman Software odmítl jakoukoliv další komunikaci se studentem a že budou komunikovat pouze přímo s potencionálním klientem. Tím pádem jsem musel i tento produkt zamítnout, protože jsem nemohl nadále čerpat informace přímo od obchodního zástupce firmy, ale pouze z veřejně dostupných zdrojů.
Velmi silnou stránkou tohoto produktu je konkrétně pro náš případ práce s iLO zařízeními, kde produkt umí nejen reset hesla iLO karty, ale také vypnout/zapnout zařízení, které iLO karta spravuje a zjistit jeho stav.
Další silnou stránkou rozsáhlost správy Windows účtů a stanic. Produkt umí vylistovat všechny uživatele, kteří jsou přihlášení ke kterým systémům, a které aplikace, služby a úlohy jsou jimi spuštěny. Dále také umí jejich heslo změnit a automaticky delegovat nové hesla do aplikací, služeb a úloh, které toto heslo

využívají (jsou spuštěny pod identitou tohoto uživatele).
Za zmínku také stojí robustní nástroj na vyhledávání bezpečnostních děr a odhalování backdoor účtů, které nejsou spravovány systémem. Systém stále prohledává síť a spravované systémy a aplikace (ISS, SQL Server, Microsoft SCOM, SharePoint, Windows aplikace, a další) a případné hrozby odesílá emailem.

Kapitola 10

Závěrečné testování

Bohužel nebylo možné vytvořit testovací prostředí ve firmě DHL International Services, kde by bylo možné otestovat, zda řešení funguje správně vůči požadovanému HW. To ovšem nevadí, protože tato funkcionalita lze ošetřit definovatelným SLA a za předpokladu, že by sjednané funkcionality nebyly v praxi funkční, lze od smlouvy odstoupit.
V této kapitole se budu u každého produktu zabývat následujícími třemi oblastmi:

1. **Trial verze**
   Dostupnost trial verze, její instalace, integrace s AD, import záznamů, přidělení politik na složitost hesla, nastavení ACL a reset hesel.

2. **Technická podpora**
   Dostupnost technické podpory v ČR a její cena podle modelové situace z 6. kapitoly.

3. **Reference**
   Reference na produkt od firem, které ho využívají a jsou obdobného rozsahu firmy DHL International Services.

10.1 Popis testovacího prostředí

Celé testovací prostředí běželo pod VirtualBoxem na počítači s procesorem Intel Core i5-4460 s 16GB DDR3 RAM s operačním systémem Windows 7 Professional 64bit. Jeho součástí byli:
Microsoft Windows Server 2008 R2 Standard s DHCP serverem a ActiveDirectory doménou, ve které jsou přidáni uživatelé roztřídění podle skupin a do které jsou přidány další dva servery (Windows Server 2012 R2 Standard a druhý Windows Server 2008 R2 Standard na kterém běžel MS SQL Server 2012 Expres Edition a na který jsem instaloval testované produkty). Dva virtuální Linux stroje a to sice Debian 7.8 a Ubuntu 14.04 LTS.

10.2 Password Manager Pro

Trial verze
Trial verze produktu je volně dostupná ke stažení po registraci na jeho webových stránkách. Bylo velmi snadné produkt nainstalovat a nastavit, jelikož jeden instalátor obsahuje webový server, databázový server, službu i konzoli pro správu. Navíc mi byla poskytnuta instalační příručka, kde je vše detailně popsáno a pro případ nouze mi byla nabídnuta i technická podpora, kterou jsem nemusel využít.

Produkt je velmi intuitivní, po nastavení integrace s AD bylo možné se do webové aplikace přihlásit pomocí přihlašovacích údajů z AD. Import záznamů šel jednoduše jak přímým importem z AD, tak importem z csv souboru, taktéž fungovalo automatické skenování sítě, kterým jsem odhalil oba Linux stroje. Záznamy jsou pojmenovány jako prostředky (aneb „resources“) a lze je seskupovat do složek, na které lze jednoduše nastavit politiky na hesla, nebo ACL pro jednotlivé uživatele, nebo pro skupiny uživatelů. Reset hesel se dá snadno nastavit periodicky, nebo jednorázově pro jednotlivé prostředky, nebo složky.

