ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

PROVOZNĚ EKONOMICKÁ FAKULTA

KATEDRA INFORMAČNÍCH TECHNOLOGIÍ

DIPLOMOVÁ PRÁCE

ZABEZPEČENÍ IT INFRASTRUKTURY A ZÁLOHA DAT V MALÝCH A STŘEDNÍCH PODNICÍCH

(Bc.) Radek ČERŇANSKÝ

vedoucí: Mgr. Ing. Vladimír Očenášek

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Katedra informačních technologií

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Radek Čerňanský

Veřejná správa a regionální rozvoj

Název práce

Zabezpečení IT infrastruktury a záloha dat v malých a středních podnicích

Název anglicky

IT Infrastructure Security and data backup in small and medium-sized enterprises

---

Cíle práce

1) analýza současného stavu zabezpečení perimetru sítí LAN a WLAN
2) analýza současné formy zálohování podnikových dat
3) návrhy nového zabezpečení podnikové IT infrastruktury
4) návrhy nového systému zálohy dat
5) kalkulace všech zhodnocených návrhů

Metodika

Diplomová práce je členěna do dvou dílčích částí, teoretické a praktické. V teoretické části je na základě rešerší odborné literatury, odborně zaměřených tiskovin a elektronických zdrojů shrnut základní teoretický aparát. V praktické části je analyzován současný stav zabezpečení firemní infrastruktury ve společnosti, dále je analyzován současný systém archivace a zálohování dat. Výsledky těchto analýz, společně s vyhodnocením rizik jsou výchozím bodem pro návrhy a zlepšení v oblasti bezpečnosti, systému záloh a archivace podnikových dat. Nově navržená koncepce je kalkulována dle aktuálních tržních cen. Očekávaným přínosem pro zkoumaný podnik jsou: analýzy současného stavu, identifikace a vyhodnocení potenciálních rizik, návrh nové bezpečnostní koncepce, kalkulace všech doporučených řešení a opatření.

Doporučený rozsah práce

60 – 80 stran

Klíčová slova

IT infrastruktura, síťová architektura, bezpečnost, záloha dat, archivace

---

Doporučené zdroje informací

Bejtlich R.: The Practice of Network Security Monitoring, No Starch Press, 2013, ISBN 978-1-59327-509-9
Keršláger M., Horák J.: Počítačové sítě, Cpress 2011, ISBN 978-80-251-3176-3
Sosinsky B.: Mistrovství počítačové sítě, Cpress 2010, ISBN 9788025133637

Předběžný termín obhajoby

2015/06 (červen)

Vedoucí práce

Mgr. Ing. Vladimír Očenášek

Elektronicky schváleno dne 11. 3. 2015

Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 11. 3. 2015

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 23. 03. 2015

Čestné prohlášení

Tímto čestně prohlašuji, že jsem diplomovou práci na téma *„Zabezpečení IT infrastruktury a záloha dat v malých a středních podnicích“* zpracovával samostatně, pouze s použitím uvedené literatury, metod a zdrojů.

V Praze, dne 25. března 2015 …….

Poděkování

Tímto bych rád poděkoval Mgr. Ing Vladimíru Očenáškovi za přínosné rady, náměty a připomínky, které dopomohly ke zdárnému dokončení práce. Jednateli firmy Ašské služby s.r.o., panu Karlu Školovi, za poskytnutou vnitropodnikovou dokumentaci a přístup k infrastruktuře podniku. Jednateli firmy Ašské lesy, s.r.o., panu Ing. Jiřímu Červenkovi, za přístup k infrastruktuře podniku.

Zabezpečení IT infrastruktury a záloha dat v malých a středních podnicích

Souhrn: Diplomová práce je zaměřena na zabezpečení firemní infrastruktury a zálohu dat v malých a středně velkých podnicích. Teoretická část je rešerší odborné literatury a elektronických zdrojů. V praktické části autor analyzuje současný stav zabezpečení firemní IT infrastruktury malého a středně velkého podniku, včetně systémů pro zálohu dat. Analýza je provedena formou bezpečnostního auditu, který je cílený na komplexní přehled, reflektující současný stav zabezpečení a zálohy dat. Výsledky auditu jsou východiskem pro formulaci nápravných opatření a doporučení, která zajistí vyšší úroveň zabezpečení infrastruktury a zajistí cenná podniková data. Autor předkládá bezpečnostní řešení v několika variantách a jednotlivé návrhy kalkuluje dle aktuálních tržních cen.

Klíčová slova: IT infrastruktura, síťová architektura, bezpečnost, záloha dat, archivace

IT Infrastructure Security and Data Backup in small and medium-sized enterprises

Summary: This diploma thesis is aimed on a security of corporate network infrastructures and data backup in small and medium sized enterprises. The theoretical part is a summary and research of literature and electronical resources. In the practical part, author analyzes current level (state) of security of a small and mid-sized company, including their data backup systems. The analysis is made as a kind of security audit, aiming on a comprehensive review, reflecting the current level (state) of security and data backup systems. The audit‘s results are starting points to further submission of remedies, which should provide higher level of infrastructure security and should better protect valuable corporate data. Author provides all of the remedies in a bunch of variants, and calculates all the suggestions according to actual market prices.

Keywords: IT infrastructure, network architecture,security, data backup, data archivation

Obsah

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

ÚVOD

Zabezpečení firemní infrastruktury a záloha podnikových dat je oblast, bedlivě sledovaná zejména u velkých a nadnárodních organizací a podniků. Na úrovni malých a středních podniků je téma bezpečnosti upozaděno, oproti jiným hrozbám, které jsou pro podniky zjevnější a snáze uchopitelné. U malých podniků, napojených na městské rozpočty, jsou klíčovým mezníkem finance, které nepřímo ovlivňují investice do modernějších technologií a konceptů pro nakládání s podnikovými daty.

Autor se zabývá uvedenou problematikou, neboť je přesvědčen o hloubce a vážnosti významu bezpečnosti firemní infrastruktury i na úrovni malých a středních podniků. V regionálním rozvoji, stejně tak jako ve veřejné správě, plní pracovní stanice, přenosný počítač či smartphone, důležitou úlohu – jsou základním pracovním nástrojem úředníků, manažerů a inovátorů. Výstupy a výsledky pracovní činnosti úředníka či manažera mikroregionu, jsou ve valné většině zpracovány, některým z výše zmíněných prostředků, které propojeny sítěmi různého typu, kvality a charakteru, tvoří IT infrastrukturu organizací všech úrovní a velikostí. Cenné výsledky výzkumů, analýz, bádání a kvalifikované práce, putující infrastrukturou, lze souhrnně označit, jako produkční data. Způsoby, jakými data (výsledky svých činností) chráníme proti poškození, zcizení, ztrátě a nenávratnému zničení, determinují systémy pro jejich zálohu a archivaci.

Aktuálnost zmíněné problematiky reflektují útoky a průniky do firemních infrastruktur organizací, všech velikostí i zaměření, které byly zaznamenány v nedávné době. Příklady jsou nadnárodní společnosti – Sony; pojišťovny s celosvětovou působností – Anthem USA; bezpečnostní složky států – Centcom (Twitterový účet Centrálního velení USA); dopravní infrastruktury států – Brněnské letiště; zdravotnictví – Nemocnice Na Bulovce; finanční instituce – Komerční banka, ČSOB, Česká spořitelna, Raiffeisen bank; městské úřady – Valašské Meziříčí, Česká Lípa, Nymburk, Uherské Hradiště, Praha 2 a jiní, kteří byli nuceni, po prolomení bezpečnostních bariér svých IT infrastruktur, omezit svou činnost a provoz, u některých ze zmíněných případů, i v řádu několika dní.

Diplomová práce je strukturována do teoretické a praktické části. Teoretickou část práce tvoří čtyři kapitoly. První kapitola se zabývá síťovými architekturami, výhodami plynoucími z užití sítí v infrastruktuře podniků, hardwarovým prvkům a standardům síťové

architektury. Předmětem druhé kapitoly je systémová architektura, serverové ekosystémy, a síťové operační systémy. Ve třetí kapitole jsou shrnuty základní prvky bezpečnosti podnikové infrastruktury, aktivní prvky ochrany, systémy pro detekci malwaru, spywaru a spamu a podnikové firewally. Čtvrtá kapitola pojednává o systémech pro zálohu a archivaci dat, topologii ukládaných dat, typech datových úložišť a cloudových řešeních. Praktická část je členěna do pěti úseků. Autor provádí analýzu zabezpečení podnikové infrastruktury v malém (Ašské lesy, s.r.o.) a středně velkém (Ašské služby, s.r.o.) podniku. Výsledky z provedených šetření jsou následně formulovány do řady nápravných opatření, doporučení a návrhů, které zajistí vyšší úroveň zabezpečení infrastruktury zkoumaných podniků a vyšší stupeň ochrany podnikových dat. Návrhy a doporučení autor následně kalkuluje dle aktuálních tržních cen. Pro jednotlivá nápravná opatření jsou autorem připravena variantní řešení, které podnikům umožní alokovat dodatečnou úroveň zabezpečení s ohledem na limitní rozpočet organizace.

CÍL PRÁCE

Autorovým záměrem je posoudit a vyhodnotit současný stav zabezpečení IT infrastruktury a systémů pro zálohování a archivaci dat v malých a středních podnicích. Úroveň zabezpečení bude podrobena důkladnému testování a přezkoumávána ve vrstvách.

Dílčími cíli je konkrétní analýza stavu zabezpečení perimetrů lokálních sítí a bezdrátových sítí v malém a středně velkém podniku na regionální úrovni.

Následným dílčím cílem je prověřit aktuální stav systémů pro zálohování a archivaci dat v podnicích s regionální působností. Dále vyšetřit, jak je nakládáno s podnikovými daty a jakým způsobem jsou data archivována.

Výsledky z provedených šetření, uvažuje autor využít při formulaci nápravných opatření a doporučení pro posílení zabezpečení infrastruktury podniků a bezpečnějšímu systému pro zálohování a archivaci dat, která budou třetím dílčím cílem.

Nápravná opatření a doporučení, které autor hodlá předložit, budou kalkulována dle aktuálních tržních cen.

METODIKA

Problematikou diplomové práce je zabezpečení podnikové infrastruktury organizací regionální úrovně a způsob jakým malé a středně velké podniky nakládají s produkčními daty. Analýzy a testování jsou směřovány na jeden malý (Ašské lesy, s.r.o.) a jeden středně velký (Ašské služby, s.r.o.) podnik.

Sběr dat

Informace a data nezbytná k provedení podrobného přezkumu současné úrovně zabezpečení v podnicích, byla čerpána ze široké škály zdrojů a šetření.

Primární data – byla získána skrze vlastní výzkumná šetření, analýzy a realizovaná testování přímo v produkčním prostředí u obou podniků. Využity byly rovněž konzultace se systémovými administrátory, zodpovědnými za provoz a údržbu stávající infrastruktury a dodavatelem hardwarového vybavení.

Sekundární data – Interním zdrojem byla podniková dokumentace podniku Ašské lesy, s.r.o a Ašské služby, s.r.o. Jako externích zdrojů, autor využil dokumenty, příručky, doporučení a webináře společností Cisco, Autocont, Kaspersky, Sophos, Symantec, Fortinet, Kerio a TrendMicro.

Přehledová data a informace o stavu zabezpečení a zálohování dat, jsou výsledkem provedené analýzy, testování a šetření, která byla realizována přímo v podnicích, na on-line běžících systémech infrastruktury. Výstupy z provedených zjišťování, jsou pro autora výchozím bodem pro formulaci opatření, návrhů a doporučení, která mají jediný cíl – posílit bezpečnost v organizacích a zajistit integritu a funkční zálohu produkčních dat.

Metody a postupy

Analýza zabezpečení IT infrastruktury v podnicích

Analýza je cílena na objevení slabých míst a ohrožení, která vyplívají z nedostatečného zabezpečení perimetrů firemního prostředí. Pro komplexní testování infrastruktury podniku je nutno zvolit takové řešení, které obsáhne všechny parametry a atributy, které jsou součástí aktivit a prostředků, s přímým vlivem na funkčnost a stabilitu infrastruktury.

Bezpečnostní audit

Bezpečnostní audit firemní infrastruktury zkoumaných podniků, je zvolen jako testovací nástroj, který poskytne kompletní přehled o všech slabinách a nedostatcích uvnitř infrastruktury.

V přípravné fázi auditu autor definuje rozsah a plán auditu v organizacích. Vymezeny jsou segmenty sítí a hardwaru, které budou testovány.

Fáze sběru dat představovala samotné testování dílčích prvků infrastruktury. Dále rozhovory se zaměstnanci, studium podnikové dokumentace a směrnic. V neposlední řadě jsou provedeny operativní testy na aktivních částech ekosystému.

Ve fázi analýzy dat, jsou zpracovány výsledky dílčích šetření, rozhovorů a rozborů podnikové dokumentace a směrnic bezpečnostní politiky. Zjištěná rizika jsou kategorizována. Následně jsou formulována opatření a doporučení, která umožní nápravu v problémových oblastech a zeštíhlí slabá místa systémů.

Finálním výstupem auditu je výsledná zpráva, která poskytuje kompletní přehled o současném stavu infrastruktury, zjištěné hrozby a nedostatky, včetně nápravných opatření a řešení ve formě návrhů a připomínek.

Analýza fyzické vrstvy zabezpečení

Testování spočívá v ověření přítomnosti a funkčnosti jednotek pro autorizovaný přístup. Ověření funkčnosti terminálů. Přezkum seznamu distribuovaných čipů, karet a generálních klíčů. Testování funkčnosti bezpečnostních prvků v okenních rámech a dveřích. Posouzení kvality a vhodného umístění datových sejfů a pokladních systémů.

Analýza elektronického zabezpečovacího systému

Funkčnost všech komponent EZS je ověřena skrze revizi PIR čidel, sběrnicové ústředny, čidel environmentálního prostředí a stavu záložních jednotek. Revize spočívá v ověření všech funkcionalit prvků, v případě sběrnicové ústředny hlubší analýze její konfigurace. Systém EZ jako celek je testován vyvoláním falešného poplachu, s přesným odpočtem dojezdové doby zaměstnance bezpečnostní agentury a verifikací jeho postupu během zásahu v objektech.

Analýza dohledového systému

Stav a funkčnost kamerového systému je vyhodnocena na základě úrovně kvality pořízených záznamů. Sledován je záběr jednotlivých kamer a lokalizace kamer v prostoru. Ověřena je funkčnost nočního přísvitu a schopnost distribuovat záznamy mimo perimetr infrastruktury.

Analýza systému záložního napájení

U jednotek UPS je změřena kapacita akumulátorů, funkčnost spínačů, kvalita zásuvek a teplota jednotek v zátěži i mimo zátěž.

Analýza kabeláže

Kvalitu a ztrátovost metalického vedení je možno ověřit přístrojem FLUKE DTS 1800, který podá komplexní informace o stavu vodičů, jejich stínění, kvalitě, útlumu. Dále je vhodné posoudit způsob uspořádání vodičů v patch panelu a rackové skříni.

Analýza síťového hardware

Komponenty jsou sledovány v produkčním prostředí. Nejprve je posouzena vhodnost umístění, následně je ověřena konfigurace prvků, aktuálnost firmwaru a teplota při zátěži.

Analýza bezdrátové sítě

Bezdrátová síť WLAN byla analyzována prostřednictvím aplikací Wifi Overview 360 a Wifi Analyzer, které poskytnou potřebné údaje o stavu sítí, kvalitě přenosu, konfiguraci přístupových bodů a pokrytí perimetrů signálem.

Analýza pracovních stanic

Stav zabezpečení pracovních stanic je ověřen na základě posudku konfiguračních nastavení systému. Přehledové informace poskytne software Microsoft Baseline Security Analyzer a Farbar Recovery Scan Tool.

Analýza serverů

Servery jsou podrobeny skenování bezpečnostním skenerem NMAP. Ověřena jsou konfigurační nastavení rolí, hardwarových prvků a instalovaného softwaru. Překontrolována je přítomnost náhradních, klíčových, hardwarových komponent.

Analýza systému zálohování dat

Přezkoumán je způsob nakládání s podnikovými daty. Způsob, jakým jsou data klasifikována a tříděna. Datová úložiště jsou v případě pevných disků testována programy Crystal Disk Info, HD Tune a HD Sentinel. Ověřeny jsou Stínové kopie svazků MS Exchange. Provedena je zkušební záloha SQL databáze prostřednictvím Microsoft SQL Management studia. Integrita a konzistence zkušební zálohy je ověřena nástrojem společnosti Microsoft – WINS.

Analýza mobilních zařízení

Notebooky a smartphony jsou podrobeny analýze spuštěných služeb, konfiguracím systémových nastavení, aplikacím běžícím na pozadí. Zabezpečení notebooků je vyhodnoceno nástroji Microsoft Baseline Security Analyzer a Farbar Security Scan Tool. Zkoumána je i kapacita a stav akumulátorů v mobilních zařízeních.

Analýza UTM firewallu

Podnikový UTM firewall je skenován nástrojem ZENMAP, který poskytne informace o otevřených portech a běžících službách. Dále jsou přezkoumány konfigurační pravidla v produktech Kerio Control a Connect. Posouzena je i pozice UTM firewallu v síťové architektuře.

Analýza antivirového, antispamového a antispywarového řešení

V podnikovém antivirovém řešení Kaspersky jsou ověřena pravidla bezpečnostní politiky. Přezkoumány jsou restrikce a operabilita řešení. Funkčnost rezidentních štítů je ověřena testovacím souborem EICAR. Test antispamových filtrů proběhl odesláním zkušebního řetězce: >>**XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X**<< směrem do firemní infrastruktury na vybrané mailové adresy zaměstnanců. Antispywarové řešení bylo testováno utilitou SpyCar, která vyhodnocuje ochranné schopnosti systému.

TEORETICKÁ ČÁST

1 Síťová infrastruktura

1.1 Definice a přínosy sítí

Počítačová síť představuje vzájemné propojení dvou a více počítačů, na základě kterého si tyto vyměňují data. Jednotlivými prvky sítí jsou, kromě počítačů samotných, také ostatní stavební bloky jako přepínače, kabeláž, *routery*[1]. Způsob segmentace těchto prvků determinuje klasifikaci dané sítě. Klíčovým atributem každé sítě je schopnost sdílet data a informace.

Spojení je hlavním rysem, na jehož základě je možné odlišit skutečnou síť od sítě typu *sneaker*[2].Ve skutečných sítích je nezbytným prvkem propojení adresování a identifikace uzlů v síti, na jejichž základě je spojení realizováno.

Propojení v počítačových sítích je realizováno nejčastěji prostřednictvím strukturované kabeláže, optických vláken a spojů či bezdrátově pomocí rádiových vln.

Nejmenším možným typem sítě, je propojení dvou počítačů, prostřednictvím strukturované kabeláže, či bezdrátového spojení standardu *802.11*[3], tzv. peer-to-peer spojení. Sítě peer-to-peer jsou jednoduchým propojením stanic, které umožňuje základní sdílení dat, popisuje Bigelow (2004).[4] Dalším minimalistickým řešením jsou tzv. privátní sítě – pLan, které jsou realizovány pomocí technologie *Bluetooth*[5].

1.2 Definice počítačových sítí

Sosinsky (2010) definuje počítačovou síť jako skupinu prvků, která je formována atributy: propojovacího softwaru, síťových systémů a síťových prvků. Většina počítačových sítí je tvořena následujícími prvky:[6]

[1]Router je směrovač, který pracuje na úrovni síťové vrstvy ISO/OSI
[2] Síť typu sneaker představuje přenos dat mezi dvěma počítači například prostřednictvím disku typu Flash, či jiného média.
[3]Standard 802.11 definuje různé typy modulace vysílání rádiového signálu, při použití jednotného protokolu.
[4]BIGELOW, Stephen J. *Mistrovství v počítačových sítích: správa, konfigurace, diagnostika a řešení problémů*. Vyd. 1. Překlad Petr Matějů. Brno: ComputerPress, 2004, 990 s. ISBN 80-251-0178-9.
[5]Bluetooth je standard bezdrátové komunikace, schopný propojit dvě zařízení pro vzájemný přenos dat.
[6]SOSINSKY, Barrie A. *Mistrovství – počítačové sítě*. Vyd. 1. Brno: ComputerPress, 2010, 840 s. Mistrovství (ComputerPress). ISBN 978-80-251-3363-7.

- propojené systémy
- propojovací software
- síťový hardware
- fyzická přenosová média
- adresní systém pro výše uvedené komponenty

Toto pojetí síťového prostředí, pokrývá jak oblast počítačových systémů, tak systémy mobilních telefonů, systémů *VOIP*[7] telefonie, systémy paměťových zařízení, bezdrátové sítě, širokopásmová spojení a jiné.

Propojovací software – je obsažen ve všech zařízeních, která tvoří různé klasifikace sítí. Je součástí operačních systémů, stejně jako hardwarových prvků, některých integrovaných obvodů v paměťových modulech síťových prvků a některých přenosných médiích.

Fyzické přenosové médium – představují zařízení schopná generovat a přenášet elektromagnetický signál. Tento signál je výsledkem v čase fluktuujícího vzorku amplitudy napětí, či frekvence, který představuje informace, vysílané na určitou vzdálenost s předpokladem rozpoznání vysílaného na straně přijímače. Signály pak řadíme do dvou kategorií. Zaprvé jsou jimi signály proměnlivé – analogové a zadruhé signály vymezené přesným spektrem stavů – digitální.

V síťové, respektive počítačové terminologii, je výhradně užíváno digitálních, přesněji binárních systémů, jak uvádí Sosinsky (2010).[8] V binárním, někdy také uváděném jako dvojkovém, systému lze evidovat pouze dvě proměnné. Těmito proměnnými jsou 0 a 1. Tyto proměnné lze definovat jako stav zapnuto a vypnuto, či ano a ne. Výhodou těchto systémů je jednoduchost a rychlost.

1.3 Výhody sítí

Níže uvádím klíčové přednosti, které propojení dnešních systémů do síťových architektur rozličných typů přináší.

[7] VOIP – přenos hlasu skrze protokol IP
[8] SOSINSKY, Barrie A. *Mistrovství – počítačové sítě*. Vyd. 1. Brno: ComputerPress, 2010, 840 s. Mistrovství (ComputerPress). ISBN 978-80-251-3363-7.

Sdílení dat – přístup k důležitým datům, i pro více uživatelů současně, z lokalit, které jsou mimo kancelář, pracoviště, podnik či stát.

Jednoduchá mobilita – přenos dat skrze síť není nikterak závislý na ostatních médiích a za určitých podmínek není omezen ani objem přenášených dat.

Sdílené hardwarové prostředky – hromadný přístup k hardwarovým periferiím, například tiskárnám, datovým úložištím a jiným zařízením, která lze využívat napříč organizací.

Komunikace v síti – konference, mítinky, schůzky, vnitropodniková i externí korespondence, všechny komunikační prostředky, lze snadno využívat v síťovém provozu.

Ochrana dat – eliminovat riziko, hrozící ztráty dat z jednoho úložiště, lze úspěšně prostřednictvím vytváření kopií těchto dat a jejich následném přenosu skrze síť na jiná místa.

Sdílení programových prostředků – redukce nákladů na licence za softwarové vybavení, plynoucí ze společného užívání programového vybavení skrze síť

Vyšší spolehlivost – při poruše dílčího počítače, zůstávají ostatní jednotky nadále v provozu a nedochází tak k poklesu produktivity

1.4 Rozsah sítí

Dle rozsahu sítě, lze definovat několik typů sítí, které jsou vymezeny podle oblasti, kterou pokrývají.

Sítě typu LAN (Local Area Network) – jsou lokalizovány do určitého místa (podniku, budovy, patra) ve kterých jsou užity technologie krátkého dosahu (ethernet, Token Ring). Síť typu LAN je často pod kontrolou podniku. Nemeth (2008) definuje sítě typu LAN jako síťovou infrastrukturu vně budovy, či skupiny budov.[9]

Sítě typu WAN (Wide Area Network) – sítí typu WAN je užíváno k propojení sítí LAN, prostřednictvím poskytovatele (telekomunikačních, broadbandových služeb) ke spojení vzdálených poboček. Odom (2005) popisuje sítě typu WAN jako propojení dvou

[9] NEMETH, Evi, Garth SNYDER a Trent R HEIN. *Linux: kompletní příručka administrátora: 2. aktualizované vydání*. Vyd. 1. Brno: ComputerPress, 2008, 984 s. ISBN 978-80-251-2410-9.

vzdálených směrovačů třetí stranou v situacích, kdy nemáme možnost realizovat vlastní fyzickou formu spojení.[10]

Sítě typu CAN (Campus Area Network) – tento typ sítí propojuje sítě LAN, případně budovy, v určitém komplexu, které spravuje jediný subjekt. Se správou sítí tohoto typu mnohdy souvisí i správa ostatních systémů komplexu. Tento typ sítí je typický pro univerzitní areály a průmyslové zóny, popisuje Donahue (2009).[11]

Sítě typu MAN (metropolitan area network) – sítě typu MAN představují propojení sítí LAN v oblastech rozlehlejších, nežli jsou komplexy či průmyslové zóny. Většinou propojují pobočky či síť poboček v určité metropolitní oblasti, prostřednictvím třetí strany. Poskytovatele telekomunikačních, broadbandových a ostatních, datově vysokorychlostních, služeb.

1.5 Síťové topologie

Topologie síťové infrastruktury vymezuje způsob, jakým jsou seřazeny a rozloženy síťové prvky a to jak na úrovni zařízení tak i jejich spojů. Síťovou topologii lze posoudit na úrovni jejich fyzické topologie, která řeší vztahy mezi fyzickými zařízeními a prvky, a dále pak z hlediska logické topologie, ve které je řešeno jaké jsou vazby, případně hierarchické uspořádání jednotlivých funkčních prvků. Posledním možným způsobem, podle kterého lze popsat síťovou topologii je kombinace předešlých typů, která je označována jako hybridní.

Fyzická topologie

Fyzická topologie představuje vzájemné vazby mezi zařízeními, která tvoří síť. Zařízení představují uzly, koncové prvky sítě a spoje mezi těmito prvky.

Sosinsky (2010) uvádí následující podoby fyzické topologie:[12]

- sběrnice – všechna zařízení jsou připojena na jedno médium (přímočarý kmen)

[10] ODOM, Wendell. *Počítačové sítě bez předchozích znalostí*. Vyd. 1. Brno: CP Books, 2005, 383 s. ISBN 80-251-0538-5.
[11]DONAHUE, Gary A. *Network warrior*. 2nd ed. Beijing: O'Reilly, 2011, xxiii, 757 s. ISBN 978-1-449-38786-0.
[12]SOSINSKY, Barrie A. *Mistrovství – počítačové sítě*. Vyd. 1. Brno: ComputerPress, 2010, 840 s. Mistrovství (ComputerPress). ISBN 978-80-251-3363-7.

- hvězda – mnoho uzlů je propojeno do centrálního bodu, skrze který prochází veškerá komunikace
- kruh – představuje uspořádání do cyklické kmenové trasy
- spleť – představuje propojení uzlů s dalšími uzly, někdy také označované jako pavučina či pletivo
- strom – zde se uzly dále rozvětvují stejně jako větve skutečného stromu.

Tento výčet fyzických topologií není kompletní, běžně se užívají různé kombinace výše uvedených typů.

Topologie sběrnice – tento typ uspořádání je ve skutečnosti zcela běžný. Představuje propojení dvou a více síťových uzlů – koncových bodů. Koncové body jsou charakteristické svou adresovatelností. Koncovým bodem může být síťová karta, směrovač případně také jednotlivé porty směrovače, přepínače. Topologii sběrnice lze dále členit podle způsobu, jakým se data pohybují mezi jednotlivými koncovými body. V případě přímé sběrnice data putují po páteřní/ kmenové trase. Distribuovaná sběrnice tvoří kromě kmenové trasy další přenosové linky/větve, které spojují vlastní uzly. Na rozdíl od stromové topologie chybí v topologii distribuované sběrnice centrální uzel, a proto není definována hierarchie mezi uzly.

Topologie hvězdy – v síťové topologii typu hvězdy jsou jednotlivé body větveny z jediného centrálního uzlu. Všechna data protékají přes tento centrální uzel. V běžné síťové architektuře je toto zapojení velmi časté, kdy je řešeno pomocí patch panelu. Patch panel je spojovací matice s otevřenými zakončeními na obou stranách, která umožňují propojit kabely mezi sebou, napíchnutím vodičů do prohlubní v matici, uvádí Sosinsky (2010).[13]

I v případě sítě s topologií hvězdy je možné tyto dále členit na rozšířené a distribuované topologie hvězdy. Rozšířená hvězda utváří spojení jednoho i více opakovačů, a díky tomuto propojení je možné přenášet data na větší vzdálenosti. Distribuovaná hvězda znázorňuje propojení přímočarým způsobem do uzavřeného řetězu.

[13] SOSINSKY, Barrie A. *Mistrovství – počítačové sítě*. Vyd. 1. Brno: ComputerPress, 2010, 840 s. Mistrovství (ComputerPress). ISBN 978-80-251-3363-7.

Topologie kruhu – tato topologie je tvořena uzavřenou smyčkou, ve které je každý uzel výchozím i koncovým bodem datových přenosů. V této topologii obíhá datový paket jedním směrem všechny uzly, dokud nedorazí k uzlu, který tato data zpracuje. Zvolený směr přenosu je nezbytným krokem, který zabrání kolizi signálu a možnému rušení. Obousměrný pohyb datových paketů je možný v případě dvojitého kruhu, který je také někdy využíván jako pojistná vrstva nebo vrstva pro řídící kanál.

Topologie spleti – je spojením uzlů, kdy může být každý uzel spojen bodovým spojením s libovolným jiným uzlem. Síťové topologie ve formě spleti jsou značně větvené, mohou být částečně propojené, nebo plně propojené. Nedostatečné propojení v této síťové topologii vytváří riziko určitého zpoždění, kterému je však možno předcházet pomocí inteligentního směrování. Na síťové topologii typu částečně propojené spleti je postaven Internet.

Topologie stromu – tato topologie je determinována od kořenové úrovně, kterou tvoří jediný uzel, propojený s ostatními uzly druhé úrovně v hierarchii. Každý uzel druhé úrovně je dále propojen s jedním či více uzly na třetí úrovni v hierarchii. Tato propojení vytváří další větve, pro nové úrovně. Hierarchickou stromovou topologii představuje většina souborových systémů adresářových služeb, databázových systémů a její hojné užívání souvisí s rychlejším a efektivnějším vyhledáváním požadovaných dat oproti ostatním topologiím, jak popisuje Sosinsky (2010)[14].

Hybridní topologie

Hybridní topologie reprezentuje mix topologií odlišného typu s cílem zvýšit flexibilitu celé architektury. Příkladem hybridních topologií jsou:

Hvězdicová sběrnice – v této topologii jsou propojeny fyzické hvězdicové sítě v jedné sběrnici. Hvězdicová sběrnice ve skutečnosti tvoří řetěz uzlů, který je ukončen rozbočovači.

Hierarchická hvězda – v této topologii je každý uzel stromové struktury rozbočovačem, který větví periferní propojení hvězdy. Každá další úroveň stromu je tvořena rozbočovačem, který představuje hvězdu. Bigelow (2004) popisuje tuto topologii, jako

[14] SOSINSKY, Barrie A. *Mistrovství – počítačové sítě*. Vyd. 1. Brno: ComputerPress, 2010, 840 s. Mistrovství (ComputerPress). ISBN 978-80-251-3363-7.

datový přenos probíhající na úrovni směrovačů, které dále distribuují vše přijaté stanicím, napojeným do těchto rozbočovačů.[15]

Hvězdicový kruh – je tvořen centrálním rozbočovačem, který vysílá sekvenční signály ke všem okrajovým uzlům připojeným k tomuto rozbočovači. Jedná se o simulaci kruhové topologie.

Hybridní spleť – kombinuje topologii spleti s jinými uzly další topologie, typu spleti. Sosinsky (2010) uvádí, že technologie hybridní spleti poskytuje velmi redundantní a odolné spojení a proto je v praxi značně rozšířena.[16]

Logická topologie

Logické topologie vytváří mapu pohybu datových paketů mezi jednotlivými uzly. Nezbytnou podmínkou tohoto sestavení je dostupnost protokolu umožňujících výměnu dat. Každý prvek/zařízení musí disponovat specifickým identifikačním číslem, které mu zajišťuje jeho identifikaci – dostupnost v síti. Tento identifikátor reprezentuje MAC adresa (MEDIA ACCESS CONTROL). Konfiguraci logické topologie je možné zásadně proměnit, jsou-li užity pokročilejší směrovače. Síťová rozhraní je možné virtualizovat a přidělovat jim další MAC adresy.

Logická topologie řetězu – představuje přímý či uzavřený kruhový řetěz. Je-li do sítě topologie přímého řetězu implikován nový systém, je v podstatě zdvojeno propojení mezi novým uzlem, sousedním uzlem, případně sousedními uzly. V řetězové konfiguraci kruhové topologie protékají data pouze jednosměrně. Tento typ topologie je charakteristický větší mírou zpožďování.

Logická topologie hvězdy – v této topologii vysílá centrální uzel signál všemi směry, který vychází z jednoho z uzlů, ke všem ostatním uzlům dané sítě. Po potvrzení přebírajícím systémem, dojde k přenosu dat. Výpadek centrálního uzlu znamená kolaps celé architektury. Selhání jednoho z ostatních uzlů, ovlivní pouze funkčnost uzlů, napojených na kolizní paprsek. Hvězdicové logické topologie lze dále diverzifikovat na pasivní, tedy takové, ve kterých vysílající uzel, musí být schopen rozpoznat reflekci vlastního signálu.

[15] BIGELOW, Stephen J. *Mistrovství v počítačových sítích: správa, konfigurace, diagnostika a řešení problémů*. Vyd. 1. Překlad Petr Matějů. Brno: ComputerPress, 2004, 990 s. ISBN 80-251-0178-9.
[16] SOSINSKY, Barrie A. *Mistrovství – počítačové sítě*. Vyd. 1. Brno: ComputerPress, 2010, 840 s. Mistrovství (ComputerPress). ISBN 978-80-251-3363-7.

Zatímco v aktivním typu hvězdicové logické topologie, disponuje centrální uzel speciálními obvody, díky nimž nedochází ke zpětnému odrazu směrem k vysílajícímu uzlu. Při budování systémů, založených na hvězdicové logické topologii, je často použit hardwarový prvek přepínače, který vytváří vyhledávací tabulky typů přenosu dat, cílových systémů a portů, které jsou užity během síťové komunikace. Čím více záznamů tato tabulka obsahuje, tím efektivněji přepínač směruje vysílané pakety přímo, vstříc svému cíli, uvádí Sosinsky (2010).[17]

Logická topologie spleti **–** pro tuto topologii jsou charakteristické vícečetné cesty mezi párem uzlů v systému. I pro systémy typu logické spleti existuje více variant uspořádání takovýchto sítí. Mřížkové sítě, které jsou tvořeny buďto přímým nebo kruhovým útvarem spletí. Prstencové sítě, s několika kruhovými okruhy spletí, či konstrukce topologií typu spleti do hyperkrychlí. Propojení je úplné, toto se v praxi, vzhledem k výši nákladů na pořízení, využívá zřídka. Zatímco částečné propojení je v běžném provozu užíváno velmi často. Plného propojení je užíváno zejména u kritických aplikací, kde jsou vysoké požadavky na vícevrstvé redundantní spoje. Příkladem typu plně propojené sítě, je síť BitTorrent[18], která je primárně určena pro sdílení souborů.

Síťové architektury lze tedy specifikovat dle jejich geografického umístění, použití, uspořádání a požadavků na obslužnost a odolnost či požadavků na použité hardwarové vybavení. Dále je možné stavět síťové systémy podle různých typů topologií - hybridních, standardních a jejich kombinací. Popis této topologie zohledňuje fyzické prvky, logické uzly, případně trasy signálu šířícího se skrze síť.

1.6 Hardwarové prvky

Fyzické prvky, které jsou nástrojem, umožňujícím přenos dat po síti, představují jeden z klíčových atributů síťové architektury. Pro hladký a plynulý síťový provoz je nezbytné vhodně zvolit všechny dílčí komponenty, z nichž se budované sítě skládají.

[17] SOSINSKY, Barrie A. *Mistrovství – počítačové sítě*. Vyd. 1. Brno: ComputerPress, 2010, 840 s. Mistrovství (ComputerPress). ISBN 978-80-251-3363-7

[18] Síť BitTorrent zprostředkovává přenos souborů mezi uživateli. Tento přenos je charakteristický tím, že jednotlivé části přenášeného, jsou rozmístěny na vícero uzlech. Všechny tyto uzly jsou během přenosu propojeny, do doby, nežli je transfer dat dokončen.

Síťové rozhraní

Sosinsky (2010) definuje síťové rozhraní, jako hranici mezi dvěma typy síťových médií.[19] Tento princip je možné použít na širší spektrum prvků v síťové architektuře. Mohou jej tvořit jak síťové karty, USB konektory, ASIC chipy integrované na základní desce a ostatní typy hardwarových, síťových zařízení. Tuto hranici může tvořit i virtuální objekt operačního systému, bod připojení terminálu k virtuálnímu přepínači. Každé síťové rozhraní, musí mít přiděleno svou vlastní síťovou adresu (adresu IP), uvádí Odom (2005).[20]

Síťový hardware má klíčový vliv na rychlost sítě, kvalitu přenosu i celkový výkon celé síťové architektury. Za síťový hardware považujeme rozbočovače, opakovače, huby, přepínače, brány, fyzická síťová rozhraní, rozličné typy kabeláže a přenosových médií, patch panely, racky a jiné komponenty.

Opakovače (Repeatery) – představují jednotku, jejíž náplní je zesílení utlumeného signálu, procházejícího skrze přenosové médium. Tímto médiem může být jak strukturovaná, metalická kabeláž, tak i vzduch, jež přenáší radiové vlny. Opakovač umožňuje prodloužit dosah stávající sítě, případně zkvalitnit transport datového toku díky redukci rušení a útlumu, ke kterým při spojích na větší vzdálenosti v případě kabeláže, či hustě - bezdrátově zasíťovaným oblastem, v případě bezdrátového přenosu, dochází. Pro bezproblémovou funkci opakovačů je nezbytné dodržet používání stejných rámců, logických protokolů a přístupových metod, uvádí Bigelow (2009).[21] Sofistikované opakovače jsou schopny i přenosů mezi rámci. Jsou tedy schopny zesilovat signál například z ethernetového rámce a tento dále šířit optickým kabelem.

Rozbočovače – byly často používány v hvězdicové topologii jako centrální uzly, skrze které protékala všechna data. Jeho základní funkcí je rozbočování signálu – větvení sítě, uvádí Horák (2006).[22] Rozbočovače jsou dvojího typu: aktivní a pasivní. Pasivním

[19] SOSINSKY, Barrie A. *Mistrovství – počítačové sítě*. Vyd. 1. Brno: ComputerPress, 2010, 840 s. Mistrovství (ComputerPress). ISBN 978-80-251-3363-7.
[20] ODOM, Wendell. *Počítačové sítě bez předchozích znalostí*. Vyd. 1. Brno: CP Books, 2005, 383 s. ISBN 80-251-0538-5.
[21] BIGELOW, Stephen J. *Mistrovství v počítačových sítích: správa, konfigurace, diagnostika a řešení problémů*. Vyd. 1. Překlad Petr Matějů. Brno: ComputerPress, 2004, 990 s. ISBN 80-251-0178-9.
[22] HORÁK, Jaroslav a Milan KERŠLÁGER. *Počítačové sítě pro začínající správce*. 3., aktualiz. vyd. Brno: ComputerPress, 2006, 211 s. ISBN 80-251-0892-9.

rozbočovačem je například Patch panel, který s daty dále nijak nepracuje. Aktivním rozbočovačem je například opakovač, který obnovuje sílu signálu. Existují i sofistikované rozbočovače, které jsou schopny plnit úkoly přemostění, směrování a přepínání. Velkou výhodou síťové architektury, která užívá rozbočovače, je její vyšší odolnost vůči výpadku. V případě poruchy kabelu ve sběrnicové topologii, dojde k výpadku celé sítě, zatímco při poruše kabelu zapojeného do rozbočovače, je omezen provoz pouze jedné větve. Ve skutečnosti se používá především aktivních rozbočovačů, které vyžadují vlastní napájení pro svůj provoz. Rozbočovače, které jsou schopny konektivity různorodého typu kabeláže, nazýváme hybridními rozbočovači.

Mosty – plní funkci jednotky, která je schopna plnit roli opakovače – prodloužit tak efektivní dosah sítě, stejně jako rozdělit a směrovat síťový provoz, dle předem stanovených kritérií. Inteligentní mosty jsou schopny vyfiltrovat problematické svazky spojů a přidělit jim vlastní části kabelu, aby nezatěžovaly zbylé datové trasy. Mosty jsou dále schopny pracovat s příchozími a odchozími daty. Tato funkcionalita pracuje na principu, kdy mosty naslouchají síťovému provozu, ověřují fyzické adresy vysílače a přijímače každého rámce a utváří směrovací tabulku. Směrovací tabulka, zaplněna záznamy o probíhajících spojeních, zvyšuje efektivitu síťového provozu, protože je schopna "známá spojení" adresovat přímo od zdroje k cíli. Směrovací tabulka představuje komplexní databázi všech již realizovaných spojení a záznamů o fyzických adresách síťových prvků, které spolu skrze most komunikují.

Příznivým jevem při použití mostů je snižování zatížení počítačové sítě. S rostoucími objemy dat, přenášenými po síti, rostou i nároky na obslužnost těchto dat. Pracovní stanice zapojené do sítě potřebují odesílat data. Za předpokladu, že by každá stanice musela přijmout část dat, i těch, které nejsou určeny pro ni, zvýší se doba, po kterou nemůže tato stanice data odesílat. Při rozsáhlé síťové topologii by tak docházelo k razantním poklesům výkonu. Mosty umožňují sítě segmentovat a vytvořit tak několik dílčích skupin a tím snížit zatížení celé sítě. Další užitečnou funkcí mostů je jejich schopnost extendace dvou vzdálených samostatných sítí.

Směrovače (routery) – v síťové architektuře, která je realizována na různých komunikačních protokolech, je značně segmentovaná a její prostředí je komplikované, je efektivní komunikaci nutno zabezpečit prostřednictvím propracovaného zařízení, které je

schopno jak pojmout veškeré adresy jednotlivých segmentů, tak volit ideální trasu vhodnou pro přenosy dat, se schopností tyto data filtrovat – směrovač. Směrovač pracuje na úrovni síťové vrstvy modelu ISO/OSI, popisuje Horák (2006).[23] Oproti mostům jsou směrovače navíce schopny přepínat a směrovat přenášené pakety skrze více sítí.

Směrovače jsou schopny porovnávat data o protokolech jednotlivých sítí a jejich "přehled" jim umožňuje kvalitnější a efektivnější přenos paketů. Směrovače jsou využity zejména ve složitějších architekturách, kde zdokonalují správu a přenos dat.

Směrovače jsou dle funkčnosti děleny na statické a dynamické. Statický směrovač vyžaduje plnou konfiguraci ze strany správce sítě a vzhledem k pevně zadaným směrovacím tabulkám, nevolí vždy trasu nejrychlejší, avšak trasu stejnou. Dynamické směrovače jsou také prvotně manuálně konfigurovány, ale dále se učí a přizpůsobují, tak jak se mění podmínky přenosu uvnitř sítě a jsou schopny reagovat na tyto nahodilé stavy.

Brány – brána představuje komunikátor, který je schopen propojit zcela odlišné typy sítí. Rychlostně je brána oproti mostu či směrovači prvkem pomalejším avšak funkčně vybavenějším. Brány jsou schopny účelně přetvářet pakety dat putující z jedné sítě a předat je do jiného prostředí. Bigelow (2009) uvádí, většinu bran jako úkolově specifické prvky, které mají svou funkčnost zaměřenu na přenos a spojení určitého typu.[24]

Brány jsou schopny překládat adresy, síťové protokoly i samotná data. Sosinsky (2010) uvádí jako hlavní odlišnost brány, od jiných síťových zařízení určených k propojování sítí, ve smyslu jejich schopností operovat na vyšších vrstvách síťového modelu OSI.[25]

Síťové karty – síťová karta (*NIC – Network Interface Card*), známá jako adaptér LAN, tvoří hranici mezi pracovní stanicí či serverem a síťovým médiem. Funkčně síťová karta identifikuje stanici v síti a předem načítá, data plynoucí ze síťové komunikace, do vyrovnávací paměti.

[23] HORÁK, Jaroslav a Milan KERŠLÁGER. *Počítačové sítě pro začínající správce*. 3., aktualiz. vyd. Brno: ComputerPress, 2006, 211 s. ISBN 80-251-0892-9.
[24] BIGELOW, Stephen J. *Mistrovství v počítačových sítích: správa, konfigurace, diagnostika a řešení problémů*. Vyd. 1. Překlad Petr Matějů. Brno: ComputerPress, 2004, 990 s. ISBN 80-251-0178-9.
[25] SOSINSKY, Barrie A. *Mistrovství – počítačové sítě*. Vyd. 1. Brno: ComputerPress, 2010, 840 s. Mistrovství (ComputerPress). ISBN 978-80-251-3363-7.

Síťová karta je zařízením fyzické vrstvy, pracující na linkové vrstvě modelu ISO/OSI, popisuje Shinder (2003).[26] Je to nejdůležitější prvek stanice/serveru z hlediska síťové komunikace. Pro stanice a servery jsou důležité zejména následující parametry:

- typ sběrnice na základní desce stanice/serveru
- ovladač síťové karty pro příslušný operační systém
- standard použitého síťového hardwaru
- vstupy pro přenosové medium
- možnost duplexního provozu
- možnost vzdáleného bootování

Většina dnešních stanic a serverů má síťovou kartu integrovánu na základní desce. V případě serverů je těchto karet integrovaných na desce, více. Síťové karty standardně disponují funkcí Wake-On, která umožňuje vzdáleně probudit vypnutý počítač skrze povel přenesený po síti. Funkce vzdáleného bootování umožňuje provoz stanice prostřednictvím streamování operačního systému ze sítě.

1.7 Přenosové medium – kabeláž

Síťová architektura založená na fyzickém přenosovém médiu – kabelu, zcela dominuje provozu síťové komunikace dnešní doby. Sosinsky (2010) uvádí životnost průměrné metalické kabeláže v rozmezí deseti až patnácti let.[27]

Kabely je možné rozdělit na tři základní typy: kroucenou dvoulinku, koaxiální kabel a optický kabel, popisuje Trulove (2009).[28] Sosinsky (2010) uvádí ještě čtvrtý typ kabelového media – ethernetový.[29]

Kabelová media se liší rychlostí spojení, kterého dosahují, šířkou pásma, možností realizace síťových topologií při jejich použití, možností fyzických propojení. Zatím co kroucená dvoulinka, ethernetový kabel a koaxiální kabel jsou metalického typu a přenášejí

[26] SHINDER, DebraLittlejohn. *Počítačové sítě: nepostradatelná příručka k pochopení síťové teorie, implementace a vnitřních funkcí*. Praha: SoftPress, 2003, 752 s. ISBN 80-864-9755-0.
[27+29]SOSINSKY, Barrie A. *Mistrovství – počítačové sítě*. Vyd. 1. Brno: ComputerPress, 2010, 840 s. Mistrovství (ComputerPress). ISBN 978-80-251-3363-7.
[28]TRULOVE, James. Sítě LAN: hardware, instalace a zapojení. 1. vyd. Praha: Grada, 2009, 384 s. ISBN 978-80-247-2098-2.

tak signály v elektrické podobě, optický kabel je medium tvořené optickými vlákny, které jsou konstruovány ze skla nebo plastů a přenos je realizován pomocí světla o různé vlnové délce.

