Monitorování zaměstnanců v pracovním procesu

Monitoring Employees in the Work Process

Bc. David Kopecký

Diplomová práce
2012

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2011/2012

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. David KOPECKÝ**
Osobní číslo:	**A10426**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Monitorování zaměstnanců v pracovním procesu**

Zásady pro vypracování:

1. **Zhodnoťte možné formy monitorování pomocí dohledových a kontrolních systémů na pracovištích.**
2. **Popište význam monitorování pro vyhodnocení kvality práce.**
3. **Analyzujte systémy sloužící také jako prvek ochrany zaměstnanců a pracoviště.**
4. **Posuďte monitoring z právního a etického hlediska.**
5. **Navrhněte přiměřenou míru kontroly na pracovištích.**

Rozsah diplomové práce:

Rozsah příloh:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **LUKÁŠ, Luděk et al. Bezpečnostní technologie, systémy a management I. Zlín: Radim Bačuvčík – VeRBuM, 2011. ISBN 978-80-87500-05-7.**
2. **KINDL, Jiří. Projektování bezpečnostních systémů I. 2. vydání. Zlín: UTB, 2007. ISBN 978-80-7318-554-1.**
3. **KŘEČEK, Stanislav. Příručka zabezpečovací techniky. 3. vydání. Blatná: Cricetus – Ing. Stanislav Křeček, 2006. ISBN 80-902938-2-4.**
4. **LOVEČEK, T. a NAGY, P. Bezpečnostné systémy – Kamerové bezpečnostné systémy. Žilina: EDIS vydavatelstvo, 2008. ISBN 978-80-8070-893-1.**
5. **ČESKO. Zákon č. 2/1993 ze dne 16. prosince 1992 Usnesení předsednictva České národní rady o vyhlášení LISTINY ZÁKLADNÍCH PRÁV A SVOBOD jako součásti ústavního pořádku České republiky. In: Sbírka zákonů České republiky. 1992, částka 1, s. 17-24. Dostupný také z: http://aplikace.mvcr.cz/archiv2008/sbirka/1993/sb01-93.pdf.**
6. **ČESKO. Zákon č. 262/2006 ze dne 21. dubna 2006 Zákoník práce. In: Sbírka zákonů České republiky. 2006, částka 84, s. 3146-3241. Dostupný také z: http://aplikace.mvcr.cz/archiv2008/sbirka/1993/sb01-93.pdf.**
7. **ŠTEFKA, Vladislav. Právní řád I. 2. vydání. Zlín: UTB, 2009. ISBN 978-80-7318-805-4.**
8. **MiCoS SOFTWARE. Sledování zaměstnanců a monitoring pc [online]. 2009-2011 [cit. 2012-01-26]. Dostupné z: http://www.monitorovat-pc.cz/.**

Vedoucí diplomové práce: **JUDr. Vladislav Štefka**
Ústav bezpečnostního inženýrství

Datum zadání diplomové práce: **24. února 2012**

Termín odevzdání diplomové práce: **15. května 2012**

Ve Zlíně dne 24. února 2012

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Diplomová práce na téma Monitorování zaměstnanců v pracovním procesu se zabývá dohledovými a kontrolními systémy používanými aktuálně na pracovištích. Výstupem těchto systémů jsou data, jejichž kontrolou je zaměstnavatel schopen vyhodnotit kvalitu vykonávané práce a součinnost se zákoníkem práce či pracovním řádem. Některé z těchto systému zabezpečují současně ochranu zaměstnanců a pracoviště. V práci jsou podrobně popsány jednotlivé formy kontroly a monitorování, použité prvky systémů a programové vybavení zabezpečující jejich správnou funkci. Práce se zabývá jak posouzením monitoringu z právního hlediska tak z hlediska etického. Cílem práce je navržení přiměřené míry kontroly na pracovišti.

Klíčová slova:

monitorování, kontrola, zaměstnanec, zaměstnavatel, dohledové systémy, pracovní proces, etika, pracoviště, pracovní právo

ABSTRACT

The thesis, Monitoring of Employees at Work Process, is engaged in supervisory and control systems currently used in workplaces. The outputs of these systems are data which the employer is able to evaluate the quality of work, interaction with the law and work rules. Some of these systems also provide protection for workers and workplaces. The thesis describes in detail the various forms of control and monitoring systems. It also describes the components used at the software which ensure their functions properly. The work deals with assessment monitoring from the view of ethics and law. The focus is to propose an adequate degree of monitoring in the workplace.

Keywords:

monitoring, supervision, employee, employer, surveillance systems, work process, ethic, workplace, labour law

Na tomto místě bych chtěl poděkovat především JUDr. Vladislavu Štefkovi, za vedení a konzultace při tvorbě práce. Dále pak panu Pavlu Pernickému za inspiraci, spolupráci a podporu při tvorbě praktických částí práce. Manželce a celé rodině za neustálou podporu a motivaci po celou dobu studia.

