ANALÝZA INTERNÍ BEZPEČNOSTI

Anonymizovaná Firma, spol. s r.o.

Tento dokument představuje anonymizované výsledky bezpečnostního auditu pomocí řešení Safetica. Analýza byla provedena na 46 stanicích v období od 1. 5. 2016 do 31. 5. 2016. Výsledky se týkají pouze běžné pracovní doby (od 07:00 do 16:00 hodin). K dispozici jsou také kompletní data ve formě XLS dokumentu pro další zpracování.

safetica®

OBSAH

PRÁCE S DATY

E-maily

⚠ Zaměstnanec L.. Bartoš odeslal soubor *projekt.dwg* na e-mail konkurence *m.vrba@konkurencnifirma.cz*.

V této části jsme se zaměřili na analýzu souborů odesílaných přes e-mailové klienty. Na přání zákazníka jsme se zaměřili především na ochranu know-how společnosti, tedy na soubory CAD softwaru.

Celkem 31 e-mailů, které obsahovaly CADové soubory, bylo za toto období odesláno mimo domény *firemnidomena.cz*. Záznamy o e-mailech jsme prošli a zjistili, že v téměř všech případech se jednalo o odesílání na e-maily klientů. Nalezli jsme však **jeden případ, kdy došlo k odeslání souboru projekt.dwg na e-mail konkurence m.vrba@konkurencnifirma.cz**, a to zaměstnancem L. Bartošem dne 18. 5. 2016.

Odesílatel	Předmět	Příjemce	Datum a čas
T. Moravec	Model CX290 – Detaily	s.maly@zakaznickafirmaA.cz	3. květen 2016 11:14
R. Bureš	Kategorie C jednotlivě	jan.hrebik@zakaznickafirmaB.cz	5. květen 2016 15:35
V. Havran	BS1200	nakup@zakaznickafirmaC.cz	6. květen 2016 10:07

Odeslané soubory CAD skrze e-mail – výběr

Mezi adresáty jsme našli také domény veřejných e-mailových služeb, jako jsou *seznam.cz*, *gmail.com* nebo *outlook.com*. Doporučujeme k posouzení, zda je přípustné odesílat soubory na tyto domény (např. zákazníkům). Tyto e-mailové schránky mohou sloužit jako anonymní kanál pro únik dat ke konkurenci. Safetica umožňuje omezit odesílání e-mailů pouze na určité domény, samozřejmě s možností různého nastavení v závislosti na typu přílohy.

Je nutno poznamenat, **že všechny e-maily obsahovaly tato data nezašifrovaná, co představuje bezpečnostní riziko ohrožení důvěrnosti dat.**