Koaxiální kabel – je tvořen dvěma vodiči uzavřenými v pouzdru. Je nejstarším typem kabelu používaných v ethernetových sítích. Pochází z roku 1929 a byl používán pro spoje na dlouhé vzdálenosti zejména společností AT&T . Středovým vodičem je měděný drát, který je zapouzdřen takzvaným dielektrickým izolátorem. Některé varianty koaxiálního kabelu mají měděný středový drát pokoven stříbrem, díky kterému je zlepšena přenosová charakteristika mědi při vysokých frekvencích. Izolátor je zapouzdřen druhým vodičem, kterým je spletený drát, nebo foliové balení, jehož úkolem je odrušit elektromagnetické a radiové interference. Poslední vrstvou koaxiálního kabelu je pouzdro z plastu, teflonu, kynaru. Níže uvádím přehled typů koaxiálních kabelů:

Tabulka 1- Typy koaxiálních kabelů[30]

Analog TV	*RG59/U*	Kvalitní přenos na vzdálenosti do 225 metrů.
	RG6/U	Vynikající přenosové vlastnosti do vzdáleností 225 metrů. Použitelné pro úseky od 225 do 545 metrů.
	RG11/U	Používá se pro vedení delší 545 metrů.
CCTV	*RG59/U*	Kvalitní přenos na vzdálenosti do 225 metrů.
	RG6/U	Vynikající přenosové vlastnosti do vzdáleností 225 metrů. Použitelné pro úseky od 225 do 545 metrů.
	RG11/U	Používá se pro vedení delší 545 metrů.
DTV, CATV, SATV, MATV	*RG6/U*	Standardní kabeláž pro tento typ technologie.
	RG11/U	Doporučený pro přenosy na velké vzdálenosti a páteřní komunikace.

Zdroj: *Access Communications Ltd., 2014 (přeloženo autorem)*

V síťovém provozu se nejčastěji užívaly kabely typu RG-58, přezdívané tenký Ethernet (10Base-2) a RG-8, přezdívaný tlustý Ethernet (10 Base-5). Číselné značení 10Base2 a 10Base5 představují rychlostí omezení 10 Mb za sekundu; a druhé číslo značí maximální délku kabelů přibližně 200 a 500m.

Vzhledem k rychlostní kapacitě se koaxiální kabel dnes již téměř vůbec nepoužívá v síťovém provozu, ale je hojně užíván pro rozvody televizního signálu, signálů

[30] Access Communications. ACCESS COMMUNICATIONS PTY LTD. *Www.accesscomms.com* [online]. 2014 [cit. 2014-11-04]. Dostupné z: https://www.accesscomms.com.au/reference/coax.htm

bezpečnostních kamer a jiných zařízení. I zde však dochází k útlumu a koaxiální kabel je nahrazován novějšími typy kabelů.

Kroucená dvoulinka – je nejrozšířenějším typem přenosového media, kabelové formy dnešních počítačových sítí. Kroucená dvoulinka je schopna přenášet jak analogový tak digitální signál. Mezi přínosy kroucené dvoulinky řadíme její všestranné použití snadnou instalaci nízkou cenu, solidní výkon. V případě telefonní linky se jedná o dva kroucené páry, čili čtyři vodiče. Pro telefonní rozvody bylo využito vždy jen jednoho z páru vodičů, což umožnilo realizovat technologie jako ISDN později ADSL a VDSL skrze telefonní rozvody.

Telefonní rozvody jsou zakončovány šesti pinovým konektorem (RJ-11). Sosinsky (2010) uvádí výhodu krouceného drátu, který průměruje neblahý vliv vnějších magnetických a elektrických polí, díky čemuž výrazně snižuje riziko rušení interferencí signálu mezi jednotlivými vodiči.[31]

Nejběžnějším typem kabelu je kabel, ve čtyř-párovém provedení, který je zakončován osmi pinovým konektorem (RJ-45). Kroucená dvoulinka má takzvanou charakteristickou impedanci, která je tvořena dielektrickými vlastnostmi izolace a blízkostí vodičů, uvádí Trulove (2009).[32] Stíněná kroucená dvoulinka dosahuje impedance 100-150 ohmů. Charakteristika impedance je důležitá, protože značně ovlivňuje kvalitu příjmu.

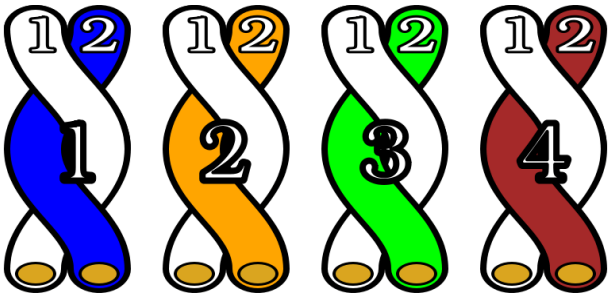
Dalším důležitým parametrem kroucené dvoulinky je kapacitance, jejíž rostoucí hodnoty zvyšují útlum přenášeného signálu. Posledním atributem je hodnota zpoždění signálu tedy časová hodnota, jež udává, za jak dlouho dorazí ve 100m dlouhém kabelu signál od začátku do konce. Kvalitu kabelového media, typu kroucené dvoulinky, významně ovlivňuje způsob instalace a případné narušení izolace.

Specifikace 5E, uvádí nutnost dodržet zkroucení do vzdálenosti ½ palce od zásuvky, uvádí Nemeth (2008).[33] U kroucené dvoulinky je nejčastěji použita plastová izolace, která je ohebná a trvanlivá. Vodiče uvnitř kroucené dvoulinky jsou barevně odlišeny. Barevné

[31] SOSINSKY, Barrie A. *Mistrovství – počítačové sítě*. Vyd. 1. Brno: ComputerPress, 2010, 840 s. Mistrovství (ComputerPress). ISBN 978-80-251-3363-7.
[32]TRULOVE, James. Sítě LAN: hardware, instalace a zapojení. 1. vyd. Praha: Grada, 2009, 384 s. ISBN 978-80-247-2098-2.
[33] NEMETH, Evi, Garth SNYDER a Trent R HEIN. *Linux: kompletní příručka administrátora: 2. aktualizované vydání*. Vyd. 1. Brno: ComputerPress, 2008, 984 s. ISBN 978-80-251-2410-9.

spektrum je definováno standardem tak, aby bylo možné každý vodič snadno najít a zakončit dle specifikace. Barevné značení čtyř-párového datového kabelu uvádím níže:

Obrázek 1 - Barevné značení kroucené dvoulinky[34]



Zdroj: *P2P. ŠVANCARA, Petr. PC sítě [online]. 1. vyd. 2006*

Optické kabely - optický kabel je tvořen jádrem, které je schopno přenosu světelných impulsů. Jádro je skleněné, plastické nebo vyrobené z média oxidů křemičitého. Základním dělením jsou optická vlákna jednovidová a vícevidová. Zatímco jednovidové vlákno přenáší pouze jeden signál, vlákna vícevidová jsou schopna přenášet více různých signálů, avšak s menším efektivním dosahem, uvádí Sosinsky (2010).[35]

Vícevidová vlákna postihuje jev zvaný modulární disperze, který je způsoben tím, že signál má tendenci rozprostírat se v čase podle rychlosti šíření optického signálu. Systém vybudovaný na přenosu prostřednictvím optických médií je na počátku datové trasy reprezentován zdrojem světla, cestu pro datový tok tvoří kabelové médium z optických vláken a na straně příjemce je cesta zakončena detektorem.

Reflekce signálu je pulzní a je založena na binárním systému. Světelný impuls, zářící vláknem značí stav 1 – zapnuto. Absence světelného impulsu značí stav 0 – vypnuto. S rostoucí intenzitou přepínání mezi stavy 0 a 1, roste množství přenesených dat.

Zdroji těchto světelných impulsů jsou jednak diody LED a za druhé polovodičové laserové diody. Shinder (2003) popisuje barevné spektrum vyzařované LED diodami, blížící se

[34]ŠVANCARA, Petr. P2P. *PC sítě* [online]. 1. vyd. 2006 [cit. 2014-11-03]. Dostupné z: http://www.p2p-aktualne.wz.cz/Kroucena_dvojlinka.htm
[35] SOSINSKY, Barrie A. *Mistrovství – počítačové sítě*. Vyd. 1. Brno: ComputerPress, 2010, 840 s. Mistrovství (ComputerPress). ISBN 978-80-251-3363-7.

červené barvě.[36] Optický kabel, ve kterém neprobíhá žádný přenos, je označován jako *tmavé vlákno.*

Bigelow (2009) uvádí ohromné množství tmavých optických vláken, v řádech tisíců kilometrů, které byly ponořeny na dno oceánů v 90. letech 20. století, díky kterým došlo k celosvětové počítačové revoluci.[37] Absence metalických součástí uvnitř optických kabelů, znamená nulové rušení elektromagnetickým vlněním či rádiovými interferencemi. Tato unikátní vlastnost je vykoupena nižší fyzickou odolností a vyššími pořizovacími náklady, oproti metalickým kabelům.

I optická kabelová vedení mají své limity. Dle zvoleného typu materiálu, ze kterého jsou vlákna vyráběna, liší se v rozsahu vlnových délek, jež jsou schopny přenášet. Jádra optických vláken jsou tvořena materiálem o šířce 50 až 62 mikrometrů, které odpovídají tloušťce lidského vlasu. Jádro je obaleno pláštěm, který má nižší index lomu světla, než jádro samotné. Plášť zadržuje světlo uvnitř jádra a odráží jej po celé délce optického vlákna. Další vrstvou je izolátor ze skla či kevlaru a ochranný obal.

Optická vlákna se sdružují do dvojic, aby bylo možno využívat duplexních přenosů. Provedení optické kabeláže je ve formě pevných trubic, které jsou odolné anebo ve formě ohebných kabelů. Nepříznivým faktorem při budování síťové architektury, založené na optických médiích, je jejich vysoká pořizovací cena. Ta je však vykoupena větší šířkou pásma, delším dosahem, odolností vůči rušením a vyšší úrovní zabezpečení. Napojit se na průběžný optický kabel, je velmi obtížné. Optická vlákna jsou rovněž charakteristická svou křehkostí.

1.8 Bezdrátové sítě

Jedním z dalších způsobů přenosu síťové komunikace je elektromagnetické záření typu rádiových vln a mikrovln. Prostředím přenosu je vzduch či vakuum. Ze spektra elektromagnetického záření se pro přenos informací mezi počítači, využívá také infračervených paprsků. Rychlost pohybu elektromagnetického vlnění uvnitř měděných a skleněných vodičů dosahuje přibližně 2/3 rychlosti světla ve vakuu. Sososinky (2010)

[36] SHINDER, DebraLittlejohn. *Počítačové sítě: nepostradatelná příručka k pochopení síťové teorie, implementace a vnitřních funkcí*. Praha: SoftPress, 2003, 752 s. ISBN 80-864-9755-0.
[37] BIGELOW, Stephen J. *Mistrovství v počítačových sítích: správa, konfigurace, diagnostika a řešení problémů*. Vyd. 1. Překlad Petr Matějů. Brno: ComputerPress, 2004, 990 s. ISBN 80-251-0178-9.

zmiňuje výsledky výzkumů, které popisují možnost světlo uvnitř magnetického pláště, složeného z Bose-Einsteinova kondenzátu[38], zastavit.[39] Bezdrátové spoje jsou tvořeny vysílačem, přenosovým médiem a přijímačem.

Přenosovým médiem je výhradně vzduch či vakuum. Pro přenosy v bezdrátových počítačových sítích jsou využívány rádiové frekvence. Oproti běžnému přenosu je rozdíl v modulaci signálu a samotné frekvenci. Nejvíce používaná, v síťových systémech, jsou pásma 900MHz; 2.4 GHz a 5.3 – 5.8 GHz. Pásma jsou označována jako WLAN (*Wireless Lan*). K těmto technologiím patří i technologie Bluetooth a WiMAX.

V současné době je masivně investováno do budování modernějších sítí a infrastruktur, především ze strany mobilních operátorů, určených pro přenos dat o rychlostech standardu 4G, známé jako LTE. Specifikace těchto sítí však patří do standardů sítí WAN. K faktorům, které ovlivňují přenosy bezdrátovými sítěmi typu WLAN, patří přímá viditelnost mezi uzly. Překážky na trase způsobují útlum signálu, či zcela znemožní přenos signálu.

Signál zpracovávají na obou stranách antény. Antény jsou dvojího typu – všesměrové a směrové. Důležitým parametrem takovýchto antén, je jejich ziskovost, uváděná v decibelech. Všesměrové antény, přesněji ziskové, mají zisk v rozmezí hodnot 3 – 6 decibelů. Směrové antény jsou dále děleny na typ Yagi, přesněji Yagi-Udova, a paraboly.

Každý rádiový přenos je náchylný na rušení. Trulove (2009) uvádí jako zdroje rušení mikrovlnné spoje, mikrovlnné trouby, radary a různé typy průmyslových zařízení.[40] Zdrojem rušení se mohou stát zařízení, která operují na stejné i příbuzné frekvenci. Zandl (2003) zmiňuje sledování výkonnostních limitů Českým telekomunikačním úřadem, který monitoruje a postihuje nadlimitní emitátory.[41]

Pro bezdrátové sítě existuje několik standardů. Nejpoužívanější a nejznámější jsou standardy dle komise IEEE 802.11, která původně vznikla s cílem sjednotit ethernetové

[38]**Boseho-Einsteinův kondenzát** je popisován jako specifická látka, která je tvořená bosony při teplotě absolutní nuly [-273,15 °C]. Při těchto podmínkách mají atomy téměř nulovou kvantovou energii.
[39] SOSINSKY, Barrie A. *Mistrovství – počítačové sítě*. Vyd. 1. Brno: ComputerPress, 2010, 840 s. Mistrovství (ComputerPress). ISBN 978-80-251-3363-7.
[40]TRULOVE, James. Sítě LAN: hardware, instalace a zapojení. 1. vyd. Praha: Grada, 2009, 384 s. ISBN 978-80-247-2098-2.
[41] ZANDL, Patrick. *Bezdrátové sítě WiFi: praktický průvodce*. Vyd. 1. Brno: ComputerPress, 2003, 190 s. ISBN 80-722-6632-2.

standardy bezdrátových sítí. Oproti drátovým ethernetovým sítím, které kolize v provozu detekují, se bezdrátové ethernetové sítě, kolizím vyhýbají. Sítě standardů 802.11 mají jmenovitou rychlost 1 – 108 Mb/s, označované jako Wi-Fi, popisuje Trulove (2009).[42]

1.9 Standardy síťového hardwaru

Předchozí kapitoly byly věnovány síťovému hardwaru a principům, na kterých síťová zařízení fungují. Většina síťových prvků je ve skutečnosti kombinována a spojována. Tato variantnost je však přímo závislá na vzájemné kompatibilitě těchto zařízení. Aby byl naplněn základní účel sítí - bezproblémový a stabilní přenos dat, je nutné, aby spolu byly všechny prvky sítě schopny komunikovat.

Vzájemnou kompatibilitu těchto zařízení zajišťují normy a standardy které přesně vymezují základní technické parametry pro realizace počítačových sítí. Nejznámější organizace *Institute of Electrical end Electronic Enginners* definuje konkrétní normy nesoucí její označení. Normy IEEE se uvádí jako součást technických parametrů hardwarových síťových komponentů.

Fast ethernet (rychlosti 100Mb/s) je v současné době nejvíce rozšířeným standardem, který odpovídá normě IEEE 802.3. Fast ethernet zcela vytlačil *ethernet* (rychlosti 10Mb/s) jehož rozvody byly realizovány koaxiálním kabelem, který je pro použití ve FastEthernetu nevhodný. Podle Horáka a Keršlágera (2006) je Fast ethernet definován ve třech variantách:[43]

- 100BASE-TX – jako kabeláž je použita kroucená dvoulinka kategorie 5, nestíněná, kdy je využito dvou párů a maximální délka segmentu je 100m.
- 100BASE-FX – využívá optických kabelů, při užití vícevidových kabelů a half-duplexu je maximální délka segmentu 412m; při použití jednovidového kabelu a duplexního režimu je maximální možná délka segmentu 10 000m.

[42]TRULOVE, James. Sítě LAN: hardware, instalace a zapojení. 1. vyd. Praha: Grada, 2009, 384 s. ISBN 978-80-247-2098-2.
[43]HORÁK, Jaroslav a Milan KERŠLÁGER. *Počítačové sítě pro začínající správce*. 3., aktualiz. vyd. Brno: ComputerPress, 2006, 211 s. ISBN 80-251-0892-9.

Gigabitový ethernet (rychlosti 1000Mb/s) tato varianta ethernetu v současnosti začíná nahrazovat Fast ethernet. Prakticky všechna nově zakoupená síťová zařízení tuto normu podporují a jsou standardizovány jak pro optické kabely, tak pro kroucenou dvoulinku.

1000BASE-X (802.3z), který standardizuje optické kabely a je dále dělen, podle typu světelného zdroje na:

- 1000BASE-SX- jako zdroj jsou použity LED diody, nebo laser, světelný zdroj emituje krátkovlnný signál délky 850nm; přenos probíhá vícevidovými optickými kabely.
- 1000BASE-LX – jako zdroj je použit výhradně laser, světelný zdroj emituje signál na delších vlnách 1310nm; použity jsou častěji jednovidové kabely a spoje jsou realizovány na větší vzdálenosti.
- 1000BASE-T (802.3ab), tento standard je definován pro metalické kabely (čtyř párové kroucené dvoulinky kategorie 5/5e). Oproti kabeláži používané u Ethernetu 10BASE-T a 100BASE-TX jsou u gigabitového Ethernetu použity čtyři páry vnitřních vodičů. V případě gigabitového Ethernetu jsou zpřísněny pravidla pro konektorování i samotné provedení kabeláže jako celku.

10GB Ethernet (802.3ae), tento standard je používán jak u sítí typu LAN, MAN tak i WAN. Horák (2006) zmiňuje maximální vzdálenost segmentu činící 40 km.[44] Přenosovým médiem jsou optické kabely.

- 10GBASE-SR je navrhován pro vzdálenosti 26 – 82m, za použití vícevidové kabeláže
- 10GBASE-LX4 je implementován u vzdáleností 240 – 320m (vícevidové kabely) a až 10km u jednovidových kabelů.
- 10GBASE-LR a 10GBASE-ER jsou užívány pro spoje o délkách 10 – 40 km, za použité jednovidových kabelů.

Bezdrátové sítě LAN jsou standardizovány dle IEEE do následujících skupin:

802.11b – maximální rychlost přenosu 11 Mb/s; frekvence 2,4 GHz; dosah 25-100m
802.11g – maximální rychlost přenosu 54 Mb/s; frekvence 2,4 GHz; dosah 25-100m
802.11n – maximální rychlost přenosu 600Mb/s;frekvece2,4/5 GHz; dosah 70 -250m
802.11a – maximální rychlost přenosu 54 Mb/s; frekvence 5 GHz; dosah 15km
802.11ac – maximální rychlost přenosu 1000Mb/s; frekvence 5 GHz; 35m

[44] HORÁK, Jaroslav a Milan KERŠLÁGER. *Počítačové sítě pro začínající správce*. 3., aktualiz. vyd. Brno: ComputerPress, 2006, 211 s. ISBN 80-251-0892-9.

2 Systémová infrastruktura

Systémová infrastruktura je jakousi další vrstvou, která navazuje na hardwarovou architekturu a implementuje do ní softwarová řešení. Mezi základní součásti systémové infrastruktury řadíme operační systémy (především serverové), systémy pro řízení souborů a databází, systémy adresářových služeb, nástroje virtualizace (aplikací i desktopů), databázové servery a systémy pro zálohování, archivaci a obnovu dat. Většina těchto komponent je součástí IT infrastruktury nezávisle na tom, zdali jde o malou organizaci či univerzitní kampus.

2.1 Servery a systémy

Za server je možné označit zařízení, které sdílí a poskytuje specifické služby, softwarová řešení, aplikace a sdílený datový prostor pro stanice či ostatní servery, které se k němu připojují. Shinder (2003) se zmiňuje o serveru jako o počítači, který zpřístupňuje své zdroje.[45] Rodina unixových systémů označuje tyto prostředky jako daemony. Rodina systémů Microsoft Windows tyto prostředky označuje jako služby.

V případě serverových zařízení jsou kladeny specifické nároky na jejich umístění a správu. U středně velkých a velkých organizací má toto nákladné vybavení vymezený vlastní prostor – serverovnu. Serverovna je (měla by být) místem dobře fyzicky zabezpečeným, s vlastní klimatizací, záložními zdroji napájení a systémy elektronických protipožárních jednotek. Server může být definován jako softwarová aplikace poskytující určitou službu ostatním systémům v síti, uvádí Sosinsky (2010).[46]

2.2 Síťový operační systém

Síťových operačních systémů existují řádově stovky. Mezi nejpoužívanější síťové operační systémy řadíme: Unix, Linux, Solaris, Novell NetWare a Open Enterprise Server, Windows Server. Síťové operační systémy je možné členit na dvě základní skupiny. První

[45] SHINDER, DebraLittlejohn. *Počítačové sítě: nepostradatelná příručka k pochopení síťové teorie, implementace a vnitřních funkcí*. Praha: SoftPress, 2003, 752 s. ISBN 80-864-9755-0.
[46] SOSINSKY, Barrie A. *Mistrovství – počítačové sítě*. Vyd. 1. Brno: ComputerPress, 2010, 840 s. Mistrovství (ComputerPress). ISBN 978-80-251-3363-7.

skupinou je rodina unixových systémů[47], které jsou většinou typu open source – čili s otevřeným zdrojovým kódem. Do této skupiny řadíme:

- Free BSD
- GNU/Linux a jeho distribuce

Druhou skupinu tvoří rodina systémů, které jsou distribuovány pod komerčními licencemi s uzavřeným zdrojovým kódem. Tuto skupinu tvoří:

- Solaris (dříve Sun) firmy Sun Microsystems
- Novell NetWare
- Microsoft Windows Server 2003
- Microsoft Windows Server 2008/2008R2
- Microsoft Windows Server 2012/2012R2

Pro hladký provoz a bezproblémové poskytování serverových služeb je zcela zásadní vhodně dimenzovat systémové prostředky, a to jak kapacitně, tak z hlediska zátěže serverových systémů. Plánování dostatečné kapacity serverových systémů je možné provádět následujícími způsoby:

- zajištěním permanentní přebytečné kapacity
- dynamickým zvětšováním potřebné kapacity
- přidělováním kapacity, dle aktuálních požadavků

Výkonnost celého systému je odvislá od precizní identifikace specifické intenzity užití klíčových služeb, které síť distribuuje. Sosinsky (2010) popisuje následující charakteristiky, které ovlivňují výkonnost sítě a které jsou determinovány těmito činnostmi[48]:

[47]THE OPEN GROUP. *The UNIX System* [online]. 1. vyd. Londýn, 2012 [cit. 2014-11-03]. Dostupné z: http://www.unix.org/what_is_unix/history_timeline.html

[48] SOSINSKY, Barrie A. *Mistrovství – počítačové sítě*. Vyd. 1. Brno: ComputerPress, 2010, 840 s. Mistrovství (ComputerPress). ISBN 978-80-251-3363-7.

- dekompozice doby odezvy pro jednotlivé komponenty
- měření a monitoring propustnosti
- kontinuální vyhodnocování spolehlivosti
- možnosti škálovatelnosti sítě

2.3 Typy síťových serverů

Zatímco Sosinského pojetí serveru jako softwarového programu, který poskytuje služby jiným systémům skrze síťovou infrastrukturu, je ve skutečnosti použití termínu server volné. Server, který plní specifickou funkci a je vázaný k určitým aplikacím, je možné dle tohoto účelu použití dále definovat. Níže uvádím nejčastější typy serverů používaných v současných IT infrastrukturách:

- *tiskové servery* – zprostředkovávají tiskové úlohy pro všechna zařízení napojená do počítačové sítě
- *file server* – zpřístupňuje větší množství souborů a dat, služby zálohování a archivace pro klienty zapojené do sítě
- *aplikační servery* – tvoří je skupina databázových serverů, webových serverů, e-mailových serverů a jiných serverů, které sdílí aplikační software v síťovém prostředí
- *backup servery* – které se zaměřují na zálohu dat různého typu, z různých zařízení a systémů včetně dat a informací ze serverů ostatních typů
- *síťové servery* – které zabezpečují provoz služeb přímo souvisejících s různými službami a funkcemi potřebnými pro provoz síťové infrastruktury
- *doménové servery* – které jsou užity v rozsáhlejších síťových infrastrukturách

2.4 Kapacita a zatížení serverů

Sosinsky (2010) popisuje kapacitu síťového serveru jako jeho schopnost zvládnout určité pracovní zatížení.[49] Zatížení síťového serveru je možné měřit pomocí různých principů, přičemž některé jsou na bázi teoretické, jiné čistě praktické.

Plánování kapacity serverového prostředí vycházející z přístupu zajištění přebytečných kapacit zohledňuje proaktivní strategii síťového provozu, která reflektuje použití prostředků, nezbytných pro efektivní a stabilní funkčnost celého systému. Proaktivní strategie je principem, který okamžitě reaguje na nárůst provozu a potřebu dodatečných systémových prostředků, které je nezbytné okamžitě uspokojit.

Reaktivní strategie vychází z přidávání potřebných kapacit dle aktuálních požadavků. Systémové prostředky jsou tedy implementovány až v době zjištění jejich skutečné potřeby. Slabinou tohoto přístupu je zpoždění, ke kterému dojde v mezidobí, než jsou tyto požadavky obslouženy.

Poslední přístup vychází z přesné komparace systémových prostředků odpovídajícím nárokům sítě, vztaženým k dostatečné kapacitě serverů. Tato strategie má analytický charakter a množství použitých prostředků se mění tak, jak se mění nároky kapacity sítě.

Adresářové služby

Adresářové služby plní hlavní úlohu v architekturách klient – server nynějších operačních systémů implementovaných do síťového prostředí. Jejich hlavní funkcí je DNS (*Domain Name Services*), archivace informací o objektech v síti a distribuce těchto informací k ostatním serverům či aplikacím.

Nejmenším prvkem v adresářových službách je doména. Sosinsky (2010) definuje doménu jako množinu systémů, které sdílejí stejnou databázi zabezpečení.[50] Nemeth (2008) popisuje doménu jako samostatný úsek jmenného prostoru, který je volně spravovaný

[49] SOSINSKY, Barrie A. *Mistrovství – počítačové sítě*. Vyd. 1. Brno: ComputerPress, 2010, 840 s. Mistrovství (ComputerPress). ISBN 978-80-251-3363-7.
[50] SOSINSKY, Barrie A. *Mistrovství – počítačové sítě*. Vyd. 1. Brno: ComputerPress, 2010, 840 s. Mistrovství (ComputerPress). ISBN 978-80-251-3363-7.

jedinou administrativní jednotkou.[51] Doména je tedy logické seskupení síťových počítačů, které sdílejí centrální databázi síťových údajů, uvádí Horák. Domény obsahují informace o organizačních jednotkách, uživatelských účtech, účtech počítačů a jiných objektech, které jsou adresovatelné skrze unikátní rozeznávací název.

Adresářové služby v současné době vychází ze standardu: X.500 (LDAP). Standard X.500 je produktem telekomunikačního průmyslu, na jehož základě jsou schopny vzájemně kooperovat různé adresáře. Výhodou tohoto protokolu je jeho použitelnost v libovolném typu sítě a jeho schopnost uchovávat data o objektech z libovolné úrovně referenčního modelu ISO/OSI. V dnešním produkčním světě, je většina adresářových služeb počítačových sítí, založena na protokolu LDAP (*Lightweight Directory Access Protocol*), který těží ze schopnosti interoperability. Na protokolu LDAP je založena velká množina adresářových služeb:

- Microsoft Active Directory
- Novell Edirectory
- 389 Directory Server
- OpenDS
- Sun Java System Directory Server
- Apple Open Directory
- Apache DS

Typy domén

Sosinsky (2010) dále uvádí doménu jako základní jednotku adresářové služby, která popisuje skupinu systémů a odpovídajících prostředků, které jsou uspořádány adresářovou službou a sdílí společnou databázi zabezpečení nebo model zabezpečení.[52] Domény lze členit podle různých schémat a tato schémata dále kombinovat. Níže uvádím příklady těchto použití:

- centrální hlavní doména s větví doménové struktury, rozbočovačem nebo hvězdou
- struktura s více hlavními doménami

[51] NEMETH, Evi, Garth SNYDER a Trent R HEIN. *Linux: kompletní příručka administrátora: 2. aktualizované vydání*. Vyd. 1. Brno: ComputerPress, 2008, 984 s. ISBN 978-80-251-2410-9.
[52+53] SOSINSKY, Barrie A. *Mistrovství – počítačové sítě*. Vyd. 1. Brno: ComputerPress, 2010, 840 s. Mistrovství (ComputerPress). ISBN 978-80-251-3363-7.

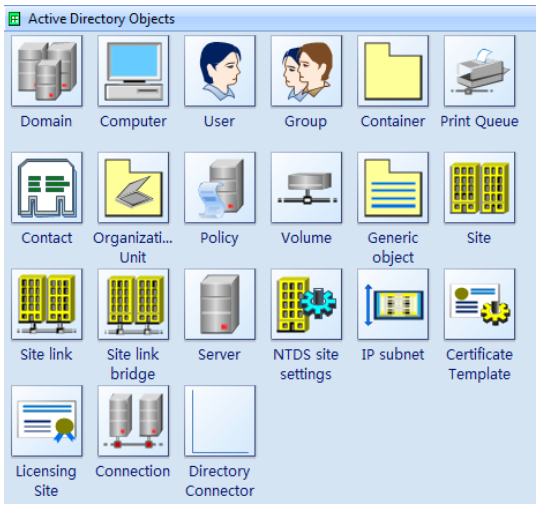
- domény prostředků
- vzdálené domény
- domény specifické pro aplikace

Servery domén – jsou systémy, na kterých je nasazena adresářová služba dané sítě nebo řadič domény. V menších organizacích obstarávají servery domén, vyjma adresářové služby, i obsluhu rolí jako DHCP/DNS, Exchange Server, Web Server, ISA Server, SQL server a jiné. Tyto funkcionality poskytuje rovněž edice *Small Business Server* od Microsoftu.

Microsoft Active Directory

Nejrozšířenější adresářovou službou je dnes Microsoft *Active Directory Domain Services* (AD/DS). Služba *Active Directory* představuje adresářovou službu, ve které je doména množinou systémů, které jsou soustředěny prostřednictvím databáze SAM (*Microsoft Security Account Manager*). Sosinsky (2010) popisuje toto seskupení jako: „*…logický celek založený na modelu zabezpečení, který je použit na členské systémy v rámci perimetru jedné sítě, členské systémy sloučené v rámci perimetru jednoho připojení WAN, vzdálené systémy, které nejsou permanentně napojeny do domény a také ostatní členské systémy, ke kterým je schopen server domény přepojit.*“[53]

Obrázek 2 - Objekty ve službě Active Directory[54]



Zdroj: *EDRAW- Visualization Solutions Inc.*

[54] Edraw Visualization Solutions. *Active Directory Diagramming Software* [online]. 2013 [cit. 2014-11-04]. Dostupné z: http://www.edrawsoft.com/Active-Directory.php

Každá takováto jednotka je členem domény, server jest serverem domény. Shinder (2003) definuje AD jako aplikaci, která je hluboce implementována do operačního systému.[55]

[55]SHINDER, DebraLittlejohn. *Počítačové sítě: nepostradatelná příručka k pochopení síťové teorie, implementace a vnitřních funkcí*. Praha: SoftPress, 2003, 752 s. ISBN 80-864-9755-0.

3 Bezpečnostní infrastruktura

Zajistit bezpečnost síťové architektury je úkol nesnadný, který klade vysoké nároky na schopnosti síťových a systémových administrátorů. Se zajištěním bezpečnosti také úzce souvisí řádné proškolení všech uživatelů stanic a zařízení, které jsou do sítě zapojeny. Bezpečnost celé IT infrastruktury je v ideálním případě vrstvena do čtyř a více bezpečnostních okruhů.

3.1 Okruh fyzického zabezpečení

Fyzické zabezpečení moderní IT infrastruktury znamená minimalizovat, lépe zcela eliminovat hrozby plynoucí z potenciálních vnějších, ale i vnitřních rizik. Mezi nejzávažnější ohrožení IT infrastruktury řadíme nenávratné škody a defekty, které zapříčiní oheň, voda, vlhkost, agresivní plyny, elektromagnetická pole, mechanická poškození, exploze, prach, neautorizovaný přístup či vloupání.

Minimalizovat tato rizika je možné skrze prostředky zvyšující celkovou fyzickou odolnost systému v podobě bezpečnostních datových komor, datových IT sejfů, media sejfů, speciálních rackových skříní, speciálních modulárních systémových řešení, systémů zálohového napájení, chladicích systémů, systémů zabezpečení a monitoringu, elektronických protipožárních systémů a elektronických zabezpečovacích systémů, stabilních hasicích zařízení a systémů detekce kouře a environmentálního prostředí.

Většina těchto zařízení a systémů je vyráběna a dodávána dle specifických norem, např. odolnosti proti požáru, bezpečnostním třídám proti vloupání, odolnosti proti mechanickému poškození, odolnosti proti vniknutí prachu a vlhkosti, specifickým požadavkům na autorizovaný přístup.

3.2 Okruh hardwarového zabezpečení

Tento okruh zabezpečení infrastruktury je definován vhodnou konfigurací všech fyzických síťových zařízeních, včetně permanentního sledování možností aktualizace firmwaru těchto zařízení. Mezi prvky hardwaru, které je nutné spravovat, řadíme inteligentní switche, routery, bridge, firewally, ISP modemy, bezdrátové přístupové body. Vhodnou konfigurací těchto prvků lze zamezit zapojení zařízení, které nemají připojení do firemní infrastruktury výhradně povoleno, a to jak připojení fyzické, prostřednictvím kabeláže, tak

připojení bezdrátové, prostřednictvím sítě WIFI. Mezi hardwarové prvky zabezpečení je možné řadit i absenci DHCP serverů na úrovni lokální sítě, volba netradičních rozsahů IP adres, pro všechna zařízení připojená do firemní sítě, znemožnění použití portů USB na všech pracovních stanicích, které jsou součástí firemní síťové architektury.

3.3 Okruh softwarového zabezpečení

Tento okruh zabezpečení firemní IT infrastruktury, je vymezen skrze softwarové řešení ochrany informačních systémů, před riziky jakými jsou: napadení systému virem, červem, trojským koněm, zneužitím dat, neoprávněného vzdáleného přístupu, průmyslové špionáže, zneužití fyzických či systémových prostředků síťové infrastruktury, zneužití hardwaru firemní infrastruktury.

Aktivní prvky ochrany

Mezi aktivní prvky ochrany, lze zařadit všechny softwarové nástroje, které svou činností předcházejí napadení či penetraci IT infrastruktury. Aktivním prvkem jsou například *Bystrá data*. Bejtlich (2013) popisuje *Bystrá data*, jako soubor informací, které vyhodnotí a interpretují neobvyklý provoz v síti a dále, prostřednictvím zprávy, informují administrátora o právě probíhající podezřelé aktivitě.[56]

Pokročilá ochrana proti virům

Základním softwarovým řešením jsou v tomto případě antivirové programy, nasazené na všech stanicích a serverech zapojených do firemní infrastruktury. Antivirové programy jsou neodmyslitelnou součástí bezpečnostní politiky každé organizace. Jejich primární funkcí je detekce virů implementovaných do souborů, zabránění replikace těchto virů a imunizace napadených součástí napadených stanic či serverů. Antivirové programy používají k odhalení škodlivého kódu specifické principy, které popisuje Surapati (2011):[57]

[56] BEJTLICH, Richard. *The practice of network security monitoring: understanding incident detection and response*. San Francisco: No Starch Press, 2013, 1 online zdroj (379 pages). ISBN 978-1-59327-534-1.
[57] SURAPATI, Taufan. How Antivirus Works: SignatureBasedDetection, HeuristicScanning and BehaviorBlocker [online]. 13. 8. 2011. [cit. 30-10-2014]. Dostupné z: http://www.articlesbase.com/security-articles/how-antivirusworks-signature-based-detection-heuristic-scanning-and-behavior-blocker-5124641.html.

- princip detekce vycházející z rozpoznání signatury – porovnáván je zdrojový kód programu se signaturami virů, respektive programů, které obsahují části škodlivého kódu
- heuristická analýza – spuštění škodlivého kódu uvnitř virtuálního prostředí antivirového programu, které je simulací procesů následujících po spuštění tohoto kódu
- detekce rootkitů – vychází ze zdvojené inspekce systému, jeho zavádění a kontroly procesů, během jeho spouštění

Pokročilá ochrana proti spamu

Moderní forma komunikace, kterou představuje e-mail, jež přináší výhody v podobě flexibility, rychlosti a adresnosti, díky které se internet masivně rozšířil, s sebou přináší, vzhledem k vysoké úrovni anonymity, prostor ke zneužití tohoto způsobu komunikace v podobě rozesílání nevyžádané pošty – spamu. Antispamová řešení představují kombinaci bezpečnostních principů, jejichž cílem je dokonalé filtrování příchozí pošty. Dle údajů ESET spol. s.r.o., tvoří nevyžádaná pošta až 80% veškeré e-mailové komunikace.[58] Antispamová softwarová řešení pracují na principu záznamu adres odesílatelů nevyžádané pošty do databází a protokolů a porovnávají veškerou příchozí komunikaci se záznamy z těchto protokolů a takto oskenovanou zprávu buďto doručí nebo přesunou do složek specifikovaných dle konfigurace antispamové aplikace.

Firewall

Nemeth (2008) definuje firewall jako základní nástroj, který je klíčovým ochranným prvkem na úrovni celé sítě.[59] Firewally monitorují veškerý síťový provoz, který jimi prochází a určují kterou komunikaci v síti propustí dále, a kterou zablokují, zahodí nebo vrátí zpět, popisuje Sosinsky (2010).[60] Strebe (2003) vymezuje firewally jako strážce na hranicích privátních sítí, kteří vytvářejí kontrolní body zabezpečení a zevrubně kontrolují všechny pakety, které mezi privátní sítí a internetem cestují, a na základě konfiguračních

[58]ESET, spol. s.r.o., Antispam vás zbaví nevyžiadanej pošty: Antispam. ESET, spol. s.r.o. w*ww.eset.com* [online]. 2014 [cit. 2014-10-30]. Dostupné z: http://www.eset.com/sk/antispam/

[59] NEMETH, Evi, Garth SNYDER a Trent R HEIN. *Linux: kompletní příručka administrátora: 2. aktualizované vydání*. Vyd. 1. Brno: ComputerPress, 2008, 984 s. ISBN 978-80-251-2410-9.

[60+62] SOSINSKY, Barrie A. *Mistrovství – počítačové sítě*. Vyd. 1. Brno: ComputerPress, 2010, 840 s. Mistrovství (ComputerPress). ISBN 978-80-251-3363-7.

pravidel příslušného firewallu tyto pakety propustí nebo zablokují.[61] Firewall tedy představuje nejvyšší, možnou ochrannou vrstvu, je-li správně nakonfigurován. Působnost firewallu sahá od druhé (síťové) vrstvy až do sedmé (aplikační) vrstvy modelu ISO/OSI. Mezi základní funkce firewallu patří:

- filtrování paketů – na úrovni protokolu ICP/IT jsou komunikačními pravidly přijímány nebo zahazovány datové pakety neautorizovaných uživatelů, je zamezeno připojení k neautorizovaným službám (tyto funkce je možné uplatnit jak v příchozím tak odchozím provozu)
- NAT (překlad síťových adres) – zprostředkovává překlad interních zařízení lokální sítě, dochází tak ke změně adresace, která je založena na tabulce, která vymezuje pravidla pro překlad; Strebe (2003) uvádí funkci NAT jako takzvané maskování adres IP.[62]
- služby Proxy – jsou realizovány na aplikační vrstvě ISO/OSI modelu, kde vytváří připojení hostitelských počítačů v rámci vnitřních požadavků, tato služba představuje jakýsi mezičlánek mezi systémem nebo stanicí uvnitř privátní sítě a klientem v externím prostředí. Přímé spojení skrze firewall neexistuje. Tato funkce je vysoce náročná na systémové prostředky, avšak je poměrně účinná proti útokům DDoS, podvržením IP adresy, a je schopna kontroly probíhající komunikace na výskyt virů, červů a trojských koňů, uvádí Sosinsky (2010).[63]
- filtrování komunikace na síťovém rozhraní – vstupní filtry na síťovém rozhraní jsou schopny zablokovat datové pakety přicházející z rozsahů IP adres, čísel portů a protokolů, které jsou komunikačními pravidly zakázány.
- stavová inspekce – provádí kontrolu odchozích datových paketů a protokoluje cíle jejich cesty do stavové tabulky. Je-li navázáno zpětné příchozí spojení, dojde k porovnání s aktuální stavovou tabulkou a je rozhodnuto, zdali bude komunikace propuštěna dále či nikoliv.
- inspekce okruhů – představuje filtrování obsahu jednotlivých relací – okruhů. Komplikované je aplikování tohoto typu filtrů na protokoly, které jsou svou povahou multirelační (HTTP, FTP, streamovaná multimédia).

[61+61] STREBE, Matthew a Charles PERKINS. *Firewally a proxy-servery*. Vyd. 1. Brno: Computer Press, 2003, xxi, 450 s. ISBN 80-722-6983-6.

- aplikační filtry – znamenají hloubkovou prověrku paketů (*Deep Packet Inspection*). Tento filtr je nejkomplexnějším, na systémové prostředky nejnáročnějším nástrojem, který je schopen zkoumaná data a pakety, také modifikovat, uvádí Sosinsky (2010).[64]

Firewally je možné rozdělit podle oblasti jejich působení do těchto skupin:

Personální firewally – někdy také označované jako osobní firewally, zprostředkovávají ochranu jediné stanice. Většinou jsou jimi komerční produkty jako Comodo Firewall, Kaspersky Internet Security, Zone Alarm, Kerio Firewall, Vipre Firewall, Trend Micro Internet Security, Norton 360 a jiné. Vlastní integrovaný personální firewall obsahují i operační systémy firmy Microsoft. Funkce integrovaného firewallu mají i distribuce Linuxu od jádra verze 2.4. Jedná se o nástroj *Netfiltr* a systém *IP tables*, který používá uspořádaného systému pravidel pro síťové pakety. Skupiny těchto pravidel tvoří tabulky, které jsou využívány pro určité typy síťových přenosů. Rodina unixových operačních systémů obsahuje také takzvané, obrněné distribuce Linuxů, které disponují širším spektrem bezpečnostních vlastností, oproti běžně dostupným distribucím. Nemeth (2008) uvádí tyto funkce ve formě speciálních přístupových kontrol a bohatých možnostech auditu.[65] Mezi nejznámější obrněné distribuce Linuxu, patří Bastille Linux, Engarde Linux, OpenWall a GNU.

Firewally ve směrovačích – inteligentní směrovače jsou funkčně vybaveny pro blokování specifických rozsahů adres a portů, umožňují překlad adres IP (NAT). Mezi nejznámější producenty těchto inteligentních switchů patří Netgear, Sonic Wall, Cisco. Inteligentní směrovače některých firem jsou schopny i antivirové kontroly a hloubkové analýzy paketu.

Hardwarové firewally – představují hardwarové zařízení se všemi funkcemi softwarového firewallu. Základními funkcemi jsou: statické filtrování paketů, překlad adres NAT, filtrování adres a portů, souběžné připojení uživatelů a jiné. Klíčovými parametry jsou: počty vysokorychlostních ethernetových a optických rozhraní, velikost mezipaměti

[64]SOSINSKY, Barrie A. *Mistrovství – počítačové sítě*. Vyd. 1. Brno: ComputerPress, 2010, 840 s. Mistrovství (ComputerPress). ISBN 978-80-251-3363-7.
[65]NEMETH, Evi, Garth SNYDER a Trent R HEIN. *Linux: kompletní příručka administrátora: 2. aktualizované vydání*. Vyd. 1. Brno: ComputerPress, 2008, 984 s. ISBN 978-80-251-2410-9.

(Cache), služby webové proxy a reverzní proxy, práce s protokolem IPSsec, šifrování SSL, modularita a škálovatelnost, uvádí Sosinsky (2010).[66]

Serverové firewally – představují obdobu hardwarových firewallů ve formě softwarového řešení operujícího nad standardním serverovým operačním systémem. Výhodou této implementace je možnost aplikace tohoto řešení na již zavedenou infrastrukturu a obslužnost této aplikace v rámci dané infrastruktury. Výhodou těchto řešení je také lepší škálovatelnost, zapojení do clusterů a tím pádem zajištění vyšší dostupnosti než v případě hardwarových prvků.

Bezpečnostní brány – jsou zařízeními, která pracují na rozhraní mezi dvěma nebo více sítěmi. Brány jsou jak hardwarového tak softwarového charakteru. Hlavní funkcí brány je konverze protokolů na sedmé (aplikační) vrstvě ISO/OSI. Brány jsou schopny fungovat i na transportní a síťové vrstvě modelu ISO/OSI, popisuje Sosinsky (2010).[67]

Stavové firewally – provádí analýzu všech spojení a na základě inspekce paketů a informacích o těchto spojeních rozhodují, zdali příslušný paket patří do povolené relace nebo zakládá relaci novou, ten je následně dále filtrován, dle komunikačních pravidel, a je rozhodnuto, zda bude spojení povoleno. Stavové filtrování je metodou dynamické filtrace, která se adaptuje na spojení a relace, a která je schopna přizpůsobit své chování, v reakci na vzájemné interakce propojených systémů.

Firewall je velmi výkonným prvkem ochrany síťové infrastruktury, ale v současné době je nutné jej doplnit o další zařízení, která pracují na sedmé (aplikační) vrstvě ISO/OSI modelu. Vzhledem k stále častějšímu zneužívání nedokonalostí a chyb aplikačního vybavení a softwaru, nejen stanic a serverů, ale také inteligentních hardwarových prvků jako jsou switche a routery, je nutné implementovat do IT infrastruktury prvky s pokročilými metodami prevence. Těmito systémy jsou zařízení se zabudovanými systémy IDS (*Intrusion Detection System*) a zařízení se zabudovanými systémy IPS (*Intrusion Prevention System*). Tato řešení mají softwarový charakter, mohou být součástí

[66+66] SOSINSKY, Barrie A. *Mistrovství – počítačové sítě*. Vyd. 1. Brno: ComputerPress, 2010, 840 s. Mistrovství (ComputerPress). ISBN 978-80-251-3363-7.

hardwarového firewallu nebo fungují samostatně, jako hardwarové sondy, zmiňuje Endorf (2005).[68]

Prvky pro detekci a prevenci průniků

Řešení na bázi softwarového nebo hardwarového systému, jejichž hlavním úkolem je rozpoznat a blokovat nežádoucí činnost uvnitř sítě. Klíčovým aspektem v ochraně před průniky je architektura všech bezpečnostních prvků a také efektivita s jakou svou činnost vykonávají. Bejtlich (2013) uvádí jako ideální způsob ochrany perimetru sítě, užití metod Network Security Monitoring, které spočívají ve sběru, vyhodnocování a varování, již při probíhajících pokusech o útok, na firemní síť.[69]

Okruh zabezpečení před chybami lidského faktoru

Tento okruh je především vymezen na základě přístupových práv, autentizace a identifikace jednotlivých uživatelů, pracujících ve firemní IT infrastruktuře. Nezbytným krokem je vhodné vybalancování pravomocí pro každého uživatele, skupinu uživatelů. Přílišná restriktivnost uživatelských pravomocí může vést k takovému stupni omezení, které znesnadňuje běžnou činnost daného uživatele a promítne se tak do jeho produktivity. Oprávnění, zabezpečení, zodpovědnosti by měly vycházet z příslušné bezpečnostní politiky, která je většinou koncipována restriktivněji. Vhodné nastavení uživatelských práv, má silně preventivní charakter před nežádoucími hrozbami vnějšího prostředí, ale také uvnitř firemní IT infrastruktury.