„Každý zvuk, který Winston vydal a jenž byl hlasitější než velmi tiché šeptání, obrazovka zachycovala; a co víc, pokud zůstával v zorném poli kovové desky, bylo ho vidět a slyšet. Samozřejmě, člověk si nikdy nebyl jist, zda ho v daném okamžiku sledují. Jak často a podle jakého systému Ideopolicie zapínala jednotlivá zařízení, bylo hádankou. Předpokládalo se, že sledují každého neustále. A rozhodně mohli zapnout vaše zařízení, kdy se jim chtělo. Člověk musel žít – a žil, ze zvyku, který se stal pudovým, v předpokladu, že každý zvuk, který vydá, je zaslechnut, a každý pohyb, pokud není tma, zaznamenán".

George Orwell „1984"

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl jsem seznámen s tím, že na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně …….

podpis diplomanta

OBSAH

ÚVOD

V dnešní době vzrůstá potřeba managementu firem získávat statistické informace o produktivitě práce zaměstnanců. Tato doba, označovaná také jako informační, si žádá použití rozličných prostředků nezbytných k vykonávání pracovní činnosti, patří mezi ně např. telefon, osobní počítač, email, internet, firemní vozidlo a v neposlední řadě data, jinými slovy informace. Bez informací nelze žít a už vůbec ne pracovat. Problematika monitorování pracoviště a zaměstnanců je dnes stále častěji probíraným tématem, a to nejen z důvodu ochrany soukromí či projevů osobní povahy. Často diskutovaným tématem je také ochrana korespondence a osobních údajů, a to jak z hlediska právního, tak etického. Ne každý zaměstnanec je ochoten přijmout fakt, že jej Orwelovský „Velký bratr" sleduje, jak se říká na každém kroku. Zaměstnanci se brání a zaměstnavatelé se snaží nacházet legální způsoby, jak co nejvíce využít tyto nástroje ke svému prospěchu. K těmto účelům zaměstnavatelům slouží rozličné nástroje určené k monitorování, jako jsou např. kamerové systémy, GPS lokátory, docházkové systémy, systémy kontroly vstupu a vjezdu a v současnosti stále více používané softwarové i hardwarové prvky sloužící pro sledování provozu na klientských stanicích, blokování určitých webových stránek či kontroly emailové pošty. Telefonní hovory bylo možno odposlouchávat již od nepaměti, což bylo více či méně činěno a hlavně politicky motivováno, dnes je ovšem možné tyto hovory sledovat, lokalizovat, nahrávat a dále vyhodnocovat jejich kvalitu v takové míře, že to ve své době výše zmíněný Orwell nemohl ani tušit. Troufám si říci, že bez těchto prvků nemůže žádná velká společnost dobře prosperovat, neboť nejslabším článkem systému je člověk (zaměstnanec) a jeho nesprávné rozhodnutí či činnost může zaměstnavateli způsobit nemalou újmu. Jde o to najít optimální míru tohoto monitoringu. V teoretické části bude čtenář uveden do problematiky a budou mu představeny aktuálně používané formy monitorovacích a kontrolních nástrojů, tyto budou dále zhodnoceny také z hlediska významu na kvalitu odvedené práce. V praktické části se pak pokusím stanovit přiměřenou míru monitoringu na pracovišti. Z důvodu toho, že společnosti se dle svého zaměření výrazně odlišují a je tudíž u nich třeba použít specifické nástroje monitoringu, bude návrh této přiměřené míry směrován na konkrétní výrobní společnost zabývající se zpracováním technické pryže. Budou zde analyzovány aktuálně používané monitorovací techniky a bude zde rovněž navrženo vhodné řešení komplexního monitorovacího systému s ohledem na cíle zaměstnavatele, ale i práva zaměstnance. Obsahem praktické části bude také posouzení monitoringu z právního a etického hlediska.

I. TEORETICKÁ ČÁST

1 MONITOROVÁNÍ PRACOVIŠTĚ

Je nutné si uvědomit, že hlavním a prvořadým zájmem monitorování pracoviště není, jak si mnozí, tedy hlavně zaměstnanci, myslí „šmírování zaměstnanců“, ale ochrana práv a majetku zaměstnavatele a často také ochrana zdraví zaměstnance. V provozu se můžeme setkat s množstvím bezpečnostních rizik a hlavně také s událostmi, které mohou mít neblahé dopady na zdraví či bezpečnost zaměstnance. Ve společnostech s rizikovým prostředím, nebo v takových kde jsou užívány nebezpečné látky, jako jsou např. jaderné elektrárny, chemické laboratoře je přítomnost monitorovacích systému neoddiskutovatelnou nezbytností. Stejně tak u bankovních institucí, pošt, čerpacích stanic je monitoring, dá se říci, nutností, neboť prvotním účelem je ochrana majetku zaměstnavatele a nikoliv monitoring zaměstnance. Ovšem i zdánlivě „neohrožený“ zaměstnanec např. telemarketingové společnosti může být vystaven riziku a to třeba ve formě výhrůžek, slovního napadání a v neposlední řadě riziku právnímu. Dalším faktorem ovlivňujícím zavedení monitoringu může být také informační bezpečnost, ztráta klíčových dat totiž může způsobit mnohdy i krach společnosti.