Technická podpora
Přímá podpora zákazníků v ČR je zprostředkována support centry z Texasu v USA a Chennai v Indii. Poskytují telefonickou podporu 24/7 a také email podporu. Na webových stránkách je také dostupná rozsáhlá sekce s návody a manuály, nebo také fórum, kde je již mnoho dotazů vyřešených ať už zaměstnanci, nebo jinými uživateli. Roční poplatek za podporu je obsažen v částce, která se platí každoročně za údržbu. Tato částka pro náš model činní 5 998 USD.

Reference
Tento produkt je nejhojněji používán napříč velkými korporacemi včetně státních úřadů, bank, zdravotnických organizací a poskytovatelů služeb. Jejich výčet lze nalézt na stránkách produktu. Za zmínku stojí, že firma spolupracuje s firmami HP Enterprise Services, IBM Corporation a Cisco Systems Inc, kterých zařízení jsou pro naši situaci klíčová. Dostal jsem kontakt na IT manažera z HP.

10.3 Privileged Access Manager

Trial verze
Trial verze je dostupná pouze na základě podepsání licenční smlouvy, kterou jsem nechtěl podepisovat z důvodu udávání osobních údajů. Namísto toho jsem si vyžádal videokonferenci s týmem z Kanady, který mi ochotně předvedl funkcionalitu programu. Instalaci programu jsem vyčetl z manuálu, který mi byl zaslán a který není veřejně dostupný a nesmí být zveřejněn.

Samotná instalace produktu si nevytvoří vlastní databázi, tu musí IT administrátor na databázovém systému vytvořit sám, včetně databázových uživatelů a databázového schématu. Podle manuálu by měla být instalace bez problémů za předpokladu, kdy jsou splněné databázové prerekvizity.

Poté lze nastavit integraci do AD domény, ze které se do produktu importují spravované systémy, a navíc je pak možná autentizace uživatelů pomocí jejich AD přihlášení. Navíc lze nastavit více faktorovou autentizaci například pomocí USB klíčenky, nebo biometrických údajů, nebo SMS kódem a různých kombinací. Funkce programu se zdály být intuitivní. Import záznamů je samozřejmostí, stejně tak jako automatické skenování sítě a odhalování zařízení a účtů, které nejsou pod správou systému. V systému jsou zavedené tzv. „Managed System Policies“, které umožňují efektivní správu importovaných záznamů (více u popisu produktu v kapitole 6.6). Tento produkt funguje na základě modelu žadatel/schvalovatel (requestor/approver), kde přístup k heslu/účtu je podmíněn schválením jiného uživatele s patřičnými právy. Počet schvalovatelů však lze nastavit i na číslo 0, takže může hned po zažádání být přístup k záznamu schválen, ale u kritických systémů můžeme nastavit libovolné číslo potřebných schvalovatelů. Nastavení ACL a politik na hesla šlo taktéž efektivně na skupiny záznamů pomocí pravidel (například: „pro všechny Linux stroje nastav tyto oprávnění skupině lidí A“). Reset hesel na cílových zařízeních/systémech je plně automatizovaný, ovšem jeho nastavení se zdálo být poněkud složitější.

Technická podpora
Technická podpora pro všechny zákazníky je dostupná přes support portal. 1st level support je poskytován autorizovanými servisními partnery, 2nd a 3rd level support je pokryt přímo Hitachi ID Systems z Kanady.
Cena technické podpory je součástí roční částky za podporu a údržbu, která činí pro náš model 33 109 EUR.

Reference
Referenčí kontakt by byl poskytnut přímo firmě DHL International Services. Z IT sektoru jsou významní klienti například VMware a Intel. Řešení správy identit od Hitachi ID Systems je navrženo, aby bylo možné ho škálovat a

aby zvládalo robustní nasazení. Největší nasazení, které spravuje přes 150 000 systémů, běží na 12 fyzických uzlech, kde všechny jsou ve stavu master, je napojeno na 8 data center ve 4 městech napříč světem.