[68] ENDORF, Carl. Detekce a prevence počítačového útoku. 1. vyd. Praha: Grada, 2005, 355 s. ISBN 80-247-1035-8.
[69] BEJTLICH, Richard. *The practice of network security monitoring: understanding incident detection and response*. San Francisco: No Starch Press, 2013, 1 online zdroj (379 pages). ISBN 978-1-59327-534-1.

4 Infrastruktura pro zálohu a archivaci dat

Ochrana datové základny je součástí celistvé bezpečnostní politiky organizace a je důležitým prvkem v zajištění kontinuity informačních systémů. Zásadními prvky, které jsou předmětem zálohování, jsou servery uvnitř IT infrastruktury a produkční data z koncových stanic. Servery plní úlohu centrálních uzlů a vzhledem k tomu, že v informačním systému mají nezastupitelnou úlohu, je zálohám jejich provozu nutné poskytnout potřebnou péči. Zálohování koncových stanic je v tomto případě upozaděno, avšak to se netýká produkčních dat, která stanice a jejich uživatelé vytvářejí. Zálohy datových základen běžného firemního prostředí jsou ukládány redundantně, jako kopie na pevných discích, záložních páskách a jiných typech velkokapacitních médií, na cloudovém úložišti. Vhodné je, důležitá data zálohovat externě tak, aby jejich fyzická podoba byla mimo budovu/komplex. Kritické zálohy bývají často ukládány na datové pásky s vysokou životností a disková pole se zvýšenou redundancí dat (RAID 1,10,01,6,7) na zálohovacích serverech, zařízeních typu NAS, SAN.

4.1 Zálohování dat

Zálohování dat probíhá v každé organizaci dle stanovené bezpečnostní politiky. Atributy a charakter těchto politik se liší podle typů organizace, její velikosti a sektoru, ve kterém působí. Zálohována jsou zejména produkční data – tedy data, která jsou vytvořena samotnými uživateli dané organizace, data pro obnovení operačních systémů po pádu, zálohy databází, dokumentů, projektů a jiných souborů vytvořených firemní infrastrukturou. Smyslem zálohy je obnova výchozího stavu v případě havárie, poruchy, odcizení anebo výpadku. V případě těchto nenadálých událostí často dochází k nevratnému poškození uložených dat, která nejsou-li zálohována, mohou mít fatální následky pro chod celé firemní infrastruktury.

4.2 Archivace dat

Úlohou archivace je ukládání důležitých dat na média dlouhodobé životnosti, s výjimečným poměrem bezztrátového uchování informací, na nich archivovaných. Oproti procesu zálohování dat se archivace liší především tím, že v případě archivace nejsou kladeny tak vysoké nároky na časovou dostupnost archivovaných dat. Proces archivace dat využívá v současné době speciální typy pevných disků a magnetických pásek. Při archivaci

dat je nutné zohlednit hardwarovou komptabilitu použitých médií s výhledem do budoucnosti.

4.3 Ukládání dat

Ukládání dat je možné dále specifikovat podle topologie, do jaké jsou data ukládána, podle vzdáleností, na jakou je nutné data dopravit a také podle typu připojení médií, na něž jsou data ukládána.

Topologie ukládání dat

NAS *(Network Atached Storage)* – představuje systém pro ukládání dat založený na protokolu ICP/IT v místní síti LAN. Systém zálohy NAS slouží k účelnému sdílení souborů a dat v lokální síti. Systém NAS je přístupný v místní síťové infrastruktuře, ale stejně tak je možné, na základě konfigurace, přistupovat i ze vzdálených sítí a stanic. Mezi výhody systému NAS patří:

- jednoduchost implementace
- jednoduchost správy
- nízká cena celého systému
- nasazení do stávající infrastruktury

SAN *(Storage Area Networks)* – systém SAN představuje dedikované datové síťové úložiště, které není součástí místní sítě LAN a slouží pouze k transferům dat, s ohledem na schopnost zpracování velkého objemu dat. Výchozím prvkem systému SAN je infrastruktura tvořená optickými přepínači a propojení optickou kabeláží. Systémy SAN jsou nasazovány zejména ve větších organizacích, které jsou závislé na nekompromisní dostupnosti datových služeb, extrémně rychlé době odezvy a škálovatelnosti tohoto systému. Nevýhodou systému SAN jsou vysoké náklady na realizaci tohoto systému. Datová pole systému SAN je možné sdílet na více serverech, kdy operační systémy těchto serverů zacházejí s tímto datovým polem, jako s lokálně připojeným oddílem. Dosah systému SAN je fyzický odvislý od schopností a parametrů optické kabeláže, čili je možné realizovat i spoje na řádově desítky kilometrů.

DAS *(Directly Atached Storage)* – systém DAS je tvořen diskovým polem, které je spojeno přímo se serverem nebo jinou stanicí. Hlavním atributem systému DAS je maximální

výkon, nevýhodou je nemožnost sdílení diskového pole. Systém DAS je realizován připojeními typu SCSI, SATA, SAS. Systém DAS je užíván hlavně v menších organizacích, protože má omezené možnosti sdílení dat a omezené možnosti škálovatelnosti.

Perimetr ukládání dat

Ukládání dat lokálně **–** představují úložiště jako pevný disk počítače, externí disk připojený k počítači, paměti typu *flash*, disky připojené rozhraním Fireware, eSata. Za lokální úložiště je možné pokládat rovněž externí disk napojený do domácí sítě.

Ukládání dat vzdáleně – vzdálené ukládání dat je možné prostřednictvím systémů úložišť NAS i DAS. Vzdáleným úložištěm, které v současné době zažívá boom, jsou Cloudová úložiště, která umožňují ukládat data skrze webová rozhraní nebo specifické aplikační vybavení, přímo na vzdálený server. Nejznámějšími službami tohoto typu jsou OneDrive (dříve SkyDrive) společnosti Microsoft, Google Drive společnosti Google Inc, iCloud společnosti Apple, Dropbox, Sinplicity, Sugarsync. S rozmachem cloudových úložišť v poslední době, souvisí značný pokles cen těchto služeb a růst prostoru pro ukládaná data. Některé služby nabízejí v rámci placených programů i „neomezený“ datový prostor pro data svých klientů.

Ukládání dat dle typu připojení

SAS připojení – nahrazuje starší sběrnici SCSI a přechází z paralelního typu připojení k sériovému. Připojení SAS je kompatibilní s připojením typu SATA a je využíváno jak v systémech DAS, tak i SAM.

Fiber Channel připojení – je založeno na optickém připojení do sítí SAN, a zajišťuje nejrychleji možný způsob přenosu dat. Nevýhodou tohoto připojení jsou vysoké pořizovací náklady.

SCSI připojení – tento typ připojení je využíván u výkonných serverů. Výhodou je vysoká rychlost a výkon. Pomocí SCSI připojení je možné zapojit pevné disky, které dosahují vysokých otáček ploten a disponují velmi krátkou přístupovou dobou.

iSCSI připojení – je kombinací výše zmíněného SCSI připojení a TCP/IP protokolu. Tento typ připojení je hojně využit v úložných systémech založených na architektuře SAN, kde částečně nahrazuje propojení Fiber Channel. Proces přenosu dat využívá protokol rozhraní SCSI, prostřednictvím kterého se zařízení vzájemně dorozumívají a samotný transfer paketů je realizován na základě protokolu TCP/IP.

4.4 Zálohovací úložiště

Zálohovací úložiště tvoří jednotky a prvky, na které je možné ukládat data plynoucí z informačních systémů v rámci firemní IT infrastruktury. Zálohování dat je dvojím způsobem:

- On-site (Online)
- Off-site (Offline)

Nejdůležitějším prvkem procesu zálohování jsou síťové protokoly, které vymezují sémantiku, syntaxi a synchronizaci komunikace mezi jednotlivými aparáty. Podle zvoleného typu architektury jsou definovány i protokoly realizující vlastní přenos dat.

Zálohovací média jsou volena s ohledem na svou kapacitu, náklady, obslužnost, zpětnou kompatibilitu, přístupovou dobu.

Disky HDD – běžné pevné disky disponují velmi nízkou přístupovou dobou, robustní kapacitou a jsou snadno použitelné a škálovatelné, jsou běžně dostupné, avšak finančně náročné. Obvyklé velikosti jsou od 500 GB až po 4 TB.

Disky SSD (*Solid State Disc*) – jsou rychlejší variantou pevného disku s extrémně rychlými přístupovými dobami, avšak menší kapacitou vzhledem k vysokým cenám NAND chipů, používaných k jejich výrobě. Obvyklé velikosti jsou od 120 GB až po 1 TB.

Magnetické pásky - jsou jedním z nejpopulárnějších medií pro archivaci dat. Technologie výroby těchto pásek jsou neustále inovovány, cena těchto médií je velmi příznivá. Pořizovací náklady na systémy schopné zápisu a čtení z těchto médií jsou však velmi nepříznivé. Výhodou magnetických pásek je jejich snadná obslužnost, přenositelnost a možnost uložení mimo organizaci.

Cloud Storage – představuje moderní způsob zálohy dat, kdy jsou data uložena na diskových polích a serverech třetích stran. Provozovatelé těchto úložišť data šifrují, jsou zodpovědní za jejich redundanci. Prvotním účelem těchto úložišť nebyla možnost zálohy dat, ale jejich dostupnost z jakéhokoliv místa v jakýkoliv čas. Výhodou cloudových úložišť je jejich, takřka nezměrný, diskový prostor a v současné době klesající náklady na jejich pronájem.

PRAKTICKÁ ČÁST

Praktická část diplomové práce bude orientována na pět dílčích úseků. Analyzován bude současný stav zabezpečení perimetrů sítí v malém a středně velkém podniku, dále bude provedena analýza systému zálohování klíčových produkčních dat. Zjištěné výsledky z obou analýz, budou následně formulovány do návrhu opatření pro posílení zabezpečení infrastruktur těchto podniků, zajištění cenných dat a případnou modernizaci IT infrastruktury, zkoumaného podniku. Doporučené návrhy, scénáře zabezpečení a modernizace budou kalkulovány a oceněny, dle aktuálních cen s ohledem na předpokládané limitní rozpočty organizací.

5 Bezpečnostní audit

Analýzu bezpečnosti firemní infrastruktury, uvažuje autor pojmout, jako provedení bezpečnostního auditu zkoumané infrastruktury, vlastními silami. Provedení takového auditu, je možné uskutečnit pouze se souhlasem jednatelů společností a za předpokladu poskytnutí nezbytných oprávnění, potřebných pro diagnostiku zkoumaného prostředí.

Bezpečnostní audit IT infrastruktury společností Ašské služby, s.r.o. a Ašské lesy, s.r.o. poskytne komplexní přehled o stavu informačních systémů organizací, odhalí případná rizika, spojená s ochranou dat. Dále pomůže jasně určit, které oblasti firemní infrastruktury, bude vhodné posílit, jaké technologie použít – do kterých investovat. V neposlední řadě odhalí nebezpečí, která těmto infrastrukturám hrozí, díky identifikaci jejích slabých míst.

Audit je členěn do několika fází, které jsou prováděny v příslušném pořadí.

Přípravná fáze – někdy též označována jako fáze plánovací, je procesem, ve kterém je auditorem nadefinován plán auditu. Je určen rozsah auditu a jeho požadavky, dále jsou určeny segmenty, kterým se bude věnovat. Definována je šíře záběru auditu a také v jakém rozsahu budou zkoumány jednotlivé elementy. Zobecněny jsou použité techniky.

Fáze sběru dat a informací – je procesem sběru dat a informací o zkoumaném prostředí, při kterém je zároveň ověřováno, nakolik jsou aplikována bezpečnostní opatření a to jak procesního, tak technického rázu. Tato fáze umožňuje základní identifikaci potenciálních rizik. V této fázi je, mimo jiné, proveden průzkum prostor a okolí, provedeno je šetření se

zaměstnanci, analýza podnikových bezpečnostních politik a směrnic a v neposlední řadě jsou prováděna technická měření a operativní testy.

Fáze analýzy dat – je procesem, ve kterém jsou zpracovány všechny výsledky z provedených šetření, kategorizována jsou rizika a je proveden návrh potřebných bezpečnostních opatření.

Prezentace výsledků a připomínek – provedená šetření a analýzy jsou sumarizovány do prezentace výsledků bezpečnostního auditu. Výsledný sumář je připomínkován ze strany subjektu, jehož infrastruktura byla podrobena prováděnému auditu. Výstupem bezpečnostního auditu je výsledná zpráva, která obsahuje seznamy prostředků infrastruktury, seznam hrozeb, seznam opatření a návrhů vhodných pro eliminaci těchto hrozeb.

Bezpečnostní audit lze pojmout z hlediska technického, procesního či komplexního. **Procesní audit** je zaměřen na vzájemnou provázanost bezpečnostní politiky organizace a systému zajištění bezpečnosti IT infrastruktury organizace. Případně posuzuje systém zabezpečení s ohledem na obvyklé normy a standardy v těchto oblastech. **Technický audit** je zaměřen na funkcionality bezpečnostního systému, penetrační testování, metodická měření a šetření technického rázu v síťovém provozu. **Komplexní audit** je kombinací výše zmíněných forem, posouzeny jsou tedy všechny faktory, které plní úlohu či ovlivňují bezpečnost firemní infrastruktury.

Přínosy plynoucí z provedeného bezpečnostního auditu mohou ústit v:

- návrh vhodně zvolené bezpečnostní politiky organizace
- cílené a efektivní investovaní do těch částí infrastruktury, kde posílení dotčených prvků výrazně zesílí bezpečnost perimetru
- ochranu podnikových dat před zneužitím, destrukcí, ztrátou
- ochranu dobrého jména organizace
- posílení důvěry v tuto organizaci
- naplňovat legislativní požadavky a normy
- použití technologií, které mohou poskytnout konkurenční výhodu
- ucházet se o rozličné certifikace

5.1 Bezpečnostní audit v podnicích Ašské služby, s.r.o. & Ašské lesy, s.r.o.

Autor této diplomové práce provede bezpečnostní audit v malém a středně velkém podniku na lokální úrovni. Autor není certifikovaným auditorem IS s potřebnou certifikací CISA, rovněž také není členem profesní asociace auditorů ISACA.

Audit bude prováděn ve středně velkém podniku Ašské služby, s.r.o. a malém podniku Ašské lesy, s.r.o. Předmětem bude IT infrastruktura organizací čítající 5 serverů, 40 pracovních stanic, 17 mobilních zařízení, metalickou kabeláž, hardwarové síťové prvky, prvky systémů záložního napájení, softwarové vybavení počítačů, stav operačních systémů, systémové konfigurace počítačů, vrstvy fyzického zabezpečení, dohledový systém a systém elektronického zabezpečení objektů. V neposlední řadě bude revidován systém zálohování podnikových dat. Cílovým požadavkem na audit, je poskytnout ucelenou správu o současném stavu zabezpečení, hrozbách, rizicích a slabých místech IT infrastruktury obou organizací.

5.1.1 Fyzické zabezpečení

Obě ústřední budovy objektů včetně 5 poboček společností jsou vybaveny elektronickým docházkovým systémem. Tento systém však není doplněn systém pro autorizovaný přístup skrze čipové karty, či terminály s klávesnicemi, omezující přístup a pohyb zaměstnanců do jednotlivých sekcí. Každý ze zaměstnanců společnosti má tedy přístup do všech částí a poboček podniku. Pro bezpečnostní audit, oddíl fyzického zabezpečení, je důležitým bodem, přístup do serverovny č. 1, serverovny číslo 2 a technické místnosti. Do těchto lokalit je umožněn vstup:

Vedení

- jednatel společnosti
- ekonomický ředitel

Sekretariát

- hlavní účetní
- projektant městských komunikací

Údržba

- správce ústředního objektu společnosti
- systémový administrátor
- pracovnice úklidu

Nekontrolovaný přístup šesti osob, jejichž pracovní náplní není údržba a správa IT infrastruktury, je bezpečnostním rizikem, představujícím neúmyslné poškození hardwarového vybavení nevhodným pohybem či manipulací s vybavením uvnitř zmiňovaných místností. Tato potenciální hrozba je zřejmá, zejména ze strany pracovnice úklidu, která dle dotazu autora, nebyla vhodně proškolena.

5.1.2 Elektronický zabezpečovací systém

Společnost AS včetně svých poboček, je vybavena elektronickým zabezpečovacím systémem firmy Jablotron, třídy JA 100, sběrnicového typu. Centrálním bodem EZS je ústředna JA-106Ka s vestavěnou GSM/GPRS bránou a komunikačním rozhraním typu LAN. Ústředna je umístěna v těžko přístupných, půdních prostorách objektu. Při zběžné kontrole, však autor zaznamenal nedostatečnou kapacitu záložního napájení ústředny, kterou signalizoval indikátor. Po prostudování dokumentace k EZS, která byla autorovi k dispozici, bylo zjištěno, že GSM brána zařízení, v případě poplachu, tento signalizuje pouze na PCO. Na ústřednu jsou napojeny detektory pohybu, PIR čidla typu Ja-110P. Součástí systému je siréna typu JA-111A-BASE-Rb. Dále pak sběrnicový přístupový modul typu JA-114E a 60 kusů RFID přístupových čipů JA-191J. Chybějícími prvky systému EZS jsou environmentální detektory teploty a kouře. Mezi chybějícími prvky systému jsou i dveřní magnetické detektory. Umístění všech pohybových detektorů, ústředny i záložního napájení, je ve shodě s projektovou dokumentací. Některé z detektorů pohybu vykazují známky konce, svého provozního období. Rizikem je absence sledování nepřiměřené teploty a kouře uvnitř serveroven a technické místnosti, jako klíčových uzlů infrastruktury. Dalším problémem je nedostatečná kapacita záložního napájení ústředny, v případě výpadku dodávek elektřiny. Konfigurace ústředny, v případě poplachu, vykazuje určité rezervy. Kontrolní cvičný poplach, který byl po dohodě s vedením společnosti, spuštěn dne 10. 10. 2014 v čase 20.30 zaznamenalo čidlo č. 2, v přízemí hlavní budovy, naproti vchodovým dveřím. Příjezd zásahového vozidla společnosti zajišťující PCO, byl zaznamenán v čase 20.35. Doba příjezdu odpovídá smluvním podmínkám, pracovník bezpečnostní agentury autora a správce budovy vyzval k prokázání své identity a vazbě na společnost AS.

5.1.3 Kamerový dohledový systém

Společnost AS není vybavena dohledovým systémem. Záznam o pohybu osob vně a vůkol objektů, tedy není pořizován ani archivován. Objekt je zajištěn kovovým oplocením o výšce 180cm. Rozloha ústředí, které tvoří 4 budovy, čítá 780m čtverečních. Absence kamerového systému uvnitř a ve venkovních prostorech, představuje riziko a znemožňuje následnou identifikaci případných penetrátorů.

Společnost AL je vybavena dohledovým systémem, instalovaném v ústředí organizace, který tvoří DVR AVC-159 700TV a 4 IR analogové kamery AVC 159. Stav systému, odpovídá jeho staří (4 roky). Systém není pravidelně servisován. Záznamy z kamer, které autor shlédl, jsou silně zašuměné a zejména kamera 2 a 3 snímá nevhodný úsek vnějšího perimetru.

5.1.4 Systém záložního napájení

Záložními zdroji elektrické energie, které jsou v organizacích využity, jsou jednotky UPS značek SWEEX (3ks) BlackOut Buster (2ks) a APC (4ks). Vlastním záložním napájením disponují v serverovně číslo 1, UTM firewall, server_01, server_02, server_03. Systémem záložního napájení, však není vybavený přepínač v rackové skříni. V serverovně číslo 2 jsou vybaveny záložním napájením, oba servery. V technické místnosti je záložním napájením vybavena telefonní ústředna i brána GSM. Použité záložní jednotky přidružené k serverům jsou schopny provozu na baterie, při plné zátěži, po dobu 10 minut. Test záložních zdrojů nemohl být, z důvodu jejich užití v produkčním prostředí, realizován. Záložní zdroje napájení, ačkoliv jsou vybaveny rozhráním pro monitoring, nejsou centrálně monitorovány. Dle údajů načtených po připojení zdrojů k aplikacím, určeným pro jejich sledování, bylo zjištěno, že stav všech akumulátorů je vyhovující. Jednotlivé parametry a kapacitu, uvádím v příloze číslo 10.1. Riziko spatřuje autor v absenci záložního napájení centrálního switche v ústředí AS a také chybějícímu monitoringu jednotlivých jednotek UPS.

5.1.5 Kabeláž síťový hardware

Ústřední budova AS a přilehlé budovy jsou plně zasíťovány strukturovanou kabeláží UTP Cat 5E. Výchozím uzlem je patch panel a centrální switch, umístěný v rackové skříni,

v serverovně číslo 1. Kabeláž je usazena v lištách s výstupy v podobě dvojitých zásuvek RJ 45 a jednoduché RJ11. Podle projektové dokumentace je užito kabeláže značkového výrobce BELDEN, provedení CU-HS2. Na základě měření přístrojem FLUKE DTS 1800[70], jsou všechny realizované spoje vyhovující a odpovídají normám pro přenosovou rychlost 10/100Mbit. Serverovna č. 1 je vybavena rackovou skříní TRITON 42U o rozměrech 600x800 mm. V rozvaděči jsou uspořádány dva patch panely a centrální switch TP-LINK TL-SG1024. Kabeláž je uspořádána chaoticky, chybí značení jednotlivých vodičů. Racková skříň je vybavena zámkem, který byl v době kontroly odemčen. Dalším problémem je chybějící chlazení switche a jeho montáž bezprostředně pod patch panely. Rizikem je přehřívání tohoto HW prvku. Dalším prvkem je VDSL modem TP-LINK TD-W8961NB. Modem TP-Link pracuje s verzí firmwaru 0.4.8. Tato revize není revizí nejnovější. Serverovna č. 2 je vybavena switchem NETGEAR GS105E a routerem TP-LINK Archer C7. Technická místnost je vybavena telefonní ústřednou typu ISDN Panasonic I6SLC a GSM bránou EasyGate 2N.

Ústřední budova AL je vybavena VDSL modemem ASUS DSL-N16U, který distribuuje připojení k internetu jednak strukturovanou kabeláží UTP Cat 5E. Dalším prvkem je 8mi portový switch TP-LINK TL-SG108.

5.1.6 Prvky bezdrátové sítě

Objekt organizace AS pokrývají 4 bezdrátové sítě. Tři jsou standardu 2,4 GHz a jedna standardu 5,0GHz. Bezdrátová síť (AS-SPOT 1) je realizována prostřednictvím integrovaného vysílače modemu TP-LINK TD-W8961NB v serverovně č. 1. Bezdrátová síť (AS-SPOT 2 – záložní provoz) je distribuována prostřednictvím routeru TP-LINK Archer C7 umístěného v serverovně č. 2. Bezdrátová síť (AS-dílny) je distribuována skrze AP TP-LINK TL-WR841ND, který je umístěn v objektu garáže. Bezdrátová síť (AS-T5) je 5,0GHz spojem mezi hlavní budovou, distribuovanou routerem TP-LINK Archer C7 a anténou AirGridM5, umístěnou pod krovem protilehlých garáží. Toto 5.0GHz spojení, připojuje WLAN AS-Dílny s ústřední budovou.

Objekt organizace AL pokrývá jediná bezdrátová síť AL – SPOT 1, kterou distribuuje VDSL modem ASUS DSL-N16U A.

[70] Za zapůjčení tohoto cenného vybavení děkuji firmě Zavoďan & syn s.r.o.

Konfigurace sítí WLAN v organizacích

Tabulka 2 - Konfigurace bezdrátových sítí v podnicích

AP	AS – Dílny	AS – Spoj	AS – Spot1	AL – Spot1
Standard:	802.11n	802.11n	802.11ac	802.11n
Frekvence:	2,4 GHz	5 GHz	2,4 GHz	2,4 GHz
Kanál:	3	6	11	7
Šifrování:	TKIP/AES	TKIP/AES	TKIP/AES	TKIP/AES
DHCP:	ANO	NE	ANO	ANO
Dosah:	40 m	300 m	50m	60m
Max. př. rychl.:	600 Mbit/s	1000 Mbit/s	600 Mbit/s	600 Mbit/s
Reál. Př. rychl.:	40/20 Mbit/s	120/80 Mbit/s	40/20 Mbit/s	40/20 Mbit/s
Trans. power:	75%	90%	60%	90%
Max. počet kli.:	10	2	15	-
Ověřová. MAC:	NE	ANO	NE	NE
WPS:	ANO	NE	NE	NE

Zdroj: vlastní tvorba

Riziko představují: přímý přístup do Internetu skrze AS-SPOT1. Neaktuální firmware modemu TP-LINK TD-W8961NB. Defaultní přístupová přihlašovací jména a hesla u zařízení: routeru TP-LINK Archer C7, AP TP-LINK TL-WR841ND, antény Airgrid M5. Šifrování u AP TP-LINK TL-WR841ND dílna. Kolizní vysílací kanál u AP TP-LINK TL-WR841ND dílna. Dosah perimetru spoje 5,0GHz. Povolená funkce WPS u AP TP-LINK TL-WR841ND dílna.

5.1.7 UTM Firewall

Funkci UTM firewallu plní server_01. Firewall je instalován jako softwarový implement. Server běží pod operačním systémem Win 7 Home Premium x64. Hardwarová konfigurace serveru_01 je v příloze 10.3.1. Softwarové řešení firewallu zpracovává produkt společnosti Kerio, Kerio Control verze 7.4.1 build 5051. Licence IPS není aktivována (vypršela ke dni 01. 11. 2014). Na témže serveru běží softwarový mail klient společnosti Kerio, Kerio Connect verze 8.00 build 639. Rizikem v případě UTM firewallu je neplatná licence IPS. Používaná zastaralá verze produktů Kerio Control a Kerio Connect. Operační systém serveru je v rozporu s licenčními podmínkami společnosti Microsoft. V operačním systému jsou instalovány problematické aplikace, které nesouvisí přímo se správou a bezpečností infrastruktury.

5.1.8 Antispamové, Antispywarové, Antivirové řešení

Funkci antispamového řešení první vrstvy plní štít *Cloudmark Gateway* poskytovatele podnikového web hostingu a domény Forpsi.com. Druhou vrstvu zastává modul SpamAssassin, který je součástí produktu Kerio Connect. Antispamový filtr vychází z databáze *Spam URI Realtime Blocklist (SURBL),* kterou průběžně aktualizuje externí systémový administrátor. Třetí vrstvou je interní databáze produktu MS Outlook. Antivirovou platformou infrastruktury, je produkt Kaspersky Endpoint Security verze 10.0. Centrum pro správu AV řešení je instalováno naserveru_02. Operačním systémem serveru je MS Windows Pro x64. Řešením Kaspersky Endpoint Security jsou vybaveny všechny pracovní stanice v ústředí organizace. Podrobnější popis celého sytému AV je rozebrán 10.2. Mezi hlavní rizika tohoto oddílu auditu patří absence antimalwarového řešení. Další hrozbou je absence AV řešení na pobočkách společnosti. Volné licence řešení Kaspersky Endpoint, jsou k dispozici. Jedním z dalších rizik je absence AV řešení v mobilních zařízeních. Opět i zde jsou volné licenční kapacity k zabezpečení těchto zařízení. Chybějící implementace kontroly, realizované Kaspersky Security Centrem, u příchozí mailové pošty je dalším rizikem. Tuto funkci částečně zastává mailový server Kerio Connect, avšak pouze na úrovni filtrování příloh u příchozí pošty. AV řešení není rovněž integrováno na serveru_04, který plní funkci Fileserveru. Zde považuje autor nenasazení ochrany, za vážné riziko. Organizace AL je vybavena jednotlivými licencemi AV produktu McAfee Internet Security 10.2, které je instalováno na všech pracovních stanicích. Stanice 3, 4 a 6 mají zastaralé virové databáze. Organizace AL rovněž neužívá antispywarového řešení.

5.1.9 Servery

Podniková síť nevyužívá doménové struktury. Pracovní stanice a servery jsou zařazeny do pracovní skupiny. Server_01, server_02 a server3 jsou lokalizovány v přízemí ústřední budovy. Server_01 plní roli UTM Firewallu a Mailového serveru. Server_02 plní funkci administračního serveru Kaspersky Security Center. Server_03 je databázovým serverem, který obstarává docházkový systém. Server_04 a Server_05 jsou umístěny v prvním patře ústřední budovy. Server_04 plní roli, databázového serveru, který spravuje databázi účetního systému Money S5. Dále plní dvakráte funkci aplikačního serveru. Za prvé zajišťuje chod účetního systému Cígler Software Money S5 a za druhé spravuje geodetický a mapový systém MySis. Server_04 rovněž plní roli WSUS, skrze který distribuuje

aktualizace k pracovním stanicím. Server_05 plní funkci Fileserveru, na který zaměstnanci ukládají svá produkční data. Každý ze serverů je vybaven záložnám napájením UPS (Uninterruptible Power Supply), umožňující chod přibližně 15 minut v případě výpadku elektrické sítě. Podrobnější informace o konfiguracích hardwaru, shrnuji v příloze 10.3.

5.1.10 Pracovní stanice

Každý zaměstnanec ve zkoumaných podnicích, z oddělení administrativy a jednotliví vedoucí a mistři každého z úseků, vlastní svou pracovní stanici. Jsou jimi desktopové stanice Dell Vostro 220s, jednotné konfigurace i operačního systému, v případě společnosti AS a Lenovo IdeaCenter H30, v případě společnosti AL. Zaměstnanci, kteří svou pracovní činností realizují využíváním aplikací, napojených na některý ze serverů, mají svá pracoviště dovybavena záložními zdroji napájení. Pracovní stanice jsou vybaveny ethernetovým adaptérem, který je jejich jediným spojem do podnikového intranetu a dále, skrze UTM firewall, který řídí síťový provoz, i do internetu. Pracovní stanice v podniku AL jsou spojeny síťovým switchem, komunikace není filtrována firewallem ani bezpečnostní bránou. Jedinou ochranou je AV řešení McAfee Internet Security. Výstup z analýz, provedených na vybraných pracovních stanicích, je uveden v příloze 10.5.

5.1.11 Mobilní zařízení

V organizaci AS jsou pracovní z úseku Noviny, Správce Hřbitova a Sběrný dvůr vybaveni notebooky značek HP. V organizaci AL jsou pobočky Areál Háje, škola v přírodě Doubrava a plavecký bazén, vybaveny notebooky značky Dell. Konfigurace referenčních zařízení je uvedena níže v tabulce číslo 3. Vedoucí úseků a management společnosti je vybaven smartphony značky Samsung Galaxy S4, s operačním systémem Android verze 4.4 (Kit Kat). Externí zaměstnanec oddělení novin, je vybaven tabletem Apple Ipad 3.

Tabulka 3 - Konfigurace notebooků AS & AL

Model / Parametry	*HP 250 G3*	*HP Probook 455*	*Dell Inspiron 14*	*Toshiba Sat. R50*
Procesor	Intel Cel. N2840	AMD DCore A6	Intel Core i5	Intel Core i3
Operační paměť	4 GB	4 GB	6 GB	4 GB
Pevný disk	500 GB	500 GB	500 GB	1 TB
Grafická karta	Intel HD 4400	AMD Radeon R4	Intel HD 4400	Intel HD 4400
OS	Windows 8	Windows 7 PRO	Windows 8.1	Windows 7 PRO

Zdroj: vlastní tvorba

5.1.12 Data a jejich klasifikace

Veškeré informace a data, se kterými se v organizacích nakládá, nejsou nikterak klasifikována. Pravidla pro přístup ke sdíleným adresářům neexistují. Produkční data, uložená na Fileserveru jsou nehomogenní, nesystematicky ukládaná a rovněž nejsou šifrována. V organizacích není zavedena žádná bezpečnostní politika, která by definovala, jaká data, v jakých místech a kým, mají být ukládána a archivována.

5.1.13 Zálohování

Zálohování produkčních dat organizace AS je realizováno nesystémově. Zálohovány jsou pouze databáze, účetního systému Money S5 a mzdového systému Target. Záloha je provedena pracovnicí z účetního oddělení, jako kopie aktuálních databází na externí pevný disk. Data vyprodukována ostatními zaměstnanci, vyjma novinářů, nejsou chráněna. Částečná záloha je prováděna pouze u pracovní stanice č. 7 (noviny). Zde je provedena záloha produkčních dat z programu QUARK, na druhý diskový oddíl, téhož fyzického disku. Servery nemají uspořádány disky, v polích typu RAID. Externí záznamové zařízení není přítomno. Zařízení typu SAN, NAS není přítomno. Zálohování do úložišť cloudového charakteru, není aplikováno. Stínové kopie vytvářených dat nejsou prováděny. Bitové kopie operačních systému provozovaných serverů, nejsou vytvořeny. Datový sejf není instalován.

Produkční data organizace AL nejsou rovněž zálohována a archivována. Cennými jsou podle analýzy, zejména data z ekonomického úseku a databáze lesního hospodářství.

5.1.14 Monitoring a logování

V organizaci AS nedochází ke kontinuálnímu logování implicitních událostí. Logování na serverech 01 a 04 je v defaultních nastaveních. Výstupy z log souborů jsou sledovány namátkově administrátorem. Nástroj pro monitoring aktuálního stavu využití, klíčových prvků infrastruktury, zejména serverů, v podobě sledování využitých systémových prostředků, není instalován.

5.2 Sumarizace výsledků šetření

5.2.1 Fyzické zabezpečení infrastruktury organizací

Zjištěnými nedostatky v zabezpečení fyzického perimetru jsou:

- absence systému pro autorizovaný přístup zaměstnanců do jednotlivých sekcí organizace
- počet nekompetentních zaměstnanců s přístupem do úseků s klíčovými částmi IT

5.2.2 Elektronický zabezpečovací systém

Slabá místa v systému elektronického zabezpečení organizací:

- chybějící senzory zaznamenávající pohyb dveří a okenních tabulí
- chybějící senzory teploty a kouře v serverovnách a technické místnosti
- nevyhovující stav 4 PIR čidel systému EZS
- kapacita a stav záložního napájení sběrnicové ústředny
- konfigurace GSM brány, směřující poplach pouze na pult CO

5.2.3 Dohledový systém uvnitř a vně organizací

Organizace AS nedisponuje žádným dohledovým systémem. Sledován a monitorován není pohyb zaměstnanců ani cizích osob uvnitř objektů, taktéž vnější prostory organizace, dílny, garáže, servisní centrum a všechny ostatní pobočky organizace nejsou sledovány. Vzhledem k rozsahu obhospodařovaných prostor, představuje nepřítomnost kamerového systému vážnou hrozbu. U podniku AL jsou nevhodně směrovány 2 z celkových 4 analogových kamer. Ve špatném stavu jsou také metalické přípojky, které se projevují v silně zašuměném záznamu, pořízením bezpečnostními kamerami.

5.2.4 Systém záložního napájení klíčových prvků infrastruktury

Slabiny záložních systémů elektrické energie:

- přestože jednotky UPS disponují podporou vzdáleného monitorování a správy, není tento systém využíván
- neexistuje vnitřní pravidlo pro termíny kontroly jejich funkčnosti a stavu
- chybějící prvek UPS v případě centrálního switche organizace AS

5.2.5 Metalická kabelová infrastruktura a síťový hardware

Nedostatky v oblasti rozvodů kabeláže a stavu síťových prvků:

- nevyhovující systém uspořádání kabelového vedení, v rackové skříni (serverovna č. 1)
- chybějící značení kabelových přípojek v serverovnách
- volný přístup do rackové skříně
- nedostatečné chlazení centrálního switche
- uspořádání prvků v rackové skříni
- verze užívaného firmware u síťových prvků TP-LINK TD-W8961NB a TP-LINK TL-WR841ND

5.2.6 Bezdrátová infrastruktura WLAN

Slabiny v systému pro bezdrátový přístup do vnitřního perimetru organizace:

- síť AS-SPOT 1 je distribuována prvkem napojeným před podnikový firewall UTM
- výchozí nastavení přihlašování, do systémů pro správu síťových prvků
- nevhodná konfigurace AP TP-Link dílna
- dosah vysílacího bodu 5.0 GHz
- funkce WPS u AP dílna v defaultním nastavení – povoleno

5.2.7 Podnikový UTM firewall Kerio Control verze 7.4.1 build 5051

- verze nasazeného operačního systému, nesoucího softwarovou nadstavbu UTM firewallu je v rozporu s licenčními pravidly společnosti Microsoft
- neaktivní licence IPS
- starší verze produktu Kerio Control postrádající důležité funkcionality
- nevhodné aplikační vybavení serveru s UTM firewallem

5.2.8 Antivirové, Antispywarové a Anstispamové řešení ochrany infrastruktury

Slabými místy v této oblasti zabezpečení IT infrastruktury jsou:

- absence systému pro ochranu a detekci průniku malwaru do běžících systémů
- chybějící implementace korporátního Antivirového řešení do všech koncových bodů infrastruktury

- chybějící ochrana mobilních zařízení, užívaných v organizaci
- absence konfigurace antispamového řešení Kaspersky Security Center do aplikace MS Outlook 2010
- AV řešení není integrováno na serveru_04 – Fileserveru
- zastaralé virové databáze AV řešení McAfee na pracovních stanicích v podniku AL

5.2.9 Servery umístěné v infrastruktuře organizace AS

Rizika a hrozby v konfiguracích jednotlivých serverů organizace:

- nevhodná konfigurace v případě přepnutí provozu na záložní napájení
- chybí základní komponenty pro výměnu poškozeného hardwarového vybavení v případě jeho selhání
- není uzavřena servisní podpora HW, ke klíčovým produkčním serverům
- absence rizikových záplat v případě Fileserveru (04) s operačním systémem DEBIAN
- nevhodná konfigurace užitných rolí databázového serveru (03) s OS Win 2008 R2
- nedostatečný diskový prostor Databázového serveru (03) s OS Win 2008 R2

5.2.10 Pracovní stanice

Nedostatky v zabezpečení jednotlivých pracovních stanic:

- na všech stanicích v organizacích se pracuje pod lokálním administrátorským účtem
- není uplatňována žádná politika či restrikce v možnostech správy a instalace SW vybavení na pracovních stanicích
- aplikační vybavení stanic 01 (Fakturace), 02 (Mzdy) a 03 (Zeleň), požírající 75% systémových prostředků
- chybějící restrikce a bezpečnostní pravidlo pro přístup k portům USB
- přítomnost nelegálních aplikací na stanicích 04 (Bazén) a 05 (Listy)
- uživatelské účty s právy lokálního administrátora nejsou chráněny heslem
- absence kritických aktualizací operačního systému Windows 7 – stanice 01,02,04
- neaktuální softwarové komponenty JAVA a Adobe Flash Player – stanice 02,03,05

5.2.11 Mobilní zařízení

Rizika spojená s užíváním mobilních zařízení v organizaci:

- chybějící bezpečnostní politika v případech BYOD
- práce pod uživatelskými účty lokálního administrátora
- účty lokálních administrátorů nejsou chráněná hesly
- smartphony nejsou vybaveny AV řešením
- smartphony a podnikové notebooky nemají restrikce pro instalaci soft. vybavení
- smartphony nejsou uzamčeny pro změnu firmware

5.2.12 Data a jejich klasifikace + oprávnění

Nedostatky při manipulaci a správě podnikových dat:

- produkční data nejsou klasifikována do tříd/skupin
- přístupová oprávnění pro čtení a manipulaci s daty nastavena "for everyone"
- data nejsou tříděna a ukládána systematicky
- data nejsou šifrována
- klíčová produkční data nejsou uložena v datovém sejfu
- data nejsou archivována

5.2.13 Systém zálohování a ochrany dat

Slabá místa v metodách pro zálohu a ochranu podnikových dat:

- nesystémový přístup k zálohám produkčních dat
- záloha prováděná neproškoleným personálem
- chybějící plán na ochranu dat
- zálohování na jediný fyzický disk
- zálohy nejsou ověřovány
- chybějící zálohy pro obnovení provozu serverů
- není instalován datový sejf
- není využit potenciál serverového vybavení pro uspořádání pevných disků do polí
- není instalováno a využíváno alternativního způsobu zálohování
- absence systému zálohování produkčních dat zaměstnanců
- v podniku AL nejsou data nikterak zálohována
- chybí bitové kopie pracovních stanic
- chybí Disaster Recovery Plan

5.2.14 Monitoring a zálohování

Nedostatky oblasti sledování provozu v infrastruktuře

- chybí systém pro monitoring provozu
- chybí systém pro sledování stavu klíčových prvků infrastruktury
- záznamy o provozu nejsou centrálně vyhodnocovány
- záznamy o provozu nejsou externě ukládány a zálohovány

6 Návrhy a doporučení pro posílení zabezpečení IT infrastruktury

Z výsledků bezpečnostního auditu je patrno několikero rizik a hrozeb, spojených s nedostatečným zajištěním perimetru vnitřní sítě lan, nevhodné konfiguraci síťových prvků, serverů a pracovních stanic. Závažným rizikem je absence plánů pro zálohování podnikových dat. V této oblasti bylo odhaleno nejvíce slabých míst a nevratná ztráta dat, je z praktického hlediska, pouze otázkou času. Doporučení budou směřována do oblastí s převahou závažných rizik, ve kterých bude mít posílení bezpečnosti výrazný, efektivní vliv na zajištění IT infrastruktury jako celku.

6.1 Návrhy pro oblast zabezpečení fyzické infrastruktury

Pro jasnou evidenci a monitoring přístupů zaměstnanců, kteří se pohybují v objektech ústředí organizací, doporučuji instalaci systému pro autorizovaný přístup v podobě čipových karet, umožňující pohyb pouze v prostorech, do kterých je zaměstnanci přiděleno oprávnění. Takovýmto systémem může být například systém ALVENO či Jablotron RP 2, dále viz tabulka číslo 4 níže.

Prostory, ve kterých jsou instalovány klíčové prvky infrastruktury, by měly být zpřístupněny pouze kompetentnímu personálu, jiné osoby by se v těchto částech pohybovat neměly. Zde je možné aplikovat nařízení či pokyn vydaný vedením organizace spojený s odevzdáním přístupových klíčů, nekompetentních zaměstnanců.

6.2 Návrhy pro posílení systému elektronického zabezpečení

Nezbytné kroky zajišťující posílení stávajícího EZS:

- výměna dosluhujících PIR čidel
- instalace senzorů pro záznam pohybu dveří a okenních tabulí v oblastech serverovna 1, serverovna 2, technická místnost, pokladna, archiv
- instalace senzorů změn environmentálního prostředí (teplota + kouř) v místnostech serverovna 1, serverovna 2, technická místnost, pokladna, archiv
- výměna stávajícího akumulátoru v jednotce záložního napájení sběrnicové ústředny
- rekonfigurace GPRS brány technikem společnosti, zdvojující poplach směrovaných k jednomu ze členů vedení organizace.

6.3 Návrhy a doporučení pro dohledový systém

V organizaci AS není instalován žádný dohledový systém, proto navrhuji pořízení komplexního systému CCTV pro monitorování vnitřních a vnějších prostor ústředí organizace. Tento systém navrhuji vystavět na technologii IPTV čítající 15 bezpečnostních kamer, typu VIVOTEK IB8168-C a VIVOTEK IP8364-C. Tento dohledový systém disponuje rozlišením Full HD (1920×1080 bodů) při snímkovací frekvenci až 30 sn/s. Kompresní algoritmus záznamu - H.264, zajišťuje dramatické snížení datového toku potřebného pro přenos obrazu. V organizaci AL doporučuji přesměrovat kamery 2 a 4, tak aby zabíraly "slepá" místa v perimetru. Dále proměřit metalickou kabeláž, lépe její náhradu typem RG59, v případě budoucího upgradu systému, typem RG6.

6.4 Doporučení pro úpravu systému sledování záložních zdrojů napájení

Nezbytným doporučením je dovybavení jedné jednotky UPS v případě hardwarového switche umístěného v serverovně 1. Dále doporučuji využít možností stávajících UPS, v podobě centrálního monitoringu a správy aktuálního stavu jednotek a jejich akumulátorů. V případě systémů záložního napájení, je nutné tento systém pravidelně kontrolovat a sledovat funkčnost celého systému.

6.5 Návrhy pro oblast metalického vedení a síťového hardware

Hardwarové prvky v rackové skříni, umístěné v serverovně č. 1, doporučuji uspořádat dle běžných standardů. Doporučuji doplnit a označit kabelové přípojky v serverovně č. 1 a serverovně č. 2, včetně lišt a zásuvek RJ45. Nezbytným opatřením je zajištění rackové skříně pro neoprávněný přístup, dále doporučuji instalaci chlazení, typu DIGITUS Profi-line Cabinet (stropní ventilátor se čtyřmi chladiči a termostatem), nad centrální switch, v rackové skříni. Dále doporučuji zálohu stávajících a instalaci aktuálních revizí firmwaru u síťových prvků TP-LINK TD-W8961NB a TP-LINK TL-WR841ND.

6.6 Návrhy pro posílení bezpečnosti bezdrátových sítí WLAN

Důrazně doporučuji realizovat distribuci sítě AS SPOT 1 prostřednictvím prvku umístěného, za stávající UTM firewall. Dalším doporučením je změna přihlašovacích údajů a změna z defaultního nastavení, u komponent AP TP-LINK TL-WR841ND a

modemu ASUS DSL-N16U. Nezbytným krokem je rovněž vypnutí funkce WPS u zařízení TP LINK TL-WR841ND (AS – dílna). Realizovaný bezdrátový spoj 5.0 GHZ doporučuji distribuovat pouze do nezbytné vzdálenosti, zajišťující bezproblémový chod spoje. U zařízení TP LINK TD – W8961 NB doporučuji zálohu aktuálního a instalaci nejnovějšího firmware. Použitý standard šifrování u AP dílna, doporučuji změnit ze stávajícího WEP, na WPA 2. Vhodné bude upravit kolizní kanál AP dílna.

6.7 Doporučení pro UTM firewall

Stávající UTM firewall Kerio Control je nezbytné upgradovat minimálně na verzi 8.2, která poskytne komplexnější zabezpečení infrastruktury. Vhodné bude zakoupit aktuální licenci pro systém podpory IPS, který je licencován samostatně. Dále doporučuji reinstalaci operačního systému, pod kterým softwarový UTM firewall běží, a to na verzi OS, která nebude porušovat licenční podmínky společnosti Microsoft. Úpravy kolizních pravidel pro síťový provoz, by měly vycházet z aktuálních potřeb a zatížení IT infrastruktury, při zpracování objemných databází systémů Money S5 a MiSys. V případě, že nebude stávající operační systém serveru s UTM firewallem přeinstalován, důrazně doporučuji deinstalaci aplikačního vybavení, které přímo nesouvisí s ochranou perimetru sítě LAN. Vzhledem ke stáří současné softwarové verze firewallu Kerio Control a nevyhovující verzi operačního systému, stojí za zvážení pořízení unifikovaného samostatného hardwarového UTM firewallu, který autor, oproti ostatním řešením, upřednostňuje.

6.8 Doporučení pro antivirové, antispywarové a antispamové řešení

Nezbytným krokem pro komplexní ochranu je instalace produktů Kaspersky Endpoint Security 10 do mobilních zařízení: 2x HP Probook 455, 1x HP 250 G3 a 1x Toshiba Satellite R50. Instalace antivirového řešení je nutné provést i u androidích smartphonů Samsung Galaxy S4 (3x) a Apple iPad 3 (1x). V podnikové infrastruktuře nebyl nalezen samostatný systém pro detekci a prevenci před spywarem, zde autor doporučuje zakoupit produkt SuperAntiSpyware v korporátní edici pro 30 uživatelů. Důležitá je rovněž integrace Kaspersky Endpoint Security do, aplikací MS Outlook 2010. Antivirové řešení je rovněž nutno nasadit na server 05 (Fileserver), který běží pod operačním systémem Debian 7.0 (Wheezy).