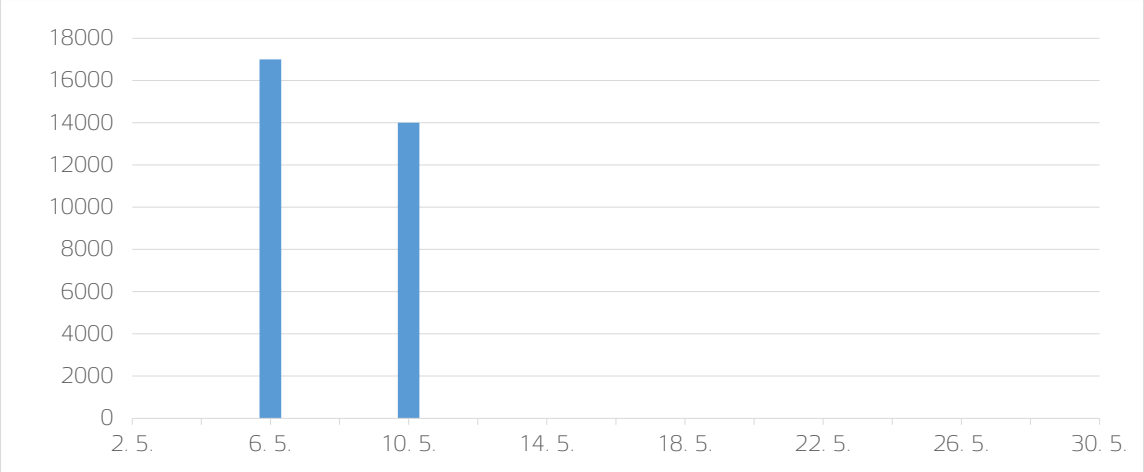
ⓘ **Doporučené nastavení v Safetica:**

- zakázat odesílání CAD souborů na e-maily konkurenčních firem
- monitorovat CAD soubory posílané na veřejné e-mailové adresy
- šifrovat CAD přílohy, aby si je neotevřel neautorizovaný příjemce

Nahrávání souborů na USB a ostatní externí zařízení

Uživatel T. Moravec a A. Holub jednorázově nahráli **32 588 citlivých dokumentů** o celkové velikosti 19,12 GB na USB disk.

Jako další potenciální kanál pro únik dat jsou USB disky a obecně externí zařízení. V analýze jsme se zaměřili na nahrávání CAD souborů na tato média a objevili jsme **dva významné výkyvy.**



Časová osa nahrávání souborů na externí média

Na svědomí je měli zaměstnanci T. Moravec a A. Holub, kteří jednorázově nahráli soubory na externí zařízení. **Nahraných bylo 32 588 dokumentů o celkové velikosti 19,12 GB. Jednalo se o dokumenty různých typů, včetně CAD souborů.** Konkrétně zaměstnanec T. Moravec překopíroval 70 DWG souborů a zaměstnanec A. Holub 23 DWG souborů. Doporučujeme prověřit tuto událost a poté nastavit bezpečnostní politiku – např. zakázat nahrávání citlivých firemních souborů na externí média.

Doporučené nastavení v Safetica:

- zakázat nahrávání CAD souborů na externí média, která nejsou v majetku firmy
- okamžité upozornění na významné množství kopírovaných souborů

Využívání internetových souborových úložišť

Všechny aktivity na internetových úložištích a filehostingových serverech byly v rámci bezpečnostních pravidel v pořádku.

Další cestou pro únik dat mohou být cloudová uložiště a obecně file hostingové servery. Jedinou navštěvovanou webovou stránkou z této kategorie byla www.dropbox.com.

Jméno souboru	Datum a čas	Cloud
Grafika.zip	20. květen 2016 15:38	Dropbox
13_0425_AnonymizovanáFirma_katalog_agregatu_rustin.PDF	22. květen 2016 15:22	Dropbox
Panel.PDF	22. květen 2016 15:48	Dropbox
1-4(950x2340).PDF	22. květen 2016 15:57	Dropbox
13_0425_AnonymizovanáFirma_katalog_produktu_RU_data(EU).PDF	26. květen 2016 9:27	Dropbox
13_0425_AnonymizovanáFirma_katalog_agregatu_rustin(EU).PDF	26. květen 2016 9:27	Dropbox
13_0425_AnonymizovanáFirma_katalog_produktu_RU_data(EU).PDF	26. květen 2016 12:31	Dropbox
13_0425_AnonymizovanáFirma_katalog_agregatu_rustin(EU).PDF	26. květen 2016 12:31	Dropbox
1-9(950x2340).PDF	29. květen 2016 9:29	Dropbox

Prověřili jsme jednotlivé záznamy a zjistili, že tato uložiště byla využívána pouze pro účely nahrávání pracovního obsahu, a to jediným zaměstnancem – A. Polákem.