10.4 Secret Server

Trial verze
Přístup ke stažení trial verze produktu spolu s licenčním klíčem mi byl poskytnut přes obchodní zástupkyni pro Evropu na základě telefonátu.

Před samotnou instalací systému bylo potřeba nainstalovat a nastavit webový server (Microsoft IIS) a databázi (MS SQL Server 2012 Express), teprve poté jsem mohl nainstalovat samotný produkt. Celý proces instalace byl perfektně popsán v instalační brožuře, která mi byla zaslána.

Integrace s AD doménou byla bezproblémová včetně následné autentizace do systému pomocí přístupových údajů z AD. Import cílových zařízení/systémů je možný z AD, skenováním sítě, nebo ze souboru formátu XLS, nebo CSV. Záznamy jsou rozděleny do složek, nad kterými je možné nastavit politiky a práva pro různé skupiny uživatelů, které jsou importovány z AD, nebo definovány v systému. Zajímavá je možnost označit záznam jako oblíbený, pokud vím, že k němu přistupuji často a uvidím ho pak na domovské stránce systému. Reset hesel probíhá pomocí heartbeat funkce. Jedná se o funkci, která automaticky kontroluje, kdy kterému heslu vyprší platnost, a když se blíží doba expirace, tak ho změní. Expiraci lze nastavit na libovolnou hodnotu, a pro resetování hesla u libovolného záznamu lze expiraci vynulovat.

Technická podpora
Technická podpora stojí ročně 20 % z ceny licence, kterou zákazník zaplatil. Součástí je technická podpora 24/7 prostřednictvím emailu, telefonu, nebo vzdáleného přístupu.

Reference
Ze zákazníků, kteří produkt využívají, jsou z IT sektoru nejznámější Microsoft, at&t, CITRIX online a Adobe. Kontakty na referenční osoby z jednotlivých firem se mi bohužel nepodařilo získat.

Kapitola 11

Doporučení produktu

Jako vítězný produkt jsem vybral **Password Manager Pro** (PMP). V této kapitole se pokusím ukázat jeho přednosti do našeho prostředí.

Hlavním argumentem pro zvolení je nejlepší poměr ceny vůči funkčnosti. Cena je nízká kvůli tomu, že licencování je prováděno na základě počtu administrátorů, kteří budou do PMP přistupovat, na rozdíl od dražších produktů, jako třeba Hitachi ID Privileged Acess Manager (HiPAM), nebo Enterprise Random Password Manager (ERPM), které jsou licencovány na základě spravovaných systémů a zařízení. Cena je navíc definovaná pomocí typu licence, kterou si chceme koupit, licence jsou odstupňované, podle funkcionalit. Tím pádem pokud bychom nelpěli na A2A správě hesel, automatickém odhalování servisních účtů na Windows strojích, nebo integrací do ticketovacího systému, dá se cena ještě snížit.

Funkcionality všech srovnávaných programů byly srovnatelné (až na Device42, to ovšem je produkt spíše z jiné kategorie). Rozdíl v tom, proč jsou produkty HiPAM a ERPM podstatně dražší jsou kromě licencování i v tom, že dokážou efektivně spravovat servisní účty, které jsou napojeny na aplikace. Secret Server (SS) tuto funkcionalitu má zpoplatněnou v licenci enterprise+, která stojí okolo 120 000 USD, PMP má tuto funkcionalitu v ceně, ale není tak intuitivní a jednoduchá jako v případě HiPAM a ERPM. Další rozdíl je například v tom, že HiPAM má propracovanější bezpečnostní opatření při spojování s koncovými systémy/zařízeními. Kromě nahrávání obrazovky lze totiž nahrávat i záznam z web kamery, nebo například při využití CLI lze například zaznamenávat všechny údery do klávesnice, nebo dokonce nahrávat celou uživatelovu plochu. Dalším rozdílem v ceně je, že i ERPM i HiPAM nabízí podporu pro HW modul na HW šifrování záznamů.