6.9 Návrhy pro zabezpečení serverů

Prvním návrhem je změna v nastavení provozu všech serverů v případě přepnutí chodu záložního napájení, kdy dojde v přesně vymezených časových intervalech k jejich pohotovostnímu vypnutí. Za další doporučuji pořídit několikero základních hardwarových komponent (zdroje, operační paměti, chladiče, pevné disky) potřebné, k výměně při selháních. Nákup lze nahradit uzavřením rámcové smlouvy, zajišťující servisní podporu k serverovému vybavení, zejména klíčového DELL serveru 04 s operačním systémem Windows Small Business 2008 R2. Následující krok by měl směřovat k alokaci dodatečného diskového prostoru v případě serveru 04, buďto migrací na HDD s větší kapacitou nebo lépe instalací diskového pole typu RAID. V případě serveru 04 dále doporučuji vypnutí rolí, které nejsou v infrastruktuře využívány. Fileserver 05 s operačním systémem Debian verze 7.0 Wheezy, je vhodné záplatovat a chránit tak, před v únoru 2015 odhalenou hrozbou (GHOST), která využívá přetečení zásobníku, prostřednictvím knihovny GLIB jazyka C.

6.10 Návrhy pro posílení slabých míst na pracovních stanicích

Za klíčové považuji změnit pracovní účty na všech stanicích a odepřít práva lokálních administrátorů všem zaměstnancům. Dále je nezbytné zavést bezpečnostní politiku a restrikce, spočívající v zamezení svévolných instalací softwaru do pracovních stanic. Na všech pracovních stanicích požadovat přihlášení, pod účtem uživatele chráněným heslem. Deinstalovat nelegální aplikace ze stanic 01, 02, 04 a 05. Vhodné je zvážit omezení přístupu k portům USB. Stanice 02, 03 a 05 je nutno podrobit hlubší analýze, spočívající ve vyhodnocení nezbytných a zbytných aplikací, potřebných pro výkon práce uživatelů těchto stanic a to vzhledem k neúměrnému využívání systémových prostředků, pramenících v pomalý chod, těchto stanic.

6.11 Doporučení pro zabezpečení mobilních zařízení

Doporučuji zavést v podniku bezpečnostní politiku pro případy, kdy zaměstnanci využívají svých privátních zařízení, zapojených do firemní infrastruktury pro pracovní účely. Opět i mobilním zařízením, odebrat účty lokálních administrátorů a umožnit práci pouze pod běžným uživatelským účtem. Všechny účty chránit heslem. Instalovat antivirová řešení do

smartphonů. Mobilní zařízení, která nakládají s produkčními daty organizace, doporučuji šifrovat, buďto vestavěným nástrojem firmy MS, BitLockerem, či open-source řešením TrueCrypt. Všechna mobilní zařízení je vhodné opatřit aplikačním vybavením pro jejich vzdálenou lokalizaci/bezpečné odstranění a uzamčení, v případě jejich ztráty či odcizení. Zmíněnými funkcemi disponuje Kaspersky Endpoint Security, které je v infrastruktuře užito.

6.12 Návrhy pro klasifikaci dat a udělení pravomocí pro jejich správu

Produkční data organizace doporučuji vhodně klasifikovat a třídit dle jejich užití v návaznosti na jednotlivé úseky a pobočky organizace. Roztříděná data doporučuji zpřístupnit pouze těm zaměstnancům, pro které je práce s nimi nezbytná a potřebná k výkonu práce. Data ukládaná na server 05 doporučuji systematicky uspořádat do logických složek a zavést přístupová oprávnění, pouze pro tvůrce/majitele těchto dat. Klíčová produkční data je nezbytné šifrovat, například nativním řešením BitLocker, či open source řešením TrueCrypt. Data, která jsou pro činnost podniků zásadní a nenahraditelná, doporučuji zálohovaná ukládat do datového sejfu.

6.13 Návrhy pro monitoring a systém vedení záznamu o událostech v infrastruktuře

Pro monitoring infrastruktury organizace, doporučuji instalaci řešení Nagios či Solarwings. Jednotné sledování a vyhodnocování záznamu o událostech navrhuji sjednotit do systému LOGalyze. Záznamy o provozu a událostech je vhodné ukládat externě, pro případ selhání infrastruktury jako celku.

6.14 Návrh systémů pro zálohování a ochranu podnikových dat

Vzhledem k chybějícímu metodickému postupu zabraňujícímu ztrátě a poškození cenných podnikových dat navrhuji níže zcela novou koncepci pro nakládání, s veškerými produkčními daty vytvořenými v organizacích.

Proces zálohování musí, má-li být systémový a úspěšný, vycházet z několika klíčových principů, které autor uvádí níže.

1. Jasně definovat oblasti dat, které jsou pro organizaci cenné a významné a tato vymezení dále specifikovat jak pro data určená k zálohám, tak u dat určených k archivaci.
2. Investicím do systémů pro zálohování a archivaci předchází identifikace a souhrn všech hrozeb a ohrožení, ztráty a poškození klíčových dat.
3. Výběr vhodného řešení podle požadavků, na systém zálohování.
4. Test systému mimo ostrý provoz.
5. Integrace nového zálohovacího systému do podnikové infrastruktury.
6. Ověření všech funkcionalit systému.
7. Ověření kvality a komplexnosti vytvářených záloh.

V organizaci AS je produkována většina dat, skrze aplikační software, který data ukládá do databází. Dále pak projekty z geodetického systému MiSys. Poslední oblastí jsou data vyprodukovaná kancelářským balíky Microsoft Office 2010. Zatímco databáze a projekty jsou ukládány centrálně na server 04. Produkční data z kancelářských balíků jsou ukládána lokálně na pevný disk jednotlivých stanic.

Ohrožení podnikových dat, tkví zejména ve ztrátě a nevratnému poškození dat, která vyplývá z absence systému pro vytváření záloh různého typu. Hrozby pramení zejména ze selhání hardwaru infrastruktury a plyne také z chyb (zapříčiněných lidským faktorem), jako je nevhodná manipulace ze strany tvůrce dat.

Pro organizaci AS, ve které je aplikován konvenční (nestrukturovaný přístup) k zálohování dat, doporučuji přechod k tradičnímu (strukturovanému přístupu) zálohování.

Systém zálohování bude postaven na schématu D2D2C (Disc_To_Disc_To_Cloud). V systému bude, na první úrovni, zálohováno na existující Fileserver_05, ve druhé úrovni budou data duplikována na zařízení typu NAS (Network Attached Storage), třetí úrovní bude záloha pomocí cloudového řešení.

První vrstva, stávající Fileserver běžící pod operačním systémem Debian, který bude doplněn o FOG server. Tento bude konfigurován na provedení úplné zálohy pracovních stanic a serverů organizace 1x měsíčně (časově vymezeno na noc, ze soboty-neděli). Dále na provedení inkrementálních záloh stanic a serverů 2x týdně (noci středa-čtvrtek a pátek-sobota).

Druhá vrstva, tvořená zařízením typu NAS, bude sloužit jako prostor pro uložení duplikátů záloh, z první vrstvy. Přenos záznamů bude vykonávat opět FOG server v intervalech: 1x měsíčně přenos vytvořených, úplných záloh a 2x týdně přenos vytvořených záloh inkrementálních. Fyzický prvek druhé vrstvy bude umístěn v jiné budově ústředí organizace. Vybaven systémem záložního napájení.

Třetí vrstvu, zálohování dat do cloudového úložiště, bude tvořit jeden z produktů z přílohy číslo 9.6, ve které jsou porovnány parametry a ceny jednotlivých řešení. Všechny produkty třetí vrstvy jsou komerčními produkty. Autor upustil od návrhu vlastního cloudového řešení, vzhledem k vysokým pořizovacím nákladům na zajištění těchto služeb, v porovnání s velikostí organizace a malých objemech dat, která jsou ošetřována.

Rotace záloh

Vzhledem k poměrně malým, realizovaným objemům dat a rovnoměrné zátěži fyzických médií, za předpokladu využití polí typu RAID, jak v serveru_04, tak v zařízení typu NAS, bude autor abstrahovat od zavedení politiky pro rotace záloh, která by zabránila ukládání zálohovaných dat, do stále stejného úložného prostoru, na jedno fyzické médium. V případě třetí vrstvy, úvahy o rotacích záloh odpadají zcela, neboť povinnost rovnoměrného vytížení jednotlivých médií, visí plně na bedrech poskytovatele cloudového řešení.

Business Continuity Management

Velikost a rozpočet organizace, neumožňuje zavedení disciplíny Business Continuity Managementu, který by se komplexně zabýval vyhledáváním a vyhodnocováním možných dopadů na organizaci, v případě katastrofického scénáře, havárie či jiné události, která by narušila vnitřní, klíčové procesy v organizaci, ale i její vnější zájmy, postavení a prestiž.

Disaster Recovery Plan

V případě, že bude v organizaci nadefinován plán pro obnovu dat, v případě selhání, bude tento jasně determinovat postupy, prostřednictvím, kterých budou potřebná data obnovena do požadovaného stavu. Obecně lze říci, že je pro organizaci přínosnější vynakládat prostředky na nástroje a postupy, předcházející stavu selhání, nežli na nástroje odstraňující vzniklé následky kritických selhání. Zvyšování připravenosti organizace v této oblasti,

přináší rychlejší dostupnost dat v případě katastrofických scénářů a rychlejší obnovu všech zásadních podnikových procesů.

Sestavení DR plánu pro malý a středně velký podnik, bude spočívat v jasném vytyčení potřeb, pro obnovu běžného provozu infrastruktury a vymezení atributů, které obnovu přímo ovlivňují.

- ✓ které komponenty jsou kritické pro běh vnitropodnikových procesů
- ✓ které prvky jsou klíčové pro zajištění funkčnosti infrastruktury organizace
- ✓ jaký časově nejdelší horizont výpadku infrastruktury, je pro organizaci přípustný
- ✓ jak nákladný bude celý systém a jeho údržba v definované kvalitě
- ✓ jak obtížné bude resuscitovat infrastrukturu, zprovoznit její klíčové prvky
- ✓ na jakých místech jsou uloženy potřebné zálohy a kdo je oprávněn s nimi nakládat
- ✓ jakým systém jsou potřebná data zálohována a kdo je schopen data obnovit
- ✓ jakým způsobem lze verifikovat stáří dat
- ✓ k jakému bodu v minulosti, jsem schopen se vrátit
- ✓ jak rychlý bude proces obnovy dat do požadovaného stavu
- ✓ v jakém pořadí budou data v infrastruktuře obnovována
- ✓ jakým způsobem lze verifikovat úplnost obnovených dat
- ✓ ověřit komplexnost a funkčnost celého DRP
- ✓ v případě iniciace stávajícího DRP, sběr podnětů pro jeho vylepšení

7 Kalkulace navrhovaných opatření a doporučení

Velikost organizace a způsob, jakým je financována (přímá vazba na městský rozpočet) značně ovlivňuje rozhodování vedení organizace, při návrzích do budoucích investic, ve všech segmentech IT infrastruktury. Omezené možnosti financování se autor pokusí reflektovat, v alternaci komerčních (nákladnějších) řešení, návrhy striktně respektujícími požadavek, co nejnižší ceny. Vždy však bude cíleno na návrhy takových opatření, které budou usilovat, o splnění jasně determinovaných požadavků na funkčnost a komplexnost celého systému.

7.1 Náklady na posílení fyzické vrstvy zabezpečení infrastruktury

Tabulka 4 – Varianty řešení a kalkulace investic do zabezpečení fyzické vrstvy

Fyzické zabezpečení	varianta A	varianta B	varianta C	varianta D	varianta E
Řešení	Integrace systému ADVENT	Nový systém AKTION	Instalace systému generálních klíčů SHERLOCK	Nový systém ALVENO	Integrace systému Jablotron RP 02
Poznámka	integrace do stávajícího docházkového systému PowerKey 3.0	nová komponenta infrastruktury	nutno provést zásah do dveří	přístup prostřednictvím biometrických údajů	integrace do stávajícího systému EZS
Výhody	jednoduchá integrace do stávající infrastruktury	univerzální možnosti licencování	jediný klíč	technologicky nejvyspělejší řešení	ověřený dodavatel, servisní středisko v lokalitě
Nevýhody	odstávka docházkového systému při instalaci	pořizovací náklady	zásah do všech dveří	náročná instalace, pořizovací náklady	omezené možnosti budoucího rozšíření
CENA	**30 000,-**	**65 000,-**	**25 000,-**	**110 000,-**	**45 000,-**

Zdroj: vlastní tvorba

Mezi výhody systému Advent, patří jeho současné nasazení ve společnosti Ašských služeb, ve formě docházkového systému. V případě Jablotronu (také integrováno), by však integrace přístupového sytému znamenala, výraznější zásahy do budovy ústředí společnosti, která by se projevila ve vyšší časové náročnosti implementace tohoto řešení.

7.2 Náklady na posílení systému elektronického zabezpečení objektů organizace

Tabulka 5 – Varianty řešení a kalkulace investic do elektronického zabezp. systému

Posílení EZS	varianta A	varianta B	varianta C	varianta D	varianta E
Řešení	Výměna dosluhujících PIR čidel	Instalace senzorů pro záznam pohybu dveří a oken	Instalace senzorů změn environmentálního prostředí	Výměna akumulátoru záložního napájení	Rekonfigurace sběrnicové ústředny a GSM brány
Poznámka	výměna nefunkčních/ částečně funkčních za nové	místnosti pokladna, serverovna 1 +2, technická místnost	místnosti serverovna 1+2, technická místnost	zásah do sběrnicové ústředny	konfigurace technikem PCO
Výhody	bezproblémový chod systému	posílení zabezpečení těchto prostorů	komplexnost ochrany infrastruktury	zajištění dostupnosti při výpadku el. sítě	informovanost managementu
Nevýhody	--	--	--	--	--
CENA	4x 900,-	12 000,-	6000,-	2000,-	1500,-

Zdroj: vlastní tvorba

7.3 Náklady na vybudování dohledového systému CCTV v organizaci

Tabulka 6 – Varianty řešení a kalkulace investic na vybudování dohledového systému

Dohledový systém	varianta A	varianta B	varianta C
Řešení	Systém postavený na analogové technologii	Systém postavený na HD Sdi technologii	Systém postavený na IPTV technologii
Poznámka	vnější perimetr 8 kamer vnitřní infrastruktura 7 kamer 1x PVR	vnější perimetr 8 kamer vnitřní infrastruktura 7 kamer 1x PVR	vnější perimetr 8 kamer vnitřní infrastruktura 7 kamer 1x PVR
Výhody	nízké pořizovací náklady	nejlepší poměr cena/výkon	jednoduchá instalace do stávající infrastruktury
Nevýhody	starší typ technologie, kvalitativní omezení	náročnější na datový přenos mimo infrastrukturu	kompatibilita systému s existujícími řešeními na pobočkách
CENA	30 000 – 45 000,-	50 000 – 60 000,-	40 000 – 80 000,-

Zdroj: vlastní tvorba

7.4 Náklady a časová náročnost při vylepšování systémů záložního napájení

Tabulka 7 – Varianty řešení a kalkulace investic do systému záložního napájení

Úprava UPS	varianta A	varianta B	varianta C	varianta D
Řešení	Výměna stávajících akumulátorů za nové	Instalace nové jednotky UPS	Zapojení jednotek UPS do jednotného management systému	Zavedení pravidla pro pravidelné kontroly jednotek
Poznámka	výměna NiMH akumulátorů a kalibrace jednotek	umístěno k centrálnímu HW přepínači	propojení jednotek se stávající infrastrukturou skrze rozhraní pro správu	pokyn pro odpovědného pracovníka, vymezující přesný termín a rozsah kontroly
Výhody	ideální startovní pozice pro zavedení pravidla varianty D	nutný krok pro zajištění funkčnosti perimetru LAN	přehledná správa a monitoring všech užitých jednotek UPS	zajištění bezproblémového chodu systému záložního napájení
Nevýhody	--	--	--	--
CENA	**10x 1500,-**	**4500,-**	**4 hodiny**	**2 hodiny**

Zdroj: vlastní tvorba

7.5 Náklady a časová náročnost při nápravě nedostatků v Cabel-Managementu

Tabulka 8 - Varianty řešení a kalkulace investic v Cabel Managementu

Cabel Management	varianta A	varianta B	varianta C	varianta D	varianta E
Řešení	Systematické uspořádání vodičů v rozvaděči	Kompletní označení vodičů a přípojek v infrastruktuře	Instalace zámku do Rackové skříně a rozvaděče	Chlazení centrálního HW switche	Upgrade firmware klíčových síťových prvků
Poznámka	předpoklad pro budoucí zpracování dokumentace síťové architektury organizace	nezbytné východisko pro realizaci dokumentace architektury	deinstalace stávajícího zámku, od něhož nebyl dohledán klíč	současný stav chlazení nedostatečný, hrozí defekt hw prvku	nutná záloha stávajících konfigurací u jednotlivých HW prvků
Výhody	přehledné uspořádání kabeláže	přehledná správa, snadná identifikace v případě poruchy	ochrana Rackové skříně a rozvaděče neautorizovaným zásahem	zajištění ideální pracovní teploty pro klíčový HW	oprava vad a slabých míst zjištěných výrobcem, širší možnosti správy
Nevýhody	odstávka LAN infrastruktury	odstávka LAN infrastruktury	--	odstávka LAN infrastruktury	odstávka LAN infrastruktury, konfigurace
CENA / ČAS	**1000,- / 4 h.**	**2 000,- / 20 h.**	**500,- / 30**	**2 500,- / 1 h.**	**0,- / 4 hodiny**

Zdroj: vlastní tvorba

7.6 Náklady a časová náročnost při odstraňování nedostatků bezdrátových sítí

Tabulka 9 - Varianty řešení a kalkulace investic do bezdrátové topologie

Konfigurace WLAN	varianta A	varianta B	varianta C	varianta D
Řešení	Relokace HW prvku vysílače AS-SPOT 1	Změna přístupových údajů pro správu HW prvků	Rekonfigurace HW prvku TP-LINK TL-WR841ND	Rekonfigurace prvku TP-LINK Archer C7
Poznámka	umístit vysílač za UTM firewall	změna defaultních nastavení, použít přístupové heslo dle standardů	změna nastavení vysílacího kanálu	úprava výkonu vysílacího modulu 5.0 GHz
Výhody	posílení bezpečnosti infrastruktury	posílení bezpečnosti infrastruktury	eliminace výpadků, lepší konektivita sítě AS - Dílny	posílení bezpečnosti infrastruktury, nižší míra zarušení okolního prostředí
Nevýhody	--	--	--	--
CENA / ČAS	**3000,- / 1 hod.**	**30 minut**	**30 minut**	**30 minut**

Zdroj: vlastní tvorba

7.7 Náklady a časová náročnost odstraňování nedostatků UTM firewallu Kerio

Tabulka 10 - Varianty řešení a kalkulace investic do podnikového UTM firewallu

Firewall	varianta A	varianta B	varianta C	varianta D	varianta E
Řešení	Reinstalace OS serveru 01	Zakoupení licence IPS	Upgrade produktu Kerio Control na novější verzi	Deinstalace aplikačního vybavení serveru 01	Konfigurace serveru 01
Poznámka	nutno zakoupit licenci OS, nutno zálohovat současnou konfiguraci KC	zvážit kompletní upgrade řešení	zvážit koupi samostatného HW prvku namísto softwarového řešení	software nesouvisející se zabezpečením infrastruktury	nastavení komunikačních pravidel, správa portů, monitorování zátěže komunikujících prvků
Výhody	užívání systému v souladu s licenčním ujednáním MS	posílení zabezpečení infrastruktury	nové funkcionality	posílení zabezpečení infrastruktury	zvýšení efektivity provozu, posílení zabezpečení infrastruktury
Nevýhody	odstávka infrastruktury	--	odstávka infrastruktury	--	--
CENA / ČAS	**3000,- / 6 hodin**	**12 000,- / 2 h.**	**14500,- / 2 hod.**	**0,- / 1 hodina**	**0,- / 1 hodina**

Zdroj: vlastní tvorba

7.8 Náklady a časová náročnost pro posílení Antivirového a Antispywarového řešení

Tabulka 11 - Varianty řešení a kalkulace investic do antivirového systému

AV AM AS	varianta A	varianta B	varianta C	varianta D	varianta E
Řešení	Instalace KES na chybějící pracovní stanice	Integrace antispywarového řešení SuperAntiSpyware v edici Corporate	Integrace stávajícího KES do MS Outlooku na všech stanicích	Instalace KES na server 04 - Debian	Integrace antispywarového řešení Spyware Terminator 2015
Poznámka	notebook Toshiba, HP, 5x MT Samsung GS4	nutné ošetřit případnou kolizi rezidentních štítů s AV	integraci nelze provést na úrovni mailového serveru, pouze u jednotlivých klientů	instalaci lze provést za běhu	nutné ošetřit případnou kolizi rezidentních štítů s AV
Výhody	komplexnost AV řešení, ucelený přehled o stavu zabezpečení skrze Kaspersky Security Center	ochrana před spyware, malware, adware, dialery, červy, keylogery a HiJackers	třetí vrstva ochrany před nevyžádanou poštou	posílení ochrany Fileserveru a kontrola všech ukládaných dat	ochrana před spyware, malware, adware, dialery, červy, keylogery a HiJackers
Nevýhody	--	nutné pokročilé nastavení rezidentních štítů, v případě kolizního jednání, které je více než pravděpodobné	--	patrné zvýšení zátěže a nároků na systémové prostředky	nutné pokročilé nastavení rezidentních štítů, v případě kolizního jednání, které je více než pravděpodobné
CENA / ČAS	**0,- / 2 hod.**	**450,-/ licence / 4 – 6 h.**	**4 hodiny**	**0,- Kč / 1 h.**	**800,- Kč/ licence / 6 h.**

Zdroj: vlastní tvorba

Podnikové korporátní antivirové řešení, Kaspersky Endpoint Security, obsahuje pokročilé nástroje detekce malwaru. Detekce spywaru je v řešení taktéž implementována, avšak nedosahuje takové úrovně záchytů, jako doporučovaný produkt SuperAntiSpyware. Licence jsou kalkulovány, dle aktuálních ceníků, získaných z domovských stránek produktů. Vzhledem k počtu plánovaných licencí, je počítáno s korporátní multilicencí. Na poli ochrany perimetru infrastruktury proti spywaru, nelze tyto placené produkty alternovat open-source řešením, které by dosahovalo minimálně srovnatelné úrovně, jako uvedené produkty SuperAntiSpyware a Spyware Terminator.

7.9 Náklady a časová náročnost pro posílení zabezpečení serverů

Tabulka 12 - Varianty řešení a kalkulace investic do zabezpečení serverů

Servery	Server 01	Server 04	Server 05	Server 03
Řešení	A) Výměna operačního systému B) deinstlalace nadbytečného aplikačního vybavení C) konfigurace bezpečného vypnutí	A) alokace dodatečného diskového prostoru + HDD B) vypnutí nepotřebných rolí C) alokace dodatečného diskového prostoru + RAID	A) instalace záplaty GHOST B) vypnutí nepotřebných démonů c) instalace diskového pole	A) instalace dodatečné operační paměti
Poznámka	zvážit koupi samostatného HW firewallu	instalace dalšího HDD, migrace serveru na větší HDD, využití systému diskového pole	vzhledem k absenci GUI instalace skrze terminál	typ ECC kapacita 2GB
Výhody	provoz v souladu s licenčními podmínkami / samostatný HW prvek nezávislý na OS, kompaktní způsob správy	zajištění integrity systému, vyšší zabezpečení dat v případě selhání, dle typu RAID zvýšení dostupnosti	posílení zabezpečení, zvýšená ochrana dat, vyšší dostupnost a propustnost	zrychlení obslužnosti, odezvy
Nevýhody	časově náročný zásah, delší odstávka infrastruktury	server nedisponuje funkcí HOT SWAP – nutno odstavit při instalaci HW komponent	--	--
CENA / ČAS	**A – 3000,- / 8 hod.** **B – 0,- / 1 hodina** **C – 0,- / 30 minut**	**A – 4 000,- / 1 hod.** **B – 0,- / 2 hod.** **C – 12 000,- / 2 hod.**	**A – 0,- / 2 hod.** **B – 0,- / 1 hod.** **C – 12 000,- / 4 h.**	**1500,- / 20 min.**

Zdroj: vlastní tvorba

Server se softwarovým firewallem, který běží nad operačním systémem Windows 7, v edici Home Premium, nelze užívat pro provoz stanice v podnikovém prostředí. Operační systém je nutné přeinstalovat, na edici systému Professional, Enterprise či Ultimate. Vzhledem k požadavkům, dostačuje edice Professional. Ceny jsou kalkulovány dle ceníků distributora Economia a.s.

Pro instalaci diskového pole v serveru 04, lze využít aktuálního hardwarového RAID řadiče, který je součástí serveru DELL. Pro rozšíření kapacity je nutné dokoupit dodatečné pevné disky. Autor doporučuje, vzhledem k 24/7 provozu disky z edice RED firmy Western Digital. Ceny disků jsou kalkulovány dle prodejce HW, společnosti ALZA.

7.10 Náklady a časová náročnost pro posílení zabezpečení pracovních stanic

Tabulka 13 - Varianty řešení a kalkulace investic do zabezpečení pracovních stanic

Pracovní stanice	Stanice 1	Stanice 2	Stanice 3	Stanice 4	Stanice 5
Řešení	A) odebrání lokálních administrátorských práv B) restrikce v instalacích C) uživatelské účty chráněné heslem D) deinstalace nelegálního software E) deinstalace nepotřebného aplikačního vybavení	A) odebrání lokálních administrátorských práv B) restrikce v instalacích C) uživatelské účty chráněné heslem	A) odebrání lokálních administrátorských práv B) restrikce v instalacích C) uživatelské účty chráněné heslem D) deinstalace nelegálního software	A) odebrání lokálních administrátorských práv B) restrikce v instalacích C) uživatelské účty chráněné heslem D) deinstalace nelegálního software E) deinstalace nepotřebného aplikačního vybavení	A) odebrání lokálních administrátorských práv B) restrikce v instalacích
Poznámka	zde aplikovat rovněž restrikce v používání USB	zvážit čistou instalaci OS + potřebného prog. vybavení	zvážit čistou instalaci OS + potřebného prog. vybavení	zde aplikovat rovněž restrikce v používání USB	zvážit čistou instalaci OS + potřebného prog. vybavení
Výhody	eliminace potenciálních hrozeb, užívání SW v souladu s lic. podmínkami	eliminace potenciálních hrozeb, rychlejší běh OS, nižší nároky na systémové prostředky	eliminace potenciálních hrozeb, rychlejší běh OS, nižší nároky na systémové prostředky	eliminace potenciálních hrozeb, užívání SW v souladu s lic. podmínkami	eliminace potenciálních hrozeb, rychlejší běh OS, nižší nároky na systémové prostředky
Nevýhody	--	časová náročnost v případě čisté instalace	časová náročnost v případě čisté instalace	--	časová náročnost v případě čisté instalace
CENA / ČAS	**0,- / 3 hodiny**	**0,- / 5 hodin**	**0,- / 5 hodin**	**0,- / 3 hodiny**	**0,- / 5 hodin**

Zdroj: vlastní tvorba

Doporučení pro úpravu konfigurací pracovních stanic jsou propočítávány pouze z hlediska časového rámce, který zaberou případné úpravy a nastavení těchto stanic. Rekonfigurace lze zajistit z vnitřních zdrojů podniků, prostřednictvím systémového administrátora.

7.11 Náklady a časová náročnost pro posílení zabezpečení mobilních zařízení

Tabulka 14 - Varianty řešení a kalkulace investic do zabezpečení mobilních zařízení

Mobilní zařízení	Notebook 1	Notebook 2	Smartphone 01	Smartphone 02
Řešení	A) Instalace KES B) Integrace antispywarového řešení SuperAntiSpyware v edici Corporate C) Integrace stávajícího KES do MS Outlooku na všech stanicích	A) Instalace KES B) Integrace antispywarového řešení SuperAntiSpyware v edici Corporate C) Integrace stávajícího KES do MS Outlooku na všech stanicích	Instalace KES	Instalace KES
Poznámka	notebook Toshiba	notebook HP	Samsung Galaxy S 4	Samsung Galaxy S 4
Výhody	komplexnost AV řešení, ucelený přehled o stavu zabezpečení skrze Kaspersky Security Center	komplexnost AV řešení, ucelený přehled o stavu zabezpečení skrze Kaspersky Security Center	komplexnost AV řešení, ucelený přehled o stavu zabezpečení skrze Kaspersky Security Center	komplexnost AV řešení, ucelený přehled o stavu zabezpečení skrze Kaspersky Security Center
Nevýhody	nutné pokročilé nastavení rezidentních štítů, v případě kolizního jednání, které je více než pravděpodobné	nutné pokročilé nastavení rezidentních štítů, v případě kolizního jednání, které je více než pravděpodobné	--	--
CENA / ČAS	**A – 0,- / 1 hodina B – 400,- / licence C – 0,- / 1 hodina**	**A – 0,- / 1 hodina B – 400,- / licence C – 0,- / 1 hodina**	**0,- / 30 minut**	**0,- / 30 minut**

Zdroj: vlastní tvorba

Doporučení směřující do oblasti zvýšení zabezpečení mobilních zařízení, rovněž spočívají především v úpravách konfiguračních nastavení a instalaci korporátního antivirového řešení Kaspersky. Notebooky je vhodné dovybavit antispywarovým řešením v rámci výše uvedené korporátní multilicence, dle zvoleného softwarového řešení. U mobilních zařízení autor dále doporučuje šifrovat data, která v případě ztráty/odcizení zařízení, zabrání úniku citlivých firemních informací. Oba šifrovací nástroje jsou bez nákladů, počítat je nutno s dobou, kterou zabere šifrování pevných disků. Čas potřebný k zašifrování diskového oddílu závisí na množství dat určených k zašifrování, rychlosti pevného disku a hardwarovém vybavení notebooku. Zejména rychlosti a počtu jader procesoru a funkci Intel® Advanced Encryption Standard (AES), která dramatický krátí čas šifrování.

7.12 Náklady a časová náročnost systému záloh podnikových dat a archivace

Tabulka 15 - Varianty řešení a kalkulace investic na systém zálohy a archivace dat

Záloha dat a archivace	varianta 1	varianta 2	varianta 3	varianta 4	varianta 5
Řešení	Záloha na Fileserver -FOG	Záloha duplikátů z první vrstvy, do NASu Synology DiskStation DS1815+	Záloha duplikátů z první vrstvy, do NASu Synology RackStation RS814RP+	Záloha duplikátů z první vrstvy, do NASu QNAP TS-470 Pro	Záloha do Cloudového řešení D2C JuctCloud - příloha
Poznámka	nutné zbudovat třídit a klasifikovat data na stanicích, definovat rozsah záloh, četnost	pořízení NAS a integrace do infrastruktury	pořízení NAS a integrace do infrastruktury	pořízení NAS a integrace do infrastruktury	výběr cloudového řešení dle požadavků na rozsah záloh a archivace
Výhody	první vrstva zajištění podnikových dat, on-site řešení, minimální náklady	duplikace dat, druhá vrstva ochrany dat, on-site řešení	duplikace dat, druhá vrstva ochrany dat, on-site řešení	duplikace dat, druhá vrstva ochrany dat, on-site řešení	archivace, levný diskový prostor, dlouhodobě kapacitně
Nevýhody	--	--	--	--	dostupnost datových záloh, off-site řešení
CENA / ČAS	**0,- / prvotní konfigurace 6 h.**	**27 000,-**	**25 000,-**	**32 000,-**	**1200 - 3800,- /ročně**

Zdroj: vlastní tvorba

Varianty pro zálohování a archivaci dat autor dělí do tří vrstev. V první vrstvě lze využít stávajícího hardwarového vybavení, které je nutné rozšířit o FOG server, který poběží pod Debianem na Fileserveru 05. Ostatní vrstvy, jsou již spojené s investicemi do pořízení nákladnějšího hardwarového vybavení, v podobě zařízení typu NAS a pronájmu cloudového úložiště. NAS jednotky Synology a QNAP jsou ceněny dle aktuálních ceníků přímo od výrobců těchto zařízení. Obě varianty jsou kalkulovány na pořízení edicí Small business, které plně vyhovují provozu v malém a středně velkém, zkoumaném podniku. Pronájem cloudového úložiště, je kalkulován na roční provoz, dle webů cloud. společností.

8 ZÁVĚR

Problematika bezpečnosti firemní infrastruktury a ochrana dat v malých a středních podnicích patří k důležitým, avšak opomíjeným tématům. Vedení organizací, problematiku bezpečnosti infrastruktury upozaďuje, oproti zřetelnějším a obvyklejším formám nebezpečí, které organizacím hrozí. Autor považuje za nezbytné upozornit na klíčový atribut, kterým nedostatečné zabezpečení perimetrů podniku a slabá ochrana dat, převyšuje ostatní rizika ohrožující organizace, činné ve veřejné správě a rozvoji regionů – bezprostřednost a okamžitost. Zatímco čerpání omezeného rozpočtu, odliv kvalifikovaných pracovníků a nevalná opora v zákonech, jsou problémem pozvolným a plíživým (organizace disponuje solidními reakčními časy, v řádech týdnu až měsíců), v případě útoku na podnikovou síť, převzetí kontroly nad klíčovým serverem infrastruktury, či ztrátě a úniku zásadních podnikových dat, je čas nutný pro obnovení původního stavu, otázkou několika hodin.

V diplomové práci autor usiluje o obsáhnutí tématu bezpečnosti infrastruktury v malých a středních podnicích a způsoby, jakými podniky nakládají s produkčními daty. Teoretická část je rešerší odborné literatury, tematicky zaměřenou na síťové architektury, bezpečnost serverů a stanic, datová úložiště, archivaci dat a cloudová řešení. Praktická část je orientována na vlastní výzkum a testování současného stavu a úrovni bezpečnosti v podnicích, v regionu.

Provedené analýzy současného stavu zabezpečení perimetrů metalických a bezdrátových sítí, serverů, pracovních stanic, mobilních zařízení a hardwarových prvků v infrastrukturách společností Ašské služby, s.r.o. a Ašské lesy, s.r.o. odhalily závažná bezpečnostní rizika a nedostatky. Rizika jsou, vzhledem ke své závažnosti, hodnocena jako kritické slabiny, s působností na funkčnost a provoz, napříč podnikovými ekosystémy.

Bezpečnostní audit realizovaný autorem v podnicích, poskytl komplexní přehled o všech hrozbách a slabých místech infrastruktury v podnicích. Závažné hrozby nalezl autor v architektuře bezdrátové sítě, kdy nevhodné umístění jednoho z hardwarových prvků a způsob jeho konfigurace, představuje snadný cíl ze strany útočníka.

Konfigurace a nedostatečné množství systémových prostředků na klíčovém aplikačním serveru se odráží v latencích a pomalé obslužnosti, při práci s hlavním nástrojem

ekonomického úseku, podniku Ašské služby – účetním systémem Money S5. Databázový server odpovídá se značným prodlením a v případě souběžné práce vícera zaměstnanců v systému, jsou odezvy téměř dvojnásobné.

Korporátní antivirové řešení Kaspersky, není v podnicích nasazeno na všech stanicích a zařízeních. Problematická je konfigurace antivirového řešení na serveru s Kerio firewallem, kde dochází ke konfliktům rezidentních štítů.

Nedostatky byly zjištěny i v případě elektronického zabezpečovacího systému. Konfigurace sběrnicové ústředny, která je centrálním bodem ochrany objektů, je problematická, stejně tak stav záložního napájení je nevyhovující.

Softwarový UTM firewall, užitý jako nadstavba operačního systému, je instalován na serveru, jehož operační systém je v rozporu s licenčními podmínkami Microsoftu.

Systém záložního napájení je projektován v souladu s normami a kapacitně odpovídá požadavkům na dodávku energie v případě výpadku elektrické sítě, s výjimkou serverovny číslo 2, kde je nutno dovybavit záložním zdrojem energie, centrální switch.

Absence dohledového systému v ústředí podniku Ašské služby, autor hodnotí negativně. Vzhledem k rozsahu objektu a jeho umístění na periferii města, je vhodné sledovat pohyb osob po objektu, zejména mimo pracovní dobu.

Závažným pochybením v bezpečnosti systémů, je výkon práce zaměstnanců na pracovních stanicích, pod lokálním administrátorským účtem. Tento nedostatek byl identifikován na všech stanicích u obou podniků a představuje kritickou slabinu.

Systém zálohování podnikových dat v podniku Ašských služeb je nesystematický. Zálohy nejsou automatizovány. Prováděny manuálně, neproškoleným zaměstnancem. Stav a integrita záloh není ověřována. Zásadní podniková data nejsou nikterak archivována.

Nedostatky a rizika byla identifikována ve třinácti z patnácti analyzovaných bezpečnostních vrstev infrastruktury podniku Ašské služby a devíti z jedenácti vrstev společnosti Ašské lesy. Uspokojivé výsledky byly zaznamenány, u obou společností, v oblastech rozvodů a kvalitě metalické kabeláže, tvořící páteřní komunikační síť v podnicích.

Nápravným opatřením a doporučeními jsou v případě podniku Ašských služeb, změny v konfiguracích serverů a uspořádání síťových hardwarových prvků. Rekonfigurace sběrnicové ústředny systému elektronického zabezpečení. Instalace nové jednotky záložního napájení do serverovny číslo 2. Výstavba dohledového systému v ústředí podniku. Integrace antivirového řešení Kaspersky Endpoint Security na všechny pracovní stanice, včetně mobilních zařízení. Změny v hardwarové konfiguraci databázového serveru. Investice do nového nárazníkového firewallu, případně výměna operačního systému pod softwarovou nadstavbou. Změna systému zálohování, spočívající v integraci zařízení typu NAS do infrastruktury a pronájem cloudového úložiště, určeného pro archivaci a duplikaci podnikových dat. V podniku Ašských lesů, je nutno rekonfigurovat nastavení přístupového bodu bezdrátové sítě. Zavést systém pro zálohu produkčních dat na externí diskové pole, případně zařízení typu NAS, pronajmout cloudový prostor. Doporučuji úpravu nastavení, restrikce oprávnění lokální správy, všech pracovních stanic.

Při sestavování variantních, nápravných opatření pro oba podniky, autor respektuje omezené rozpočty malého a středně velkého podniku. Každá varianta je kalkulována s cenovým rozpětím, které lze aplikovat, při zachování přidané hodnoty v podobě posílení stávajícího zabezpečení. Některá nápravná opatření jsou realizovatelná, bez nutnosti dalších investic. Jsou spojeny pouze s částečnou, u některých opatření kompletní, odstávkou systémů a serverů. Varianty jsou vymezeny v časových harmonogramech, které pokrývají, dobu nezbytně potřebnou, pro aplikaci nápravných kroků.

V prostředí zkoumaných podniků, autor doporučuje konzultovat nápravu současného stavu podnikové infrastruktury, se specialistou na bezpečnost. Identifikované hrozby klasifikuje jako závažné a hrozící výpadek či nevratná ztráta dat, je více než pravděpodobná.

Autor předložil výsledky šetření jednatelům obou podniků, kteří připomínkovali zkoumané oblasti auditu a vzhledem k neuspokojivému stavu současného stavu infrastruktury u obou organizací, požádali autora o další spolupráci.

Zaměření autorova výzkumu v oblasti zabezpečení a zálohy dat v malých a středních podnicích, je cíleno na technické aspekty infrastruktury. Pro svou další činnost a spolupráci s podniky, autor hodlá zpracovat bezpečnostní audit procesního charakteru, který bude cílen na vzájemnou provázanost bezpečnostní politiky s nasazenými technologiemi.

9 SEZNAM POUŽITÝCH ZDROJŮ

Tištěné zdroje

BEJTLICH, Richard. *The practice of network security monitoring: understanding incident detection and response*. San Francisco: No Starch Press, 2013, 1 online zdroj (379 pages). ISBN 978-1-59327-534-1.

BIGELOW, Stephen J. Mistrovství v počítačových sítích: správa, konfigurace, diagnostika a řešení problémů. Vyd. 1. Překlad Petr Matějů. Brno: ComputerPress, 2004, 990 s. ISBN 80-251-0178-9.

CIAMPA, Mark D. Security+ guide to network security fundamentals. 4th ed. Boston, MA: Course Technology, Cengage Learning, c2012, xxvi, 628 p. ISBN 1111640122.

DONAHUE, Gary A. Network warrior. 2nd ed. Beijing: O'Reilly, 2011, xxiii, 757 s. ISBN 978-1-449-38786-0.

ENDORF, Carl. Detekce a prevence počítačového útoku. 1. vyd. Praha: Grada, 2005, 355 s. ISBN 80-247-1035-8.

ENGEBRETSON, Pat a James BROAD. The basics of hacking and penetration testing: ethical hacking and penetration testing made easy. Waltham, MA: Syngress, c2011, xvii, 159 p. ISBN 1597496553.

ERICKSON, Jon. Hacking: the art of exploitation. 2nd ed. San Francisco, Calif.: No Starch Press, c2008, x, 472 p.

GIBSON, Darril. CompTIA security+ get certified get ahead SYO-301 study guide. North Charleston, SC: CreateSpace, c2011, xix, 559 p. ISBN 1463762364.

HARRINGTON, Jan L. Network security: a practical approach. Boston: Morgan Kaufmann Publishers, c2005, xv, 365 p. ISBN 0123116333.

HORÁK, Jaroslav a Milan KERŠLÁGER. Počítačové sítě pro začínající správce. 3., aktualiz. vyd. Brno: ComputerPress, 2006, 211 s. ISBN 80-251-0892-9.

KENNEDY, David. Metasploit: the penetration tester's guide. 1st ed. San Francisco: No Starch Press, c2011, xxiv, 299 s. ISBN 9781593272883.

NEMETH, Evi, Garth SNYDER a Trent R HEIN. Linux: kompletní příručka administrátora: 2. aktualizované vydání. Vyd. 1. Brno: ComputerPress, 2008, 984 s. ISBN 978-80-251-2410-9.

ODOM, Wendell. Počítačové sítě bez předchozích znalostí. Vyd. 1. Brno: CP Books, 2005, 383 s. ISBN 80-251-0538-5.

SHINDER, DebraLittlejohn. Počítačové sítě: nepostradatelná příručka k pochopení síťové teorie, implementace a vnitřních funkcí. Praha: SoftPress, 2003, 752 s. ISBN 80-864-9755-0.

SOSINSKY, Barrie A. Mistrovství – počítačové sítě. Vyd. 1. Brno: ComputerPress, 2010, 840 s. Mistrovství (ComputerPress). ISBN 978-80-251-3363-7.

STREBE, Matthew a Charles PERKINS. Firewally a proxy-servery. Vyd. 1. Brno: Computer Press, 2003, xxi, 450 s. ISBN 80-722-6983-6.

TRULOVE, James. Sítě LAN: hardware, instalace a zapojení. 1. vyd. Praha: Grada, 2009, 384 s. ISBN 978-80-247-2098-2.

ZANDL, Patrick. Bezdrátové sítě WiFi: praktický průvodce. Vyd. 1. Brno: ComputerPress, 2003, 190 s. ISBN 80-722-6632-2.

Elektronické zdroje

Access Communications. ACCESS COMMUNICATIONS PTY LTD. *Www.accesscomms.com* [online]. 2014 [cit. 2014-11-04]. Dostupné z: https://www.accesscomms.com.au/reference/coax.htm

Best cloud storage [online]. 2015 [cit. 2015-03-10]. Dostupné z: http://www.bestcloudstorage.net/

Edraw Visualization Solutions. *Active Directory Diagramming Software* [online]. 2013 [cit. 2014-11-04]. Dostupné z: http://www.edrawsoft.com/Active-Directory.php

ESET, spol. s.r.o Antispam vás zbaví nevyžiadanej pošty: Antispam. ESET, spol. s.r.o. w*ww.eset.com* [online]. 2014 [cit. 2014-10-30]. Dostupné z: http://www.eset.com/sk/antispam/

Qnap.com [online]. 2015 [cit. 2015-03-10]. Dostupné z: https://www.qnap.com/i/in/product/mo del.php?II=106&event=2

Reichelt.de [online]. 2015 [cit. 2015-03-10]. Dostupné z: ZDROJ:http://www.reichelt.de/QNAP-TS-470PRO/3/index.html?ACTION=3&GROUPID=5788&ARTICLE=140035&OFFSET=16&

SURAPATI, Taufan. How Antivirus Works: SignatureBasedDetection, HeuristicScanning and BehaviorBlocker [online]. 13. 8. 2011. [cit. 30-10-2014]. Dostupné z: http://www.articlesbase.com/security-articles/how-antivirusworks-signature-based-detection-heuristic-scanning-and-behavior-blocker-5124641.html.

Synology.com [online]. 2015 [cit. 2015-03-10]. Dostupné z: https://www.synology.com/en-us/products/DS1815+#photo
Synology.com [online]. 2015 [cit. 2015-03-10]. Dostupné z: https://www.synology.com/cs-cz/products/DS1815+#spec

Synology.com [online]. 2015 [cit. 2015-03-10]. Dostupné z: https://www.synology.com/img/products /photo/RS814+/001.jpg

Synology.com [online]. 2015 [cit. 2015-03-10]. Dostupné z: https://www.synology.com/cs-cz/products/RS814+#spec

ŠVANCARA, Petr. P2P. *PC sítě* [online]. 1. vyd. 2006 [cit. 2014-11-03]. Dostupné z: http://www.p2p-aktualne.wz.cz/Kroucena_dvojlinka.htm

THE OPEN GROUP. *The UNIX System* [online]. 1. vyd. Londýn, 2012 [cit. 2014-11-03]. Dostupné z: http://www.unix.org/what_is_unix/history_timeline.html

10 PŘÍLOHY

10.1 Přehled a stav jednotek záložního napájení

Tabulka 16 - Jednotky UPS

Jednotka UPS	Výkon	VA - zdánlivý výkon	Počet akumulátorů	Stav akumulátorů
APC Back CS 500L č.	300	500	1	67%
APC Back CS 500L č.	300	500	1	72%
Sweex I 1000 č. 1	600	1000	2	95%
Sweex I 1000 č. 2	600	1000	2	85%
Sweex I 1000 č. 3	600	1000	2	90%
APC Smart 1500 č. 1	980	5000	3	8%
APC Smart 1500 č. 1	980	5000	3	93%
APC Smart 1500 č. 1	980	5000	3	88%
APC Smart 420 č. 1	260W	500	1	66%
APC Smart 420 č. 2	260W	500	1	66%
APC Smart 420 č. 3	260W	500	1	56%
APC Smart 420 č. 4	260W	500	1	77%

Zdroj: vlastní tvorba

10.2 Korporátní antivirové řešení Kaspersky Endpoint Security 10

Nasazeným AV řešením je produkt společnosti Kaspersky ve verzi SELECT. Tento produkt považuje autor za vysoce účinný a sofistikovaný. Produkty společnosti Kaspersky se pravidelně umisťují, na předních pozicích, komparativních testů antivirových řešení. V společnosti AS však není tento produkt implementován na všechny stanice. Kritické je z pohledu autora, nenasazení AV řešení na linuxový Debian Fileserver a mobilní zařízení, včetně smartphonů, které jsou používány i mimo infrastrukturu společnosti.