Doporučené nastavení v Safetica:

- zakázat nahrávání citlivých dokumentů mimo (povolená) cloudová úložiště

PRODUKTIVITA

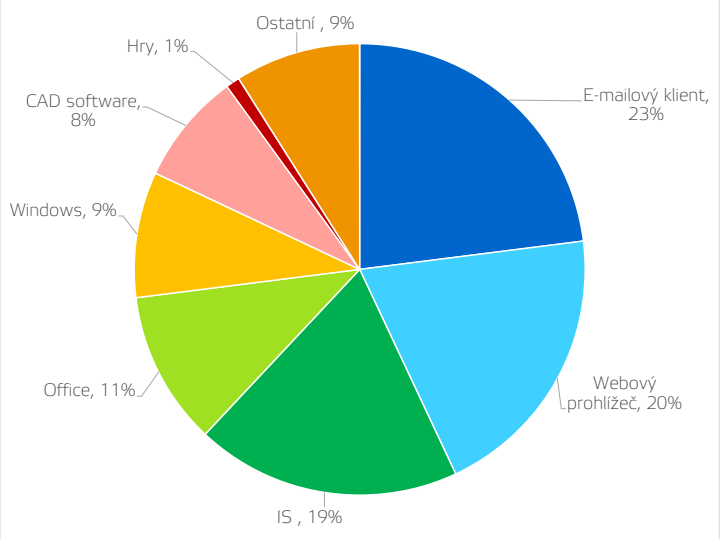
Využití aplikací

⚠ Zaměstnanci tráví čas v práci hraním her, zejména pak V. Havran (23 hodin) a T. Pokorný (12 hodin).

V analyzovaném období převažovala práce v produktivních aplikacích. Nejpoužívanější aplikace patří do kategorie E-mailový klient, další často používané aplikace spadají do produktivních kategorií IS a Office. Druhou nejpoužívanější kategorií aplikací je kategorie Webový prohlížeč, zaměstnanci tráví celkem **20 % své pracovní doby ve webovém prohlížeči.** (Více informací naleznete v kapitole Navštěvované weby.)

Název aplikace	Doba běhu
Microsoft Office Outlook (outlook.exe)	1127:22:12
Informační systém K2 (k2.exe)	931:04:13
Chrome (chrome.exe)	531:13:59
Firefox (firefox.exe)	449:10:44
Průzkumník Windows (explorer.exe)	440:34:12
Microsoft Word (word.exe)	300:04:20
SolidWorks 2014 (sldworks.exe)	287:41:54
Microsoft Excel (excel.exe)	239:21:07
AutoCAD LT Application (acadlt.exe)	107:07:45
Solitaire (solitaire.exe)	24:02:44
Heroes of M. and M. III (heroes3.exe)	11:56:43
Miny (Minesweeper.exe)	09:52:57
Adobe InDesign CS3 (indesign.exe)	02:01:36

Čas strávený ve vybraných aplikacích



Čas strávený v aplikačních kategoriích

Zcela neproduktivní je kategorie Hry. Zaměstnanec V. Havran strávil přibližně **23 hodin hraním her** Solitaire, Pinball a Hledání min. Zaměstnanec T. Pokorný strávil **12 hodin hraním hry** Heroes of Might and Magic III. Zaměstnanec J. Navrátil strávil 6 hodin hraním hry Solitaire, zaměstnanci R. Bureš a L. Bláha pak po 3 hodiny s tou samou hrou.

Doporučené nastavení v Safetica:

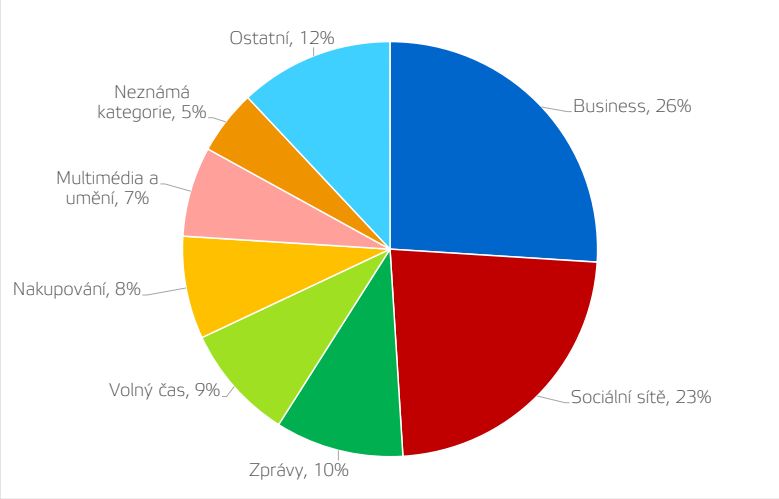
- blokování her v pracovní době nad rámec např. 30 minut denně
- měsíční souhrny používaných aplikací využít k úspoře za nepotřebné drahé licence