Mimo ceny je argumentem pro PMP jednoduchost a intuitivnost celého produktu. Od procesu instalace, která byla jednoduchá díky tomu, že je pro-

dukt samo obsažný co se databázového a webového serveru týče, až po správu záznamů a automatickou změnu hesel, která se mi zdála taktéž podstatně jednodušší a intuitivnější v PMP oproti SS a HiPAM. Další výhodou PMP je například to, že se dá nainstalovat i na Windows i na Linux server, přičemž ostatní produkty lze instalovat pouze na Windows server.

Co se bezpečnosti týče, PMP má jako jediný dvojité šifrování záznamů v databázi nejprve na aplikační úrovni a poté na databázové úrovni. Pro ještě větší bezpečnost lze nastavit šifrování disku (například BitLocker) pro trojité šifrování. Navíc oproti SS je u PMP možné mít hash pro šifrování uložený na USB disku, který připojíme jen při instalaci a pak ho můžeme ukrýt například do fyzického trezoru.

PMP má oproti ostatním produktům tři různá API, přes které se dá produkt propojit s různými nástroji a jinými systémy.
Další výhodou PMP je, že umožňuje (na rozdíl od SS) možnost HA setupu.

Poslední značnou výhodou PMP pro náš případ je, že PMP má za klienty všechny HW společnosti, jejichž HW potřebujeme mít podporovaný. Ať už se jedná o HP (HP iLO karty, BladeSystem), nebo IBM (IMM karty), nebo Cisco (síťové prvky), můžeme předpokládat, že všechny tyto společnosti používají PMP pro správu hesel na svých zařízeních.

A v neposlední řadě, je zde volně dostupná live verze produktu přímo na jeho stránkách, eventuálně je možné vyzkoušet 30ti denní trial verzi a k ní využít plnou podporu. Dále má produkt nejlepší stránky ze všech srovnávaných, díky detailnímu popisu všech funkcionalit. Komunikaci s obchodními zástupci hodnotím také za nejlepší.

Kapitola 12

Návrh implementace delegačního modelu

12.1 Popis rolí uživatelů

Za současné situace je ve firmě nadefinováno 9 rolí support teamu, 1 role security týmu a 1 role administrátora. Support tým je rozdělen do tří týmů podle spravovaných cílových zařízení/systémů: Linux, Windows a infrastruktura. Každý z těchto tří týmů je rozdělen podle úrovně supportu (1st, 2nd a 3rd level), každá úroveň má jinou roli. 2nd a 3rd level support mají možnost heslo resetovat a zobrazit, kdežto 1st level support může heslo jenom resetovat.
Tento návrh rolí byl však pro systém, který neuměl sám resetovat hesla a tak se muselo heslo, které bylo kompromitováno (mělo příznak, že bylo zobrazeno, ale nebylo resetováno), resetovat někým na vyšší úrovni. V případě nasazení PMP není nutné mít roli přímo pro resetování, jelikož lze nastavit takzvané vrácení hesla, kdy se heslo resetuje po ukončení relace, nebo nastavení časového okna, jak dlouho je heslo platné, po skončení platnosti ho systém vyresetuje.
Navrhuji tedy následné role:

- **Application administrator** - vytváří uživatele, přiděluje jim práva, má pod správou celý systém (ne nutně všechny záznamy v něm).
- **Password administrator** – může nastavovat politiky na hesla a přidělovat práva na záznamy jednotlivým týmům.
- **Security auditor** - může si zobrazovat reporty a případná kompromitovaná hesla změnit. Může být náhradou 1st level support role z původního modelu.
- **Linux/Windows/Infrastructure password user** – může číst a resetovat hesla v Linux/Windows/Infrastructure skupině.

Přehled rolí a práv je zobrazen v tabulce 12.1 .