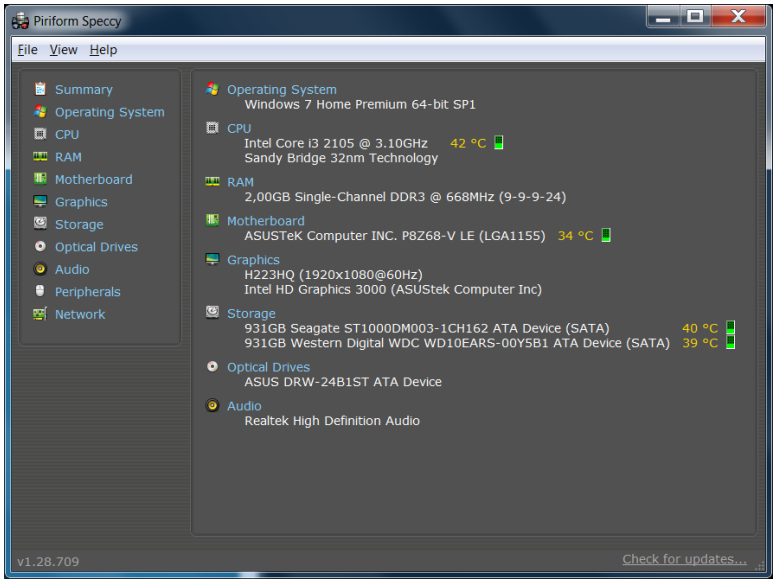
Klíčovými atributy Kaspersky Endpoint Security SELECT ve verzi 10.0 jsou:

- ochrana proti malwaru pro pracovní stanice
- Systém urgentní detekce (Urgent Detection System)
- System Watcher
- Aktivní čištění
- Cloudová ochrana
- Systém prevence vniknutí na bázi hostitele (HIPS) s osobní bránou firewall
- Network Attack Blocker
- Ochrana proti malwaru pro souborové servery
- Ochrana proti malwaru pro prostředí souborových serverů na různých platformách
- Jednoduchá správa a flexibilní hlášení
- Podpora virtualizace
- Mobilní ochrana před malwarem
- Řízení aplikací pro mobilní zařízení
- Šifrování
- Oddělení různých typů údajů
- Ochrana při krádeži mobilních zařízení
- Komplexní funkce pro správu
- Řízení (aplikace, zařízení, web)
- Správa aplikací
- Dynamický whitelist
- Správa zařízení
- Správa webových stránek
- Unifikovaná konzole pro správu

10.3 Hardwarová konfigurace serverů

10.3.1 Server 01 – Kerio Firewall

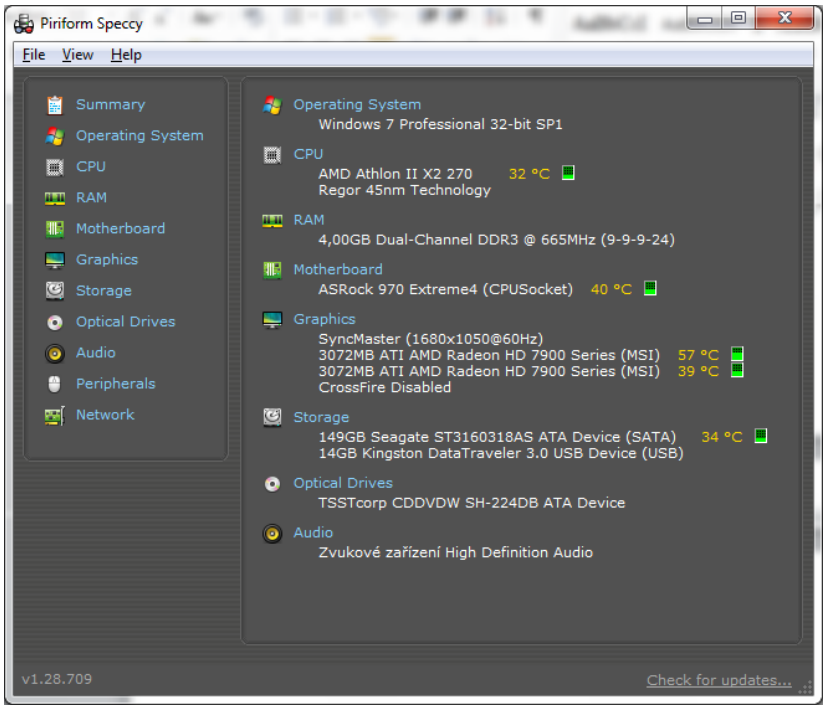
Obrázek 3 - konfigurace serveru 01



Zdroj: vlastní tvorba

10.3.2 Server 02 – Kaspersky Endpoint Security CENTER

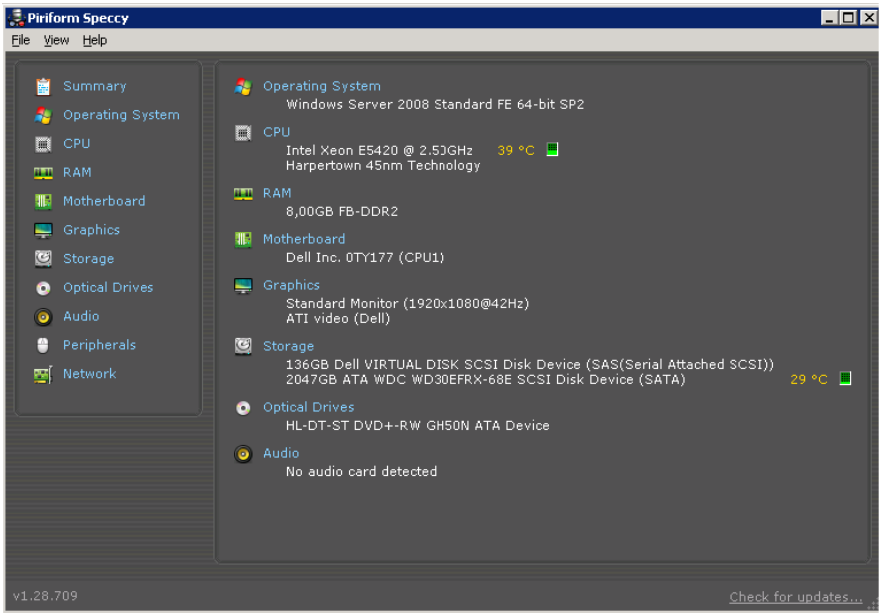
Obrázek 4 - konfigurace serveru 02



Zdroj: vlastní tvorba

10.3.3 Server 04 – SQL Server Money

Obrázek 5 - konfigurace serveru 04



Zdroj: vlastní tvorba

10.4 Zprávy o zabezpečení serverů

10.4.1 Server 01 – Kerio Firewall

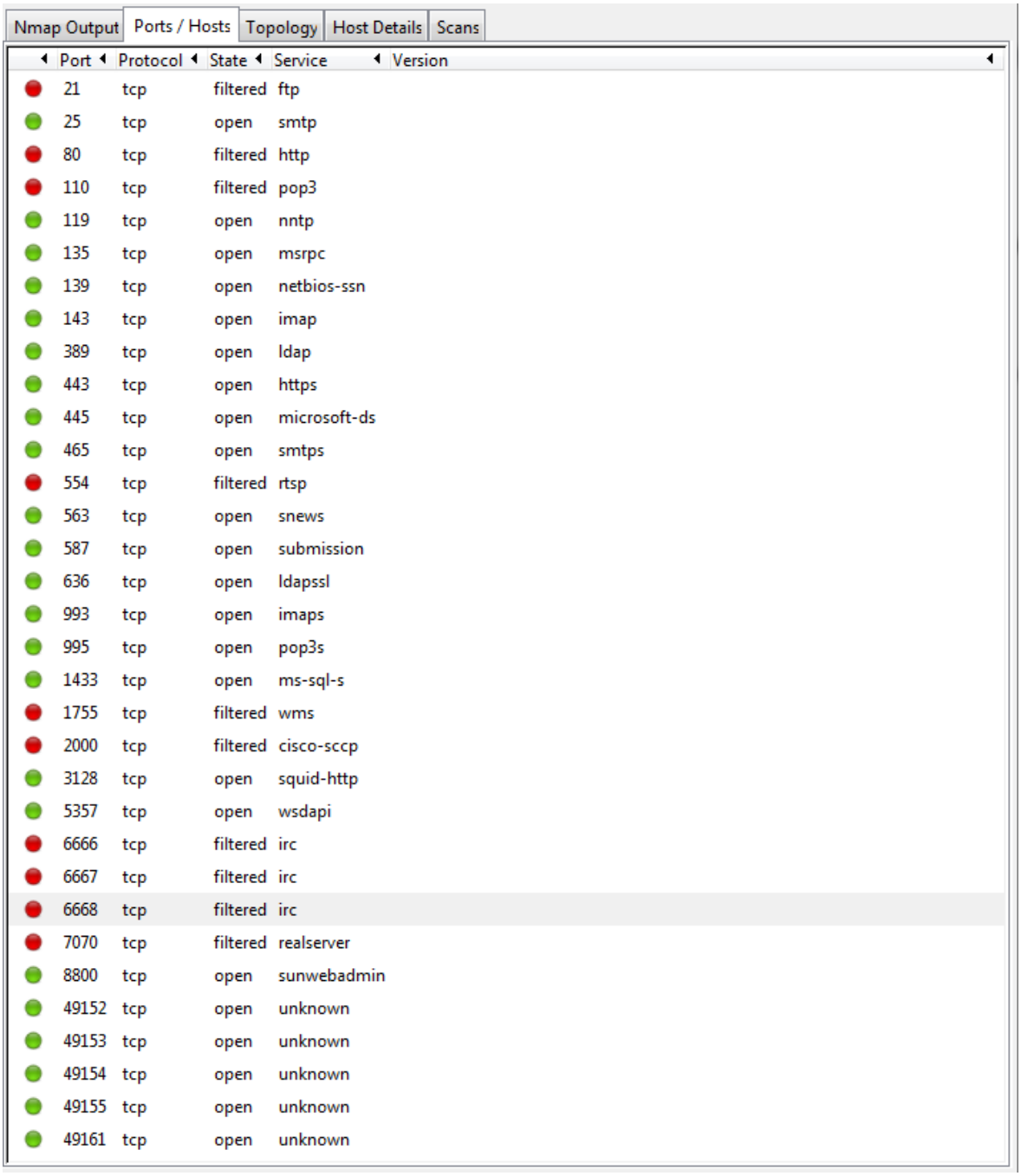
Obrázek 6 - Informace o portech a běžících službách

```
Starting Nmap 6.47 ( http://nmap.org ) at 2015-03-10 09:11 Střední Evropa (běžný čas)
Nmap scan report for 192.168.117.200
Host is up (0.0010s latency).
Not shown: 967 closed ports
PORT      STATE    SERVICE
21/tcp    filtered ftp
25/tcp    open     smtp
80/tcp    filtered http
110/tcp   filtered pop3
119/tcp   open     nntp
135/tcp   open     msrpc
139/tcp   open     netbios-ssn
143/tcp   open     imap
389/tcp   open     ldap
443/tcp   open     https
445/tcp   open     microsoft-ds
465/tcp   open     smtps
554/tcp   filtered rtsp
563/tcp   open     snews
587/tcp   open     submission
636/tcp   open     ldapssl
993/tcp   open     imaps
995/tcp   open     pop3s
1433/tcp  open     ms-sql-s
1755/tcp  filtered wms
2000/tcp  filtered cisco-sccp
3128/tcp  open     squid-http
5357/tcp  open     wsdapi
6666/tcp  filtered irc
6667/tcp  filtered irc
6668/tcp  filtered irc
7070/tcp  filtered realserver
8800/tcp  open     sunwebadmin
49152/tcp open     unknown
49153/tcp open     unknown
49154/tcp open     unknown
49155/tcp open     unknown
49161/tcp open     unknown
MAC Address: 00:21:27:C4:AA:64 (Tp-link Technology Co.)

Nmap done: 1 IP address (1 host up) scanned in 3.82 seconds
```

Zdroj: vlastní tvorba

Obrázek 7 - Stav portů – Server 01



Nmap Output | Ports / Hosts | Topology | Host Details | Scans

Port	Protocol	State	Service	Version
21	tcp	filtered	ftp	
25	tcp	open	smtp	
80	tcp	filtered	http	
110	tcp	filtered	pop3	
119	tcp	open	nntp	
135	tcp	open	msrpc	
139	tcp	open	netbios-ssn	
143	tcp	open	imap	
389	tcp	open	ldap	
443	tcp	open	https	
445	tcp	open	microsoft-ds	
465	tcp	open	smtps	
554	tcp	filtered	rtsp	
563	tcp	open	snews	
587	tcp	open	submission	
636	tcp	open	ldapssl	
993	tcp	open	imaps	
995	tcp	open	pop3s	
1433	tcp	open	ms-sql-s	
1755	tcp	filtered	wms	
2000	tcp	filtered	cisco-sccp	
3128	tcp	open	squid-http	
5357	tcp	open	wsdapi	
6666	tcp	filtered	irc	
6667	tcp	filtered	irc	
6668	tcp	filtered	irc	
7070	tcp	filtered	realserver	
8800	tcp	open	sunwebadmin	
49152	tcp	open	unknown	
49153	tcp	open	unknown	
49154	tcp	open	unknown	
49155	tcp	open	unknown	
49161	tcp	open	unknown	

Zdroj: vlastní tvorba

10.4.2 Server 04 – Aplikační a databázový server Money S5 & MiSys

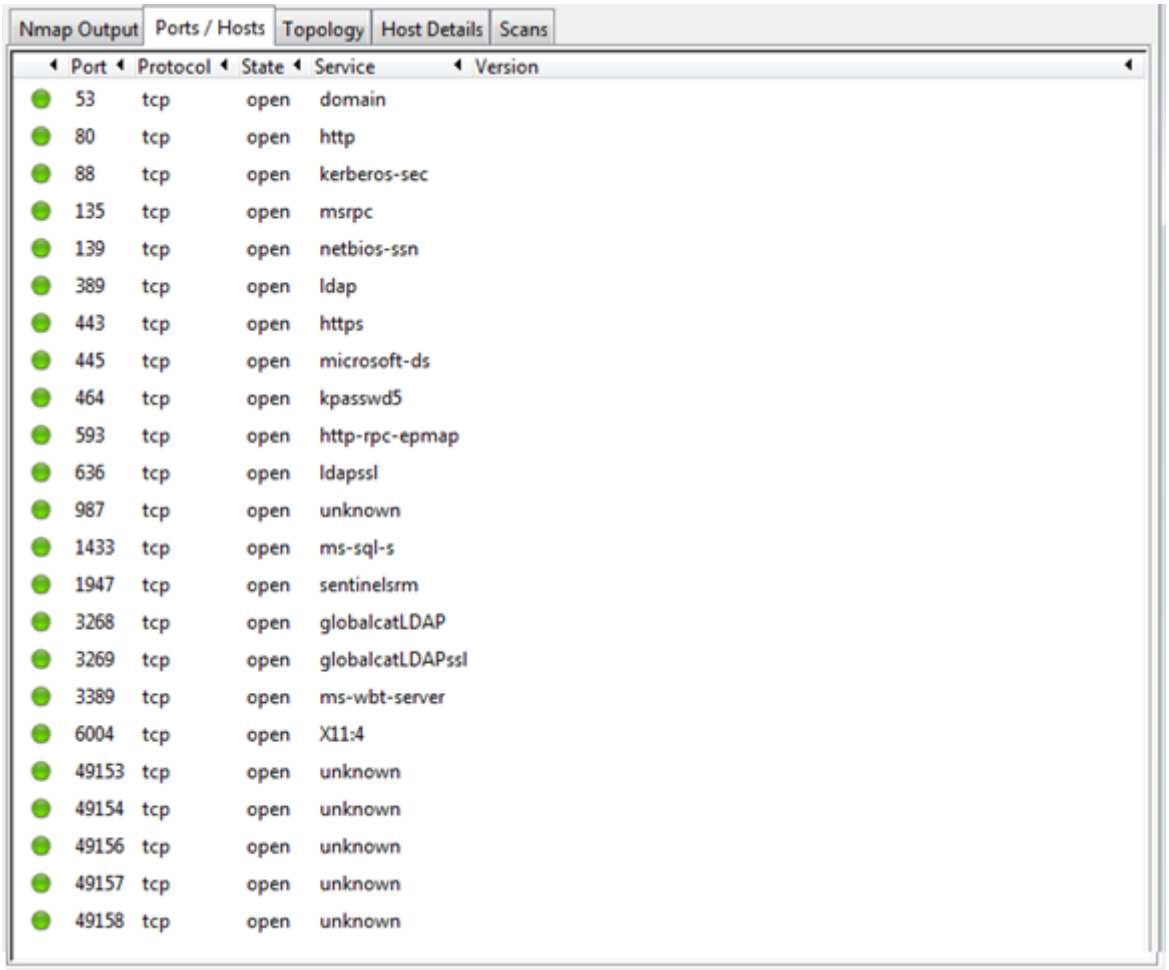
Obrázek 8 – informace o portech a běžících službách

```
Starting Nmap 6.47 ( http://nmap.org ) at 2015-03-10 09:25 Střední Evropa (běžný čas)
Nmap scan report for 192.168.117.45
Host is up (0.0019s latency).
Not shown: 977 filtered ports
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
443/tcp   open  https
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
987/tcp   open  unknown
1433/tcp  open  ms-sql-s
1947/tcp  open  sentinelsrm
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
3389/tcp  open  ms-wbt-server
6004/tcp  open  X11:4
49153/tcp open  unknown
49154/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
49158/tcp open  unknown
MAC Address: 00:26:B9:2F:42:24 (Dell)

Nmap done: 1 IP address (1 host up) scanned in 5.69 seconds
```

Zdroj: vlastní tvorba

Obrázek 9 - Stav portů - Server 04



Port	Protocol	State	Service	Version
53	tcp	open	domain	
80	tcp	open	http	
88	tcp	open	kerberos-sec	
135	tcp	open	msrpc	
139	tcp	open	netbios-ssn	
389	tcp	open	ldap	
443	tcp	open	https	
445	tcp	open	microsoft-ds	
464	tcp	open	kpasswd5	
593	tcp	open	http-rpc-epmap	
636	tcp	open	ldapssl	
987	tcp	open	unknown	
1433	tcp	open	ms-sql-s	
1947	tcp	open	sentinelsrm	
3268	tcp	open	globalcatLDAP	
3269	tcp	open	globalcatLDAPssl	
3389	tcp	open	ms-wbt-server	
6004	tcp	open	X11:4	
49153	tcp	open	unknown	
49154	tcp	open	unknown	
49156	tcp	open	unknown	
49157	tcp	open	unknown	
49158	tcp	open	unknown	

Zdroj: vlastní tvorba

10.4.3 Server 02 – Kaspersky Endpoint Security Center

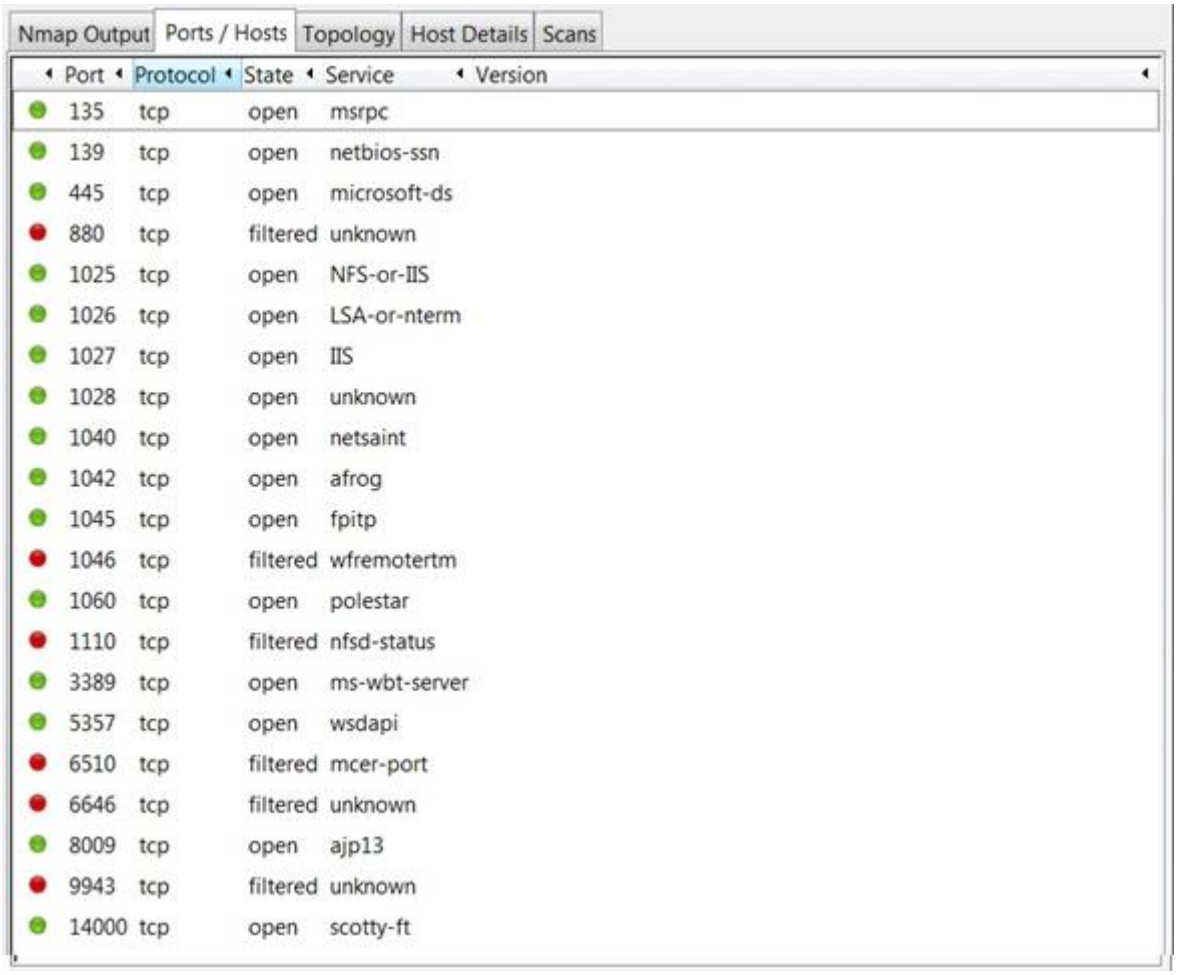
Obrázek 10 - Informace o portech a běžících službách

```
Starting Nmap 6.47 ( http://nmap.org ) at 2015-03-10 09:38 Střední Evropa (běžný čas)
Nmap scan report for 192.168.117.30
Host is up (0.00s latency).
Not shown: 979 closed ports
PORT      STATE    SERVICE
135/tcp   open     msrpc
139/tcp   open     netbios-ssn
445/tcp   open     microsoft-ds
880/tcp   filtered unknown
1025/tcp  open     NFS-or-IIS
1026/tcp  open     LSA-or-nterm
1027/tcp  open     IIS
1028/tcp  open     unknown
1040/tcp  open     netsaint
1042/tcp  open     afrog
1045/tcp  open     fpitp
1046/tcp  filtered wfremotertm
1060/tcp  open     polestar
1110/tcp  filtered nfsd-status
3389/tcp  open     ms-wbt-server
5357/tcp  open     wsdapi
6510/tcp  filtered mcer-port
6646/tcp  filtered unknown
8009/tcp  open     ajp13
9943/tcp  filtered unknown
14000/tcp open     scotty-ft
MAC Address: BC:5F:F4:BC:E4:06 (ASRock Incorporation)

Nmap done: 1 IP address (1 host up) scanned in 81.43 seconds
```

Zdroj: vlastní tvorba

Obrázek 11 - Stav portů - Server 02



Nmap Output | Ports / Hosts | Topology | Host Details | Scans

Port	Protocol	State	Service	Version
135	tcp	open	msrpc	
139	tcp	open	netbios-ssn	
445	tcp	open	microsoft-ds	
880	tcp	filtered	unknown	
1025	tcp	open	NFS-or-IIS	
1026	tcp	open	LSA-or-nterm	
1027	tcp	open	IIS	
1028	tcp	open	unknown	
1040	tcp	open	netsaint	
1042	tcp	open	afrog	
1045	tcp	open	fpitp	
1046	tcp	filtered	wfremotertm	
1060	tcp	open	polestar	
1110	tcp	filtered	nfsd-status	
3389	tcp	open	ms-wbt-server	
5357	tcp	open	wsdapi	
6510	tcp	filtered	mcer-port	
6646	tcp	filtered	unknown	
8009	tcp	open	ajp13	
9943	tcp	filtered	unknown	
14000	tcp	open	scotty-ft	

Zdroj: vlastní tvorba

10.4.4 Server 03 – Fileserver (Debian)

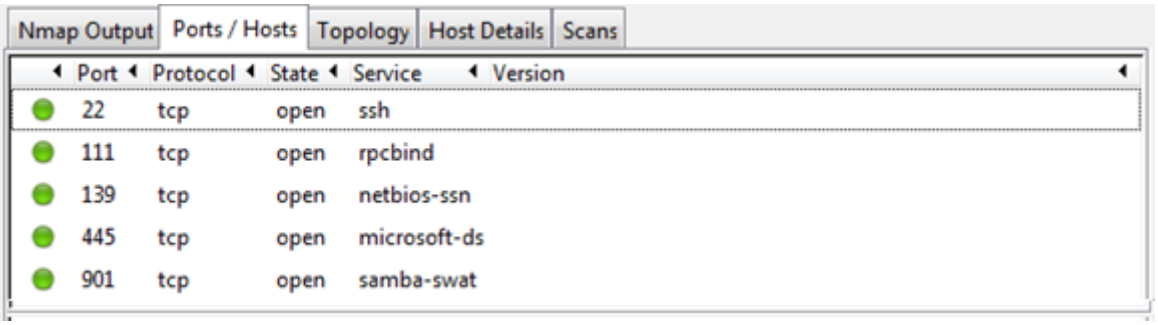
Obrázek 12 - Informace o portech a běžících službách

```
Starting Nmap 6.47 ( http://nmap.org ) at 2015-03-10 09:46 Střední Evropa (běžný čas)
Nmap scan report for 192.168.117.12
Host is up (0.000068s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
111/tcp open  rpcbind
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
901/tcp open  samba-swat
MAC Address: 00:07:E9:50:01:43 (Intel)

Nmap done: 1 IP address (1 host up) scanned in 1.33 seconds
```

Zdroj: vlastní tvorba

Obrázek 13 - Stav portů - Server 03



Zdroj: vlastní tvorba

10.5 Zprávy o zabezpečení a stavu pracovních stanic

10.5.1 Stanice 1 – Fakturace

Výstupní log z programu Farbar Recovery Scan Tool

Scan result of Farbar Recovery Scan Tool (FRST) (x86) Version: 10-03-2015
Ran by ivazad (administrator) on FAKTURACE on 10-03-2015 09:58:33
Running from C:\Users\ivazad\Desktop
Loaded Profiles: ivazad (Available profiles: ivazad)
Platform: Microsoft Windows 7 Professional Service Pack 1 (X86) OS Language: Čeština (Česká republika)
Internet Explorer Version 11 (Default browser: Chrome)
Boot Mode: Normal
Tutorial for Farbar Recovery Scan Tool: http://www.geekstogo.com/forum/topic/335081-frst-tutorial-how-to-use-farbar-recovery-scan-tool/

========== Processes (Whitelisted) ==========

(If an entry is included in the fixlist, the process will be closed. The file will not be moved.)

(Software602 a.s.) C:\Program Files\Common Files\soft602\602updsvc\602updsvc.exe
(ArcSoft Inc.) C:\Program Files\Common Files\ArcSoft\Connection Service\Bin\ACService.exe
(SafeNet, Inc.) C:\Windows\System32\dklog.exe
(SafeNet, Inc.) C:\Windows\System32\dkvcm.exe
(Sanford, L.P.) C:\Program Files\DYMO\DYMO Label Software\DymoPnpService.exe
() C:\Program Files\Canon\IJPLM\ijplmsvc.exe
(Kaspersky Lab ZAO) C:\Program Files\Kaspersky Lab\NetworkAgent\klnagent.exe
(Microsoft Corporation) C:\Program Files\Common Files\microsoft shared\VS7DEBUG\MDM.EXE
(Microsoft Corporation) C:\Program Files\Microsoft SQL Server\MSSQL$SPZSQL2013\Binn\sqlservr.exe
(TeamViewer GmbH) C:\Program Files\TeamViewer\Version9\TeamViewer_Service.exe
(Kaspersky Lab ZAO) C:\Program Files\Kaspersky Lab\Kaspersky Endpoint Security 10 for Windows\avp.exe
(SafeNet, Inc.) C:\Windows\System32\dkcktkn.exe
(Kaspersky Lab ZAO) C:\Program Files\Kaspersky Lab\NetworkAgent\vapm.exe
(SafeNet, Inc.) C:\Program Files\SafeNet\BSecClient\AXMonitor.exe
(SafeNet, Inc.) C:\Program Files\SafeNet\BSecClient\dkAutoReg.exe
(Software602) C:\Program Files\Software602\Print2PDF\Print2PDF.exe
(ArcSoft Inc.) C:\Program Files\Common Files\ArcSoft\Connection Service\Bin\ACDaemon.exe
(Intel Corporation) C:\Windows\System32\igfxtray.exe
(Intel Corporation) C:\Windows\System32\hkcmd.exe
(Intel Corporation) C:\Windows\System32\igfxpers.exe
(Oracle Corporation) C:\Program Files\Common Files\Java\Java Update\jusched.exe
(Microsoft Corporation) C:\Program Files\Microsoft SQL Server\80\Tools\Binn\sqlmangr.exe
(Microsoft Corporation) C:\Program Files\Microsoft Office\Office14\ONENOTEM.EXE
(Microsoft Corporation) C:\Windows\System32\wbem\unsecapp.exe
(ArcSoft Inc.) C:\Program Files\Common Files\ArcSoft\Connection Service\Bin\ArcCon.ac
(Microsoft Corporation) C:\Windows\System32\mobsync.exe
(Oracle Corporation) C:\Program Files\Common Files\Java\Java Update\jucheck.exe
(Cígler software, a.s.) C:\Money\Mons5\S5.exe
(Microsoft Corporation) C:\Program Files\Common Files\microsoft shared\OfficeSoftwareProtectionPlatform\OSPPSVC.EXE
(Microsoft Corporation) C:\Program Files\Microsoft Office\Office14\OIS.EXE

(Kaspersky Lab ZAO) C:\Program Files\Kaspersky Lab\Kaspersky Endpoint Security 10 for Windows\wmi32.exe

========== Registry (Whitelisted) ==========

(If an entry is included in the fixlist, the registry item will be restored to default or removed. The file will not be moved.)

HKLM\...\Run: [Adobe Reader Speed Launcher] => C:\Program Files\Adobe\Reader 9.0\Reader\Reader_sl.exe [34672 2008-06-12] (Adobe Systems Incorporated)
HKLM\...\Run: [DkStartup] => C:\Program Files\SafeNet\BSecClient\dkstartup.exe [54560 2010-02-04] (SafeNet, Inc.)
HKLM\...\Run: [AxMonitor] => C:\Program Files\SafeNet\BSecClient\axmonitor.exe [455968 2010-02-04] (SafeNet, Inc.)
HKLM\...\Run: [DkAutoReg] => C:\Program Files\SafeNet\BSecClient\DkAutoReg.exe [259360 2010-02-04] (SafeNet, Inc.)
HKLM\...\Run: [Print2PDF Print Monitor] => C:\Program Files\Software602\Print2PDF\Print2PDF.exe [220992 2011-10-04] (Software602)
HKLM\...\Run: [CanonSolutionMenu] => C:\Program Files\Canon\SolutionMenu\CNSLMAIN.exe [722256 2008-12-12] (CANON INC.)
HKLM\...\Run: [ArcSoft Connection Service] => C:\Program Files\Common Files\ArcSoft\Connection Service\Bin\ACDaemon.exe [207424 2010-10-27] (ArcSoft Inc.)
HKLM\...\Run: [AVP] => C:\Program Files\Kaspersky Lab\Kaspersky Endpoint Security 10 for Windows\avp.exe [741360 2013-11-27] (Kaspersky Lab ZAO)
HKLM\...\Run: [MpsOnn] => C:\Windows\system32\spool\DRIVERS\W32X86\3\MpsOnn.exe [28232 2007-05-27] (CANON INC.)
HKLM\...\Run: [DLSService] => "C:\Program Files\DYMO\DYMO Label Software\DLSService.exe"
HKLM\...\Run: [SunJavaUpdateSched] => C:\Program Files\Common Files\Java\Java Update\jusched.exe [271744 2014-09-26] (Oracle Corporation)
Winlogon\Notify\DkWLNP: C:\Windows\system32\DkWLNP.dll (SafeNet, Inc.)
HKU\S-1-5-21-121953044-1552604426-1140142799-1000\...\MountPoints2: {8b2845fb-22c6-11e0-b539-002564cb6bcb} - F:\LaunchU3.exe -a
HKU\S-1-5-21-121953044-1552604426-1140142799-1000\...\MountPoints2: {a79e2875-00fe-11e0-8e9a-002564cb6bcb} - F:\LaunchU3.exe -a
Startup: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\Service Manager.lnk
ShortcutTarget: Service Manager.lnk -> C:\Program Files\Microsoft SQL Server\80\Tools\Binn\sqlmangr.exe (Microsoft Corporation)
Startup: C:\Users\ivazad\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Výřezy obrazovky a spuštění aplikace OneNote 2010.lnk
ShortcutTarget: Výřezy obrazovky a spuštění aplikace OneNote 2010.lnk -> C:\Program Files\Microsoft Office\Office14\ONENOTEM.EXE (Microsoft Corporation)

========== Internet (Whitelisted) ==========

(If an item is included in the fixlist, if it is a registry item it will be removed or restored to default.)

ProxyServer: [S-1-5-21-121953044-1552604426-1140142799-1000] => 192.168.117.17:3128
HKU\S-1-5-21-121953044-1552604426-1140142799-1000\Software\Microsoft\Internet Explorer\Main,Start Page = http://www.seznam.cz/
BHO: Adobe PDF Link Helper -> {18DF081C-E8AD-4283-A596-FA578C2EBDC3} -> C:\Program Files\Common Files\Adobe\Acrobat\ActiveX\AcroIEHelperShim.dll [2008-06-11] (Adobe Systems Incorporated)
BHO: Java(tm) Plug-In SSV Helper -> {761497BB-D6F0-462C-B6EB-D4DAF1D92D43} -> C:\Program Files\Java\jre7\bin\ssv.dll [2014-11-26] (Oracle Corporation)
BHO: Google Toolbar Helper -> {AA58ED58-01DD-4d91-8333-CF10577473F7} -> C:\Program Files\Google\Google Toolbar\GoogleToolbar_32.dll [2015-03-03] (Google Inc.)
BHO: Office Document Cache Handler -> {B4F3A835-0E21-4959-BA22-42B3008E02FF} -> C:\Program Files\Microsoft Office\Office14\URLREDIR.DLL [2013-03-06] (Microsoft Corporation)
BHO: Java(tm) Plug-In 2 SSV Helper -> {DBC80044-A445-435b-BC74-9C25C1C588A9} -> C:\Program Files\Java\jre7\bin\jp2ssv.dll [2014-11-26] (Oracle Corporation)
Toolbar: HKLM - Google Toolbar - {2318C2B1-4965-11d4-9B18-009027A5CD4F} - C:\Program Files\Google\Google Toolbar\GoogleToolbar_32.dll [2015-03-03] (Google Inc.)
Toolbar: HKU\S-1-5-21-121953044-1552604426-1140142799-1000 -> Google Toolbar - {2318C2B1-4965-11D4-9B18-009027A5CD4F} - C:\Program Files\Google\Google Toolbar\GoogleToolbar_32.dll [2015-03-03] (Google Inc.)
DPF: {672EE252-D813-4F5E-81BB-5DD163DD4FA5} https://www.mojedatovaschranka.cz/static/pages/isds/cab/filleractivex.cab?3,16,13,0
DPF: {D27CDB6E-AE6D-11CF-96B8-444553540000} http://fpdownload2.macromedia.com/get/shockwave/cabs/flash/swflash.cab
Handler: linkscanner - {F274614C-63F8-47D5-A4D1-FBDDE494F8D1} - No File []
Tcpip\..\Interfaces\{74E3B942-5FC1-42CC-AC80-D75B4896D69D}: [NameServer] 192.168.117.200,8.8.8.8

FireFox:
========
FF ProfilePath: C:\Users\ivazad\AppData\Roaming\Mozilla\Firefox\Profiles\n0pgffn1.default
FF Homepage: www.seznam.cz
FF NetworkProxy: "backup.ftp", "192.168.117.16"
FF NetworkProxy: "backup.ftp_port", 80
FF NetworkProxy: "backup.gopher", "192.168.117.16"
FF NetworkProxy: "backup.gopher_port", 80
FF NetworkProxy: "backup.socks", "192.168.117.16"
FF NetworkProxy: "backup.socks_port", 80

FF NetworkProxy: "backup.ssl", "192.168.117.16"
FF NetworkProxy: "backup.ssl_port", 80
FF NetworkProxy: "ftp", "192.168.117.17"
FF NetworkProxy: "ftp_port", 3128
FF NetworkProxy: "gopher", "192.168.117.17"
FF NetworkProxy: "gopher_port", 3128
FF NetworkProxy: "http", "192.168.117.17"
FF NetworkProxy: "http_port", 3128
FF NetworkProxy: "share_proxy_settings", true
FF NetworkProxy: "socks", "192.168.117.17"
FF NetworkProxy: "socks_port", 3128
FF NetworkProxy: "ssl", "192.168.117.17"
FF NetworkProxy: "ssl_port", 3128
FF NetworkProxy: "type", 0
FF Plugin: @adobe.com/FlashPlayer -> C:\Windows\system32\Macromed\Flash\NPSWF32_16_0_0_305.dll [2015-02-05] ()
FF Plugin: @dymo.com/DymoLabelFramework -> C:\Program Files\DYMO\DYMO Label Software\Framework\npDYMOLabelFramework.dll [2014-03-20] (Sanford L.P.)
FF Plugin: @java.com/DTPlugin,version=10.71.2 -> C:\Program Files\Java\jre7\bin\dtplugin\npDeployJava1.dll [2014-11-26] (Oracle Corporation)
FF Plugin: @java.com/JavaPlugin,version=10.71.2 -> C:\Program Files\Java\jre7\bin\plugin2\npjp2.dll [2014-11-26] (Oracle Corporation)
FF Plugin: @microsoft.com/GENUINE -> disabled No File
FF Plugin: @Microsoft.com/NpCtrl,version=1.0 -> c:\Program Files\Microsoft Silverlight\5.1.30514.0\npctrl.dll [2014-05-13] (Microsoft Corporation)
FF Plugin: @microsoft.com/OfficeAuthz,version=14.0 -> C:\PROGRA~1\MICROS~1\Office14\NPAUTHZ.DLL [2010-01-09] (Microsoft Corporation)
FF Plugin: @microsoft.com/SharePoint,version=14.0 -> C:\PROGRA~1\MICROS~1\Office14\NPSPWRAP.DLL [2010-03-24] (Microsoft Corporation)
FF Plugin: @software602.cz/602XML Filler -> C:\Program Files\Software602\602XML\Filler\npfiller.dll [2011-11-24] (Software602 a.s.)
FF Plugin: @tools.google.com/Google Update;version=3 -> C:\Program Files\Google\Update\1.3.26.9\npGoogleUpdate3.dll [2015-02-05] (Google Inc.)
FF Plugin: @tools.google.com/Google Update;version=9 -> C:\Program Files\Google\Update\1.3.26.9\npGoogleUpdate3.dll [2015-02-05] (Google Inc.)
FF Plugin ProgramFiles/Appdata: C:\Program Files\mozilla firefox\plugins\npnul32.dll [2011-01-06] (mozilla.org)
FF SearchPlugin: C:\Program Files\mozilla firefox\searchplugins\jyxo-cz.xml [2011-01-06]
FF SearchPlugin: C:\Program Files\mozilla firefox\searchplugins\mall-cz.xml [2011-01-06]

Chrome:
=======
CHR HomePage: Default -> hxxp://www.google.com/
CHR StartupUrls: Default -> "hxxp://www.google.com/"
CHR Plugin: (Shockwave Flash) - C:\Program Files\Google\Chrome\Application\40.0.2214.111\PepperFlash\pepflashplayer.dll ()
CHR Plugin: (Shockwave Flash) - C:\Windows\system32\Macromed\Flash\NPSWF32_11_4_402_287.dll No File
CHR Plugin: (Chrome Remote Desktop Viewer) - internal-remoting-viewer
CHR Plugin: (Native Client) - C:\Program Files\Google\Chrome\Application\40.0.2214.111\ppGoogleNaClPluginChrome.dll No File
CHR Plugin: (Chrome PDF Viewer) - C:\Program Files\Google\Chrome\Application\40.0.2214.111\pdf.dll ()
CHR Plugin: (AVG Internet Security) - C:\Users\ivazad\AppData\Local\Google\Chrome\User Data\Default\Extensions\jmfkcklnlgedgbglfkkgedjfmejoahla\12.0.0.2210_0\plugins/avgnpss.dll No File
CHR Plugin: (Adobe Acrobat) - C:\Program Files\Adobe\Reader 9.0\Reader\Browser\nppdf32.dll (Adobe Systems Inc.)
CHR Plugin: (Java Deployment Toolkit 6.0.270.7) - C:\Program Files\Java\jre6\bin\new_plugin\npdeployJava1.dll No File
CHR Plugin: (Java(TM) Platform SE 6 U27) - C:\Program Files\Java\jre6\bin\new_plugin\npjp2.dll No File
CHR Plugin: (Google Earth Plugin) - C:\Program Files\Google\Google Earth\plugin\npgeplugin.dll No File
CHR Plugin: (Google Update) - C:\Program Files\Google\Update\1.3.21.123\npGoogleUpdate3.dll No File
CHR Plugin: (Software602 Form Filler) - C:\Program Files\Software602\602XML\Filler\npfiller.dll (Software602 a.s.)
CHR Profile: C:\Users\ivazad\AppData\Local\Google\Chrome\User Data\Default
CHR Extension: (YouTube) - C:\Users\ivazad\AppData\Local\Google\Chrome\User Data\Default\Extensions\blpcfgokakmgnkcojhhkbfbldkacnbeo [2012-11-14]
CHR Extension: (Google Search) - C:\Users\ivazad\AppData\Local\Google\Chrome\User Data\Default\Extensions\coobgpohoikkiipiblmjeljniedjpjpf [2012-11-14]
CHR Extension: (Google Wallet) - C:\Users\ivazad\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda [2013-09-15]
CHR Extension: (Gmail) - C:\Users\ivazad\AppData\Local\Google\Chrome\User Data\Default\Extensions\pjkljhegncpnkpknbcohdijeoejaedia [2012-11-14]

========================== Services (Whitelisted) =================

(If an entry is included in the fixlist, the service will be removed from the registry. The file will not be moved unless listed separately.)

R2 602XML Updater; C:\Program Files\Common Files\soft602\602updsvc\602updsvc.exe [84520 2011-03-14] (Software602 a.s.)
R2 ACDaemon; C:\Program Files\Common Files\ArcSoft\Connection Service\Bin\ACService.exe [113152 2010-03-18] (ArcSoft Inc.)
U2 AVP; C:\Program Files\Kaspersky Lab\Kaspersky Endpoint Security 10 for Windows\avp.exe [741360 2013-11-27] (Kaspersky Lab ZAO)

R2 DkLogger; C:\Windows\system32\dklog.exe [111904 2010-02-04] (SafeNet, Inc.)
R2 DkTknSrv; C:\Windows\system32\dkcktkn.exe [763168 2010-02-04] (SafeNet, Inc.)
R2 DkVcm; C:\Windows\system32\dkvcm.exe [128288 2010-02-04] (SafeNet, Inc.)
R2 DymoPnpService; C:\Program Files\DYMO\DYMO Label Software\DymoPnpService.exe [33072 2014-03-20] (Sanford, L.P.)
R2 IJPLMSVC; C:\Program Files\Canon\IJPLM\IJPLMSVC.EXE [107912 2008-10-09] ()
R2 klnagent; C:\Program Files\Kaspersky Lab\NetworkAgent\klnagent.exe [132600 2013-11-18] (Kaspersky Lab ZAO)
R2 MSSQL$SPZSQL2013; C:\Program Files\Microsoft SQL Server\MSSQL$SPZSQL2013\Binn\sqlservr.exe [7520337 2002-12-17] (Microsoft Corporation) [File not signed]
S3 MSSQLServerADHelper; C:\Program Files\Microsoft SQL Server\80\Tools\Binn\sqladhlp.exe [66112 2002-12-17] (Microsoft Corporation) [File not signed]
R2 Net Driver HPZ12; C:\Windows\system32\HPZinw12.dll [44032 2009-05-14] (Hewlett-Packard) [File not signed]
R2 Pml Driver HPZ12; C:\Windows\system32\HPZipm12.dll [53760 2009-05-14] (Hewlett-Packard) [File not signed]
S3 SQLAgent$SPZSQL2013; C:\Program Files\Microsoft SQL Server\MSSQL$SPZSQL2013\Binn\sqlagent.EXE [311872 2002-12-17] (Microsoft Corporation) [File not signed]
R2 WinDefend; C:\Program Files\Windows Defender\mpsvc.dll [680960 2013-05-27] (Microsoft Corporation)

========== Drivers (Whitelisted) ==========

(If an entry is included in the fixlist, the service will be removed from the registry. The file will not be moved unless listed separately.)

R3 iKeyEnum; C:\Windows\System32\DRIVERS\ikeyenum.sys [11616 2010-07-15] (SafeNet, Inc.)
R3 iKeyIFD; C:\Windows\System32\DRIVERS\ikeyifd.sys [18080 2010-07-15] (SafeNet, Inc.)
R0 KL1; C:\Windows\System32\DRIVERS\kl1.sys [135776 2013-09-05] (Kaspersky Lab ZAO)
R1 KLFLTDEV; C:\Windows\System32\DRIVERS\klfltdev.sys [25696 2013-07-08] (Kaspersky Lab ZAO)
R1 KLIF; C:\Windows\System32\DRIVERS\klif.sys [624736 2014-05-27] (Kaspersky Lab ZAO)
R1 KLIM6; C:\Windows\System32\DRIVERS\klim6.sys [25696 2013-07-11] (Kaspersky Lab ZAO)
R1 kltdi; C:\Windows\System32\DRIVERS\kltdi.sys [43864 2012-11-22] (Kaspersky Lab ZAO)
R1 kneps; C:\Windows\System32\DRIVERS\kneps.sys [144224 2013-07-01] (Kaspersky Lab ZAO)
R3 npf; C:\Windows\System32\drivers\npf.sys [36600 2014-08-19] (Riverbed Technology, Inc.)
S3 RnbToken; C:\Windows\System32\DRIVERS\rnbtoken.sys [21472 2010-07-15] (SafeNet, Inc.)
U5 klflt; C:\Windows\System32\Drivers\klflt.sys [80480 2014-05-27] (Kaspersky Lab ZAO)

========== NetSvcs (Whitelisted) ==========

(If an item is included in the fixlist, it will be removed from the registry. Any associated file could be listed separately to be moved.)

========== One Month Created Files and Folders ========

(If an entry is included in the fixlist, the file\folder will be moved.)