Navštěvované weby

74 % času na internetu je tráveno neproduktivní činností, nejvíc na neproduktivní weby přistupují zaměstnanci J. Novák a J. Navrátil.

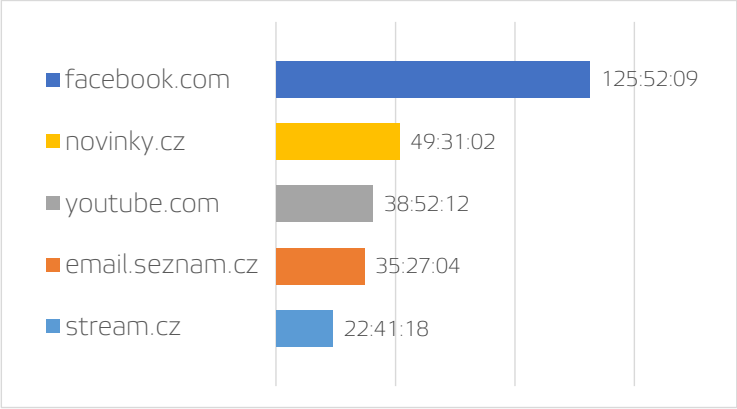
Nejvíce času zaměstnanci tráví na serverech typu Sociální sítě, Zprávy a Volný čas. Mezi neproduktivní patří také kategorie Nakupování a Multimédia a umění.

Dále bychom chtěli upozornit na návštěvnost webů s **pornografií a hrami,** které spadají do kategorie Ostatní. Kromě toho, že jde o neproduktivně strávený čas v rozporu s interními směrnicemi, jde také o vysoké riziko infekce počítače škodlivým software. Nejaktivnějšími v této kategorii byli zaměstnanci J. Novák a P. Novotný.

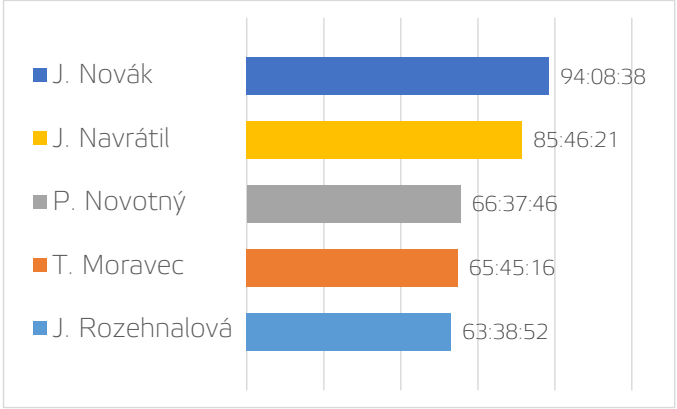


Čas strávený ve webových kategoriích

Celkově z analýzy navštěvovaných webů vyplývá, že zaměstnanci tráví z celkového času na Internetu až 74 % neproduktivní činností. Nejvíce času je tráveno na serveru www.facebook.com.