	Správa uživatelů	Správa záznamů	Čtení/reset hesel	Čtení reportů a audit logu
Application administrator	*	*	*	*
Password administrator		*	*	
Security auditor			*	*
Team password user			*	

Tabulka 12.1: Přehled rolí a práv

12.2 Doporučený postup instalace a nastavení

Instalace
Vzhledem k tomu, že se jedná o instalaci do prostředí, kde se využívají Microsoft technologie, doporučuji instalaci produktu na MS Windows Server (dle zvážení verze 2008R2, nebo 2012) s MS SQL databázovým backendem. Celý postup instalace včetně vytvoření a importu SSL certifikátu je detailně popsaný na stránkách produktu.[40]
Dále také doporučuji před nastavením systému nainstalovat sekundární instanci PMP a nastavení HA setupu podle detailního popisu dostupného taktéž na stránkách produktu.[41]

Nastavení
Nejprve je potřeba nastavit integraci do AD domény, kterou firma využívá. Pomocí ní importujeme do systému uživatele. Doporučuji využít autentizaci pomocí přihlašovacích údajů do AD spolu s více faktorovou autentizací, protože se jedná o systém, který pracuje s citlivými daty. Importované uživatele poté roztřídíme podle členství ve skupinách v AD na Linux team, Windows team, infrastructure team, password administrators, security auditors a application administrators do stejně pojmenovaných skupin v PMP.

Poté vytvoříme 3 resource groups do kterých naimportujeme pomocí CSV souborů záznamy z KeePassu a z in house systému. Importované záznamy roztřídíme podle typu do námi vytvořených resource groups (Linux, Windows, Infrastructure).

Dále nastavíme vlastnictví na resource groups podle členství ve skupinách. Jednotlivým týmům (Linux/Windows/Infrastructure) dáme pouze View práva na příslušné skupiny záznamů a skupinám Security, Password a Application administators dáme Manage práva na všechny resource groups.
Tímto nastavením je funkčnost programu nastavena tak, aby splňovala požadovaná bezpečnostní i funkční kritéria.

Závěr

Tato práce si kladla za cíl přinést detailní srovnání produktů, které se věnují správě hesel ve firemním prostředí a následně vybrat vhodný produkt pro firmu DHL International Services. Přestože většinou není dostatek veřejně dostupných informací o jednotlivých produktech, setkal jsem se spíše s ochotou od obchodníků, technických konzultantů a programátorů z jednotlivých firem. Díky tomu jsem mohl vypracovat tuto práci a přinést srovnání alespoň několika produktů, které jsou na trhu.

Vzhledem k tomu, že produkty jsou stále vyvíjeny, přibyl jeden produkt (o kterém vím) splňující základní funkční požadavky (viz 5. kapitola). Tento produkt jsem do srovnání již nestihl zahrnout. Práce také bohužel není úplná vzhledem k neochotě některých firem k poskytnutí informací.

I přes mnohé překážky se mi však podařilo dostatek produktů popsat, srovnat, eliminovat nevyhovující a otestovat závěrečné kandidáty, ze kterých jsem vybral a doporučil finální produkt – Password Manager Pro. Pro tento produkt jsem uvedl i doporučený postup k nasazení produktu do firmy DHL International Services.

Jelikož jsou na trhu dostupné pouze komerční řešení pro firemní správu hesel, jako možnost navazující diplomové práce vidím implementaci open-sourcového nástroje, který by umožňoval alespoň sdílení a automatickou správu hesel při dodržení vysokých bezpečnostních standardů.

Literatura

[1] ORDERLØKKEN, T. L.: NorSIS Password Survey 2012 [online]. 2012, [cit. 2015-04-30]. Dostupné z: http://passwords12.at.ifi.uio.no/NorSIS/NorSIS_Passwords12.pdf

[2] FISHER, T.: Password Manager. About Tech [online]. 2015, [cit. 2015-04-30]. Dostupné z: http://pcsupport.about.com/od/termsp/g/password-manager.htm

[3] EXCEL BEE: Excel Password Remover [online]. 2015, [cit. 2015-04-30]. Dostupné z: http://www.excelbee.com/excel-password-remover

[4] CITRIX: XenApp [online]. 2015, [cit. 2015-04-30]. Dostupné z: https://www.citrix.cz/products/xenapp/overview.html

[5] REICHL, D.: KeePass Password Safe [online]. 2015, [cit. 2015-04-30]. Dostupné z: http://keepass.info/

[6] ROBERTSON, J.; ROBERTSON, S.: *Mastering the requirements process*. Addison-Wesley Professional, ACM Press, 11 vydání, 1999, ISBN 02-013-6046-2.