2015-03-10 09:58 - 2015-03-10 09:59 - 00015694 _____ () C:\Users\ivazad\Desktop\FRST.txt
2015-03-10 09:54 - 2015-03-10 09:54 - 01134592 _____ (Farbar) C:\Users\ivazad\Desktop\FRST.exe
2015-03-10 09:54 - 2015-03-10 09:54 - 00000000 ____D () C:\Users\ivazad\Desktop\FRST-OlderVersion
2015-03-10 09:48 - 2015-03-10 09:58 - 00000000 ____D () C:\FRST
2015-03-10 09:44 - 2015-03-10 09:44 - 00001093 _____ () C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Microsoft Baseline Security Analyzer 2.3.lnk
2015-03-10 09:44 - 2015-03-10 09:44 - 00001081 _____ () C:\Users\Public\Desktop\Microsoft Baseline Security Analyzer 2.3.lnk
2015-03-10 09:44 - 2015-03-10 09:44 - 00000000 ____D () C:\Program Files\Microsoft Baseline Security Analyzer 2
2015-03-10 09:37 - 2015-03-10 09:42 - 00000000 ____D () C:\Users\ivazad\.zenmap
2015-03-10 09:37 - 2015-03-10 09:37 - 00000921 _____ () C:\Users\ivazad\Desktop\Nmap - Zenmap GUI.lnk
2015-03-10 09:36 - 2015-03-10 09:37 - 00000000 ____D () C:\Program Files\Nmap
2015-03-10 09:36 - 2015-03-10 09:36 - 00000000 ____D () C:\Program Files\WinPcap
2015-03-09 09:07 - 2015-03-09 09:08 - 00000000 ____D () C:\Users\ivazad\Desktop\Ondrášek
2015-03-04 07:18 - 2015-01-09 03:48 - 00635904 _____ (Microsoft Corporation) C:\Windows\system32\perftrack.dll
2015-03-04 07:18 - 2015-01-09 03:48 - 00076800 _____ (Microsoft Corporation) C:\Windows\system32\wdi.dll
2015-03-04 07:18 - 2015-01-09 03:48 - 00027136 _____ (Microsoft Corporation) C:\Windows\system32\powertracker.dll
2015-02-26 07:04 - 2015-01-09 00:44 - 00419936 _____ () C:\Windows\system32\locale.nls
2015-02-17 14:40 - 2015-02-17 14:40 - 00233391 _____ () C:\Users\ivazad\Desktop\Sia-Chandelier.htm
2015-02-17 09:26 - 2015-02-17 09:26 - 00000000 _____ () C:\Users\ivazad\Desktop\Nový textový dokument.txt
2015-02-13 07:12 - 2015-01-23 04:43 - 00620032 _____ (Microsoft Corporation) C:\Windows\system32\jscript9diag.dll
2015-02-13 07:12 - 2015-01-23 04:17 - 04300800 _____ (Microsoft Corporation) C:\Windows\system32\jscript9.dll
2015-02-11 07:17 - 2015-01-15 08:46 - 00136640 _____ (Microsoft Corporation) C:\Windows\system32\Drivers\ksecpkg.sys
2015-02-11 07:17 - 2015-01-15 08:46 - 00067520 _____ (Microsoft Corporation) C:\Windows\system32\Drivers\ksecdd.sys
2015-02-11 07:17 - 2015-01-15 08:43 - 00100352 _____ (Microsoft Corporation) C:\Windows\system32\sspicli.dll
2015-02-11 07:17 - 2015-01-15 08:43 - 00015872 _____ (Microsoft Corporation) C:\Windows\system32\sspisrv.dll
2015-02-11 07:17 - 2015-01-15 08:42 - 01061376 _____ (Microsoft Corporation) C:\Windows\system32\lsasrv.dll
2015-02-11 07:17 - 2015-01-15 08:42 - 00050176 _____ (Microsoft Corporation) C:\Windows\system32\auditpol.exe
2015-02-11 07:17 - 2015-01-15 08:42 - 00022528 _____ (Microsoft Corporation) C:\Windows\system32\lsass.exe
2015-02-11 07:17 - 2015-01-15 08:42 - 00022016 _____ (Microsoft Corporation) C:\Windows\system32\secur32.dll
2015-02-11 07:17 - 2015-01-15 08:39 - 00146432 _____ (Microsoft Corporation) C:\Windows\system32\msaudite.dll
2015-02-11 07:17 - 2015-01-15 08:39 - 00060416 _____ (Microsoft Corporation) C:\Windows\system32\msobjs.dll
2015-02-11 07:17 - 2015-01-15 08:37 - 00686080 _____ (Microsoft Corporation) C:\Windows\system32\adtschema.dll

2015-02-11 07:17 - 2015-01-15 05:21 - 00369968 _____ (Microsoft Corporation) C:\Windows\system32\Drivers\cng.sys
2015-02-11 07:17 - 2015-01-14 06:44 - 03972544 _____ (Microsoft Corporation) C:\Windows\system32\ntkrnlpa.exe
2015-02-11 07:17 - 2015-01-14 06:44 - 03917760 _____ (Microsoft Corporation) C:\Windows\system32\ntoskrnl.exe
2015-02-11 07:17 - 2015-01-09 02:45 - 02380288 _____ (Microsoft Corporation) C:\Windows\system32\win32k.sys
2015-02-11 07:17 - 2014-11-26 04:32 - 00571904 _____ (Microsoft Corporation) C:\Windows\system32\oleaut32.dll
2015-02-11 07:16 - 2015-02-04 03:54 - 00482304 _____ (Microsoft Corporation) C:\Windows\system32\generaltel.dll
2015-02-11 07:16 - 2015-02-04 03:53 - 00767488 _____ (Microsoft Corporation) C:\Windows\system32\appraiser.dll
2015-02-11 07:16 - 2015-02-04 03:53 - 00621056 _____ (Microsoft Corporation) C:\Windows\system32\invagent.dll
2015-02-11 07:16 - 2015-02-04 03:53 - 00325632 _____ (Microsoft Corporation) C:\Windows\system32\devinv.dll
2015-02-11 07:16 - 2015-02-04 03:53 - 00202752 _____ (Microsoft Corporation) C:\Windows\system32\aepdu.dll
2015-02-11 07:16 - 2015-02-04 03:53 - 00159744 _____ (Microsoft Corporation) C:\Windows\system32\aepic.dll
2015-02-11 07:16 - 2015-02-04 03:49 - 00886784 _____ (Microsoft Corporation) C:\Windows\system32\aeinv.dll
2015-02-11 07:16 - 2015-01-28 00:36 - 01167520 _____ (Microsoft Corporation) C:\Windows\system32\aitstatic.exe
2015-02-11 07:16 - 2015-01-14 06:09 - 00342712 _____ (Microsoft Corporation) C:\Windows\system32\iedkcs32.dll
2015-02-11 07:16 - 2015-01-12 03:25 - 19740160 _____ (Microsoft Corporation) C:\Windows\system32\mshtml.dll
2015-02-11 07:16 - 2015-01-12 03:21 - 02724864 _____ (Microsoft Corporation) C:\Windows\system32\mshtml.tlb
2015-02-11 07:16 - 2015-01-12 03:21 - 00004096 _____ (Microsoft Corporation) C:\Windows\system32\ieetwcollectorres.dll
2015-02-11 07:16 - 2015-01-12 03:08 - 00503296 _____ (Microsoft Corporation) C:\Windows\system32\vbscript.dll
2015-02-11 07:16 - 2015-01-12 03:07 - 00062464 _____ (Microsoft Corporation) C:\Windows\system32\iesetup.dll
2015-02-11 07:16 - 2015-01-12 03:07 - 00047616 _____ (Microsoft Corporation) C:\Windows\system32\ieetwproxystub.dll
2015-02-11 07:16 - 2015-01-12 03:05 - 00064000 _____ (Microsoft Corporation) C:\Windows\system32\MshtmlDac.dll
2015-02-11 07:16 - 2015-01-12 03:02 - 02277888 _____ (Microsoft Corporation) C:\Windows\system32\iertutil.dll
2015-02-11 07:16 - 2015-01-12 03:00 - 00047104 _____ (Microsoft Corporation) C:\Windows\system32\jsproxy.dll
2015-02-11 07:16 - 2015-01-12 02:59 - 00030720 _____ (Microsoft Corporation) C:\Windows\system32\iernonce.dll
2015-02-11 07:16 - 2015-01-12 02:57 - 00478208 _____ (Microsoft Corporation) C:\Windows\system32\ieui.dll
2015-02-11 07:16 - 2015-01-12 02:55 - 00115712 _____ (Microsoft Corporation) C:\Windows\system32\ieUnatt.exe
2015-02-11 07:16 - 2015-01-12 02:55 - 00102912 _____ (Microsoft Corporation) C:\Windows\system32\ieetwcollector.exe
2015-02-11 07:16 - 2015-01-12 02:48 - 00667648 _____ (Microsoft Corporation) C:\Windows\system32\MsSpellCheckingFacility.exe
2015-02-11 07:16 - 2015-01-12 02:45 - 00418304 _____ (Microsoft Corporation) C:\Windows\system32\dxtmsft.dll
2015-02-11 07:16 - 2015-01-12 02:40 - 00060416 _____ (Microsoft Corporation) C:\Windows\system32\JavaScriptCollectionAgent.dll
2015-02-11 07:16 - 2015-01-12 02:36 - 00168960 _____ (Microsoft Corporation) C:\Windows\system32\msrating.dll
2015-02-11 07:16 - 2015-01-12 02:35 - 00076288 _____ (Microsoft Corporation) C:\Windows\system32\mshtmled.dll
2015-02-11 07:16 - 2015-01-12 02:33 - 00285696 _____ (Microsoft Corporation) C:\Windows\system32\dxtrans.dll
2015-02-11 07:16 - 2015-01-12 02:23 - 02052608 _____ (Microsoft Corporation) C:\Windows\system32\inetcpl.cpl
2015-02-11 07:16 - 2015-01-12 02:23 - 00688640 _____ (Microsoft Corporation) C:\Windows\system32\msfeeds.dll
2015-02-11 07:16 - 2015-01-12 02:23 - 00684544 _____ (Microsoft Corporation) C:\Windows\system32\ie4uinit.exe
2015-02-11 07:16 - 2015-01-12 02:22 - 01155072 _____ (Microsoft Corporation) C:\Windows\system32\mshtmlmedia.dll
2015-02-11 07:16 - 2015-01-12 02:14 - 12829184 _____ (Microsoft Corporation) C:\Windows\system32\ieframe.dll
2015-02-11 07:16 - 2015-01-12 02:00 - 01888256 _____ (Microsoft Corporation) C:\Windows\system32\wininet.dll
2015-02-11 07:16 - 2015-01-12 01:56 - 01307136 _____ (Microsoft Corporation) C:\Windows\system32\urlmon.dll
2015-02-11 07:16 - 2015-01-12 01:55 - 00710144 _____ (Microsoft Corporation) C:\Windows\system32\ieapfltr.dll
2015-02-11 07:16 - 2015-01-10 07:27 - 00550912 _____ (Microsoft Corporation) C:\Windows\system32\kerberos.dll
2015-02-11 07:16 - 2015-01-10 07:27 - 00259584 _____ (Microsoft Corporation) C:\Windows\system32\msv1_0.dll
2015-02-11 07:16 - 2015-01-10 07:27 - 00248832 _____ (Microsoft Corporation) C:\Windows\system32\schannel.dll
2015-02-11 07:16 - 2015-01-10 07:27 - 00221184 _____ (Microsoft Corporation) C:\Windows\system32\ncrypt.dll
2015-02-11 07:16 - 2015-01-10 07:27 - 00172032 _____ (Microsoft Corporation) C:\Windows\system32\wdigest.dll
2015-02-11 07:16 - 2015-01-10 07:27 - 00065536 _____ (Microsoft Corporation) C:\Windows\system32\TSpkg.dll
2015-02-11 07:16 - 2015-01-10 07:27 - 00017408 _____ (Microsoft Corporation) C:\Windows\system32\credssp.dll
2015-02-11 07:15 - 2015-01-13 03:49 - 01230336 _____ (Microsoft Corporation) C:\Windows\system32\WindowsCodecs.dll
2015-02-11 07:15 - 2014-12-12 06:07 - 01174528 _____ (Microsoft Corporation) C:\Windows\system32\crypt32.dll
2015-02-11 07:15 - 2014-12-08 03:46 - 00308224 _____ (Microsoft Corporation) C:\Windows\system32\scesrv.dll
2015-02-11 07:15 - 2014-07-07 02:40 - 00179200 _____ (Microsoft Corporation) C:\Windows\system32\wintrust.dll
2015-02-11 07:15 - 2014-07-07 02:40 - 00143872 _____ (Microsoft Corporation) C:\Windows\system32\cryptsvc.dll

========== One Month Modified Files and Folders =======

(If an entry is included in the fixlist, the file\folder will be moved.)

2015-03-10 09:58 - 2012-08-08 12:15 - 00000940 _____ () C:\Windows\Tasks\GoogleUpdateTaskMachineUA.job
2015-03-10 09:56 - 2012-05-10 06:01 - 00000914 _____ () C:\Windows\Tasks\Adobe Flash Player Updater.job
2015-03-10 09:47 - 2009-07-14 05:34 - 00026544 ____H () C:\Windows\system32\7B296FB0-376B-497e-B012-9C450E1B7327-5P-1.C7483456-A289-439d-8115-601632D005A0
2015-03-10 09:47 - 2009-07-14 05:34 - 00026544 ____H () C:\Windows\system32\7B296FB0-376B-497e-B012-9C450E1B7327-5P-0.C7483456-A289-439d-8115-601632D005A0
2015-03-10 09:46 - 2014-09-02 09:15 - 28868144 _____ () C:\psfparse.txt
2015-03-10 09:39 - 2009-11-05 09:49 - 01724466 _____ () C:\Windows\system32\PerfStringBackup.INI
2015-03-10 09:37 - 2009-11-05 08:48 - 00000000 ____D () C:\Users\ivazad
2015-03-10 09:36 - 2014-06-02 08:51 - 00026022 _____ () C:\Windows\setupact.log
2015-03-10 09:14 - 2014-05-27 13:39 - 00000000 ____D () C:\ProgramData\Kaspersky Lab
2015-03-10 08:33 - 2014-09-02 10:11 - 01848832 ___SH () C:\Users\ivazad\Desktop\Thumbs.db
2015-03-10 08:05 - 2014-08-27 08:51 - 00000000 ____D () C:\Users\ivazad\Desktop\SCAN
2015-03-10 08:03 - 2009-11-05 09:48 - 01501254 _____ () C:\Windows\WindowsUpdate.log
2015-03-10 06:54 - 2009-07-14 05:53 - 00000006 ____H () C:\Windows\Tasks\SA.DAT

2015-03-09 14:14 - 2015-01-05 14:36 - 00394752 _____ () C:\Users\ivazad\Desktop\Odeslaná pošta 2015.xls
2015-03-06 13:13 - 2015-01-05 13:02 - 00252928 _____ () C:\Users\ivazad\Desktop\Doručená pošta 2015.xls
2015-03-06 07:02 - 2009-07-14 05:53 - 00032586 _____ () C:\Windows\Tasks\SCHEDLGU.TXT
2015-03-05 07:27 - 2009-07-14 03:37 - 00000000 ____D () C:\Windows\tracing
2015-03-04 07:03 - 2014-06-03 05:55 - 00015268 _____ () C:\Windows\PFRO.log
2015-02-24 07:40 - 2009-07-14 03:37 - 00000000 ____D () C:\Windows\Microsoft.NET
2015-02-24 03:23 - 2009-11-06 12:27 - 00246920 ____N (Microsoft Corporation) C:\Windows\system32\MpSigStub.exe
2015-02-20 12:02 - 2012-11-14 07:11 - 00002129 _____ () C:\Users\Public\Desktop\Google Chrome.lnk
2015-02-16 09:27 - 2009-07-14 03:37 - 00000000 ____D () C:\Windows\rescache
2015-02-16 07:18 - 2015-01-10 10:06 - 00001060 _____ () C:\ProgramData\Microsoft\Windows\Start Menu\Programs\TeamViewer 9.lnk
2015-02-16 07:18 - 2015-01-10 10:06 - 00001048 _____ () C:\Users\Public\Desktop\TeamViewer 9.lnk
2015-02-12 08:13 - 2014-06-03 05:56 - 00419048 _____ () C:\Windows\system32\FNTCACHE.DAT
2015-02-12 08:10 - 2014-12-11 07:41 - 00000000 ____D () C:\Windows\system32\appraiser
2015-02-12 08:10 - 2014-05-02 07:58 - 00000000 ___SD () C:\Windows\system32\CompatTel
2015-02-12 07:32 - 2013-08-15 16:39 - 00000000 ____D () C:\Windows\system32\MRT
2015-02-12 07:25 - 2009-11-06 12:27 - 113756392 _____ (Microsoft Corporation) C:\Windows\system32\MRT.exe
2015-02-12 07:22 - 2014-06-01 14:04 - 00000000 ____D () C:\ProgramData\Microsoft Help
2015-02-12 07:22 - 2009-07-14 03:04 - 00000478 _____ () C:\Windows\win.ini

========== Files in the root of some directories =======

2014-09-05 10:08 - 2014-09-05 10:11 - 0039887 __RSH () C:\Program Files\DLS8Uninstall.log
2011-01-28 09:36 - 2011-01-28 09:36 - 0004096 ____H () C:\Users\ivazad\AppData\Local\keyfile3.drm

Some content of TEMP:
==========
C:\Users\ivazad\AppData\Local\Temp\jre-7u67-windows-i586-iftw.exe
C:\Users\ivazad\AppData\Local\Temp\jre-7u71-windows-i586-iftw.exe
C:\Users\ivazad\AppData\Local\Temp\x4fypig3.dll

========== Bamital & volsnap Check ==========

(There is no automatic fix for files that do not pass verification.)

C:\Windows\explorer.exe => File is digitally signed
C:\Windows\system32\winlogon.exe => File is digitally signed
C:\Windows\system32\wininit.exe => File is digitally signed
C:\Windows\system32\svchost.exe => File is digitally signed
C:\Windows\system32\services.exe => File is digitally signed
C:\Windows\system32\User32.dll => File is digitally signed
C:\Windows\system32\userinit.exe => File is digitally signed
C:\Windows\system32\rpcss.dll => File is digitally signed
C:\Windows\system32\Drivers\volsnap.sys => File is digitally signed

LastRegBack: 2015-02-25 07:43

========== End Of Log ==========

Výstupní log z programu Microsoft Baseline Security Analyzer

Security assessment:
Severe Risk (One or more critical checks failed.)

Computer name:	WORKGROUP\FAKTURACE
IP address:	192.168.117.69
Security report name:	WORKGROUP - FAKTURACE (10.3.2015 10-16)
Scan date:	10.3.2015 10:16
Catalog synchronization date:	
Security update catalog:	Microsoft Update

Security Updates

Score	Issue	Result
	Developer Tools, Runtimes, and Redistributables Security Updates	No security updates are missing.
	Office Security Updates	No security updates are missing.
	SDK Components Security Updates	No security updates are missing.
	SQL Server Security Updates	No security updates are missing.
	Silverlight Security Updates	No security updates are missing.
	Windows Security Updates	No security updates are missing.

Current Update Compliance

Score	ID	Description	Maximum Severity
Installed	MS11-025	Security Update for Microsoft Visual C++ 2005 Service Pack 1 Redistributable Package (KB2538242)	Important
Installed	MS11-025	Security Update for Microsoft Visual C++ 2010 Service Pack 1 Redistributable Package (KB2565063)	Important
Installed	MS11-025	Security Update for Microsoft Visual C++ 2008 Service Pack 1 Redistributable Package (KB2538243)	Important

Current Update Compliance

Score	ID	Description	Maximum Severity
Installed	MS13-091	Security Update for Microsoft Office 2010 (KB2553284) 32-Bit Edition	Important
Installed	MS14-024	Security Update for Microsoft Office 2010 (KB2810073) 32-Bit Edition	Important
Installed	MS15-012	Security Update for Microsoft Word 2010 (KB2956066) 32-Bit Edition	Important
Installed	MS13-074	Security Update for Microsoft Office 2010 (KB2687423) 32-Bit Edition	Important
Installed	MS14-036	Security Update for Microsoft Office 2010 (KB2881071) 32-Bit Edition	Important
Installed	MS15-013	Security Update for Microsoft Office 2010 (KB2920748) 32-Bit Edition	Important
Installed	MS14-024	Security Update for Microsoft Office 2010 (KB2880971) 32-Bit Edition	Important
Installed	2687455	Service Pack 2 for Microsoft Office 2010 (KB2687455) 32-Bit Edition	
Installed	MS14-082	Security Update for Microsoft Office 2010 (KB2553154) 32-Bit Edition	Important
Installed	MS15-012	Security Update for Microsoft Excel 2010 (KB2956081) 32-Bit Edition	Important
Installed	MS13-106	Security Update for Microsoft Office 2010 (KB2850016) 32-Bit Edition	Important
Installed	MS15-012	Security Update for Microsoft Office 2010 (KB2956073) 32-Bit Edition	Important

Current Update Compliance

Score	ID	Description	Maximum Severity
Installed	MS07-028	Security Update for CAPICOM (KB931906)	Critical

Current Update Compliance

Score	ID	Description	Maximum Severity
Installed	MS06-061	MSXML 6.0 RTM Security Update (925673)	Critical

Current Update Compliance

Score	ID	Description	Maximum Severity
Installed	2977218	Update for Microsoft Silverlight (KB2977218)	

Current Update Compliance

Score	ID	Description	Maximum Severity
Installed	MS15-009	Security Update for Internet Explorer 11 for Windows 7 (KB3034196)	Low
Installed	MS15-016	Security Update for Windows 7 (KB3029944)	Important
Installed	MS14-074	Security Update for Windows 7 (KB3003743)	Important
Installed	MS15-014	Security Update for Windows 7 (KB3004361)	Important

Windows Scan Results

Administrative Vulnerabilities

Score	Issue	Result
	Local Account Password Test	Some user accounts (2 of 4) have blank or simple passwords, or could not be analyzed.

User	Weak Password	Locked Out	Disabled
Administrator	Weak	-	Disabled
Guest	Weak	-	-
HomeGroupUser$	-	-	-
ivazad	-	-	-

	Guest Account	The Guest account is not disabled on this computer.
	Password Expiration	All user accounts (4) have non-expiring passwords.

User
Administrator
Guest
HomeGroupUser$
ivazad

	Windows Firewall	Windows Firewall is disabled and has exceptions configured.

Connection Name	Firewall	Exceptions
All Connections	Off	Ports, Programs, Services
Připojení k místní síti	Off*	Ports*, Programs*, Services*

	Incomplete Updates	No incomplete software update installations were found.
	File System	All hard drives (2) are using the NTFS file system.

Drive Letter	File System
C:	NTFS
D:	NTFS

	Autologon	Autologon is not configured on this computer.
	Restrict Anonymous	Computer is properly restricting anonymous access.
	Administrators	No more than 2 Administrators were found on this computer.

User
Administrator
ivazad

	Automatic	Updates are automatically downloaded and installed on this computer.

Additional System Information

Score	Issue	Result
ℹ	Windows Version	Computer is running Microsoft Windows 7.
ℹ	Auditing	Neither Logon Success nor Logon Failure auditing are enabled. Enable auditing and turn on auditing for specific events such as logon and logoff. Be sure to monitor your event log to watch for unauthorized access.
ℹ	Shares	8 share(s) are present on your computer.

Share	Directory	Share ACL	Directory ACL
LaserJet 1320 - Zadinová	hp LaserJet 1320 series UPD PCL 5,LocalsplOnly	Print Queue Share	Directory ACL can not be read.
RICOH Aficio - IVANA	RICOH Aficio - IVANA,LocalsplOnly	Print Queue Share	Directory ACL can not be read.
ADMIN$	C:\Windows	Admin Share	NT SERVICE\TrustedInstaller - F, NT AUTHORITY\SYSTEM - RWXD, BUILTIN\Administrators - RWXD, BUILTIN\Users - RX
C$	C:\	Admin Share	BUILTIN\Administrators - F, NT AUTHORITY\SYSTEM - F, BUILTIN\Users - RX, NT AUTHORITY\Authenticated Users - D
D$	D:\	Admin Share	BUILTIN\Administrators - F, NT AUTHORITY\SYSTEM - F, NT AUTHORITY\Authenticated Users - RWXD, BUILTIN\Users - RX
Users	C:\Users	Administrators - F, Everyone - F	NT AUTHORITY\SYSTEM - F, BUILTIN\Administrators - F, BUILTIN\Users - RX, Everyone - RX
print$	C:\Windows\system32\spool\drivers	Everyone - R, Administrators - F	NT AUTHORITY\SYSTEM - F, BUILTIN\Administrators - F, Everyone - RX
prnproc$	C:\Windows\system32\spool\PRTPROCS	Everyone - R, Administrators - F	NT SERVICE\TrustedInstaller - F, NT AUTHORITY\SYSTEM - F, BUILTIN\Administrators - F, BUILTIN\Users - RX

ℹ	Services	No potentially unnecessary services were found.

Internet Information Services (IIS) Scan Results

Score	Issue	Result
▬	IIS Status	IIS is not running on this computer.

SQL Server Scan Results: Instance SPZSQL2013

Administrative Vulnerabilities

Score	Issue	Result
⚠	SQL Server/MSDE Security Mode	SQL Server and/or MSDE authentication mode is set to SQL Server and/or MSDE and Windows (Mixed Mode).
ℹ	Sysadmin role members	BUILTIN\Administrators group should not be part of sysadmin role.
ℹ	Service Accounts	SQL Server, SQL Server Agent, MSDE and/or MSDE Agent service accounts should not be members of the local Administrators group or run as LocalSystem.

Instance	Service	Account	Issue
SPZSQL2013	MSSQL$SPZSQL2013	SYSTEM	LocalSystem account.
SPZSQL2013	SQLAgent$SPZSQL2013	SYSTEM	LocalSystem account.

✓	Exposed SQL Server/MSDE Password	The 'sa' password and SQL service account password are not exposed in text files.
✓	CmdExec role	CmdExec is restricted to sysadmin only.
✓	Registry Permissions	The Everyone group does not have more than Read access to the SQL Server and/or MSDE registry keys.

10.5.2 Stanice 2 – Mzdy

Výstupní log z programu Farbar Recovery Scan Tool

Scan result of Farbar Recovery Scan Tool (FRST) (x86) Version: 12-02-2015 ([color=red]ATTENTION: ====> FRST version is 26 days old and could be outdated[/color])
Ran by Jiřina Kolářová (administrator) on MZDY on 10-03-2015 10:18:41
Running from C:\Users\Jiřina Kolářová\Desktop
Loaded Profiles: Jiřina Kolářová (Available profiles: Jiřina Kolářová)
Platform: Microsoft Windows 7 Professional Service Pack 1 (X86) OS Language: Čeština (Česká republika)
Internet Explorer Version 11 (Default browser: IE)
Boot Mode: Normal
Tutorial for Farbar Recovery Scan Tool: http://www.geekstogo.com/forum/topic/335081-frst-tutorial-how-to-use-farbar-recovery-scan-tool/

========== Processes (Whitelisted) ==========

(If an entry is included in the fixlist, the process will be closed. The file will not be moved.)

(Apple Inc.) C:\Program Files\Common Files\Apple\Mobile Device Support\AppleMobileDeviceService.exe
(Apple Inc.) C:\Program Files\Bonjour\mDNSResponder.exe
(Kaspersky Lab ZAO) C:\Program Files\Kaspersky Lab\NetworkAgent\klnagent.exe
(TeamViewer GmbH) C:\Program Files\TeamViewer\TeamViewer_Service.exe
(Intel Corporation) C:\Windows\System32\igfxtray.exe
(Intel Corporation) C:\Windows\System32\hkcmd.exe
(Intel Corporation) C:\Windows\System32\igfxpers.exe
(Apple Inc.) C:\Program Files\iTunes\iTunesHelper.exe
(Apple Inc.) C:\Program Files\iPod\bin\iPodService.exe
(Cígler software, a.s.) C:\money\mons5\S5.exe
(TeamViewer GmbH) C:\Program Files\TeamViewer\TeamViewer.exe
(TeamViewer GmbH) C:\Program Files\TeamViewer\tv_w32.exe
(Kaspersky Lab ZAO) C:\Program Files\Kaspersky Lab\NetworkAgent\vapm.exe
(Microsoft Corporation) C:\Windows\System32\wbem\unsecapp.exe
(M-PRO s.r.o.) C:\Program Files\M-PRO\Person\mzdy.exe
(M-PRO s.r.o.) C:\Program Files\M-PRO\Person\ErrorScan.exe
(Hewlett-Packard) C:\Windows\System32\spool\drivers\w32x86\3\hpmup091.bin
(Microsoft Corporation) C:\Program Files\Common Files\microsoft shared\OfficeSoftwareProtectionPlatform\OSPPSVC.EXE
(Microsoft Corporation) C:\Windows\System32\dllhost.exe

========== Registry (Whitelisted) ==========

(If an entry is included in the fixlist, the registry item will be restored to default or removed. The file will not be moved.)

HKLM\...\Run: [WSUSOfflineUpdate] => C:\Windows\Temp\WOURecall\RecallStub.cmd [1262 2013-10-19] () <===== ATTENTION
HKLM\...\Run: [AVP] => C:\Program Files\Kaspersky Lab\Kaspersky Endpoint Security 10 for Windows\avp.exe [741360 2013-11-27] (Kaspersky Lab ZAO)
HKLM\...\Run: [iTunesHelper] => C:\Program Files\iTunes\iTunesHelper.exe [157480 2014-10-15] (Apple Inc.)

========== Internet (Whitelisted) ==========

(If an item is included in the fixlist, if it is a registry item it will be removed or restored to default.)

HKU\S-1-5-21-2784774652-2162229512-1527570647-1000\Software\Microsoft\Internet Explorer\Main,Start Page = http://www.centrum.cz/
HKU\S-1-5-21-2784774652-2162229512-1527570647-1000\Software\Microsoft\Internet Explorer\Main,Default_Page_URL = http://www.dell.com
SearchScopes: HKU\S-1-5-21-2784774652-2162229512-1527570647-1000 -> {C4B75887-6E4D-4097-A1A7-4F30F0CEDF78} URL = http://www.search.ask.com/web?tpid=ORJ-SPE&o=APN11406&pf=V7&p2=%5EBBE%5EOSJ000%5EYY%5ECZ&gct=&itbv=12.15.5.30&apn_uid=EE4AA27A-59DD-44A5-AD9C-58918EC285BE&apn_ptnrs=BBE&apn_dtid=%5EOSJ000%5EYY%5ECZ&apn_dbr=ie_11.0.9600.17239&doi=2014-08-26&trgb=IE&q={searchTerms}&psv=&pt=tb
BHO: Java(tm) Plug-In SSV Helper -> {761497BB-D6F0-462C-B6EB-D4DAF1D92D43} -> C:\Program Files\Java\jre1.8.0_31\bin\ssv.dll (Oracle Corporation)
BHO: Office Document Cache Handler -> {B4F3A835-0E21-4959-BA22-42B3008E02FF} -> C:\Program Files\Microsoft Office\Office14\URLREDIR.DLL (Microsoft Corporation)
BHO: Java(tm) Plug-In 2 SSV Helper -> {DBC80044-A445-435b-BC74-9C25C1C588A9} -> C:\Program Files\Java\jre1.8.0_31\bin\jp2ssv.dll (Oracle Corporation)
Winsock: Catalog5 07 C:\Program Files\Bonjour\mdnsNSP.dll [121704] (Apple Inc.)

Tcpip\..\Interfaces\{4280B01C-013F-4C9F-8C49-16B58D739873}: [NameServer] 192.168.117.200,8.8.8.8

FireFox:
========
FF Plugin: @Apple.com/iTunes,version=1.0 -> C:\Program Files\iTunes\Mozilla Plugins\npitunes.dll ()
FF Plugin: @java.com/DTPlugin,version=11.31.2 -> C:\Program Files\Java\jre1.8.0_31\bin\dtplugin\npDeployJava1.dll (Oracle Corporation)
FF Plugin: @java.com/JavaPlugin,version=11.31.2 -> C:\Program Files\Java\jre1.8.0_31\bin\plugin2\npjp2.dll (Oracle Corporation)
FF Plugin: @microsoft.com/GENUINE -> disabled No File
FF Plugin: @Microsoft.com/NpCtrl,version=1.0 -> c:\Program Files\Microsoft Silverlight\5.1.30514.0\npctrl.dll (Microsoft Corporation)
FF Plugin: @microsoft.com/OfficeAuthz,version=14.0 -> C:\PROGRA~1\MICROS~1\Office14\NPAUTHZ.DLL (Microsoft Corporation)
FF Plugin: @microsoft.com/SharePoint,version=14.0 -> C:\PROGRA~1\MICROS~1\Office14\NPSPWRAP.DLL (Microsoft Corporation)
FF Plugin: Adobe Reader -> C:\Program Files\Adobe\Reader 11.0\Reader\AIR\nppdf32.dll (Adobe Systems Inc.)

========================== Services (Whitelisted) =================

(If an entry is included in the fixlist, the service will be removed from the registry. The file will not be moved unless listed separately.)

S2 AVP; C:\Program Files\Kaspersky Lab\Kaspersky Endpoint Security 10 for Windows\avp.exe [741360 2013-11-27] (Kaspersky Lab ZAO)
R2 klnagent; C:\Program Files\Kaspersky Lab\NetworkAgent\klnagent.exe [132600 2013-11-18] (Kaspersky Lab ZAO)
R2 Net Driver HPZ12; C:\Windows\system32\HPZinw12.dll [44032 2009-05-14] (Hewlett-Packard) [File not signed]
R2 Pml Driver HPZ12; C:\Windows\system32\HPZipm12.dll [53760 2009-05-14] (Hewlett-Packard) [File not signed]
R2 TeamViewer; C:\Program Files\TeamViewer\TeamViewer_Service.exe [5436176 2015-02-17] (TeamViewer GmbH)
R2 WinDefend; C:\Program Files\Windows Defender\mpsvc.dll [680960 2014-05-25] (Microsoft Corporation)

========== Drivers (Whitelisted) ==========

(If an entry is included in the fixlist, the service will be removed from the registry. The file will not be moved unless listed separately.)

R0 KL1; C:\Windows\System32\DRIVERS\kl1.sys [135776 2013-09-05] (Kaspersky Lab ZAO)
R1 KLFLTDEV; C:\Windows\System32\DRIVERS\klfltdev.sys [25696 2013-07-08] (Kaspersky Lab ZAO)
R1 KLIF; C:\Windows\System32\DRIVERS\klif.sys [624736 2014-05-27] (Kaspersky Lab ZAO)
R1 KLIM6; C:\Windows\System32\DRIVERS\klim6.sys [25696 2013-07-11] (Kaspersky Lab ZAO)
R1 kltdi; C:\Windows\System32\DRIVERS\kltdi.sys [43864 2012-11-22] (Kaspersky Lab ZAO)
R1 kneps; C:\Windows\System32\DRIVERS\kneps.sys [144224 2013-07-01] (Kaspersky Lab ZAO)
U5 klflt; C:\Windows\System32\Drivers\klflt.sys [80480 2014-05-27] (Kaspersky Lab ZAO)

========== NetSvcs (Whitelisted) ==========

(If an item is included in the fixlist, it will be removed from the registry. Any associated file could be listed separately to be moved.)

========== One Month Created Files and Folders ========

(If an entry is included in the fixlist, the file\folder will be moved.)

2015-03-10 10:18 - 2015-03-10 10:19 - 00007005 _____ () C:\Users\Jiřina Kolářová\Desktop\FRST.txt
2015-03-10 10:18 - 2015-03-10 10:18 - 00000000 ____D () C:\FRST
2015-03-10 10:18 - 2015-02-14 08:44 - 01125376 _____ (Farbar) C:\Users\Jiřina Kolářová\Desktop\FRST.exe
2015-02-28 21:49 - 2015-03-02 19:25 - 00007487 _____ () C:\Users\Jiřina Kolářová\Desktop\Jizda.xlsx
2015-02-28 10:30 - 2015-02-28 10:30 - 00109639 _____ () C:\Users\Jiřina Kolářová\Documents\Jizda.xlsx
2015-02-25 18:24 - 2015-01-09 00:44 - 00419936 _____ () C:\Windows\system32\locale.nls
2015-02-24 16:27 - 2015-02-24 16:27 - 00004095 _____ () C:\Users\Jiřina Kolářová\Desktop\DPZVD6-0025222571-20150224-162631.xml
2015-02-24 16:25 - 2015-02-24 16:27 - 00003918 _____ () C:\Users\Jiřina Kolářová\Desktop\DPZVD6-0025222571-20150224-161051-pracovni.xml
2015-02-24 14:12 - 2015-02-24 14:15 - 00077824 _____ () C:\Users\Jiřina Kolářová\Desktop\výpočet daně a dan.zvýhodnění.xls
2015-02-24 13:31 - 2015-02-24 13:31 - 00000544 _____ () C:\Users\Jiřina Kolářová\Desktop\DPZVD6-0025222571-20150224-131344-pracovni1.xml
2015-02-24 13:31 - 2015-02-24 13:31 - 00000544 _____ () C:\Users\Jiřina Kolářová\Desktop\DPZVD6-0025222571-20150224-131344-pracovni.xml
2015-02-24 13:14 - 2015-02-24 13:14 - 00000281 _____ () C:\Users\Jiřina Kolářová\Desktop\DPZVD6-XXXXXXXXXX-20150224-131344-pracovni-20141.xml
2015-02-24 13:03 - 2015-02-24 13:03 - 00003608 _____ () C:\Users\Jiřina Kolářová\Desktop\DPZVD6.xml
2015-02-24 13:03 - 2015-02-24 13:03 - 00002650 _____ () C:\Users\Jiřina Kolářová\Desktop\DPSVD2.xml
2015-02-24 12:57 - 2015-02-24 12:57 - 00008222 _____ () C:\Users\Jiřina Kolářová\Desktop\Daň z příjmů - příloha č. 2.XLSX
2015-02-24 10:32 - 2015-02-24 10:32 - 00438103 _____ () C:\Users\Jiřina Kolářová\Desktop\DPFDP5-5755221780-20150224-102837-1611129886-potvrzeni.p7s

2015-02-24 10:27 - 2015-02-24 10:29 - 00217544 _____ () C:\Users\Jiřina Kolářová\Desktop\DPFDP5-5755221780-20150224-102526.xml
2015-02-24 10:21 - 2015-02-24 10:21 - 00108936 _____ () C:\Users\Jiřina Kolářová\Desktop\DPFDP5-5755221780-20150224-102043-pracovni.xml
2015-02-24 09:53 - 2015-02-24 09:53 - 00001130 _____ () C:\Users\Jiřina Kolářová\Desktop\DPFDP5-5755221780-20150224-095325-pracovni.xml
2015-02-20 15:36 - 2015-02-20 15:36 - 00000929 _____ () C:\ProgramData\Microsoft\Windows\Start Menu\Programs\TeamViewer 10.lnk
2015-02-20 08:41 - 2015-02-20 08:43 - 41021787 _____ () C:\Users\Jiřina Kolářová\Downloads\MzdyV5.ADO_15.01.002_Komplet.exe
2015-02-19 14:02 - 2015-02-19 14:02 - 00377979 _____ () C:\Users\Jiřina Kolářová\Downloads\DDZ_257247550.zfo
2015-02-18 11:18 - 2015-02-18 11:18 - 00000000 ____D () C:\Program Files\Common Files\Java
2015-02-17 11:09 - 2015-02-17 11:09 - 00015901 _____ () C:\Users\Jiřina Kolářová\Downloads\OSVC_2014.xml
2015-02-16 12:53 - 2015-02-16 12:54 - 06520378 _____ () C:\Users\Jiřina Kolářová\Downloads\Doplnky_Platby_Rep3v_015.01.001_01.sfx.exe
2015-02-14 09:16 - 2015-02-14 09:25 - 00000000 ____D () C:\Users\Jiřina Kolářová\Desktop\mons5
2015-02-14 09:10 - 2015-02-13 14:26 - 2656110143 _____ () C:\Users\Jiřina Kolářová\Desktop\mons5.zip
2015-02-12 07:54 - 2015-01-23 04:43 - 00620032 _____ (Microsoft Corporation) C:\Windows\system32\jscript9diag.dll
2015-02-12 07:54 - 2015-01-23 04:17 - 04300800 _____ (Microsoft Corporation) C:\Windows\system32\jscript9.dll
2015-02-11 08:44 - 2015-02-11 08:44 - 00384985 _____ () C:\Users\Jiřina Kolářová\Desktop\S5ImportLog_11.02.2015.xml
2015-02-11 07:21 - 2015-01-15 08:46 - 00136640 _____ (Microsoft Corporation) C:\Windows\system32\Drivers\ksecpkg.sys
2015-02-11 07:21 - 2015-01-15 08:46 - 00067520 _____ (Microsoft Corporation) C:\Windows\system32\Drivers\ksecdd.sys
2015-02-11 07:21 - 2015-01-15 08:43 - 00100352 _____ (Microsoft Corporation) C:\Windows\system32\sspicli.dll
2015-02-11 07:21 - 2015-01-15 08:43 - 00015872 _____ (Microsoft Corporation) C:\Windows\system32\sspisrv.dll
2015-02-11 07:21 - 2015-01-15 08:42 - 01061376 _____ (Microsoft Corporation) C:\Windows\system32\lsasrv.dll
2015-02-11 07:21 - 2015-01-15 08:42 - 00050176 _____ (Microsoft Corporation) C:\Windows\system32\auditpol.exe
2015-02-11 07:21 - 2015-01-15 08:42 - 00022528 _____ (Microsoft Corporation) C:\Windows\system32\lsass.exe
2015-02-11 07:21 - 2015-01-15 08:42 - 00022016 _____ (Microsoft Corporation) C:\Windows\system32\secur32.dll
2015-02-11 07:21 - 2015-01-15 08:39 - 00146432 _____ (Microsoft Corporation) C:\Windows\system32\msaudite.dll
2015-02-11 07:21 - 2015-01-15 08:39 - 00060416 _____ (Microsoft Corporation) C:\Windows\system32\msobjs.dll
2015-02-11 07:21 - 2015-01-15 08:37 - 00686080 _____ (Microsoft Corporation) C:\Windows\system32\adtschema.dll
2015-02-11 07:21 - 2015-01-15 05:21 - 00369968 _____ (Microsoft Corporation) C:\Windows\system32\Drivers\cng.sys
2015-02-11 07:21 - 2015-01-14 06:44 - 03972544 _____ (Microsoft Corporation) C:\Windows\system32\ntkrnlpa.exe
2015-02-11 07:21 - 2015-01-14 06:44 - 03917760 _____ (Microsoft Corporation) C:\Windows\system32\ntoskrnl.exe
2015-02-11 07:21 - 2015-01-09 03:48 - 00635904 _____ (Microsoft Corporation) C:\Windows\system32\perftrack.dll
2015-02-11 07:21 - 2015-01-09 03:48 - 00076800 _____ (Microsoft Corporation) C:\Windows\system32\wdi.dll
2015-02-11 07:21 - 2015-01-09 03:48 - 00027136 _____ (Microsoft Corporation) C:\Windows\system32\powertracker.dll
2015-02-11 07:21 - 2015-01-09 02:45 - 02380288 _____ (Microsoft Corporation) C:\Windows\system32\win32k.sys
2015-02-11 07:20 - 2015-02-04 03:54 - 00482304 _____ (Microsoft Corporation) C:\Windows\system32\generaltel.dll
2015-02-11 07:20 - 2015-02-04 03:53 - 00767488 _____ (Microsoft Corporation) C:\Windows\system32\appraiser.dll
2015-02-11 07:20 - 2015-02-04 03:53 - 00621056 _____ (Microsoft Corporation) C:\Windows\system32\invagent.dll
2015-02-11 07:20 - 2015-02-04 03:53 - 00325632 _____ (Microsoft Corporation) C:\Windows\system32\devinv.dll
2015-02-11 07:20 - 2015-02-04 03:53 - 00202752 _____ (Microsoft Corporation) C:\Windows\system32\aepdu.dll
2015-02-11 07:20 - 2015-02-04 03:53 - 00159744 _____ (Microsoft Corporation) C:\Windows\system32\aepic.dll
2015-02-11 07:20 - 2015-02-04 03:49 - 00886784 _____ (Microsoft Corporation) C:\Windows\system32\aeinv.dll
2015-02-11 07:20 - 2015-01-28 00:36 - 01167520 _____ (Microsoft Corporation) C:\Windows\system32\aitstatic.exe
2015-02-11 07:20 - 2015-01-14 06:09 - 00342712 _____ (Microsoft Corporation) C:\Windows\system32\iedkcs32.dll
2015-02-11 07:20 - 2015-01-12 03:25 - 19740160 _____ (Microsoft Corporation) C:\Windows\system32\mshtml.dll
2015-02-11 07:20 - 2015-01-12 03:21 - 02724864 _____ (Microsoft Corporation) C:\Windows\system32\mshtml.tlb
2015-02-11 07:20 - 2015-01-12 03:21 - 00004096 _____ (Microsoft Corporation) C:\Windows\system32\ieetwcollectorres.dll
2015-02-11 07:20 - 2015-01-12 03:08 - 00503296 _____ (Microsoft Corporation) C:\Windows\system32\vbscript.dll
2015-02-11 07:20 - 2015-01-12 03:07 - 00062464 _____ (Microsoft Corporation) C:\Windows\system32\iesetup.dll
2015-02-11 07:20 - 2015-01-12 03:07 - 00047616 _____ (Microsoft Corporation) C:\Windows\system32\ieetwproxystub.dll
2015-02-11 07:20 - 2015-01-12 03:05 - 00064000 _____ (Microsoft Corporation) C:\Windows\system32\MshtmlDac.dll
2015-02-11 07:20 - 2015-01-12 03:02 - 02277888 _____ (Microsoft Corporation) C:\Windows\system32\iertutil.dll
2015-02-11 07:20 - 2015-01-12 03:00 - 00047104 _____ (Microsoft Corporation) C:\Windows\system32\jsproxy.dll
2015-02-11 07:20 - 2015-01-12 02:59 - 00030720 _____ (Microsoft Corporation) C:\Windows\system32\iernonce.dll
2015-02-11 07:20 - 2015-01-12 02:57 - 00478208 _____ (Microsoft Corporation) C:\Windows\system32\ieui.dll
2015-02-11 07:20 - 2015-01-12 02:55 - 00115712 _____ (Microsoft Corporation) C:\Windows\system32\ieUnatt.exe
2015-02-11 07:20 - 2015-01-12 02:55 - 00102912 _____ (Microsoft Corporation) C:\Windows\system32\ieetwcollector.exe
2015-02-11 07:20 - 2015-01-12 02:48 - 00667648 _____ (Microsoft Corporation) C:\Windows\system32\MsSpellCheckingFacility.exe
2015-02-11 07:20 - 2015-01-12 02:45 - 00418304 _____ (Microsoft Corporation) C:\Windows\system32\dxtmsft.dll
2015-02-11 07:20 - 2015-01-12 02:40 - 00060416 _____ (Microsoft Corporation) C:\Windows\system32\JavaScriptCollectionAgent.dll
2015-02-11 07:20 - 2015-01-12 02:36 - 00168960 _____ (Microsoft Corporation) C:\Windows\system32\msrating.dll
2015-02-11 07:20 - 2015-01-12 02:35 - 00076288 _____ (Microsoft Corporation) C:\Windows\system32\mshtmled.dll
2015-02-11 07:20 - 2015-01-12 02:33 - 00285696 _____ (Microsoft Corporation) C:\Windows\system32\dxtrans.dll
2015-02-11 07:20 - 2015-01-12 02:23 - 02052608 _____ (Microsoft Corporation) C:\Windows\system32\inetcpl.cpl
2015-02-11 07:20 - 2015-01-12 02:23 - 00688640 _____ (Microsoft Corporation) C:\Windows\system32\msfeeds.dll
2015-02-11 07:20 - 2015-01-12 02:23 - 00684544 _____ (Microsoft Corporation) C:\Windows\system32\ie4uinit.exe
2015-02-11 07:20 - 2015-01-12 02:22 - 01155072 _____ (Microsoft Corporation) C:\Windows\system32\mshtmlmedia.dll
2015-02-11 07:20 - 2015-01-12 02:14 - 12829184 _____ (Microsoft Corporation) C:\Windows\system32\ieframe.dll
2015-02-11 07:20 - 2015-01-12 02:00 - 01888256 _____ (Microsoft Corporation) C:\Windows\system32\wininet.dll
2015-02-11 07:20 - 2015-01-12 01:56 - 01307136 _____ (Microsoft Corporation) C:\Windows\system32\urlmon.dll

2015-02-11 07:20 - 2015-01-12 01:55 - 00710144 _____ (Microsoft Corporation) C:\Windows\system32\ieapfltr.dll
2015-02-11 07:20 - 2015-01-10 07:27 - 00550912 _____ (Microsoft Corporation) C:\Windows\system32\kerberos.dll
2015-02-11 07:20 - 2015-01-10 07:27 - 00259584 _____ (Microsoft Corporation) C:\Windows\system32\msv1_0.dll
2015-02-11 07:20 - 2015-01-10 07:27 - 00248832 _____ (Microsoft Corporation) C:\Windows\system32\schannel.dll
2015-02-11 07:20 - 2015-01-10 07:27 - 00221184 _____ (Microsoft Corporation) C:\Windows\system32\ncrypt.dll
2015-02-11 07:20 - 2015-01-10 07:27 - 00172032 _____ (Microsoft Corporation) C:\Windows\system32\wdigest.dll
2015-02-11 07:20 - 2015-01-10 07:27 - 00065536 _____ (Microsoft Corporation) C:\Windows\system32\TSpkg.dll
2015-02-11 07:20 - 2015-01-10 07:27 - 00017408 _____ (Microsoft Corporation) C:\Windows\system32\credssp.dll
2015-02-11 07:20 - 2014-11-26 04:32 - 00571904 _____ (Microsoft Corporation) C:\Windows\system32\oleaut32.dll
2015-02-11 07:19 - 2015-01-13 03:49 - 01230336 _____ (Microsoft Corporation) C:\Windows\system32\WindowsCodecs.dll
2015-02-11 07:19 - 2014-12-12 06:07 - 01174528 _____ (Microsoft Corporation) C:\Windows\system32\crypt32.dll
2015-02-11 07:19 - 2014-12-08 03:46 - 00308224 _____ (Microsoft Corporation) C:\Windows\system32\scesrv.dll
2015-02-11 07:19 - 2014-07-07 02:40 - 00179200 _____ (Microsoft Corporation) C:\Windows\system32\wintrust.dll
2015-02-11 07:19 - 2014-07-07 02:40 - 00143872 _____ (Microsoft Corporation) C:\Windows\system32\cryptsvc.dll
2015-02-09 14:55 - 2015-02-09 14:56 - 18285551 _____ () C:\Users\Jiřina Kolářová\Downloads\PartnerLink_1.9.6_x86.zip

========== One Month Modified Files and Folders =======

(If an entry is included in the fixlist, the file\folder will be moved.)