1.1 Význam monitorování pro vyhodnocení kvality práce

Dalším významem monitorování, je využití těchto systémů ke zvýšení výkonnosti pracovníků a zkvalitnění odvedené práce. Zde tyto systémy slouží k ověření výkonnosti a zvýšení produktivity.

Při bližším pohledu na statistiky se zdá, že někteří zaměstnanci se stále chovají jako v nadčasové povídce Šimka a Grossmanna, kde bylo vtipně řečeno „V odpolední půlhodinové pauze, kdy bývá dílna nejméně dvě hodiny prázdná...“. Pro mnohé zaměstnance to možná bude překvapující zjištění, ale dle zákona musí zaměstnanec 100 % pracovní doby strávit prací. Mnozí dodnes slova „pracovat“ a „být v práci“ považují za dva zcela odlišné pojmy. Samozřejmě, všichni jsme jen lidé a určitá tolerance zde je na místě. Samotné výzkumy dokonce ukazují na vyšší produktivitu práce při proložení pracovní doby krátkými přestávkami mezi pracovními úkony. Ne každý zaměstnanec také odvede stejné množství práce jako jiný, mnohdy se můžeme setkat s výrazně odlišnou výkonností a není se tedy čemu divit, když zaměstnanec, který zvládne, jak se říká „za dva“, část pracovní doby prosufuje na internetu, protože se mu zcela logicky nechce pracovat „za tři“. Při posuzování výkonnosti je nezbytné důkladné posouzení stavu pracoviště jako celku, protože takto extremně výkonnému zaměstnanci by mohlo být zbytečně ublíženo a firma

by o něj mohla přijít a to by bylo zcela jistě kontraproduktivní. Tento zaměstnanec by měl být spíše motivován k vyššímu výkonu, namísto toho aby zaměstnavatel použil prostředky monitoringu proti němu.

V dnešní době číhá na zaměstnance spousta lákadel, které jej mohou odvést od podstaty toho, proč jsou v zaměstnání. Zde se bavíme hlavně o zaměstnancích pracujících v administrativě a využívající osobní počítače. Doba legendární karetní hry Solitaire (karty na PC) je již dávno pryč a na scénu nastoupily mnohé další lákadla jako např. sociální sítě, chat, on-line hry, nákupy na internetu a nepřeberné množství webových stránek. Takovéto činnosti jsou schopny zaměstnance strhnout z cesty závratným způsobem. Jeho výkonnost se rapidně sníží a zaměstnavateli vznikají nemalé finanční ztráty.

K monitorování práce na PC mohou současní zaměstnavatelé využít mnohé z dostupných produktů k tomu účelu sloužících, výstupy z těchto aplikací pak mohou jednoduše analyzovat a odhalit tak ty zaměstnance, kteří se v pracovní době věnují činnostem nesouvisejícím s výkonem povolání. Již samotný fakt, že zaměstnanci vědí, že jsou monitorováni, je může vést k vyšší výkonnosti. Tyto nástroje mohou zaměstnavatele taktéž ochránit před neoprávněným šířením firemních dat.

V některých společnostech pak hrají významnou roli kamerové systémy, díky nimž získá zaměstnavatel přehled o tom co se právě děje či dělo v určitou dobu na pracovišti. Získá tak zpětnou kontrolu o činnostech ve snímaných prostorách a je schopen posoudit, zda je dění na pracovišti v souladu se zákoníkem práce.

Systémy kontroly vstupu a vjezdu v kombinaci s docházkovým systémem zajistí zaměstnancům vstup na pracoviště pomocí přístupového média a zaměstnavatel získá přehled o docházce zaměstnanců. Tyto systémy především zjednodušují činnosti spjaté s přístupem na pracoviště.

GPS lokátory vozidel pomohou zaměstnavateli získat dokonalý přehled o pohybu monitorovaného vozidla resp. zaměstnance. Zaměstnavatel má tak možnost kontroly toho, zda se zaměstnanec opravdu nachází na místě, spjatém s výkonem povolání a nevyřizuje například své soukromé záležitosti na místě jiném. Tyto systémy přinášejí vyšší efektivitu práce a šetří náklady zaměstnavatele.

1.2 Vymezení pojmů

V následujících kapitolách budou vysvětleny základní pojmy týkající se monitoringu zaměstnanců.

1.2.1 Monitoring zaměstnanců

Sledování (anglicky surveillance) představuje činnost nebo způsob, jakým je monitorováno chování zaměstnanců. Používá se zpravidla za účelem potvrzení žádoucího nebo nežádoucího, mnohdy očekávaného chování či jednání.

Jedná se tak z důvodu zaručení bezpečnosti zaměstnanců nebo jejich kontroly, ale také k ochraně práv zaměstnavatele. K monitoringu lze použít různé technické prostředky, jako jsou kamery, sledovací software, GPS a další.