[7] CARNEGIE MELLON UNIVERSITY: Windows Administrator Accounts Guideline [online]. 2015, [cit. 2015-05-15]. Dostupné z: https://www.cmu.edu/iso/governance/guidelines/win-admin.html

[8] THE LINUX INFORMATION PROJECT: Root Definition [online]. 2005, [cit. 2015-05-15]. Dostupné z: http://www.linfo.org/root.html

[9] HEWLET-PACKARD: HP Integrity Integrated Lights-Out (iLO): Manage all HP servers, from anywhere [online]. 2015, [cit. 2015-05-20]. Dostupné z: http://www8.hp.com/us/en/products/servers/ilo/integrated-lights-out.html

[10] HEWLET-PACKARD: HP BladeSystem: One infrastructure with one management platform. That's the Power of One [online]. 2015, [cit. 2015-05-20]. Dostupné z: http://www8.hp.com/us/en/products/servers/bladesystem/index.html

[11] HEWLET-PACKARD: HP OneView: Take control of HP server, storage, and networking with our latest infrastructure management software [online]. 2015, [cit. 2015-05-20]. Dostupné z: http://www8.hp.com/cz/cs/business-solutions/converged-systems/oneview.html

[12] CISCO SYSTEMS: Integrated Management Module User Guide [online]. 2011, [cit. 2015-05-20]. Dostupné z: http://www.cisco.com/c/en/us/td/docs/wireless/module/imm/user/guide/imm_guide.pdf

[13] GARTNER: Gartner Clarifies the Definition of the Term 'Enterprise Architecture'. In: Gartner Research G00156559 [online]. 2008, [cit. 2015-05-15]. Dostupné z: https://online.ist.psu.edu/sites/gettingstarted/files/gartnerclarifies.pdf

[14] MICROSOFT: *.NET application architecture guide. 2nd ed.* Redmond, Wash.: Microsoft, xxxi vydání, 2009, ISBN 07-356-2710-X.

[15] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY: ADVANCED ENCRYPTION STANDARD (AES). Federal Information Processing Standards Publication, 197 [online]. 2001, [cit. 2015-05-15]. Dostupné z: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[16] ARORA, Mohit: How secure is AES against brute force attacks? EE Times: Connecting the Global Elcectronics Community [online]. 2012, [cit. 2015-05-20]. Dostupné z: http://www.eetimes.com/document.asp?doc_id=1279619

[17] CYBERARK: Enterprise Password Vault: Security for the Heart of the Enterprise [online]. 2015, [cit. 2015-05-30]. Dostupné z: http://www.cyberark.com/products/privileged-account-security-solution/enterprise-password-vault/

[18] FICHER INTERNATIONAL: Privileged Access Management: Take back the keys to the kingdom [online]. 2015, [cit. 2015-05-30]. Dostupné z: http://www.fischerinternational.com/competencies/privileged_account_management.htm

[19] CLICKSTUDIOS: Privileged Password Manager for all size Enterprises [online]. 2015, [cit. 2015-05-30]. Dostupné z: http://www.clickstudios.com.au/

[20] DEVICE42: Enterprise Password Management Software: Features tour [online]. 2015, [cit. 2015-05-30]. Dostupné z: http://www.device42.com/features/enterprise-password-management/

[21] LIEBERMAN SOFTWARE: Enterprise Random Password Manager: Owerview. Privilege Management from Lieberman Software [online]. 2015, [cit. 2015-05-30]. Dostupné z: http://www.liebsoft.com/Enterprise_Random_Password_Manager/