2015-03-10 10:18 - 2009-07-14 05:39 - 00049113 _____ () C:\Windows\setupact.log
2015-03-10 09:48 - 2014-05-27 12:50 - 00000914 _____ () C:\Windows\Tasks\Adobe Flash Player Updater.job
2015-03-10 09:14 - 2014-05-27 12:54 - 00000000 ____D () C:\ProgramData\Kaspersky Lab
2015-03-10 08:54 - 2014-05-25 20:54 - 01644214 _____ () C:\Windows\WindowsUpdate.log
2015-03-10 08:53 - 2014-05-26 14:49 - 00000000 ____D () C:\Users\Jiřina Kolářová\Documents\Soubory aplikace Outlook
2015-03-10 08:14 - 2014-06-06 12:37 - 00000522 _____ () C:\Windows\MZDY.INI
2015-03-10 07:44 - 2009-07-14 05:34 - 00036336 ____H () C:\Windows\system32\7B296FB0-376B-497e-B012-9C450E1B7327-5P-1.C7483456-A289-439d-8115-601632D005A0
2015-03-10 07:44 - 2009-07-14 05:34 - 00036336 ____H () C:\Windows\system32\7B296FB0-376B-497e-B012-9C450E1B7327-5P-0.C7483456-A289-439d-8115-601632D005A0
2015-03-10 07:36 - 2014-05-25 21:08 - 00028657 _____ () C:\Windows\wsusofflineupdate.log
2015-03-10 07:35 - 2009-07-14 05:53 - 00000006 ____H () C:\Windows\Tasks\SA.DAT
2015-03-04 11:58 - 2014-06-03 13:19 - 00000000 ____D () C:\Users\Jiřina Kolářová\Desktop\Dokumenty
2015-03-04 11:26 - 2014-09-18 11:08 - 00001079 _____ () C:\Windows\system32\debug.log
2015-03-04 09:28 - 2014-05-26 15:06 - 00000000 ____D () C:\Program Files\Zákon 4
2015-02-28 14:54 - 2014-05-26 14:40 - 00000000 ____D () C:\Program Files\TeamViewer
2015-02-24 03:23 - 2014-05-25 21:18 - 00246920 ____N (Microsoft Corporation) C:\Windows\system32\MpSigStub.exe
2015-02-23 07:20 - 2009-07-14 05:33 - 00335984 _____ () C:\Windows\system32\FNTCACHE.DAT
2015-02-23 07:17 - 2014-05-26 15:03 - 00086536 _____ () C:\Users\Jiřina Kolářová\AppData\Local\GDIPFONTCACHEV1.DAT
2015-02-19 09:09 - 2014-05-26 15:03 - 00001043 _____ () C:\Users\Jiřina Kolářová\Desktop\PDF Signer.lnk
2015-02-19 03:29 - 2009-07-14 03:37 - 00000000 ____D () C:\Windows\Microsoft.NET
2015-02-19 03:04 - 2010-11-20 22:01 - 01565732 _____ () C:\Windows\system32\PerfStringBackup.INI
2015-02-18 11:20 - 2014-06-12 06:20 - 00000000 ____D () C:\ProgramData\Oracle
2015-02-18 11:17 - 2014-08-26 08:23 - 00272296 _____ (Oracle Corporation) C:\Windows\system32\javaws.exe
2015-02-18 11:17 - 2014-08-26 08:23 - 00176552 _____ (Oracle Corporation) C:\Windows\system32\javaw.exe
2015-02-18 11:17 - 2014-08-26 08:23 - 00176552 _____ (Oracle Corporation) C:\Windows\system32\java.exe
2015-02-18 11:17 - 2014-08-26 08:23 - 00096680 _____ (Oracle Corporation) C:\Windows\system32\WindowsAccessBridge.dll
2015-02-18 11:17 - 2014-08-26 08:23 - 00000000 ____D () C:\Program Files\Java
2015-02-13 12:31 - 2009-07-14 03:37 - 00000000 ____D () C:\Windows\rescache
2015-02-12 15:00 - 2009-07-14 03:37 - 00000000 ____D () C:\Program Files\Common Files\microsoft shared
2015-02-12 07:42 - 2014-12-11 07:44 - 00000000 ____D () C:\Windows\system32\appraiser
2015-02-12 07:42 - 2014-05-26 14:58 - 00000000 ___SD () C:\Windows\system32\CompatTel
2015-02-12 07:42 - 2009-07-14 03:37 - 00000000 ____D () C:\Windows\tracing
2015-02-11 18:23 - 2014-05-26 13:38 - 00000000 ____D () C:\Windows\system32\MRT
2015-02-11 18:21 - 2014-05-26 13:38 - 113756392 _____ (Microsoft Corporation) C:\Windows\system32\MRT.exe
2015-02-11 18:19 - 2014-05-26 13:27 - 00000000 ____D () C:\ProgramData\Microsoft Help
2015-02-11 18:19 - 2009-07-14 03:04 - 00000478 _____ () C:\Windows\win.ini
2015-02-09 14:58 - 2014-05-26 15:17 - 00002591 _____ () C:\Users\Public\Desktop\PartnerLink.lnk

========== Files in the root of some directories =======

2014-05-26 15:03 - 2014-05-26 15:03 - 0000055 _____ () C:\ProgramData\pconfig.dat

Files to move or delete:
==========
C:\Windows\Temp\WOURecall\RecallStub.cmd
C:\ProgramData\pconfig.dat

Some content of TEMP:
==========
C:\Users\Jiřina Kolářová\AppData\Local\Temp\APNSetup.exe
C:\Users\Jiřina Kolářová\AppData\Local\Temp\jre-7u65-windows-i586-iftw.exe

C:\Users\Jiřina Kolářová\AppData\Local\Temp\jre-7u67-windows-i586-iftw.exe
C:\Users\Jiřina Kolářová\AppData\Local\Temp\jre-8u31-windows-au.exe

========== Bamital & volsnap Check ==========

(There is no automatic fix for files that do not pass verification.)

C:\Windows\explorer.exe => File is digitally signed
C:\Windows\system32\winlogon.exe => File is digitally signed
C:\Windows\system32\wininit.exe => File is digitally signed
C:\Windows\system32\svchost.exe => File is digitally signed
C:\Windows\system32\services.exe => File is digitally signed
C:\Windows\system32\User32.dll => File is digitally signed
C:\Windows\system32\userinit.exe => File is digitally signed
C:\Windows\system32\rpcss.dll => File is digitally signed
C:\Windows\system32\Drivers\volsnap.sys => File is digitally signed

LastRegBack: 2015-03-05 07:31

========== End Of Log ==========

Výstupní log z programu Microsoft Baseline Security Analyzer

Security assessment:
Severe Risk (One or more critical checks failed.)

Computer name:	WORKGROUP\MZDY
IP address:	192.168.117.59
Security report name:	WORKGROUP - MZDY (10.3.2015 10-27)
Scan date:	10.3.2015 10:27
Catalog synchronization date:	
Security update catalog:	Microsoft Update

Security Updates

Score	Issue	Result
	SQL Server Security Updates	1 service packs or update rollups are missing.

Update Rollups and Service Packs

Score	ID	Description
Missing	2546951	Microsoft SQL Server 2008 Service Pack 3 (KB2546951)

Current Update Compliance

Score	ID	Description	Maximum Severity
Installed	MS06-061	MSXML 6.0 RTM Security Update (925673)	Critical

	Developer Tools, Runtimes, and Redistributables Security Updates	No security updates are missing.

Current Update Compliance

Score	ID	Description	Maximum Severity
Installed	MS11-025	Security Update for Microsoft Visual C++ 2010 Service Pack 1 Redistributable Package (KB2565063)	Important
Installed	MS11-049	Security Update for Microsoft Visual Studio 2008 Service Pack 1 XML Editor (KB2251487)	Important

	Office Security Updates	No security updates are missing.

Current Update Compliance

Score	ID	Description	Maximum Severity
Installed	MS13-091	Security Update for Microsoft Office 2010 (KB2553284) 32-Bit Edition	Important
Installed	MS14-024	Security Update for Microsoft Office 2010 (KB2810073) 32-Bit Edition	Important
Installed	MS15-012	Security Update for Microsoft Word 2010 (KB2956066) 32-Bit Edition	Important
Installed	MS13-074	Security Update for Microsoft Office 2010 (KB2687423) 32-Bit Edition	Important
Installed	MS14-036	Security Update for Microsoft Office 2010 (KB2881071) 32-Bit Edition	Important
Installed	MS15-013	Security Update for Microsoft Office 2010 (KB2920748) 32-Bit Edition	Important
Installed	MS14-024	Security Update for Microsoft Office 2010 (KB2880971) 32-Bit Edition	Important
Installed	2687455	Service Pack 2 for Microsoft Office 2010 (KB2687455) 32-Bit Edition	
Installed	MS14-082	Security Update for Microsoft Office 2010 (KB2553154) 32-Bit Edition	Important
Installed	MS15-012	Security Update for Microsoft Excel 2010 (KB2956081) 32-Bit Edition	Important
Installed	MS13-106	Security Update for Microsoft Office 2010 (KB2850016) 32-Bit Edition	Important
Installed	MS15-012	Security Update for Microsoft Office 2010 (KB2956073) 32-Bit Edition	Important

	Silverlight Security Updates	No security updates are missing.

Current Update Compliance

Score	ID	Description	Maximum Severity
Installed	2977218	Update for Microsoft Silverlight (KB2977218)	

	Windows Security Updates	No security updates are missing.

Current Update Compliance

Score	ID	Description	Maximum Severity
Installed	MS15-009	Security Update for Internet Explorer 11 for Windows 7 (KB3034196)	Low
Installed	MS15-016	Security Update for Windows 7 (KB3029944)	Important

Windows Scan Results

Administrative Vulnerabilities

Score	Issue	Result
	Local Account Password Test	Some user accounts (3 of 3) have blank or simple passwords, or could not be analyzed.

User	Weak Password	Locked Out	Disabled
Administrator	Weak	-	Disabled
Guest	Weak	-	Disabled
Jiřina Kolářová	Weak	-	-

	Password	All user accounts (3) have non-expiring passwords.
	Windows Firewall	Windows Firewall is disabled and has exceptions configured.

Connection Name	Firewall	Exceptions
All Connections	Off	Ports, Programs, Services
Připojení k místní síti	Off*	Ports*, Programs*, Services*

	Incomplete Updates	No incomplete software update installations were found.
	File System	All hard drives (1) are using the NTFS file system.

Drive Letter	File System
C:	NTFS

	Guest Account	The Guest account is disabled on this computer.
	Autologon	Autologon is not configured on this computer.
	Restrict Anonymous	Computer is properly restricting anonymous access.
	Administrators	No more than 2 Administrators were found on this computer.

User
Administrator
Jiřina Kolářová

	Automatic Updates	Updates are automatically downloaded and installed on this computer.

Additional System Information

Score	Issue	Result
	Windows Version	Computer is running Microsoft Windows 7.
	Auditing	Neither Logon Success nor Logon Failure auditing are enabled. Enable auditing and turn on auditing for specific events such as logon and logoff. Be sure to monitor your event log to watch for unauthorized access.
	Shares	2 share(s) are present on your computer.

Share	Directory	Share ACL	Directory ACL
ADMIN$	C:\Windows	Admin Share	NT SERVICE\TrustedInstaller - F, NT AUTHORITY\SYSTEM - RWXD, BUILTIN\Administrators - RWXD, BUILTIN\Users - RX
C$	C:\	Admin Share	BUILTIN\Administrators - F, NT AUTHORITY\SYSTEM - F, BUILTIN\Users - RX, NT AUTHORITY\Authenticated Users - D

	Services	No potentially unnecessary services were found.

10.5.3 Stanice 3 – Zeleň

Výstupní log z programu Farbar Recovery Scan Tool

Scan result of Farbar Recovery Scan Tool (FRST) (x86) Version: 12-02-2015 ([color=red]ATTENTION: ====> FRST version is 26 days old and could be outdated[/color])
Ran by Jiří Holeček (administrator) on ZELEN on 10-03-2015 10:07:32
Running from C:\Users\Jiří Holeček\Desktop
Loaded Profiles: Jiří Holeček (Available profiles: Jiří Holeček)
Platform: Microsoft Windows 7 Professional Service Pack 1 (X86) OS Language: Čeština (Česká republika)
Internet Explorer Version 11 (Default browser: FF)
Boot Mode: Normal
Tutorial for Farbar Recovery Scan Tool: http://www.geekstogo.com/forum/topic/335081-frst-tutorial-how-to-use-farbar-recovery-scan-tool/

========== Processes (Whitelisted) ==========

(If an entry is included in the fixlist, the process will be closed. The file will not be moved.)

(SafeNet Inc.) C:\Windows\System32\hasplms.exe
(Kaspersky Lab ZAO) C:\Program Files\Kaspersky Lab\NetworkAgent\klnagent.exe
(Kaspersky Lab ZAO) C:\Program Files\Kaspersky Lab\Kaspersky Endpoint Security 10 for Windows\avp.exe
(Intel Corporation) C:\Windows\System32\igfxtray.exe
(Intel Corporation) C:\Windows\System32\hkcmd.exe
(Intel Corporation) C:\Windows\System32\igfxpers.exe
(Kaspersky Lab ZAO) C:\Program Files\Kaspersky Lab\NetworkAgent\vapm.exe
(Microsoft Corporation) C:\Windows\System32\wbem\unsecapp.exe
(Microsoft Corporation) C:\Program Files\Common Files\microsoft shared\OfficeSoftwareProtectionPlatform\OSPPSVC.EXE
(Microsoft Corporation) C:\Windows\System32\msiexec.exe
(Microsoft Corporation) C:\Windows\System32\wbem\WMIADAP.exe

========== Registry (Whitelisted) ==========

(If an entry is included in the fixlist, the registry item will be restored to default or removed. The file will not be moved.)

HKLM\...\Run: [AVP] => C:\Program Files\Kaspersky Lab\Kaspersky Endpoint Security 10 for Windows\avp.exe [741360 2013-11-27] (Kaspersky Lab ZAO)

========== Internet (Whitelisted) ==========

(If an item is included in the fixlist, if it is a registry item it will be removed or restored to default.)

HKU\S-1-5-21-1520735465-4222121814-4137135182-1000\Software\Microsoft\Internet Explorer\Main,Start Page = http://www.dell.com
HKU\S-1-5-21-1520735465-4222121814-4137135182-1000\Software\Microsoft\Internet Explorer\Main,Default_Page_URL = http://www.dell.com
BHO: Office Document Cache Handler -> {B4F3A835-0E21-4959-BA22-42B3008E02FF} -> C:\Program Files\Microsoft Office\Office14\URLREDIR.DLL (Microsoft Corporation)
Tcpip\..\Interfaces\{E0CB7D8C-60FB-4040-866F-BD3F909C9D9F}: [NameServer] 192.168.117.200,8.8.8.8

FireFox:
========
FF ProfilePath: C:\Users\Jiří Holeček\AppData\Roaming\Mozilla\Firefox\Profiles\ucvro453.default
FF Homepage: hxxp://www.seznam.cz/
FF Plugin: @adobe.com/FlashPlayer -> C:\Windows\system32\Macromed\Flash\NPSWF32_16_0_0_305.dll ()
FF Plugin: @microsoft.com/GENUINE -> disabled No File
FF Plugin: @Microsoft.com/NpCtrl,version=1.0 -> c:\Program Files\Microsoft Silverlight\5.1.30514.0\npctrl.dll (Microsoft Corporation)
FF Plugin: @microsoft.com/OfficeAuthz,version=14.0 -> C:\PROGRA~1\MICROS~1\Office14\NPAUTHZ.DLL (Microsoft Corporation)
FF Plugin: @microsoft.com/SharePoint,version=14.0 -> C:\PROGRA~1\MICROS~1\Office14\NPSPWRAP.DLL (Microsoft Corporation)
FF Plugin: Adobe Reader -> C:\Program Files\Adobe\Reader 11.0\Reader\AIR\nppdf32.dll (Adobe Systems Inc.)

========== Services (Whitelisted) ==========

(If an entry is included in the fixlist, the service will be removed from the registry. The file will not be moved unless listed separately.)

S2 AVP; C:\Program Files\Kaspersky Lab\Kaspersky Endpoint Security 10 for Windows\avp.exe [741360 2013-11-27] (Kaspersky Lab ZAO)
R2 hasplms; C:\Windows\system32\hasplms.exe [4609928 2013-08-01] (SafeNet Inc.)
R2 klnagent; C:\Program Files\Kaspersky Lab\NetworkAgent\klnagent.exe [132600 2013-11-18] (Kaspersky Lab ZAO)
R2 WinDefend; C:\Program Files\Windows Defender\mpsvc.dll [680960 2014-05-21] (Microsoft Corporation)

========== Drivers (Whitelisted) ==========

(If an entry is included in the fixlist, the service will be removed from the registry. The file will not be moved unless listed separately.)

R2 aksfridge; C:\Windows\system32\drivers\aksfridge.sys [376200 2013-08-01] (SafeNet Inc.)
S3 athur; C:\Windows\System32\DRIVERS\athur.sys [1500160 2010-01-05] (Atheros Communications, Inc.)
R2 hardlock; C:\Windows\system32\drivers\hardlock.sys [608648 2013-08-01] (SafeNet Inc.)
R0 KL1; C:\Windows\System32\DRIVERS\kl1.sys [135776 2013-09-05] (Kaspersky Lab ZAO)
R1 KLFLTDEV; C:\Windows\System32\DRIVERS\klfltdev.sys [25696 2013-07-08] (Kaspersky Lab ZAO)
R1 KLIF; C:\Windows\System32\DRIVERS\klif.sys [624736 2014-05-28] (Kaspersky Lab ZAO)
R1 KLIM6; C:\Windows\System32\DRIVERS\klim6.sys [25696 2013-07-11] (Kaspersky Lab ZAO)
R1 kltdi; C:\Windows\System32\DRIVERS\kltdi.sys [43864 2012-11-22] (Kaspersky Lab ZAO)
R1 kneps; C:\Windows\System32\DRIVERS\kneps.sys [144224 2013-07-01] (Kaspersky Lab ZAO)
U5 klflt; C:\Windows\System32\Drivers\klflt.sys [80480 2014-05-28] (Kaspersky Lab ZAO)

========== NetSvcs (Whitelisted) ==========

(If an item is included in the fixlist, it will be removed from the registry. Any associated file could be listed separately to be moved.)

========== One Month Created Files and Folders ========

(If an entry is included in the fixlist, the file\folder will be moved.)

2015-03-10 10:07 - 2015-03-10 10:08 - 00005419 _____ () C:\Users\Jiří Holeček\Desktop\FRST.txt
2015-03-10 10:07 - 2015-03-10 10:07 - 00000000 ____D () C:\FRST
2015-03-10 10:06 - 2015-03-10 10:06 - 00001093 _____ () C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Microsoft Baseline Security Analyzer 2.3.lnk
2015-03-10 10:06 - 2015-03-10 10:06 - 00001081 _____ () C:\Users\Public\Desktop\Microsoft Baseline Security Analyzer 2.3.lnk
2015-03-10 10:06 - 2015-03-10 10:06 - 00000000 ____D () C:\Program Files\Microsoft Baseline Security Analyzer 2
2015-03-10 10:06 - 2015-02-14 08:44 - 01125376 _____ (Farbar) C:\Users\Jiří Holeček\Desktop\FRST.exe
2015-03-06 04:25 - 2015-03-06 04:25 - 00000000 ____D () C:\Program Files\Mozilla Firefox
2015-03-04 06:00 - 2015-01-09 03:48 - 00635904 _____ (Microsoft Corporation) C:\Windows\system32\perftrack.dll
2015-03-04 06:00 - 2015-01-09 03:48 - 00076800 _____ (Microsoft Corporation) C:\Windows\system32\wdi.dll
2015-03-04 06:00 - 2015-01-09 03:48 - 00027136 _____ (Microsoft Corporation) C:\Windows\system32\powertracker.dll
2015-02-25 14:26 - 2015-01-09 00:44 - 00419936 _____ () C:\Windows\system32\locale.nls
2015-02-12 06:10 - 2015-01-23 04:43 - 00620032 _____ (Microsoft Corporation) C:\Windows\system32\jscript9diag.dll
2015-02-12 06:10 - 2015-01-23 04:17 - 04300800 _____ (Microsoft Corporation) C:\Windows\system32\jscript9.dll
2015-02-11 06:17 - 2015-01-09 02:45 - 02380288 _____ (Microsoft Corporation) C:\Windows\system32\win32k.sys
2015-02-11 06:16 - 2015-01-15 08:46 - 00136640 _____ (Microsoft Corporation) C:\Windows\system32\Drivers\ksecpkg.sys
2015-02-11 06:16 - 2015-01-15 08:46 - 00067520 _____ (Microsoft Corporation) C:\Windows\system32\Drivers\ksecdd.sys
2015-02-11 06:16 - 2015-01-15 08:43 - 00100352 _____ (Microsoft Corporation) C:\Windows\system32\sspicli.dll
2015-02-11 06:16 - 2015-01-15 08:43 - 00015872 _____ (Microsoft Corporation) C:\Windows\system32\sspisrv.dll
2015-02-11 06:16 - 2015-01-15 08:42 - 01061376 _____ (Microsoft Corporation) C:\Windows\system32\lsasrv.dll
2015-02-11 06:16 - 2015-01-15 08:42 - 00050176 _____ (Microsoft Corporation) C:\Windows\system32\auditpol.exe
2015-02-11 06:16 - 2015-01-15 08:42 - 00022528 _____ (Microsoft Corporation) C:\Windows\system32\lsass.exe
2015-02-11 06:16 - 2015-01-15 08:42 - 00022016 _____ (Microsoft Corporation) C:\Windows\system32\secur32.dll
2015-02-11 06:16 - 2015-01-15 08:39 - 00146432 _____ (Microsoft Corporation) C:\Windows\system32\msaudite.dll
2015-02-11 06:16 - 2015-01-15 08:39 - 00060416 _____ (Microsoft Corporation) C:\Windows\system32\msobjs.dll
2015-02-11 06:16 - 2015-01-15 08:37 - 00686080 _____ (Microsoft Corporation) C:\Windows\system32\adtschema.dll
2015-02-11 06:16 - 2015-01-15 05:21 - 00369968 _____ (Microsoft Corporation) C:\Windows\system32\Drivers\cng.sys
2015-02-11 06:14 - 2015-01-14 06:44 - 03972544 _____ (Microsoft Corporation) C:\Windows\system32\ntkrnlpa.exe
2015-02-11 06:14 - 2015-01-14 06:44 - 03917760 _____ (Microsoft Corporation) C:\Windows\system32\ntoskrnl.exe
2015-02-11 06:13 - 2015-02-04 03:54 - 00482304 _____ (Microsoft Corporation) C:\Windows\system32\generaltel.dll
2015-02-11 06:13 - 2015-02-04 03:53 - 00767488 _____ (Microsoft Corporation) C:\Windows\system32\appraiser.dll
2015-02-11 06:13 - 2015-02-04 03:53 - 00621056 _____ (Microsoft Corporation) C:\Windows\system32\invagent.dll
2015-02-11 06:13 - 2015-02-04 03:53 - 00325632 _____ (Microsoft Corporation) C:\Windows\system32\devinv.dll
2015-02-11 06:13 - 2015-02-04 03:53 - 00202752 _____ (Microsoft Corporation) C:\Windows\system32\aepdu.dll
2015-02-11 06:13 - 2015-02-04 03:53 - 00159744 _____ (Microsoft Corporation) C:\Windows\system32\aepic.dll
2015-02-11 06:13 - 2015-02-04 03:49 - 00886784 _____ (Microsoft Corporation) C:\Windows\system32\aeinv.dll
2015-02-11 06:13 - 2015-01-28 00:36 - 01167520 _____ (Microsoft Corporation) C:\Windows\system32\aitstatic.exe
2015-02-11 06:13 - 2015-01-14 06:09 - 00342712 _____ (Microsoft Corporation) C:\Windows\system32\iedkcs32.dll
2015-02-11 06:13 - 2015-01-12 03:21 - 02724864 _____ (Microsoft Corporation) C:\Windows\system32\mshtml.tlb
2015-02-11 06:13 - 2015-01-12 03:21 - 00004096 _____ (Microsoft Corporation) C:\Windows\system32\ieetwcollectorres.dll
2015-02-11 06:13 - 2015-01-12 03:07 - 00062464 _____ (Microsoft Corporation) C:\Windows\system32\iesetup.dll
2015-02-11 06:13 - 2015-01-12 03:07 - 00047616 _____ (Microsoft Corporation) C:\Windows\system32\ieetwproxystub.dll
2015-02-11 06:13 - 2015-01-12 03:00 - 00047104 _____ (Microsoft Corporation) C:\Windows\system32\jsproxy.dll

2015-02-11 06:13 - 2015-01-12 02:59 - 00030720 _____ (Microsoft Corporation) C:\Windows\system32\iernonce.dll
2015-02-11 06:13 - 2015-01-12 02:55 - 00115712 _____ (Microsoft Corporation) C:\Windows\system32\ieUnatt.exe
2015-02-11 06:13 - 2015-01-12 02:55 - 00102912 _____ (Microsoft Corporation) C:\Windows\system32\ieetwcollector.exe
2015-02-11 06:13 - 2015-01-12 02:48 - 00667648 _____ (Microsoft Corporation) C:\Windows\system32\MsSpellCheckingFacility.exe
2015-02-11 06:13 - 2015-01-12 02:45 - 00418304 _____ (Microsoft Corporation) C:\Windows\system32\dxtmsft.dll
2015-02-11 06:13 - 2015-01-12 02:40 - 00060416 _____ (Microsoft Corporation) C:\Windows\system32\JavaScriptCollectionAgent.dll
2015-02-11 06:13 - 2015-01-12 02:36 - 00168960 _____ (Microsoft Corporation) C:\Windows\system32\msrating.dll
2015-02-11 06:13 - 2015-01-12 02:23 - 02052608 _____ (Microsoft Corporation) C:\Windows\system32\inetcpl.cpl
2015-02-11 06:13 - 2015-01-12 02:23 - 00688640 _____ (Microsoft Corporation) C:\Windows\system32\msfeeds.dll
2015-02-11 06:13 - 2015-01-12 02:23 - 00684544 _____ (Microsoft Corporation) C:\Windows\system32\ie4uinit.exe
2015-02-11 06:13 - 2015-01-12 02:00 - 01888256 _____ (Microsoft Corporation) C:\Windows\system32\wininet.dll
2015-02-11 06:13 - 2015-01-12 01:56 - 01307136 _____ (Microsoft Corporation) C:\Windows\system32\urlmon.dll
2015-02-11 06:13 - 2015-01-12 01:55 - 00710144 _____ (Microsoft Corporation) C:\Windows\system32\ieapfltr.dll
2015-02-11 06:13 - 2015-01-10 07:27 - 00550912 _____ (Microsoft Corporation) C:\Windows\system32\kerberos.dll
2015-02-11 06:13 - 2015-01-10 07:27 - 00259584 _____ (Microsoft Corporation) C:\Windows\system32\msv1_0.dll
2015-02-11 06:13 - 2015-01-10 07:27 - 00248832 _____ (Microsoft Corporation) C:\Windows\system32\schannel.dll
2015-02-11 06:13 - 2015-01-10 07:27 - 00221184 _____ (Microsoft Corporation) C:\Windows\system32\ncrypt.dll
2015-02-11 06:13 - 2015-01-10 07:27 - 00172032 _____ (Microsoft Corporation) C:\Windows\system32\wdigest.dll
2015-02-11 06:13 - 2015-01-10 07:27 - 00065536 _____ (Microsoft Corporation) C:\Windows\system32\TSpkg.dll
2015-02-11 06:13 - 2015-01-10 07:27 - 00017408 _____ (Microsoft Corporation) C:\Windows\system32\credssp.dll
2015-02-11 06:13 - 2014-11-26 04:32 - 00571904 _____ (Microsoft Corporation) C:\Windows\system32\oleaut32.dll
2015-02-11 06:12 - 2015-01-12 03:25 - 19740160 _____ (Microsoft Corporation) C:\Windows\system32\mshtml.dll
2015-02-11 06:12 - 2015-01-12 03:08 - 00503296 _____ (Microsoft Corporation) C:\Windows\system32\vbscript.dll
2015-02-11 06:12 - 2015-01-12 03:05 - 00064000 _____ (Microsoft Corporation) C:\Windows\system32\MshtmlDac.dll
2015-02-11 06:12 - 2015-01-12 03:02 - 02277888 _____ (Microsoft Corporation) C:\Windows\system32\iertutil.dll
2015-02-11 06:12 - 2015-01-12 02:57 - 00478208 _____ (Microsoft Corporation) C:\Windows\system32\ieui.dll
2015-02-11 06:12 - 2015-01-12 02:35 - 00076288 _____ (Microsoft Corporation) C:\Windows\system32\mshtmled.dll
2015-02-11 06:12 - 2015-01-12 02:33 - 00285696 _____ (Microsoft Corporation) C:\Windows\system32\dxtrans.dll
2015-02-11 06:12 - 2015-01-12 02:22 - 01155072 _____ (Microsoft Corporation) C:\Windows\system32\mshtmlmedia.dll
2015-02-11 06:12 - 2015-01-12 02:14 - 12829184 _____ (Microsoft Corporation) C:\Windows\system32\ieframe.dll
2015-02-11 06:12 - 2014-12-12 06:07 - 01174528 _____ (Microsoft Corporation) C:\Windows\system32\crypt32.dll
2015-02-11 06:12 - 2014-12-08 03:46 - 00308224 _____ (Microsoft Corporation) C:\Windows\system32\scesrv.dll
2015-02-11 06:12 - 2014-07-07 02:40 - 00179200 _____ (Microsoft Corporation) C:\Windows\system32\wintrust.dll
2015-02-11 06:12 - 2014-07-07 02:40 - 00143872 _____ (Microsoft Corporation) C:\Windows\system32\cryptsvc.dll
2015-02-11 06:11 - 2015-01-13 03:49 - 01230336 _____ (Microsoft Corporation) C:\Windows\system32\WindowsCodecs.dll

========== One Month Modified Files and Folders =======

(If an entry is included in the fixlist, the file\folder will be moved.)

2015-03-10 10:05 - 2009-07-14 05:39 - 00051383 _____ () C:\Windows\setupact.log
2015-03-10 09:37 - 2014-05-22 14:15 - 00000914 _____ () C:\Windows\Tasks\Adobe Flash Player Updater.job
2015-03-10 09:14 - 2014-05-28 12:03 - 00000000 ____D () C:\ProgramData\Kaspersky Lab
2015-03-10 07:15 - 2014-05-22 14:08 - 00028160 _____ () C:\Users\Jiří Holeček\Desktop\Zaměstnanci.xls
2015-03-10 05:01 - 2014-05-20 13:37 - 02081429 _____ () C:\Windows\WindowsUpdate.log
2015-03-10 04:20 - 2014-05-22 13:41 - 00000000 ____D () C:\Users\Jiří Holeček\Documents\Soubory aplikace Outlook
2015-03-10 04:07 - 2009-07-14 05:34 - 00036336 ____H () C:\Windows\system32\7B296FB0-376B-497e-B012-9C450E1B7327-5P-1.C7483456-A289-439d-8115-601632D005A0
2015-03-10 04:07 - 2009-07-14 05:34 - 00036336 ____H () C:\Windows\system32\7B296FB0-376B-497e-B012-9C450E1B7327-5P-0.C7483456-A289-439d-8115-601632D005A0
2015-03-10 03:59 - 2009-07-14 05:53 - 00000006 ____H () C:\Windows\Tasks\SA.DAT
2015-03-09 05:51 - 2014-05-22 14:11 - 00000000 ____D () C:\Program Files\Mozilla Maintenance Service
2015-03-06 07:36 - 2015-02-03 09:28 - 00019083 _____ () C:\Users\Jiří Holeček\Desktop\ZU - Výk.Pr..xlsx
2015-03-06 07:27 - 2009-07-14 05:52 - 00000000 ____D () C:\Windows\system32\FxsTmp
2015-03-05 05:51 - 2009-07-14 03:37 - 00000000 ____D () C:\Windows\tracing
2015-03-04 08:47 - 2014-05-22 14:08 - 01311232 _____ () C:\Users\Jiří Holeček\Desktop\FAKTURY.xls
2015-02-24 03:23 - 2014-05-20 14:01 - 00246920 ____N (Microsoft Corporation) C:\Windows\system32\MpSigStub.exe
2015-02-13 07:34 - 2009-07-14 03:37 - 00000000 ____D () C:\Windows\rescache
2015-02-13 06:25 - 2009-07-14 03:37 - 00000000 ____D () C:\Windows\Microsoft.NET
2015-02-12 15:12 - 2009-07-14 03:37 - 00000000 ____D () C:\Program Files\Common Files\microsoft shared
2015-02-12 06:02 - 2009-07-14 05:33 - 00342176 _____ () C:\Windows\system32\FNTCACHE.DAT
2015-02-12 06:00 - 2014-12-11 05:51 - 00000000 ____D () C:\Windows\system32\appraiser
2015-02-12 06:00 - 2014-05-21 14:54 - 00000000 ___SD () C:\Windows\system32\CompatTel
2015-02-11 14:22 - 2014-05-21 14:41 - 00000000 ____D () C:\Windows\system32\MRT
2015-02-11 14:19 - 2014-05-21 14:41 - 113756392 _____ (Microsoft Corporation) C:\Windows\system32\MRT.exe
2015-02-11 14:18 - 2014-05-22 13:11 - 00000000 ____D () C:\ProgramData\Microsoft Help
2015-02-11 14:18 - 2009-07-14 03:04 - 00000478 _____ () C:\Windows\win.ini

========== End Of Log ==========

Výstupní log z programu Microsoft Baseline Security Analyzer

Security assessment:
Severe Risk (One or more critical checks failed.)

Computer name: WORKGROUP\ZELEN
IP address: 192.168.117.56
Security report name: WORKGROUP - ZELEN (10.3.2015 10-20)
Scan date: 10.3.2015 10:20
Catalog synchronization date:
Security update catalog: Microsoft Update

Security Updates

Score	Issue	Result
	Developer Tools, Runtimes, and Redistributables Security Updates	No security updates are missing.
	Office Security Updates	No security updates are missing.
	SQL Server Security Updates	No security updates are missing.
	Silverlight Security Updates	No security updates are missing.
	Windows Security Updates	No security updates are missing.

Current Update Compliance

Score	ID	Description	Maximum Severity
Installed	MS11-025	Security Update for Microsoft Visual C++ 2010 Service Pack 1 Redistributable Package (KB2565063)	Important

Current Update Compliance

Score	ID	Description	Maximum Severity
Installed	MS13-091	Security Update for Microsoft Office 2010 (KB2553284) 32-Bit Edition	Important
Installed	MS14-024	Security Update for Microsoft Office 2010 (KB2810073) 32-Bit Edition	Important
Installed	MS15-012	Security Update for Microsoft Word 2010 (KB2956066) 32-Bit Edition	Important
Installed	MS13-074	Security Update for Microsoft Office 2010 (KB2687423) 32-Bit Edition	Important
Installed	MS14-036	Security Update for Microsoft Office 2010 (KB2881071) 32-Bit Edition	Important
Installed	MS15-013	Security Update for Microsoft Office 2010 (KB2920748) 32-Bit Edition	Important
Installed	MS14-024	Security Update for Microsoft Office 2010 (KB2880971) 32-Bit Edition	Important
Installed	2687455	Service Pack 2 for Microsoft Office 2010 (KB2687455) 32-Bit Edition	
Installed	MS14-082	Security Update for Microsoft Office 2010 (KB2553154) 32-Bit Edition	Important
Installed	MS15-012	Security Update for Microsoft Excel 2010 (KB2956081) 32-Bit Edition	Important
Installed	MS13-106	Security Update for Microsoft Office 2010 (KB2850016) 32-Bit Edition	Important
Installed	MS15-012	Security Update for Microsoft Office 2010 (KB2956073) 32-Bit Edition	Important

Current Update Compliance

Score	ID	Description	Maximum Severity
Installed	MS06-061	MSXML 6.0 RTM Security Update (925673)	Critical

Current Update Compliance

Score	ID	Description	Maximum Severity
Installed	2977218	Update for Microsoft Silverlight (KB2977218)	

Current Update Compliance

Score	ID	Description	Maximum Severity
Installed	MS15-009	Security Update for Internet Explorer 11 for Windows 7 (KB3034196)	Low
Installed	MS15-016	Security Update for Windows 7 (KB3029944)	Important
Installed	2894854	Security Update for Microsoft .NET Framework 4.5 and 4.5.1 on Windows 7, Windows Vista and Windows Server 2008 x86 (KB2894854)	
Installed	MS14-074	Security Update for Windows 7 (KB3003743)	Important
Installed	MS15-014	Security Update for Windows 7 (KB3004361)	Important
Installed	2973351	Security Update for Windows 7 (KB2973351)	

Windows Scan Results

Administrative Vulnerabilities

Score	Issue	Result
	Local Account Password Test	Some user accounts (3 of 3) have blank or simple passwords, or could not be analyzed.

User	Weak Password	Locked Out	Disabled
Administrator	Weak	-	Disabled
Guest	Weak	-	Disabled
Jiří Holeček	Weak	-	-

	Password Expiration	All user accounts (3) have non-expiring passwords.

User
Administrator
Guest
Jiří Holeček

	Windows Firewall	Windows Firewall is disabled and has exceptions configured.

Connection Name	Firewall	Exceptions
All Connections	Off	Ports, Programs, Services
Připojení k místní síti	Off*	Ports*, Programs*, Services*

	Incomplete Updates	No incomplete software update installations were found.
	File System	All hard drives (1) are using the NTFS file system.

Drive Letter	File System
C:	NTFS

	Guest Account	The Guest account is disabled on this computer.
	Autologon	Autologon is not configured on this computer.
	Restrict Anonymous	Computer is properly restricting anonymous access.
	Administrators	No more than 2 Administrators were found on this computer.

User
Administrator
Jiří Holeček

	Automatic Updates	Updates are automatically downloaded and installed on this computer.

Additional System Information

Score	Issue	Result
	Windows Version	Computer is running Microsoft Windows 7.
	Auditing	Neither Logon Success nor Logon Failure auditing are enabled. Enable auditing and turn on auditing for specific events such as logon and logoff. Be sure to monitor your event log to watch for unauthorized access.
	Shares	2 share(s) are present on your computer.

Share	Directory	Share ACL	Directory ACL
ADMIN$	C:\Windows	Admin Share	NT SERVICE\TrustedInstaller - F, NT AUTHORITY\SYSTEM - RWXD, BUILTIN\Administrators - RWXD, BUILTIN\Users - RX
C$	C:\	Admin Share	BUILTIN\Administrators - F, NT AUTHORITY\SYSTEM - F, BUILTIN\Users - RX, NT AUTHORITY\Authenticated Users - D

	Services	No potentially unnecessary services were found.

10.5.4 Stanice 5 – Bazén

Výstupní log z programu Farbar Recovery Scan Tool

Scan result of Farbar Recovery Scan Tool (FRST) (x86) Version: 12-02-2015 ([color=red]ATTENTION: ====> FRST version is 26 days old and could be outdated[/color])
Ran by Jit-Ra (administrator) on BAZEN on 10-03-2015 13:36:50
Running from C:\Users\Jit-Ra\Desktop
Loaded Profiles: Jit-Ra (Available profiles: Jit-Ra & Bára - Dáda - Štěpán & Guest)
Platform: Microsoft Windows 8.1 Pro (X86) OS Language: Čeština (Česká republika)
Internet Explorer Version 11 (Default browser: IE)
Boot Mode: Normal
Tutorial for Farbar Recovery Scan Tool: http://www.geekstogo.com/forum/topic/335081-frst-tutorial-how-to-use-farbar-recovery-scan-tool/

========== Processes (Whitelisted) ==========

(If an entry is included in the fixlist, the process will be closed. The file will not be moved.)

(SUPERAntiSpyware.com) C:\Program Files\SUPERAntiSpyware\SASCORE.EXE
(Intel Corporation) C:\Program Files\Intel\AMT\atchksrv.exe
(Microsoft Corporation) C:\Windows\System32\dasHost.exe
(Foxit Software Inc.) C:\Program Files\FOXIT SOFTWARE\FOXIT READER\Foxit Cloud\FCUpdateService.exe
(Garmin Ltd or its subsidiaries) C:\Program Files\Garmin\Core Update Service\Garmin.Cartography.MapUpdate.CoreService.exe
(Intel) C:\Program Files\Intel\AMT\LMS.exe
(TeamViewer GmbH) C:\Program Files\TeamViewer\Version9\TeamViewer_Service.exe
(TomTom) C:\Program Files\TomTom HOME 2\TomTomHOMEService.exe
(Intel) C:\Program Files\Intel\AMT\UNS.exe
(Microsoft Corporation) C:\Program Files\Windows Defender\MsMpEng.exe
(Microsoft Corporation) C:\Program Files\Windows Defender\NisSrv.exe
(Microsoft Corporation) C:\Program Files\Common Files\microsoft shared\OfficeSoftwareProtectionPlatform\OSPPSVC.EXE
(IvoSoft) C:\Program Files\Classic Shell\ClassicStartMenu.exe
(Intel Corporation) C:\Program Files\Intel\AMT\atchk.exe
(SUPERAntiSpyware) C:\Program Files\SUPERAntiSpyware\SUPERANTISPYWARE.EXE
(Akamai Technologies, Inc.) C:\Users\Jit-Ra\AppData\Local\Akamai\netsession_win.exe
(Akamai Technologies, Inc.) C:\Users\Jit-Ra\AppData\Local\Akamai\netsession_win.exe
(Microsoft Corporation) C:\Program Files\Windows Defender\MpCmdRun.exe
(Microsoft Corporation) C:\Windows\System32\dllhost.exe
(Microsoft Corporation) C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
(Microsoft Corporation) C:\Windows\splwow64.exe
(Microsoft Corporation) C:\Windows\System32\PrintIsolationHost.exe

========== Registry (Whitelisted) ==========

(If an entry is included in the fixlist, the registry item will be restored to default or removed. The file will not be moved.)

HKLM\...\Run: [atchk] => C:\Program Files\Intel\AMT\atchk.exe [401408 2009-12-01] (Intel Corporation)
HKLM\...\Run: [Zune Launcher] => C:\Program Files\Zune\ZuneLauncher.exe [159456 2011-08-05] (Microsoft Corporation)
HKLM\...\Run: [Windows Mobile Device Center] => C:\WINDOWS\WindowsMobile\wmdc.exe [648072 2007-05-31] (Microsoft Corporation)
HKLM\...\Run: [KiesTrayAgent] => C:\Program Files\Samsung\Kies\KiesTrayAgent.exe [311152 2013-11-06] (Samsung Electronics Co., Ltd.)
HKLM\...\Run: [Classic Start Menu] => C:\Program Files\Classic Shell\ClassicStartMenu.exe [150208 2014-04-20] (IvoSoft)
HKU\S-1-5-21-3003923011-533000253-2755679090-1001\...\Run: [SUPERAntiSpyware] => C:\Program Files\SUPERAntiSpyware\SUPERAntiSpyware.exe [6699800 2015-01-28] (SUPERAntiSpyware)
HKU\S-1-5-21-3003923011-533000253-2755679090-1001\...\Run: [DAEMON Tools Lite] => C:\Program Files\DAEMON Tools Lite\DTLite.exe [3672640 2013-03-14] (Disc Soft Ltd)
HKU\S-1-5-21-3003923011-533000253-2755679090-1001\...\Run: [KiesPreload] => C:\Program Files\Samsung\Kies\Kies.exe [1564528 2013-11-06] (Samsung)
HKU\S-1-5-21-3003923011-533000253-2755679090-1001\...\Run: [GarminExpressTrayApp] => C:\Program Files\Garmin\Express Tray\ExpressTray.exe [688984 2014-12-31] (Garmin Ltd or its subsidiaries)
HKU\S-1-5-21-3003923011-533000253-2755679090-1001\...\Run: [NokiaSuite.exe] => C:\Program Files\Nokia\Nokia Suite\NokiaSuite.exe [1090912 2013-10-02] (Nokia)
HKU\S-1-5-21-3003923011-533000253-2755679090-1001\...\Run: [Akamai NetSession Interface] => C:\Users\Jit-Ra\AppData\Local\Akamai\netsession_win.exe [4673432 2014-10-29] (Akamai Technologies, Inc.)
HKU\S-1-5-18\...\Run: [GarminExpressTrayApp] => C:\Program Files\Garmin\Express Tray\ExpressTray.exe [688984 2014-12-31] (Garmin Ltd or its subsidiaries)
ShellIconOverlayIdentifiers: [ShareOverlay] -> {594D4122-1F87-41E2-96C7-825FB4796516} => C:\Program Files\Classic Shell\ClassicExplorer32.dll (IvoSoft)

========== Internet (Whitelisted) ==========

(If an item is included in the fixlist, if it is a registry item it will be removed or restored to default.)