Nejnavštěvovanější neproduktivní weby (hod)



Zaměstnanci nejvíce přistupující na neproduktivní weby (hod)

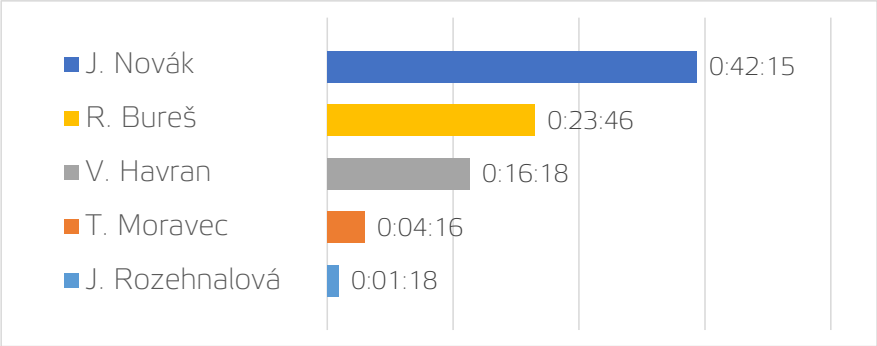
Doporučené nastavení v Safetica:

- blokování vybraných serverů nesouvisejících s pracovní činností (v pracovní době)

Vyhledávání práce

⚠ Zaměstnanec J. Novák vyhledával vzor pro výpověď z pracovního poměru.

Z naší zkušenosti vyplývá, že zaměstnanci, kteří aktivně tráví čas na webech kategorie pro vyhledávání práce, obvykle neodvádí odpovídající pracovní výsledky a ze společnosti do několika měsíců odcházejí. Představují také zvýšené riziko úniku dat.



Nejaktivnější zaměstnanci v kategorii Vyhledávání práce (hod)

Zaměstnanec J. Novák vyhledával vzor pro výpověď z pracovního poměru. Zaměstnanci R. Bureš, V. Havran a T. Moravec aktivně vyhledávali pracovní nabídky. Zaměstnankyně J. Rozehnalová se na web kategorie dostala otevřením zaslaného odkazu, šlo o krátký jednorázový přístup, který lze označit za nevýznamný.

Doporučujeme se zamyslet nad řešením této situace. Mezi dobré postupy patří diskuze ohledně spokojenosti s prací a kolektivem, změna pracovní náplně nebo pracovních podmínek.

Doporučené nastavení v Safetica:

- varování, které na vyhledávání práce upozorní
- je možné zakázat přístup na tyto servery, ale tím se problém neodstraní

Celkový neproduktivní čas a jeho náklady

V Aplikacích jsme zjistili, že 20 % pracovní doby je tráveno ve webových prohlížečích. Celkový čas strávený jejich používáním je pak ze 74 % tráven neproduktivně. Aplikace byly využívány neproduktivně v 1 % případů. Z toho vyplývá, že zhruba 15 % veškeré činnosti je neproduktivní. To odpovídá průměru **45 minut neproduktivní činnosti za pracovní den na 1 zaměstnance.** Pohledem do Safetica je pak možné odhalit nejméně produktivní zaměstnance. Doporučujeme tento čas částečně omezit např. interní směrnicí a poté vynutit její dodržování naším produktem.

Jednoduchým výpočtem zjistíme, kolik společnost platí ve formě mzdy za tuto neproduktivní činnost. V úvahu bereme náklady na průměrnou superhrubou mzdu 31 817 Kč za měsíc a 100 zaměstnanců. Na mzdách tedy společnost vyplatí 38,2 mil. Kč/rok. 15 % neproduktivního času tak znamená **5,8 mil. Kč/rok vynaložených na činnosti nesouvisející s výkonem práce**.