[22] MANAGEENGINE: Privileged Password Manager for Enterprises: Secure Password Vault Software [online]. 2015, [cit. 2015-05-30]. Dostupné z: https://www.manageengine.com/products/passwordmanagerpro/

[23] BEYOND TRUST: PowerBroker Password Safe: Privileged Password Management Software: Password Safe [online]. 2015, [cit. 2015-05-30]. Dostupné z: http://www.beyondtrust.com/Products/PowerBrokerPasswordSafe/

[24] HITACHI ID: Hitachi ID Privileged Access Manager. Hitachi ID Systems, Inc. [online]. 2015, [cit. 2015-05-30]. Dostupné z: http://hitachi-id.com/privileged-access-manager/

[25] DELL SOFTWARE: Privileged Password Manager: Automate and secure the use of privileged account credentials [online]. 2015, [cit. 2015-05-30]. Dostupné z: http://software.dell.com/products/privileged-password-manager/

[26] THYOTIC: Privileged Account Management: Enterprise Password Management for IT Admins. Thyotic: Enterprise Password Management Software [online]. 2015, [cit. 2015-05-30]. Dostupné z: http://thycotic.com/products/secret-server/

[27] PCMAG DIGITAL GROUP: Definition of API. PCMag [online]. 2015, [cit. 2015-04-25]. Dostupné z: http://www.pcmag.com/encyclopedia/term/37856/api

[28] VMWARE, INC.: VMware [online]. 2015, [cit. 2015-04-25]. Dostupné z: http://www.vmware.com/cz

[29] ORACLE: VirtualBox [online]. 2015, [cit. 2015-04-25]. Dostupné z: https://www.virtualbox.org/

[30] PCMAG DIGITAL GROUP: Definition of virtual appliance. PCMag [online]. 2015, [cit. 2015-04-25]. Dostupné z: http://www.pcmag.com/encyclopedia/term/58704/virtual-appliance

[31] PCMAG DIGITAL GROUP: Definition of hardware appliance. PCMag [online]. 2015, [cit. 2015-04-25]. Dostupné z: http://www.pcmag.com/encyclopedia/term/58536/hardware-appliance

[32] DESMOND, B.; RICHARDS, J.; ALLEN, R.; aj.: *Active Directory: Designing, Deploying, and Running Active Directory*. O'Reilly Media, 2013, ISBN 978-1-449-32002-7.

[33] ANDREWS, J.: *A+ Guide to Managing & Maintaining Your PC*. Course Technology, 8 vydání, 2014, ISBN 11-331-3508-0.

[34] CIAMPA, M.: *Security+ Guide to Network Security Fundamentals (Cyber Security)*. Cengage Learning, třetí vydání, 2008, ISBN 14-283-4066-1.

[35] FERRAIOLO, D. F.; KUHN, D. R.; CHANDRAMOULI, R.: *Role-Based Access Control*. Artech House, 2003, ISBN 15-805-3370-1.

[36] HOFSTETTER, J. a R. DIJKMAN: *Business process model and notation third International Workshop*. proceedings. Berlin, Heidelberg: Springer-Verlag GmbH Berlin Heidelberg, 2011, ISBN 978-364-2251-603.

[37] MICROSOFT: AD DS: Fine-Grained Password Policies [online]. 2015, [cit. 2015-05-25]. Dostupné z: https://technet.microsoft.com/en-us/library/cc770394(v=ws.10).aspx

[38] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION: ISO/IEC 27001 - Information security management [online]. 2013, [cit. 2015-05-25]. Dostupné z: http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

[39] SEIBERT MEDIA: How secure is Password Manager Pro? [online]. 2015, [cit. 2015-05-17]. Dostupné z: https://www.seibert.biz/pmpsecurity

[40] MANAGEENIGE: Installation & Getting Started [online]. 2015, [cit. 2015-06-15]. Dostupné z: https://www.manageengine.com/products/passwordmanagerpro/help/installation.html