HKLM\Software\Microsoft\Internet Explorer\Main,Start Page = http://www.msn.com/?pc=MSE1
HKLM\Software\Microsoft\Internet Explorer\Main,Search Page =
http://www.istartsurf.com/web/?type=ds&ts=1409490190&from=amt&uid=ST3160815AS_6RA8VD7VXXXX6RA8VD7V&q={search Terms}
HKLM\Software\Microsoft\Internet Explorer\Main,Default_Page_URL = www.google.com
HKLM\Software\Microsoft\Internet Explorer\Main,Default_Search_URL = www.google.com
HKU\S-1-5-21-3003923011-533000253-2755679090-1001\Software\Microsoft\Internet Explorer\Main,Start Page =
http://www.msn.com/?pc=MSE1
HKU\S-1-5-21-3003923011-533000253-2755679090-1001\Software\Microsoft\Internet Explorer\Main,ICQ Search =
http://search.icq.com/search/results.php?q={searchTerms}&ch_id=osd
SearchScopes: HKU\S-1-5-21-3003923011-533000253-2755679090-1001 -> {6552C7DD-90A4-4387-B795-F8F96747DE19} URL =
http://search.icq.com/search/results.php?q={searchTerms}&ch_id=osd
BHO: ExplorerBHO Class -> {449D0D6E-2412-4E61-B68F-1CB625CD9E52} -> C:\Program Files\Classic Shell\ClassicExplorer32.dll (IvoSoft)
BHO: Groove GFS Browser Helper -> {72853161-30C5-4D22-B7F9-0BBC1D38A37E} -> C:\Program Files\Microsoft Office\Office14\GROOVEEX.DLL (Microsoft Corporation)
BHO: Java(tm) Plug-In SSV Helper -> {761497BB-D6F0-462C-B6EB-D4DAF1D92D43} -> C:\Program Files\Java\jre1.8.0_31\bin\ssv.dll (Oracle Corporation)
BHO: Office Document Cache Handler -> {B4F3A835-0E21-4959-BA22-42B3008E02FF} -> C:\Program Files\Microsoft Office\Office14\URLREDIR.DLL (Microsoft Corporation)
BHO: Java(tm) Plug-In 2 SSV Helper -> {DBC80044-A445-435b-BC74-9C25C1C588A9} -> C:\Program Files\Java\jre1.8.0_31\bin\jp2ssv.dll (Oracle Corporation)
BHO: ClassicIEBHO Class -> {EA801577-E6AD-4BD5-8F71-4BE0154331A4} -> C:\Program Files\Classic Shell\ClassicIEDLL_32.dll (IvoSoft)
Toolbar: HKLM - Classic Explorer Bar - {553891B7-A0D5-4526-BE18-D3CE461D6310} - C:\Program Files\Classic Shell\ClassicExplorer32.dll (IvoSoft)
DPF: {14711E5F-189F-4D07-9D41-9EB57F547DD8} http://kamera2.alesovka.net/Option/Media.CAB
DPF: {CF84DAC5-A4F5-419E-A0BA-C01FFD71112F}
http://content.systemrequirementslab.com.s3.amazonaws.com/global/bin/srldetect_intel_4.5.13.0.cab
Handler: osf - {D924BDC6-C83A-4BD5-90D0-095128A113D1} - C:\Program Files\Microsoft Office\Office15\MSOSB.DLL (Microsoft Corporation)
Handler: skype4com - {FFC8B962-9B40-4DFF-9458-1830C7DD7F5D} - C:\Program Files\Common Files\Skype\Skype4COM.dll (Skype Technologies)
ShellExecuteHooks: SABShellExecuteHook Class - {5AE067D3-9AFB-48E0-853A-EBB7F4A000DA} - C:\Program Files\SUPERAntiSpyware\SASSEH.DLL [113024 2011-07-19] (SuperAdBlocker.com)
Hosts: 127.0.0.1 activation.acronis.com
Tcpip\Parameters: [DhcpNameServer] 217.77.161.131 217.77.165.81

FireFox:
========
FF ProfilePath: C:\Users\Jit-Ra\AppData\Roaming\Mozilla\Firefox\Profiles\y7p8em5g.default
FF Homepage: https://www.google.cz/?gws_rd=ssl
FF Plugin: @adobe.com/FlashPlayer -> C:\WINDOWS\system32\Macromed\Flash\NPSWF32_16_0_0_305.dll ()
FF Plugin: @divx.com/DivX VOD Helper,version=1.0.0 -> C:\Program Files\DivX\DivX OVS Helper\npovshelper.dll (DivX, LLC.)
FF Plugin: @divx.com/DivX Web Player Plug-In,version=1.0.0 -> C:\Program Files\DivX\DivX Web Player\npdivx32.dll (DivX, LLC)
FF Plugin: @foxitsoftware.com/Foxit PhantomPDF Plugin,version=1.0,application/pdf -> C:\Program Files\Foxit Software\Foxit PhantomPDF\plugins\npFoxitPhantomPDFPlugin.dll (Foxit Corporation)
FF Plugin: @foxitsoftware.com/Foxit PhantomPDF Plugin,version=1.0,application/vnd.fdf -> C:\Program Files\Foxit Software\Foxit PhantomPDF\plugins\npFoxitPhantomPDFPlugin.dll (Foxit Corporation)
FF Plugin: @foxitsoftware.com/Foxit PhantomPDF Plugin,version=1.0,application/vnd.xdp -> C:\Program Files\Foxit Software\Foxit PhantomPDF\plugins\npFoxitPhantomPDFPlugin.dll (Foxit Corporation)
FF Plugin: @foxitsoftware.com/Foxit PhantomPDF Plugin,version=1.0,application/vnd.xfdf -> C:\Program Files\Foxit Software\Foxit PhantomPDF\plugins\npFoxitPhantomPDFPlugin.dll (Foxit Corporation)
FF Plugin: @foxitsoftware.com/Foxit Reader Plugin,version=1.0,application/vnd.fdf -> C:\Program Files\FOXIT SOFTWARE\FOXIT READER\plugins\npFoxitReaderPlugin.dll (Foxit Corporation)
FF Plugin: @idsoftware.com/QuakeLive -> C:\ProgramData\id Software\QuakeLive\npquakezero.dll (id Software Inc.)
FF Plugin: @java.com/DTPlugin,version=11.31.2 -> C:\Program Files\Java\jre1.8.0_31\bin\dtplugin\npDeployJava1.dll (Oracle Corporation)
FF Plugin: @java.com/JavaPlugin,version=11.31.2 -> C:\Program Files\Java\jre1.8.0_31\bin\plugin2\npjp2.dll (Oracle Corporation)
FF Plugin: @Microsoft.com/NpCtrl,version=1.0 -> c:\Program Files\Microsoft Silverlight\5.1.30514.0\npctrl.dll (Microsoft Corporation)
FF Plugin: @microsoft.com/OfficeAuthz,version=14.0 -> C:\PROGRA~1\MICROS~1\Office14\NPAUTHZ.DLL (Microsoft Corporation)
FF Plugin: @microsoft.com/SharePoint,version=14.0 -> C:\PROGRA~1\MICROS~1\Office15\NPSPWRAP.DLL (Microsoft Corporation)
FF Plugin: @nokia.com/EnablerPlugin -> C:\Program Files\Nokia\Nokia Suite\npNokiaSuiteEnabler.dll ( )
FF Plugin: @tools.google.com/Google Update;version=3 -> C:\Program Files\Google\Update\1.3.26.9\npGoogleUpdate3.dll (Google Inc.)

FF Plugin: @tools.google.com/Google Update;version=9 -> C:\Program Files\Google\Update\1.3.26.9\npGoogleUpdate3.dll (Google Inc.)
FF Plugin: @videolan.org/vlc,version=2.1.3 -> C:\Program Files\VideoLAN\VLC\npvlc.dll (VideoLAN)
FF Plugin HKU\S-1-5-21-3003923011-533000253-2755679090-1001: @citrixonline.com/appdetectorplugin -> C:\Users\Jit-Ra\AppData\Local\Citrix\Plugins\104\npappdetector.dll (Citrix Online)
FF Plugin HKU\S-1-5-21-3003923011-533000253-2755679090-1001: @unity3d.com/UnityPlayer,version=1.0 -> C:\Users\Jit-Ra\AppData\LocalLow\Unity\WebPlayer\loader\npUnity3D32.dll (Unity Technologies ApS)
FF user.js: detected! => C:\Users\Jit-Ra\AppData\Roaming\Mozilla\Firefox\Profiles\y7p8em5g.default\user.js
FF Extension: Seznam lištička - C:\Users\Jit-Ra\AppData\Roaming\Mozilla\Firefox\Profiles\y7p8em5g.default\Extensions\{ea614400-e918-4741-9a97-7a972ff7c30b} [2014-09-02]
FF Extension: X-notifier - C:\Users\Jit-Ra\AppData\Roaming\Mozilla\Firefox\Profiles\y7p8em5g.default\Extensions\{37fa1426-b82d-11db-8314-0800200c9a66}.xpi [2013-12-22]

Chrome:
=======
CHR Profile: C:\Users\Jit-Ra\AppData\Local\Google\Chrome\User Data\Default
CHR Extension: (Dokumenty Google) - C:\Users\Jit-Ra\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake [2013-11-05]
CHR Extension: (Disk Google) - C:\Users\Jit-Ra\AppData\Local\Google\Chrome\User Data\Default\Extensions\apdfllckaahabafndbhieahigkjlhalf [2013-11-05]
CHR Extension: (Seznam Lištička - Email) - C:\Users\Jit-Ra\AppData\Local\Google\Chrome\User Data\Default\Extensions\bgjpfhpjcgdppjbgnpnjllokbmcdllig [2014-07-24]
CHR Extension: (Seznam Lištička - Slovník) - C:\Users\Jit-Ra\AppData\Local\Google\Chrome\User Data\Default\Extensions\blmojkbhnkkphngknkmgccmlenfaelkd [2014-07-24]
CHR Extension: (YouTube) - C:\Users\Jit-Ra\AppData\Local\Google\Chrome\User Data\Default\Extensions\blpcfgokakmgnkcojhhkbfbldkacnbeo [2013-11-05]
CHR Extension: (Vyhledávání Google) - C:\Users\Jit-Ra\AppData\Local\Google\Chrome\User Data\Default\Extensions\coobgpohoikkiipiblmjeljniedjpjpf [2013-11-05]
CHR Extension: (Peněženka Google) - C:\Users\Jit-Ra\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda [2013-11-05]
CHR Extension: (Seznam Lištička - Rychlá volba) - C:\Users\Jit-Ra\AppData\Local\Google\Chrome\User Data\Default\Extensions\olfeabkoenfaoljndfecamgilllcpiak [2014-08-31]
CHR Extension: (Gmail) - C:\Users\Jit-Ra\AppData\Local\Google\Chrome\User Data\Default\Extensions\pjkljhegncpnkpknbcohdijeoejaedia [2013-11-05]

========================== Services (Whitelisted) =================

(If an entry is included in the fixlist, the service will be removed from the registry. The file will not be moved unless listed separately.)

R2 !SASCORE; C:\Program Files\SUPERAntiSpyware\SASCORE.EXE [142648 2014-08-19] (SUPERAntiSpyware.com)
R2 atchksrv; C:\Program Files\Intel\AMT\atchksrv.exe [176128 2009-12-01] (Intel Corporation) [File not signed]
R2 FoxitCloudUpdateService; C:\Program Files\FOXIT SOFTWARE\FOXIT READER\Foxit Cloud\FCUpdateService.exe [244448 2014-10-28] (Foxit Software Inc.)
R2 Garmin Core Update Service; C:\Program Files\Garmin\Core Update Service\Garmin.Cartography.MapUpdate.CoreService.exe [451416 2014-12-31] (Garmin Ltd or its subsidiaries)
R2 LMS; C:\Program Files\Intel\AMT\LMS.exe [102400 2009-12-01] (Intel) [File not signed]
S3 ScDeviceEnum; C:\WINDOWS\System32\ScDeviceEnum.dll [105472 2013-08-22] (Microsoft Corporation)
R2 UNS; C:\Program Files\Intel\AMT\UNS.exe [2519040 2009-12-01] (Intel) [File not signed]
R3 WdNisSvc; C:\Program Files\Windows Defender\NisSrv.exe [288128 2014-09-22] (Microsoft Corporation)
S3 WEPHOSTSVC; C:\WINDOWS\system32\wephostsvc.dll [20992 2013-08-22] (Microsoft Corporation)
R2 WinDefend; C:\Program Files\Windows Defender\MsMpEng.exe [22192 2014-09-22] (Microsoft Corporation)
S3 workfolderssvc; C:\WINDOWS\system32\workfolderssvc.dll [1222144 2014-09-24] (Microsoft Corporation)

========================= Drivers (Whitelisted) ====================

(If an entry is included in the fixlist, the service will be removed from the registry. The file will not be moved unless listed separately.)

R1 BasicRender; C:\WINDOWS\System32\drivers\BasicRender.sys [25600 2014-09-24] (Microsoft Corporation)
R3 dtsoftbus01; C:\WINDOWS\System32\drivers\dtsoftbus01.sys [242240 2013-05-03] (DT Soft Ltd)
S3 GPIO; C:\WINDOWS\System32\drivers\iaiogpio.sys [22016 2013-07-23] (Intel Corporation)
S3 kvnet; C:\WINDOWS\system32\DRIVERS\kvnet.sys [26624 2013-10-09] (Kerio Technologies Inc.)
R3 mf; C:\WINDOWS\System32\drivers\mf.sys [30208 2014-09-24] (Microsoft Corporation)
R1 MpKslacb36f71; C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{936A8CE4-B3C9-497B-9594-1512DA38E55F}\MpKslacb36f71.sys [39464 2015-03-10] (Microsoft Corporation)
R3 NmPar; C:\WINDOWS\system32\DRIVERS\NmPar.sys [81920 2010-01-12] (Windows (R) Codename Longhorn DDK provider)
R3 nmserial; C:\WINDOWS\system32\DRIVERS\nmserial.sys [70656 2010-01-07] (Windows (R) Codename Longhorn DDK provider)
R1 SASDIFSV; C:\Program Files\SUPERAntiSpyware\SASDIFSV.SYS [12880 2011-07-22] (SUPERAdBlocker.com and SUPERAntiSpyware.com)
R1 SASKUTIL; C:\Program Files\SUPERAntiSpyware\SASKUTIL.SYS [67664 2011-07-12] (SUPERAdBlocker.com and SUPERAntiSpyware.com)
R3 WdNisDrv; C:\WINDOWS\System32\Drivers\WdNisDrv.sys [84800 2014-09-22] (Microsoft Corporation)
R0 Wof; C:\WINDOWS\system32\Drivers\Wof.sys [138584 2014-09-24] (Microsoft Corporation)
R3 WUDFSensorLP; C:\WINDOWS\system32\DRIVERS\WUDFRd.sys [188416 2014-05-31] (Microsoft Corporation)

R3 WUDFWpdMtp; C:\WINDOWS\system32\DRIVERS\WUDFRd.sys [188416 2014-05-31] (Microsoft Corporation)

========== NetSvcs (Whitelisted) ==========

(If an item is included in the fixlist, it will be removed from the registry. Any associated file could be listed separately to be moved.)

========== One Month Created Files and Folders ========

(If an entry is included in the fixlist, the file\folder will be moved.)

2015-03-10 13:36 - 2015-03-10 13:37 - 00015891 _____ () C:\Users\Jit-Ra\Desktop\FRST.txt
2015-03-10 13:36 - 2015-03-10 13:36 - 00000000 ____D () C:\FRST
2015-03-10 13:20 - 2015-03-10 13:24 - 00000000 ____D () C:\Users\Jit-Ra\SecurityScans
2015-03-10 13:20 - 2015-03-10 13:20 - 00001138 _____ () C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Microsoft Baseline Security Analyzer 2.3.lnk
2015-03-10 13:20 - 2015-03-10 13:20 - 00001126 _____ () C:\Users\Public\Desktop\Microsoft Baseline Security Analyzer 2.3.lnk
2015-03-10 13:20 - 2015-03-10 13:20 - 00000000 ____D () C:\Program Files\Microsoft Baseline Security Analyzer 2
2015-03-10 13:20 - 2015-02-14 08:44 - 01125376 _____ (Farbar) C:\Users\Jit-Ra\Desktop\FRST.exe
2015-03-08 15:23 - 2015-03-08 15:24 - 00000000 ____D () C:\Users\Bára - Dáda - Štěpán\Downloads\0#_Sociální a regionální rozvoj
2015-03-08 14:54 - 2015-03-08 15:21 - 724961888 _____ () C:\Users\Bára - Dáda - Štěpán\Downloads\Sociální a regionální rozvoj.zip
2015-03-03 16:09 - 2015-03-10 13:23 - 00220499 _____ () C:\Users\Jit-Ra\Desktop\Plán směn - Březen 2015.xlsm
2015-02-25 10:27 - 2014-12-13 22:29 - 00513488 _____ () C:\WINDOWS\system32\locale.nls
2015-02-25 10:27 - 2014-10-29 02:04 - 00868352 _____ (Microsoft Corporation) C:\WINDOWS\system32\Windows.Globalization.dll
2015-02-25 10:27 - 2014-10-29 02:04 - 00200704 _____ (Microsoft Corporation) C:\WINDOWS\system32\GlobCollationHost.dll
2015-02-19 07:13 - 2015-02-19 07:13 - 00000000 ____D () C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Garmin
2015-02-18 14:28 - 2015-02-18 14:28 - 00000000 ____D () C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Foxit PhantomPDF
2015-02-18 13:39 - 2015-02-18 14:28 - 00000000 ____D () C:\Users\Public\Foxit Software
2015-02-18 13:39 - 2015-02-18 13:39 - 00000000 ____D () C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Foxit Reader
2015-02-12 07:53 - 2015-01-23 04:17 - 04300800 _____ (Microsoft Corporation) C:\WINDOWS\system32\jscript9.dll
2015-02-11 13:29 - 2015-02-11 13:29 - 00408896 _____ () C:\WINDOWS\system32\FNTCACHE.DAT
2015-02-11 08:11 - 2015-02-11 08:11 - 00000000 ____D () C:\WINDOWS\PCHEALTH
2015-02-11 07:46 - 2015-01-19 19:36 - 01192552 _____ (Microsoft Corporation) C:\WINDOWS\system32\sppobjs.dll
2015-02-11 07:46 - 2015-01-13 23:04 - 01489072 _____ (Microsoft Corporation) C:\WINDOWS\system32\WindowsCodecs.dll
2015-02-11 07:46 - 2015-01-12 03:25 - 19740160 _____ (Microsoft Corporation) C:\WINDOWS\system32\mshtml.dll
2015-02-11 07:46 - 2015-01-12 03:08 - 00503296 _____ (Microsoft Corporation) C:\WINDOWS\system32\vbscript.dll
2015-02-11 07:46 - 2015-01-12 03:05 - 00064000 _____ (Microsoft Corporation) C:\WINDOWS\system32\MshtmlDac.dll
2015-02-11 07:46 - 2015-01-12 03:02 - 02277888 _____ (Microsoft Corporation) C:\WINDOWS\system32\iertutil.dll
2015-02-11 07:46 - 2015-01-12 02:55 - 00664064 _____ (Microsoft Corporation) C:\WINDOWS\system32\jscript.dll
2015-02-11 07:46 - 2015-01-12 02:45 - 00418304 _____ (Microsoft Corporation) C:\WINDOWS\system32\dxtmsft.dll
2015-02-11 07:46 - 2015-01-12 02:34 - 00128000 _____ (Microsoft Corporation) C:\WINDOWS\system32\iepeers.dll
2015-02-11 07:46 - 2015-01-12 02:30 - 00880128 _____ (Microsoft Corporation) C:\WINDOWS\system32\inetcomm.dll
2015-02-11 07:46 - 2015-01-12 02:25 - 00230400 _____ (Microsoft Corporation) C:\WINDOWS\system32\webcheck.dll
2015-02-11 07:46 - 2015-01-12 02:23 - 02052608 _____ (Microsoft Corporation) C:\WINDOWS\system32\inetcpl.cpl
2015-02-11 07:46 - 2015-01-12 02:23 - 00688640 _____ (Microsoft Corporation) C:\WINDOWS\system32\msfeeds.dll
2015-02-11 07:46 - 2015-01-12 02:23 - 00684544 _____ (Microsoft Corporation) C:\WINDOWS\system32\ie4uinit.exe
2015-02-11 07:46 - 2015-01-12 02:23 - 00327168 _____ (Microsoft Corporation) C:\WINDOWS\system32\iedkcs32.dll
2015-02-11 07:46 - 2015-01-12 02:14 - 12829184 _____ (Microsoft Corporation) C:\WINDOWS\system32\ieframe.dll
2015-02-11 07:46 - 2015-01-12 02:00 - 01888256 _____ (Microsoft Corporation) C:\WINDOWS\system32\wininet.dll
2015-02-11 07:46 - 2015-01-12 01:56 - 01307136 _____ (Microsoft Corporation) C:\WINDOWS\system32\urlmon.dll
2015-02-11 07:46 - 2015-01-12 01:55 - 00710144 _____ (Microsoft Corporation) C:\WINDOWS\system32\ieapfltr.dll
2015-02-11 07:46 - 2015-01-10 07:38 - 00359424 _____ (Microsoft Corporation) C:\WINDOWS\system32\schannel.dll
2015-02-11 07:45 - 2015-02-04 00:43 - 00202752 _____ (Microsoft Corporation) C:\WINDOWS\system32\aepdu.dll
2015-02-11 07:45 - 2015-02-04 00:08 - 00620544 _____ (Microsoft Corporation) C:\WINDOWS\system32\invagent.dll
2015-02-11 07:45 - 2015-02-04 00:08 - 00325120 _____ (Microsoft Corporation) C:\WINDOWS\system32\devinv.dll
2015-02-11 07:45 - 2015-02-03 00:11 - 00886784 _____ (Microsoft Corporation) C:\WINDOWS\system32\aeinv.dll
2015-02-11 07:45 - 2015-02-03 00:11 - 00766976 _____ (Microsoft Corporation) C:\WINDOWS\system32\appraiser.dll
2015-02-11 07:45 - 2015-02-03 00:11 - 00482304 _____ (Microsoft Corporation) C:\WINDOWS\system32\generaltel.dll
2015-02-11 07:45 - 2015-01-15 23:37 - 00478776 _____ (Microsoft Corporation) C:\WINDOWS\system32\Drivers\cng.sys
2015-02-11 07:45 - 2015-01-15 23:37 - 00148288 _____ (Microsoft Corporation) C:\WINDOWS\system32\Drivers\ksecpkg.sys
2015-02-11 07:45 - 2015-01-10 09:28 - 05769024 _____ (Microsoft Corporation) C:\WINDOWS\system32\ntoskrnl.exe
2015-02-11 07:45 - 2015-01-10 09:28 - 01468408 _____ (Microsoft Corporation) C:\WINDOWS\system32\ntdll.dll
2015-02-11 07:45 - 2015-01-10 08:38 - 03550720 _____ (Microsoft Corporation) C:\WINDOWS\system32\win32k.sys
2015-02-11 07:45 - 2014-12-19 09:25 - 00602776 _____ (Microsoft Corporation) C:\WINDOWS\system32\oleaut32.dll
2015-02-11 07:45 - 2014-12-09 04:45 - 00393728 _____ (Microsoft Corporation) C:\WINDOWS\system32\scesrv.dll
2015-02-11 07:45 - 2014-12-09 00:11 - 00391526 _____ () C:\WINDOWS\system32\ApnDatabase.xml
2015-02-11 07:45 - 2014-10-29 03:06 - 00736768 _____ (Microsoft Corporation) C:\WINDOWS\system32\adtschema.dll
2015-02-11 07:45 - 2014-10-29 03:06 - 00154112 _____ (Microsoft Corporation) C:\WINDOWS\system32\msaudite.dll
2015-02-11 07:45 - 2014-10-29 02:03 - 01117696 _____ (Microsoft Corporation) C:\WINDOWS\system32\lsasrv.dll

========== One Month Modified Files and Folders =======

(If an entry is included in the fixlist, the file\folder will be moved.)

2015-03-10 13:36 - 2015-01-27 18:02 - 01841809 _____ () C:\WINDOWS\WindowsUpdate.log
2015-03-10 13:30 - 2015-01-28 20:10 - 00000580 _____ () C:\WINDOWS\Tasks\G2MUpdateTask-S-1-5-21-3003923011-533000253-2755679090-1001.job
2015-03-10 13:22 - 2014-09-24 04:06 - 01754508 _____ () C:\WINDOWS\system32\PerfStringBackup.INI
2015-03-10 13:20 - 2014-12-03 20:10 - 00000000 ____D () C:\Users\Jit-Ra
2015-03-10 13:19 - 2015-01-27 19:37 - 00012238 _____ () C:\WINDOWS\setupact.log
2015-03-10 13:19 - 2013-01-25 18:00 - 00000000 ____D () C:\Program Files\SUPERAntiSpyware
2015-03-10 13:18 - 2013-01-16 11:03 - 00000000 ____D () C:\ProgramData\Skype
2015-03-10 13:17 - 2014-10-28 14:29 - 00000000 ____D () C:\Users\Bára - Dáda - Štěpán\AppData\Roaming\ClassicShell
2015-03-10 13:09 - 2013-01-22 17:53 - 00000914 _____ () C:\WINDOWS\Tasks\Adobe Flash Player Updater.job
2015-03-10 13:00 - 2013-08-22 09:17 - 00000000 ____D () C:\WINDOWS\system32\sru
2015-03-10 12:43 - 2014-10-23 07:28 - 00000960 _____ () C:\WINDOWS\Tasks\GoogleUpdateTaskMachineUA.job
2015-03-10 05:05 - 2013-08-22 09:17 - 00000000 ____D () C:\WINDOWS\Microsoft.NET
2015-03-09 13:01 - 2014-10-28 14:59 - 00000000 ____D () C:\Users\Bára - Dáda - Štěpán\Documents\Soubory aplikace Outlook
2015-03-08 17:58 - 2013-11-06 20:19 - 00000000 ____D () C:\Users\Jit-Ra\AppData\Roaming\ClassicShell
2015-03-08 14:21 - 2015-01-27 17:42 - 00067666 _____ () C:\Users\Jit-Ra\Desktop\Radek volno.xlsx
2015-03-06 13:56 - 2014-08-29 12:10 - 00000000 ____D () C:\Users\Jit-Ra\Documents\Jitka
2015-03-06 13:52 - 2013-08-22 09:17 - 00000000 ____D () C:\WINDOWS\AppReadiness
2015-03-06 13:46 - 2014-10-28 15:49 - 00000000 ____D () C:\Users\Jit-Ra\Documents\Soubory aplikace Outlook
2015-03-05 19:26 - 2013-01-22 17:43 - 00000000 ____D () C:\Users\Jit-Ra\Documents\Radek
2015-03-04 18:58 - 2014-11-21 15:44 - 00000000 ____D () C:\Users\Bára - Dáda - Štěpán\AppData\Roaming\vlc
2015-03-03 16:30 - 2013-01-29 19:53 - 00000000 ___RD () C:\Users\Jit-Ra\Desktop\Programy
2015-03-03 14:16 - 2013-01-22 17:43 - 00246920 ____N (Microsoft Corporation) C:\WINDOWS\system32\MpSigStub.exe
2015-03-03 13:33 - 2012-07-26 07:43 - 00000000 ____D () C:\WINDOWS\CbsTemp
2015-03-03 09:20 - 2014-01-12 18:05 - 00000214 _____ () C:\WINDOWS\Tasks\AutoKMS.job
2015-03-03 09:20 - 2013-08-22 08:23 - 00000006 ____H () C:\WINDOWS\Tasks\SA.DAT
2015-03-03 09:19 - 2013-08-22 07:13 - 00524288 ___SH () C:\WINDOWS\system32\config\BBI
2015-02-26 11:00 - 2014-08-29 12:12 - 00000000 ____D () C:\Users\Bára - Dáda - Štěpán\Documents\Dáda
2015-02-22 17:53 - 2014-04-27 18:21 - 00000000 ____D () C:\Users\Bára - Dáda - Štěpán\Documents\Bára Š
2015-02-19 07:14 - 2014-03-11 13:56 - 00000000 ____D () C:\ProgramData\Package Cache
2015-02-19 07:13 - 2014-03-11 13:56 - 00000000 ____D () C:\Program Files\Garmin
2015-02-19 07:13 - 2013-03-12 17:48 - 00000000 ____D () C:\ProgramData\Garmin
2015-02-18 14:29 - 2013-06-12 14:23 - 00000000 ____D () C:\Users\Jit-Ra\AppData\Roaming\Foxit Software
2015-02-18 14:27 - 2014-03-12 14:55 - 00000000 ____D () C:\Program Files\FOXIT SOFTWARE
2015-02-18 13:45 - 2014-08-09 09:46 - 00001109 _____ () C:\ProgramData\Microsoft\Windows\Start Menu\Programs\TeamViewer 9.lnk
2015-02-18 13:39 - 2013-08-22 07:21 - 00000000 ___RD () C:\Users\Public
2015-02-14 14:58 - 2015-02-03 20:28 - 00000000 ____D () C:\Users\Jit-Ra\Desktop\Dp
2015-02-13 12:54 - 2014-07-25 10:52 - 00000000 ____D () C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Microsoft Office 2013
2015-02-13 12:53 - 2013-01-16 10:23 - 00000000 ____D () C:\ProgramData\Microsoft Help
2015-02-11 17:46 - 2013-08-22 09:17 - 00000000 ____D () C:\WINDOWS\rescache
2015-02-11 13:28 - 2013-12-17 14:12 - 00000000 ____D () C:\Program Files\Mozilla Maintenance Service
2015-02-11 08:33 - 2013-08-16 08:18 - 00000000 ____D () C:\WINDOWS\system32\MRT
2015-02-11 08:15 - 2013-01-23 15:50 - 113756392 _____ (Microsoft Corporation) C:\WINDOWS\system32\MRT.exe
2015-02-11 08:08 - 2014-12-10 13:08 - 00000000 ____D () C:\WINDOWS\system32\appraiser
2015-02-11 08:08 - 2014-09-24 04:44 - 00000000 ___SD () C:\WINDOWS\system32\CompatTel
2015-02-11 08:08 - 2012-07-26 05:17 - 00000297 _____ () C:\WINDOWS\win.ini

========== Files in the root of some directories =======

2015-02-06 13:23 - 2015-02-06 13:23 - 0002528 _____ () C:\Users\Jit-Ra\AppData\Roaming\$_hpcst$.hpc
2013-01-20 14:13 - 2013-01-31 17:48 - 0005188 _____ () C:\Users\Jit-Ra\AppData\Roaming\froggy_scorebox
2013-01-20 14:13 - 2013-01-31 17:48 - 0000914 _____ () C:\Users\Jit-Ra\AppData\Roaming\pl_accounts.pl_acc
2013-01-20 14:13 - 2013-01-31 17:48 - 0000556 _____ () C:\Users\Jit-Ra\AppData\Roaming\Troll.options
2013-06-02 13:55 - 2014-10-10 13:30 - 0001980 _____ () C:\Users\Jit-Ra\AppData\Local\SRDownloader.err
2013-06-02 13:43 - 2014-10-10 13:31 - 0001760 _____ () C:\Users\Jit-Ra\AppData\Local\SRDownloader.nast

Some content of TEMP:
==========
C:\Users\Jit-Ra\AppData\Local\Temp\FoxitUpdater.exe

========== Bamital & volsnap Check ==========

C:\WINDOWS\explorer.exe => File is digitally signed
C:\WINDOWS\system32\winlogon.exe => File is digitally signed

LastRegBack: 2015-03-10 05:04

========== End Of Log ==========

Výstupní log z programu Microsoft Baseline Security Analyzer

Security assessment:
Potential Risk (One or more non-critical checks failed.)

Computer name:	WORKGROUP\BAZEN
IP address:	10.0.0.33
Security report name:	WORKGROUP - BAZEN (10. 3. 2015 13-24)
Scan date:	10. 3. 2015 13:24
Catalog synchronization date:	
Security update catalog:	Microsoft Update

Security Updates

Score	Issue	Result
	Skype Security Updates	1 service packs or update rollups are missing. **Update Rollups and Service Packs** Score ID Description Missing 2876229 Update for Skype for Windows desktop 6.11 (KB2876229)
	Developer Tools, Runtimes, and Redistributables Security Updates	No security updates are missing. **Current Update Compliance** Score ID Description Maximum Severity Installed MS11-025 Security Update for Microsoft Visual C++ 2005 Service Pack 1 Redistributable Package (KB2538242) Important Installed MS11-025 Security Update for Microsoft Visual C++ 2010 Service Pack 1 Redistributable Package (KB2565063) Important
	Office Security Updates	No security updates are missing. **Current Update Compliance** Score ID Description Maximum Severity Installed MS13-091 Security Update for Microsoft Office 2010 (KB2553284) 32-Bit Edition Important Installed MS14-024 Security Update for Microsoft Office 2010 (KB2810073) 32-Bit Edition Important Installed MS15-012 Security Update for Microsoft Word 2010 (KB2956066) 32-Bit Edition Important Installed MS13-074 Security Update for Microsoft Office 2010 (KB2687423) 32-Bit Edition Important Installed MS14-036 Security Update for Microsoft Office 2010 (KB2881071) 32-Bit Edition Important Installed MS15-013 Security Update for Microsoft Office 2010 (KB2920748) 32-Bit Edition Important Installed MS14-024 Security Update for Microsoft Office 2013 (KB2880502) 32-Bit Edition Important Installed MS14-024 Security Update for Microsoft Office 2010 (KB2880971) 32-Bit Edition Important Installed 2687455 Service Pack 2 for Microsoft Office 2010 (KB2687455) 32-Bit Edition Installed MS14-082 Security Update for Microsoft Office 2010 (KB2553154) 32-Bit Edition Important Installed MS15-012 Security Update for Microsoft Excel 2010 (KB2956081) 32-Bit Edition Important Installed MS13-106 Security Update for Microsoft Office 2010 (KB2850016) 32-Bit Edition Important Installed MS15-012 Security Update for Microsoft Office 2010 (KB2956073) 32-Bit Edition Important Installed MS14-082 Security Update for Microsoft Office 2013 (KB2726958) 32-Bit Edition Important
	SQL Server Security Updates	No security updates are missing. **Current Update Compliance** Score ID Description Maximum Severity Installed MS06-061 MSXML 6.0 RTM Security Update (925673) Critical
	Silverlight Security Updates	No security updates are missing. **Current Update Compliance** Score ID Description Maximum Severity Installed 2977218 Update for Microsoft Silverlight (KB2977218)
	Windows Security Updates	No security updates are missing. **Current Update Compliance**

Windows Scan Results

Administrative Vulnerabilities

Score	Issue	Result
	Password Expiration	All user accounts (4) have non-expiring passwords. **User** Administrator Bára - Dáda - Štěpán Guest Jit-Ra
	Windows Firewall	Windows Firewall is enabled and has exceptions configured. Windows Firewall is enabled on all network connections. **Connection Name** / **Firewall** / **Exceptions** All Connections / On / Programs Síť Ethernet / On / Programs*
	Incomplete Updates	No incomplete software update installations were found.
	Local Account Password Test	Some user accounts (2 of 4) have blank or simple passwords, or could not be analyzed. **User** / **Weak Password** / **Locked Out** / **Disabled** Administrator / Weak / - / Disabled Guest / Weak / - / Disabled Bára - Dáda - Štěpán / - / - / - Jit-Ra / - / - / -
	File System	All hard drives (1) are using the NTFS file system. **Drive Letter** / **File System** C: / NTFS
	Guest Account	The Guest account is disabled on this computer.
	Autologon	Autologon is not configured on this computer.
	Restrict Anonymous	Computer is properly restricting anonymous access.
	Administrators	No more than 2 Administrators were found on this computer. **User**

	Automatic Updates	Updates are automatically downloaded and installed on this computer.

Additional System Information

Score	Issue	Result
	Windows Version	Computer is running Microsoft Windows 8.1.
	Auditing	Neither Logon Success nor Logon Failure auditing are enabled. Enable auditing and turn on auditing for specific events such as logon and logoff. Be sure to monitor your event log to watch for unauthorized access.
	Shares	4 share(s) are present on your computer.

Share	Directory	Share ACL	Directory ACL
ADMIN$	C:\WINDOWS	Admin Share	NT SERVICE\TrustedInstaller - F, NT AUTHORITY\SYSTEM - RWXD, BUILTIN\Administrators - RWXD, BUILTIN\Users - RX, AUTORITA PRO BALÍČKY APLIKACÍ\VŠECHNY BALÍČKY APLIKACÍ - RX
C	C:\	Everyone - R	BUILTIN\Administrators - F, NT AUTHORITY\SYSTEM - F, BUILTIN\Users - RX, Everyone - RX
C$	C:\	Admin Share	BUILTIN\Administrators - F, NT AUTHORITY\SYSTEM - F, BUILTIN\Users - RX, Everyone - RX
Users	C:\Users	Administrators - F, Everyone - F	NT AUTHORITY\SYSTEM - F, BUILTIN\Administrators - F, BUILTIN\Users - RX, Everyone - RX

	Services	No potentially unnecessary services were found.

Internet Information Services (IIS) Scan Results

Score	Issue	Result
	IIS Status	IIS is not running on this computer.

SQL Server Scan Results

Score	Issue	Result
	SQL Server/MSDE Status	SQL Server and/or MSDE is not installed on this computer.

Desktop Application Scan Results

Administrative Vulnerabilities

Score	Issue	Result
	IE Zones	Internet Explorer zones have secure settings for all users.
	Macro Security	No supported Microsoft Office products are installed.

10.6 Cloudová řešení pro zálohu a rchivaci dat

Obrázek 14 - Cloudová úložiště

1.	justcloud.com www.justcloud.com	editor: user: 5 votes	**Unlimited GB** $ 4.49 per month $ 53.88 per year all plans	sync	sharing	free storage	14 days trial	1 machines	system
2.	BACKBLAZE www.backblaze.com video review	editor: user: 5 votes	**Unlimited GB** $ 5.00 per month $ 50.00 per year all plans	sync	sharing	free storage	15 days trial	1 machines	system
3.	zoolz www.zoolz.com video review	editor: user: 8 votes	**Unlimited GB** $ 14.17 per month* $ 169.99 per year all plans	sync	sharing	free storage	14 days trial	1 machines	system
4.	CRASHPLAN www.crashplan.com video review	editor: user: 3 votes	**Unlimited GB** $ 5.99 per month $ 59.99 per year all plans	sync	sharing	free storage	30 days trial	1 machines	system
5.	CARBONITE www.carbonite.com	editor: user: 13 votes	**Unlimited GB** $ 4.92 per month $ 59.99 per year all plans	sync	sharing	free storage	15 days trial	1 machines	system
8.	SOS Online Backup www.sosonlinebackup.com	editor: user: 11 votes	**Unlimited GB** $ 5.00 per month* $ 59.99 per year all plans	sync	sharing	free storage	14 days trial	1 machines	system

Zdroj: *Best cloud storage* [online]. 2015 [cit. 2015-03-10]. Dostupné z: http://www.bestcloudstorage.net/

10.7 Zařízení NAS

Obrázek 15 - Zařízení NAS Qnap TS 470 PRO

Zdroj: *Reichelt.de* [online]. 2015 [cit. 2015-03-10]. Dostupné z: ZDROJ:http://www.reichelt.de/QNAP-TS-470PRO/3/index.html?ACTION=3&GROUPID=5788&ARTICLE=140035&OFFSET=16&

Tabulka 17 - Parametry QNAP TS 470 Pro

CPU	**Intel® Core™ i3-3220 3.3 GHz Dual-core Processor**
DRAM	TS-470 Pro-16G: 16GB SO-DIMM RAM TS-470 Pro: 2GB SO-DIMM RAM
Flash Memory	512MB DOM
Hard Disk Drive	4 x 3.5” or 2.5” SATA 6Gb/s, SATA 3Gb/s hard drive or SSD **NOTE:** 1. The system is shipped without HDD. 2.For the HDD compatibility list, please visit www.qnap.com/compatibility
LAN Port	2 x Gigabit RJ-45 Ethernet ports (expandable to 4 x GbE ports or 2 x GbE + 2 x 10GbE ports)
LED Indicators	Status, USB, LAN, HDD 1 - 4
USB	2 x USB 3.0 port (rear) 3 x USB 2.0 port (front: 1, rear:2) Support USB printer, pen drive, USB hub (front), and USB UPS etc.
Hard Disk Tray	4 x Hot-swappable tray with key lock
eSATA	2 x eSATA port (rear)
HDMI	HDMI x 1
Audio Out	1(reserved)

Audio In	1(reserved)
Buttons	Power, Reset, USB One Touch Backup
Alarm Buzzer	System warning
LCD Panel	Monochrome LCD display with backlight, Enter and Select buttons for configuration
Form Factor	Tower
Secure Design	K-lock security slot for theft prevention
Fan	1 x quiet cooling fan (9 cm, 12V DC)
PCI-E Slot	1 (for optional network or storage capacity expansion)
Dimensions	177 (H) x 180 (W) x 235 (D) mm 6.97 (H) x7.09 (W) x 9.25 (D) inch
Weight	Net weight: 4.56 kg (10.05 lbs) Gross weight: 5.7 kg (12.57 lbs)
Power Consumption (W)	Sleep mode: 22.8W In Operation: 38.2W Power-off (in WOL mode): 1W (with 4 x 2TB HDD installed)
Temperature	0-40˚C
Humidity	5~95% RH non-condensing, wet bulb: 27˚C
Power Supply	Input: 100-240V AC, 50/60Hz Output: 250W

ZDROJ: *Qnap.com* [online]. 2015 [cit. 2015-03-10]. Dostupné z: https://www.qnap.com/i/in/product/model.php?II=106&event=2

Tabulka 18 - Zařízení NAS Synology DS1815

Zdroj: *Synology.com* [online]. 2015 [cit. 2015-03-10]. Dostupné z: https://www.synology.com/en-us/products/DS1815+#photo

Tabulka 19 - Parametry Synology DS 1815

Procesor model CPU	**Intel Atom C2538**
Frekvence CPU	Čtyři jádra 2.4 GHz
Plovoucí desetinná čárka	**ANO**
Systém hardwarového šifrování (AES-NI)	**ANO**
Paměť	
Systémová paměť	2 GB DDR3
Předinstalovaný paměťový modul	2 GB X 1
Celkový počet paměťových slotů	2
Paměť rozšiřitelná až na	6 GB (2 GB + 4 GB)
Úložiště	
Šachta(y) pevného disku	8
Maximální počet šachet pevného disku s rozšiřující jednotkou	18
Kompatibilní typ disku	• 3.5" SATA(III) / SATA(II) HDD • 2.5" SATA(III) / SATA(II) HDD • 2.5" SATA(III) / SATA(II) SSD
Maximální interní hrubá kapacita	48 TB (6 TB HDD X 8) (Kapacita se může lišit podle typu RAID)
Disky vyměnitelné za provozu	**ANO**

Externí porty	
Port USB 3.0	4
Port eSATA	2
Systém souborů	
Interní zařízení	EXT4
Externí zařízení	• EXT4 • EXT3 • FAT • NTFS • HFS+
Vzhled	
Velikost (výška x šířka x hloubka)	157 mm X 340 mm X 233 mm
Hmotnost	5.29 kg
Ostatní	
RJ-45 1GbE LAN port	4 (s podporou funkcí Link Aggregation / Failover)
Probuzení přes LAN/WAN	**ANO**
Ventilátor systému	120 mm X 120 mm X 2 pcs
Snadno vyměnitelný systémový ventilátor	**ANO**
Podpora bezdrátového zařízení (hardwarový klíč)	**ANO**
Hladina hluku*	24.3 dB(A)
Zotavení po ztrátě napájení	**ANO**
Plánované zapnutí/vypnutí	**ANO**
Jednotka/adaptér zdroje energie	250W
Vstupní střídavé napětí	100V na 240V AC
Frekvence napájení	50/60 HZ, Jednofázový
Spotřeba energie*	45.88W (za chodu) 25.23W (hibernace pevného disku)
prostředí Teplota	
Provozní teplota	5°C na 35°C (40°F na 95°F)

Teplota pro skladování	**-20°C na 60°C (-5°F na 140°F)**
Relativní vlhkost	5% to 95% RV
Certifikace	• FCC Class B • CE Class B • BSMI Class B
Záruka	3 let
Poznámky	• Spotřeba energie se měří při plném zatížení s jedním nebo více disky Western Digital 1 TB WD10EFRX. • Testovací prostředí pro měření hladiny hluku: Při plném zatížení s pevnými disky Seagate 1 TB ST31000520AS v klidovém režimu; dva mikrofony G.R.A.S. typu 40AE, každý umístěný 1 metr od přední a zadní části Synology NAS serveru; hluk na pozadí: 16,49-17,51 dB(A); teplota: 24,25-25,75 ˚C; vlhkost: 58.2-61.8%

Zdroj: *Synology.com* [online]. 2015 [cit. 2015-03-10]. Dostupné z: https://www.synology.com/cs-cz/products/DS1815+#spec

Obrázek 16 - Zařízení NAS Synology RS 814

ZDROJ: *Synology.com* [online]. 2015 [cit. 2015-03-10]. Dostupné z: https://www.synology.com/img/products /photo/RS814+/001.jpg

Tabulka 20 - Parametry NAS Synology RS 814

Procesor	
model CPU	INTEL Atom D2700
Frekvence CPU	Dvě jádra 2.13 GHz
Plovoucí desetinná čárka	ANO
Paměť	
Systémová paměť	2 GB DDR3
Předinstalovaný paměťový modul	2 GB X 1
Celkový počet paměťových slotů	2
Paměť rozšiřitelná až na	4 GB (2 GB X 2)
Úložiště	
Šachta(y) pevného disku	4
Maximální počet šachet pevného disku s rozšiřující jednotkou	8

Kompatibilní typ disku	• 3.5" SATA(III) / SATA(II) HDD • 2.5" SATA(III) / SATA(II) HDD • 2.5" SATA(III) / SATA(II) SSD
Maximální interní hrubá kapacita	24 TB (6 TB HDD X 4) (Kapacita se může lišit podle typu RAID)
Disky vyměnitelné za provozu	ANO
Externí porty	
Port USB 3.0	2
Port eSATA	1
Systém souborů	
Interní zařízení	EXT4
Externí zařízení	• EXT4 • EXT3 • FAT • NTFS • HFS+
Vzhled	
Velikost (výška x šířka x hloubka)	44 mm X 430.5 mm X 457.5 mm 44 mm X 430.5 mm X 591.8 mm (pro model RP)
Hmotnost	7.11 kg 9.43 kg (pro model RP)
Ostatní	
RJ-45 1GbE LAN port	4 (s podporou funkcí Link Aggregation / Failover)
Probuzení přes LAN/WAN	ANO
Ventilátor systému	40 mm X 40 mm X 3 pcs
Podpora bezdrátového zařízení (hardwarový klíč)	ANO
Hladina hluku*	25.1 dB(A) 52.6 dB(A) (pro model RP)
Zotavení po ztrátě napájení	ANO
Plánované zapnutí/vypnutí	ANO
Jednotka/adaptér zdroje	200W

energie	2 X 250W (pro model RP)
Vstupní střídavé napětí	100V na 240V AC
Frekvence napájení	50/60 HZ, Jednofázový
Spotřeba energie*	37.29W (za chodu) 22.82W (hibernace pevného disku) 45.55W (za chodu, pro model RP) 33.26W (hibernace pevného disku, pro model RP)
Náhradní zdroj energie (pro modely xs+ a RP)	ANO
prostředí Teplota	
Provozní teplota	5°C na 35°C (40°F na 95°F)
Teplota pro skladování	-10°C na 70°C (15°F na 155°F)
Relativní vlhkost	5% to 95% RV
Certifikace	• FCC Class A • CE Class A • BSMI Class A
Záruka	3 let
Poznámky	• Spotřeba energie se měří při plném zatížení s jedním nebo více disky Western Digital 1 TB WD10EFRX. • Testovací prostředí pro měření hladiny hluku: Při plném zatížení s pevnými disky Seagate 1 TB ST31000520AS v klidovém režimu; dva mikrofony G.R.A.S. typu 40AE, každý umístěný 1 metr od přední a zadní části Synology NAS serveru; hluk na pozadí: 16,49-17,51 dB(A); teplota: 24,25-25,75 ˚C; vlhkost: 58.2-61.8%

ZDROJ: *Synology.com* [online]. 2015 [cit. 2015-03-10]. Dostupné z: https://www.synology.com/cs-cz/products/RS814+#spec