1.2.2 Kontrola zaměstnanců

Kontrola zaměstnanců je proces, který probíhá nepravidelně a zaměstnavatel při něm kontroluje pracovní morálku svého zaměstnance. Definice může znít takto: *„Proces, v němž zaměstnavatel zjišťuje, zda zaměstnanci podniku provádějí řádně a hospodárně jim svěřené úkoly. Zejména se jedná o osobní schopnosti, spolehlivost, přesnost, dovednost a výkonnost zaměstnaného personálu.“* [10]

1.2.3 Zamezení činností spojených s užíváním PC

Omezení plné využitelnosti PC. S využitím softwarových nástrojů dochází k zamezení nežádoucích aplikací, procesů, možností provádět určité akce např. instalovat, měnit nastavení, prohlížet určitě www stránky.

2 MOŽNÉ ZPŮSOBY MONITOROVÁNÍ

V této kapitole jsou popsány nejčastěji využívané formy monitorovacích systému, tyto mohou být nasazeny jednotlivě či integrovány v komplexním monitorovacím systému. Cílem každého zaměstnavatele by mělo být využití takových, které jsou pro fungování jeho společnosti potřebné. Ne vždy je třeba aplikovat všechny způsoby, jejich využití by mohlo být shledáno jako nadbytečné a nepřiměřené. Monitorování je jistým zásahem do soukromí jednotlivce, proto je tato činnost podřízena několika zákonům, o kterých bude pojednáno v dalších kapitolách.

2.1 Kamerové systémy

Asi nejčastěji se v praxi setkáváme s touto formou monitoringu, jedná se o uzavřený kamerový systém s možností integrace. Využití v praxi nachází hlavně jako systém bezpečnostní, ale mnohým zaměstnavatelům slouží i jako systém kontroly zaměstnanců. Téma monitoringu pomocí kamerového systému je také asi nejdiskutovanějším tématem, neboť dosti výrazně zasahuje do práv jednotlivce. Na straně monitorovaných osob stojí Úřad pro ochranu osobních údajů (ÚOOÚ), u kterého je třeba registrovat každé monitorování se záznamem. Kamerové systémy jsou nejrozšířenější v odvětví průmyslu a obchodu. V administrativě využití pravděpodobně nenajdou, zde se nabízí jiná řešení dále zmiňovaná. U kamerových systémů je velmi důležité přidělení práv a jmenování zodpovědných osob, ne každý by měl mít k datům přístup, neboť by mohla být zneužita.

2.1.1 Analogové a hybridní systémy

I přes značnou zastaralost analogových systémů a postupné nahrazování systémy digitálními jsou stále v praxi používány. Hlavním důvodem použití těchto systémů je jejich nízká cena. Analogové systémy používají jak analogové kamery (obr. 1), tak analogové zobrazovací a záznamové zařízení. Jako přenosový kanál je použito nesymetrické vedení tj. koaxiální kabel s impedancí 75 ohmů.

Obr. 1 SONY SSC-E413P

(Převzato: http://www.elviacctv.cz)

U analogových kamer je mezi jednotlivým snímáním časový posun, což při pohybu kamery či snímaného objektu znamená rozmazání detailů. Snímání obrazu zajišťuje snímací čip s velikostí 1/3”, 1/2" nebo 2/3”. Digitální signál se zde musí převádět na analogový, což způsobuje zkreslení a ztrátu kvality obrazu. Rozlišení analogových kamer je omezeno možnostmi formátu PAL, kde je maximální velikost snímku 704 x 576 obrazových bodů.

Plně analogové systémy využívají jako médium magnetickou pásku. Největším úskalím těchto systémů je zdlouhavost vyhledávání záznamu na pásce v případě nutnosti dohledání konkrétní události. Analogové záznamy je obtížné dále zpracovávat (přiblížení, úprava kontrastu nebo jasu, apod.). U zařízení jsme limitováni maximální kvalitou záznamu na pásek (VHS 240 řádků, S-VHS 400 řádků, Betacam 600 řádků).

Hybridní kamerové systémy jsou jakýmsi mezičlánkem mezi analogovými a digitálními systémy, kombinují prvky obou skupin. Jsou u nich použity analogové kamery propojené nesymetrickým vedením s digitálním záznamovým a zobrazovacím systémem. Tyto zařízení jsou vybaveny n-počtem kanálů, což v praxi znamená n-počet BNC konektorů pro připojení jednotlivých kamer. Nejčastější varianty jsou 4, 8, 16 a 32 kanálové DVR. Jako záznamové zařízení slouží buďto samostatný DVR rekordér (obr. 2), nebo hardwarová karta do PC s obslužným software.