[41] MANAGEENIGE: High Availability (with MS SQL server) [online]. 2015, [cit. 2015-06-15]. Dostupné z: https://www.manageengine.com/products/passwordmanagerpro/help/high-availability-mssql.html

Příloha **A**

Seznam použitých zkratek

ACL Access control list

AD Active Directory

AES Advanced Encryption Standard

API Application Program Interface

CSV Comma-separated Values

DB Databáze

DLL Dynamic-link library

ERPM Enterprise Random Password Manager

FTP File Transfer Protocol

HA High Availibility

HDD Hard Disk Drive

HiPAM Hitachi Privileged Access Manager

HSM Hardware Security Module

HTML Hyper Text Markup Language

HTTPS Hyper Text Transfer Protocol Secure

HW Hardware

IE Internet Explorer

IIS Internet Information Services

IPMI Inteligen Platform Management Interface

ISO International Organization for Standartization

IT Informační Technologie

LDAP Lightweight Access Protocol

NIC Network Interface Card

NIST National Institut of Standards and Technologies

OS Operační systém

PKCS Public Key Cryptographic Standards

PMP Password Manager Pro

RAM Random Access Memory

RBAC Role-Based Acess Control

SLA Service-Level Agreement

SOAP Simple Object Access Protocol

SQL Structured Query Language

SS Secret Server

SSH Secure Shell

SSL/TLS Secure Socets Layer/Transport Layer Security

SSO Single Sign On

TPM Trusted Platform Module

USA United States of America

vCPU Virtual Central Processing Unit

Příloha **B**

Produkty nesplňující základní požadavky

Tato příloha obsahuje seznam zamítnutých produktů z důvodu nesplnění základních funkčních a nefunkčních požadavků specifikovaných ve 4. kapitole. Veškeré uvedené odkazy jsou platné k datu 10.6.2015.

AES Password Manager `http://www.aespasswordmanager.com/`

Aurora Password Manager `http://www.animabilis.com/`

Avatier Password Station `http://www.avatier.com/products/identity-management/password-management/password-station/`

CloudEntr Password Manager `http://www.cloudentr.com/product/password-manager/`

Crypt-o `http://www.soft-o.com/products/crypt-o.html`

Duo Security `https://www.duosecurity.com/`

Enterprise Password Management Vault `http://www.elitser-me.com/products/log-analysis-and-security/enterprise-password-management-vault/`

Enterprise Password Vault `http://www.cyberark.com/products/privileged-account-security-solution/enterprise-password-vault/`

FastPass Enterprise Password Manager `http://www.fastpasscorp.com/password-reset/enterprise-password-manager.aspx`

Fischer Identity `http://www.fischerinternational.com/`

KeyPass Enterprise `http://www.dobysoft.com/products/keypass/enterprise.html`

Last Pass https://lastpass.com/

My1Login https://www.my1login.com/

Network Password Manager - Enterprise Password Management http://usefulsoft.com/network-password-manager/

Passpack Password Manager https://www.passpack.com/

Password Safe Enterprise Edition http://www.passwordsafe.de/en/products/business/enterprise-edition.html

Password Vault Manager http://passwordvaultmanager.com/

PasswordCourier http://www.courion.com/products/passwordcourier-password-management

Passwordstate 7 http://www.clickstudios.com.au/

Plesant Password Server ttp://pleasantsolutions.com/PasswordServer/Features.aspx

Roboform Enterprise http://enterprise.roboform.com/

SFLvault http://www.sflvault.org/

Splash ID Safe for Teams https://splashid.com/teams.php

Team password manager http://teampasswordmanager.com/

Teampass http://www.teampass.net/

Vaultier Enterprise Edition http://www.vaultier.org/products/

Web password safe https://code.google.com/p/webpasswordsafe/

Příloha C

Obsah přiloženého CD

- `readme.txt` ..... stručný popis obsahu CD
- `src`
  - `thesis` ..... zdrojová forma práce ve formátu LaTeX
- `text` ..... text práce
  - `thesis.pdf` ..... text práce ve formátu PDF