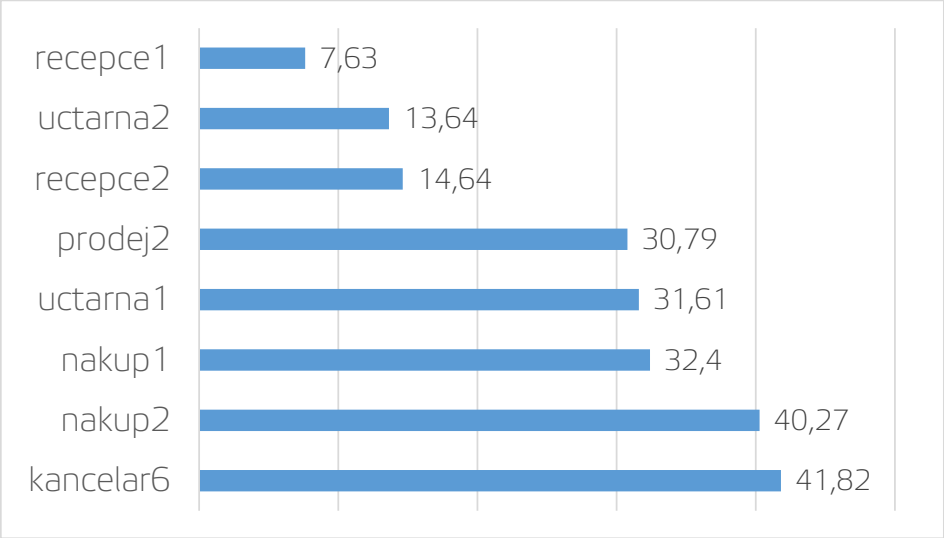
Je nutno poznamenat, že 55 % celkové neproduktivní činnosti všech monitorovaných zaměstnanců pochází od výše zmíněných zaměstnanců J. Nováka, J. Navrátila, P. Novotného, V. Havrana a T. Pokorného. Těchto 5 zaměstnanců tedy představuje největší prostor k optimalizaci produktivity práce.

VYUŽITÍ IT PROSTŘEDKŮ

Využití pracovních stanic

⚠ Počítač *Recepce1* byl využit pouze v 7,63 % z celkové doby běhu.

V této části se zaměřujeme na využití IT prostředků. Jako příklad prezentujeme souhrnnou tabulku nejméně využitých stanic:



Využití pracovních stanic (%) – stanice s nejnižší aktivitou

Za zmínku stojí počítač *Recepce1*, kde je celková aktivní činnost v tomto měsíci 7,63 %. Na této stanici nebyla provedena téměř žádná aktivní činnost a běžela téměř 226 hodin nevyužita. I u dalších zobrazených počítačů je míra využití poměrně nízká. Průměrně jsou počítače používány na 56,14 %. Vidíme zde tedy prostor ke zlepšení: zavedení politiky na vypínání počítačů po pracovní době kvůli šetření firemních nákladů. Míra aktivního využití by měla být alespoň 75 %.

Doporučené opatření:

- zavedení pravidel na vypínání počítačů po pracovní době kvůli šetření firemních nákladů

Tisk

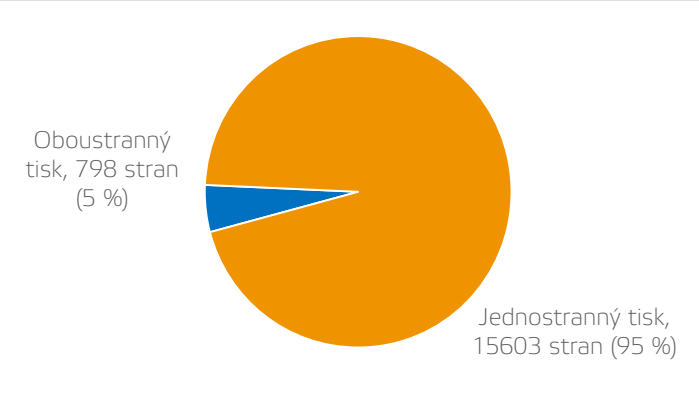
Nepracovní tisk se pohybuje pouze v řádu desítek stran. Poměr černobílého a barevného tisku je přiměřený.