Obr. 2 KGUARD 16ti kanálový rekordér DVR

(Převzato: http://www.czc.cz/kguard-16-kanalovy-profi-rekorder-dvr)

Každá z variant má své pro a proti. Samostatný DVR má mnoho stejných fyzických prvků jako PC, tyto zařízení jsou menší a funkční pouze k tomu k čemu jsou vyrobeny. Mají pevně dané funkce a nelze je dále rozšiřovat, upgradovat CPU, paměť RAM, nebo přidat další video kanály. Může se tedy stát, že za určitý čas, kdy nám výkon stroje nebude dostačovat, bude nutné celé zařízení vyměnit. Obecně platí, že PC DVR mají více

pokročilých funkcí, které jsou závislé právě na výpočetním výkonu, možnost upgradu software i hardware, rozšíření o další kanály bez nutnosti se učit pracovat s dalším novým zařízením. Hybridní kamerové systémy jsou však limitovány rozlišením analogových kamer, to však nemusí nutně být přílišnou nevýhodou, tyto systémy mohou být vybaveny kamerami s vysoce kvalitní optikou, možností natáčení, optickým přiblížením atd. Zobrazení videosignálu probíhá na monitoru PC popř. na připojeném LCD či CRT monitoru (obr. 3). Vybrané DVR systémy po svém zhruba desetiletém vývoji, umožňují i relativně komfortní přístup k záznamům díky jejich sdílení v LAN a internetu, umožňují také on-line sledování snímaného obrazu.

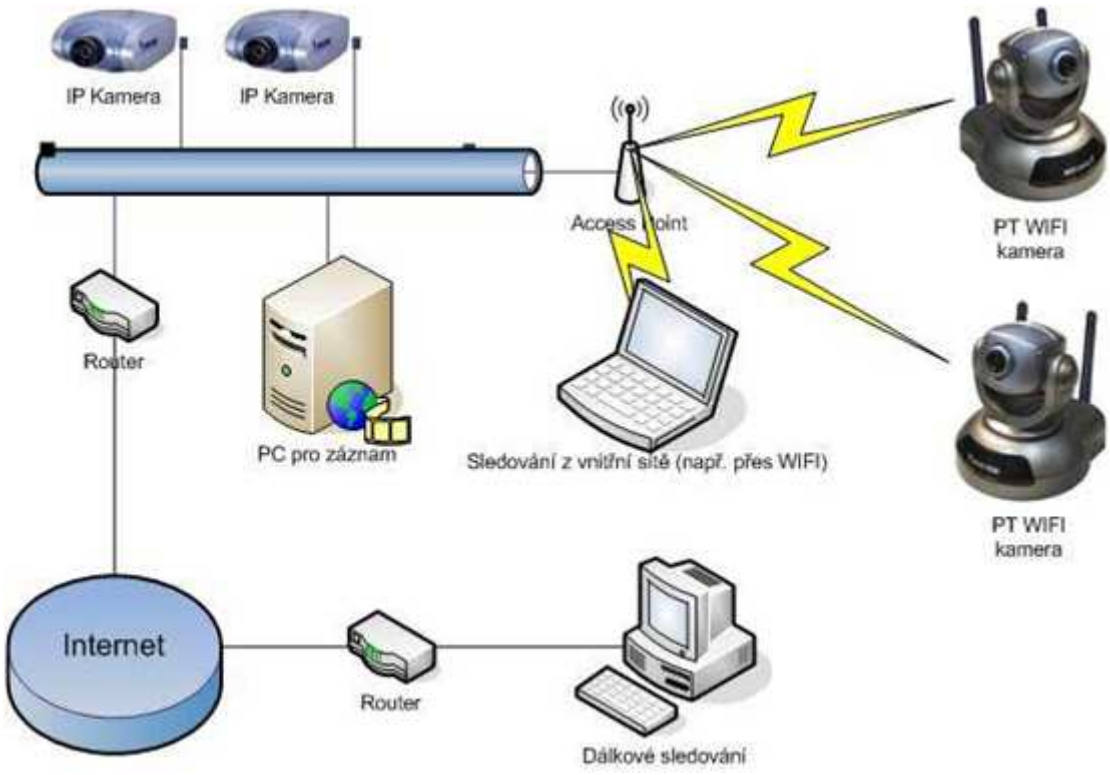
Obr. 3 Klientský software DVR

(Převzato: http://www.besy.cz/dokumenty/manualy/CMS_manual.pdf)

2.1.2 Digitální IP systémy

Digitální technologie v oblasti kamerových systémů se od poloviny 90. let značně vyvinula a dnes jsou nejčastěji nasazovanými systémy vůbec. Digitální kamery využívají k zachycení obrazu CCD nebo CMOS snímač. Každý z nich má své pro a proti, v současnosti převládá použití CCD snímače, ovšem nedávno technologický pokrok dovedl CMOS snímače na úroveň CCD a možná jej dokonce v mnohém předčil. Na kvalitu záznamu má největší vliv právě snímač a to jak velikost, tak i jejich počet. Běžné bezpečnostní kamery mají jeden snímač, který zaznamenává všechny barvy dohromady.

Mezi špičku dnešní doby patří HD bezpečnostní kamery, které přenášejí obraz v rozlišení Full HD 1080p (1920 x 1080). Např. kamera TOSHIBA s označení IK-WD14A (obr. 5) díky HD rozlišení dovoluje svým uživatelům rozeznat jemné obličejové rysy, ale i SPZ vzdálených vozidel, má také integrován trojnásobný optický zoom, je otočná a díky použitým kodekům H.264/MPEG4/JPEG nezatěžuje síť zbytečně vysokým datovým tokem. IP kamerové systémy využívají rozvodů LAN, lze i stávajících a jejich nasazení je tak mnohem jednodušší (obr. 4).



Obr. 4 Obrázek připojení IP kamer

(Převzato: vlastní tvorba)

Standardně pracují v rámci vnitřní sítě připojeny k video serveru se záznamem. Pro přenos je využívám protokol TCP/IP a lze nekonfigurovat cestu na vnější síť pomocí zabezpečeného přístupu a definování využitého přenosového portu. Prakticky kdekoli na světě můžeme sledovat co se doma či v zaměstnání děje, dnes dokonce na svém „chytrém“ mobilním telefonu. Video server může být integrován buďto přímo v kameře popř. v PC nebo NVR zařízení. Některé IP kamery používají k přenosu na server bezdrátové

sítě Wi-Fi. Zobrazení videosignálu zabezpečují dnes běžné digitální LCD, LED nebo starší CRT monitory.

Obr. 5 Toshiba IK-WD14A

(Převzato: http://www.toshibasecurity.com)

2.2 Odposlouchávací zařízení prostor

Odposlouchávací zařízení nám poskytují přenos audio signálu z monitorovaných prostor pomocí vhodně použitých technických prostředků. Audio signál může být zaznamenáván a dále zpracováván. Odposlech může být prováděn skrytě či otevřeně. Obecně se dá říci, že tato forma monitoringu není příliš používaná a to zejména kvůli nesouladu se zákonem. Přesto ale mnohé společnosti využívají otevřenou formu odposlechu pro záznam konferencí, školení či obchodních jednání.

Je třeba uvést, že dle §316 odst. 2 zákoníku práce „Zaměstnavatel nesmí bez závažného důvodu spočívajícího ve zvláštní povaze činnosti zaměstnavatele narušovat soukromí zaměstnance na pracovištích a ve společných prostorách zaměstnavatele tím, že podrobuje zaměstnance otevřenému nebo skrytému sledování, odposlechu a záznamu jeho telefonických hovorů, kontrole elektronické pošty nebo kontrole listovních zásilek adresovaných zaměstnanci.“ [6]

Podle způsobu přenosu informace dělíme odposlechy na [11]:

2.2.1 Minidiktafony

Jsou použitelné v případech kdy má osoba snadný přístup bez doprovodu a dohledu do zájmového prostoru, dále pokud je v časových možnostech uživatele mini-mikrodiktafonu vyhodnocovat dlouhé hodiny záznamu a především tehdy, pokud je zájem o eliminování

možnosti náhodným naladěním rádiového odposlechu jinou osobou. Rozměry zařízení jsou zpravidla velice malé, což platí také v případě zařízení Edic-mini tiny A22 (obr. 6). Rozšířené jsou i kombinace se záznamem videa. Bohužel jejich použití slouží i různým kriminálním živlům pro "zmapování terénu" a následné přípravě k páchání trestné činnosti.

Obr. 6 Edic-mini tiny A22

(Převzato: http://www.ts-market.com/products/models/239)

2.2.2 Linkové (drátové) odposlechy

Jsou velmi jednoduché a prakticky nejrozšířenější, protože slouží například k veřejným, nebo skrytým záznamům firemních a obchodních jednání, bezpečnostním záznamům jako doplněk standardních kamerových systémů, sledování dění v kancelářských, průmyslových ale i bytových prostorách apod.

2.2.3 Rádiové (bezdrátové) odposlechy

Jsou ideální pro operativní použití např. při obchodních a jiných strategických jednáních, nebo na druhou stranu v případech, kdy je nutné pomocí odposlechu chytit pachatele přímo při páchání trestné nebo jiné činnosti. Jsou také velmi dobře použitelné rodiči při odhalení začínající drogové závislosti dětí a mladistvých, případně při odhalování nevěry nebo jiné nekalé činnosti partnerů.