Následující graf zobrazuje počet vytištěných stran za monitorované období. V grafu vidíme, že v průběhu měsíce je tisk na obdobné velikosti a podrobné záznamy nenasvědčují o zneužívání tisku pro soukromé účely ve velké míře. Za den bylo nejvíce tisknuto 1090 stran a nejméně 510 stran.

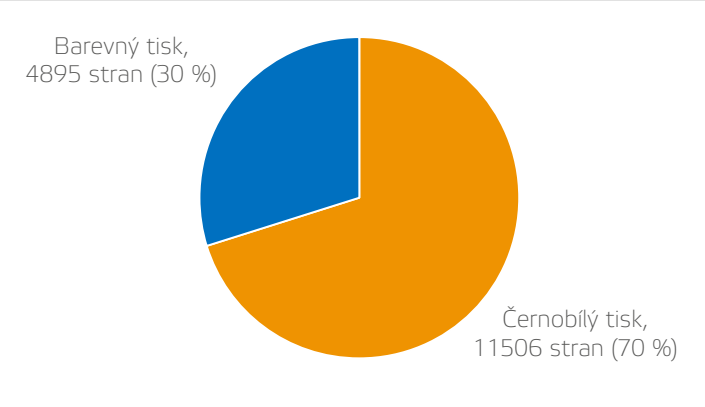
Nepracovní tisk se pohybuje v řádu desítek stran:

- P. Novotný – soubory z web mailu (49 černobílých stran)
- R. Bureš – panasonic-manual.pdf (34 černobílých stran)
- A. Bláha – Mikrobiologie1a.pdf (20 černobílých stran)

Necháváme na uvážení společnosti, zda umožní zaměstnancům tisk soukromých dokumentů nebo zavede nějakou politiku. Se Safetica dokážete blokovat tisk globálně nebo jen u vybraných souborů, případně nastavit kvótu, kolik stran mohou zaměstnanci tisknout.



Poměr oboustranného a jednostranného tisku



Poměr černobílého a barevného tisku

U všech uvedených zaměstnanců jde zejména o pracovní dokumenty, nicméně jak můžeme vidět, je zde prostor k optimalizaci nákladů v případě jak barevného tisku, tak jednostranného tisku.

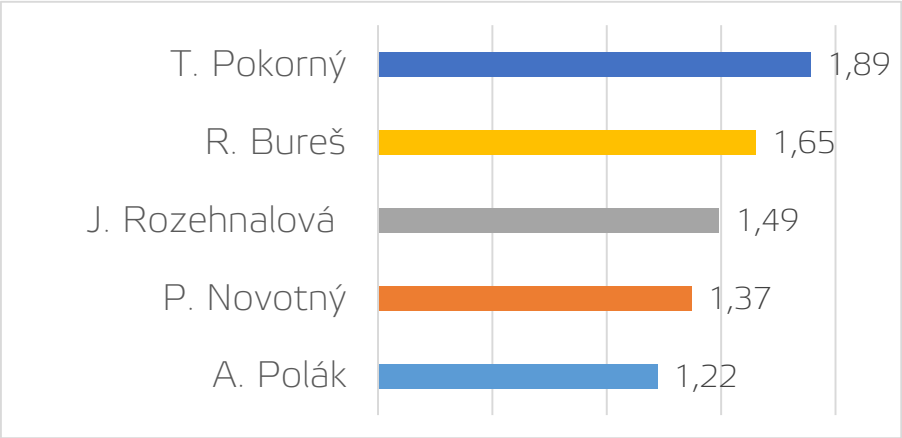
Doporučené nastavení v Safetica:

- Safetica dokáže blokovat tisk globálně, u vybraných souborů, případně nastavit kvótu, kolik stran mohou zaměstnanci tisknout
- necháváme na uvážení společnosti, zda umožní zaměstnancům tisk soukromých dokumentů nebo zavede nějakou politiku

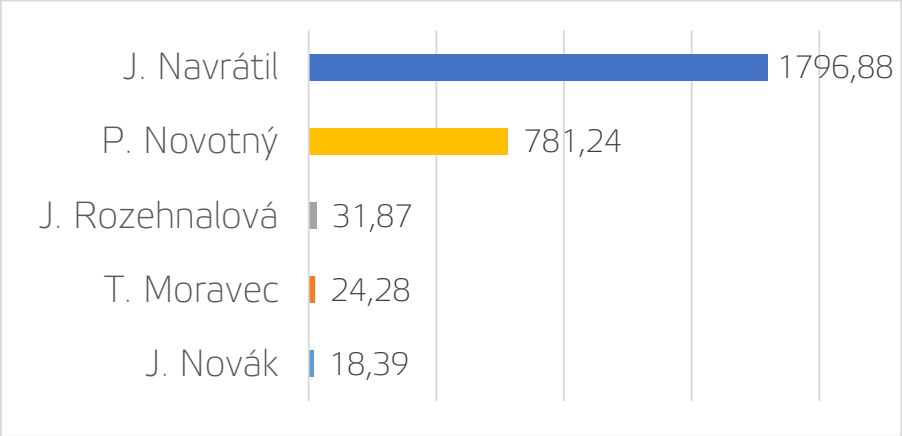
Stahování či nahrávání velkého objemu dat

Zaměstnanec J. Navrátil využíval bittorrent klienta pro stahování nelegálního materiálu o velikosti 1,8 TB.

Důležité z hlediska optimálního využití IT prostředků je využití síťového připojení. Zaměřili jsme se na extrémy, které se v této oblasti nacházejí.



Odeslaná data podle zaměstnanců (GB)



Přijatá data podle zaměstnanců (GB)

Doporučené nastavení v Safetica:

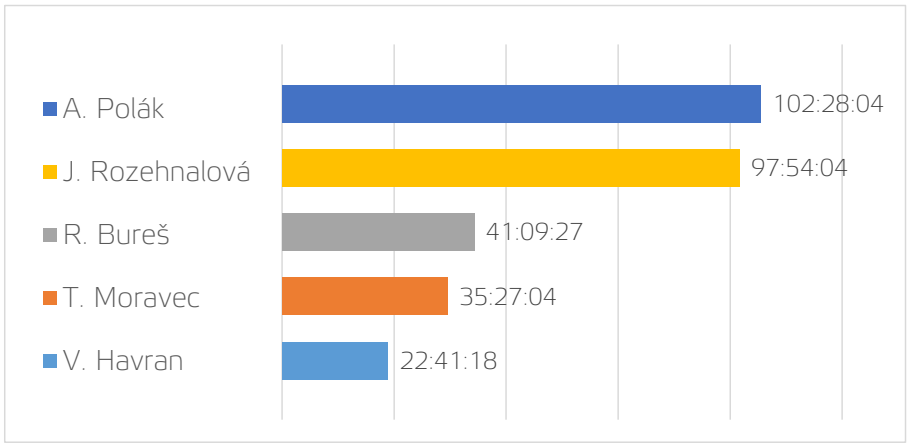
- blokování torrent aplikací pro stahování
- okamžité upozornění na významné množství stahovaných souborů

Nákladné licence

Aplikace SolidWorks 2014 byla aktivně využívána téměř 288 hodin.

AutoCAD programy jsou aktivně využívané. Na druhou stranu **program Adobe InDesign CS3 byl využíván pouze po dobu 2 hodin.**

V této části jsme se dále zaměřili na využití aplikací, na které společnost vynakládá poměrně vysoké částky a je v zájmu společnosti, aby tyto aplikace byly využívány co nejefektivněji. Speciálně jsme se zaměřili na využití nákladné aplikace Solid Works 2014. S touto aplikací v dobu monitorování pracovalo celkem 5 zaměstnanců. Aktivně byla využita 287 h 41 m a 54 s.



Využití SolidWorks 2014 (hod)

Doporučené nastavení v Safetica:

- reporty o využití aplikací, na které jsou použité drahé licence