2.2.4 GSM/3G odposlechy

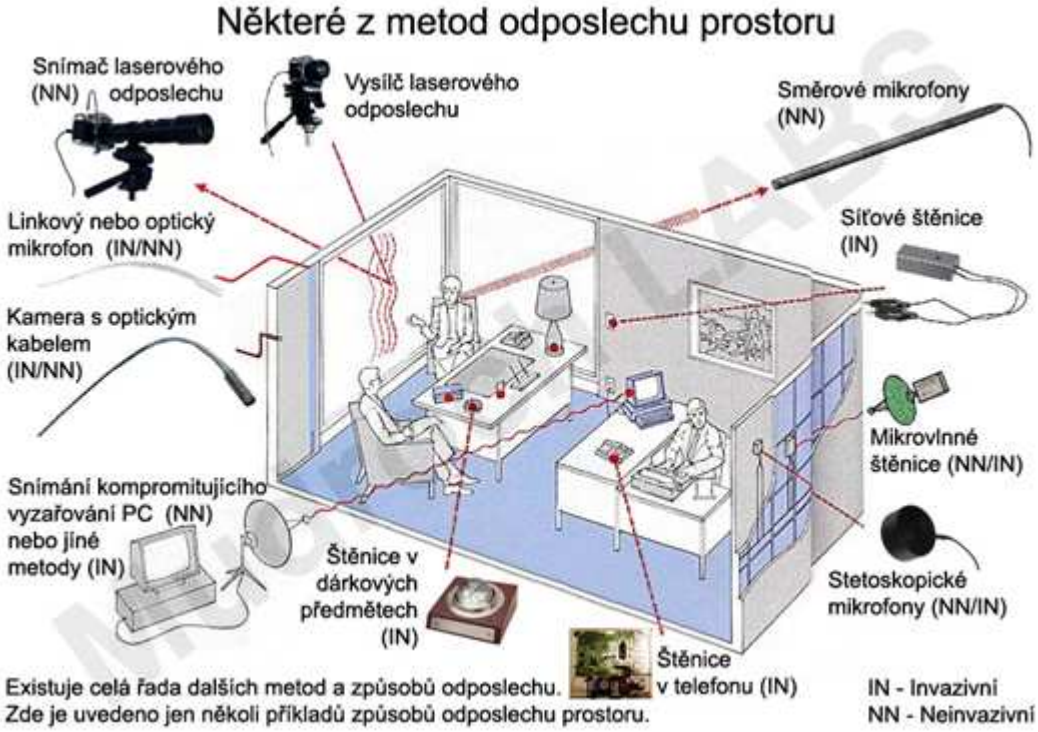
Jsou velmi rozšířeným artiklem poslední doby. Jejich použitelnost je podobná jako u rádiových odposlechů, ale v tomto případě prakticky s neomezeným dosahem. Tento odposlech zajišťuje dosah, dá se říci, po celém světě, nevýhodou je ovšem dosti vysoká energetická náročnost.

2.2.5 Laserové odposlechy

Jsou známy především z filmového plátna. Nicméně jejich použitelnost si vyžaduje vysokou dávku zkušeností a praktických dovedností při řešení potíží s volbou stanoviště vhodného pro realizaci tohoto typu odposlechu. Jedná se o jednu z neinvazivních metod odposlechu. Existuje několik principů snímání chvění okenních tabulí (zachycení přímého odrazu laseru, snímání stopy odraženého paprsku mimo úhel dopadu, snímání změn laserového paprsku způsobených odrazy od lesklých předmětů uvnitř zájmového prostoru). U tohoto druhu odposlechu není vysílán žádný rádiový signál, tudíž je prakticky nemožné jej odhalit jinak než vizuálně. Nevýhodou je ovšem obtížná dosažitelnost na trhu, náročná příprava instalace a vysoká pořizovací cena

2.2.6 Hybridní kombinace předešlých způsobů

Jsou například kombinace záznamového zařízení a digitálního bezdrátového rádiového přenosu, nebo přenosu přes WiFi, GSM, 3G-UMTS a jiné telekomunikační standardy a veřejné sítě. Tyto kombinace umožňují on-line i off-line přenos obsahu paměti – tedy záznamu, díky čemuž se řadí tato operativní technika mezi nejsofistikovanější a nejnebezpečnější formy odposlechu.



Obr. 7 Ukázka metod odposlechu prostoru

(Převzato: http://www.mudrochlabs.sk/cz/odposlechy.htm)

2.3 Kontrola vstupu a vjezdu, docházkové systémy

Systémy kontroly vjezdu mají dnes velmi široké uplatnění. Setkáváme se s nimi u vjezdu do areálu firem nebo se vyskytují velmi rozšířeně jako regulování vjezdu veřejnosti na parkoviště například u nákupních center, tyto jsou pak spojeny s parkovacími systémy.

Systémy pro kontrolu vjezdu jsou zpravidla spojeny s elektromechanickými zařízeními, které fyzicky omezují vjezd vozidel do chráněných zón, nejčastěji formou závory.

Systémy kontroly vstupu zajišťují autorizaci a přístup osob do chráněných zón, jsou zde také používána elektromechanická zařízení, jedná se například o turnikety nebo elektromagnetické zámky dveří.

Docházkový systém zajišťuje sledování odchodů a příchodů zaměstnanců ze zaměstnání v průběhu pracovní doby a následně pak zaměstnavatelům umožňují přípravu podkladů pro zpracování mzdové agendy.

Tyto systémy mohou být budovány jako nezávislé, ale častěji se setkáváme s komplexním řešením, které zajišťuje vzájemné propojení kompletního systému docházky, vjezdu i přístupu. Díky integraci je používána jediná databáze osob, kde lze jednoduše definovat pro konkrétního zaměstnance nebo skupinu zaměstnanců práva pro povolení či zamítnutí vjezdu a vstupu. Systém nabízí možnost využívání jednoho identifikačního media pro všechny funkce.

V praxi bývá často provázán systém kontroly vstupu s docházkovým systémem. Docházkový systém supluje také funkci přístupového systému.

Vjezdový, přístupový i docházkový systém může být propojen se systémem kamerovým. Tohoto propojení se využívá hlavně kvůli zajištění vyšší bezpečnosti a přesnosti systému, záznamy z kamerového systému mohou sloužit ke kontrole, zda pokus o přístup byl opravdu proveden vlastníkem daného identifikačního média, neboť v praxi je třeba s tímto zneužitím identifikačního media jinou osobou počítat, na základě záznamu z kamer lze jednoduše tohoto hříšníka usvědčit.

Kamerové systémy mohou zajistit současně také autorizaci vjezdu, a to v případě využití systému schopného rozpoznávat SPZ vozidla. Při příjezdu k bráně vjezdový systém vyhodnotí tuto SPZ, pokud se shoduje se záznamem v databázi, je automaticky povolen vjezd vozidla do chráněné zóny.

Pro identifikaci oprávněných osob jsou v těchto systémech používány následující varianty

- Přístup na základě bezpečnostního kódu (PIN)
- Přístup na základě identifikačního media
- Biometrické rozpoznávání

Přístupový systém pracující na základě bezpečnostního kódu patří mezi jednoduché, ale často nespolehlivé metody rozpoznávání identity osoby. Nevýhodou je právě relativně snadná zneužitelnost tohoto přístupového kódu. Oprávnění na základě bezpečnostního kódu je často využíváno u autonomního systému vjezdu, kde je využíván jednoduchý kódový zámek pro odjištění závory a to v případech ve kterých není nutná vysoká míra zabezpečení.

Přístup na základě identifikačního media je velmi rozšířenou technologií. Každý zaměstnanec nebo oprávněná osoba dostane identifikační medium (kontaktní čip, bezkontaktní karta, přívěšek). Identifikační medium v sobě nese jedinečný kód, při přiložení ke čtečce je tento kód vyčten a uživateli je na základě oprávnění povolen nebo zamítnu vstup, respektive povolení zadání operace na docházkovém terminálu. Oproti předchozí metodě s kódem PIN je tato varianta spolehlivější, riziko zneužití je mnohem nižší.

Rozpoznávání na základě biometrických údajů je metoda autentizace, která je založena na předpokladu rozdílných biologických znaků u osob. Nejčastějším způsobem je identifikace otisku prstů, je však možné rozpoznávat i jiné znaky, například oční duhovku, obličej či charakteristiku hlasu. V databázi systému jsou uložena binární data charakterizující konkrétní model biologického znaku. V případě shody je osobě umožněna žádaná operace. Biometrické systémy jsou nejčastěji využívány v kombinaci s docházkovými terminály. V současnosti je biometrie považována za velmi účinnou metodu, možnosti oklamání systému zaměstnancem jsou velmi omezené.

Při požadavcích na vyšší stupeň zabezpečení je možná kombinace výše uvedených variant.

2.4 Monitorování přítomnosti osob v zabezpečených prostorách

Pro zaměstnavatele není vždy žádoucí přístup svých zaměstnanců do všech prostor společnosti, zvláště pokud se jedná o rozsáhlé provozy. K zajištění prostorové ochrany s možností monitorování nám slouží PZTS (poplachový zabezpečovací a tísňový systém)

dříve EZS (elektronický zabezpečovací systém) s případnou integrací přístupových, docházkových a kamerových systémů popsaných v předešlých kapitolách.

Systémové požadavky PZTS stanoví norma ČSN EN 50131-1 ed. 2. Tyto systémy nikterak nebrání narušiteli vstupu do střežených prostor, avšak ihned tento vstup nebo přítomnost nežádoucího jevu detekují. Na tento nežádoucí jev mají systémy PZTS za úkol reagovat buďto akusticky, opticky či skrytým podáním zprávy kompetentní osobě.

Zařízení elektronické zabezpečovací signalizace je souborem detektorů, tísňových hlásičů, ústředen, prostředků poplachové signalizace, přenosových a ovládacích zařízení, jejichž pomocí je opticky nebo akusticky signalizováno na určeném místě narušení střeženého objektu nebo prostoru. [3]

Signalizační zařízení jsou akustická, optická nebo kombinovaná zařízení. Zajišťují nám signalizaci informace narušení z ústředny. Pokud jsou uvedeny v činnost, pak většinou vylekají pachatele nebo upozorní kompetentní osoby.

Ústředna je řídící jednotka PZTS. K nastavení a komunikaci ústředny s uživatelem slouží ovládací klávesnice. Ústředna komunikuje s detektory a přijímá a vyhodnocuje změny jejich stavu. Při vyhodnocení narušení předává zprávu dále na patřičná místa.

Detektory – zařízení reagující na fyzikální změny, související s narušením střeženého prostoru. Změny stavu jsou předávány k ústředně.

Typy detektorů:

- Magnetický
- Destrukční
- Mikrovlnný
- Ultrazvukový
- Pasivní detektor rozbití skla
- Pasivní infračervený (PIR)
- Infračervená závora, záclona, bariéra

Napájení – slouží jako zdroj nepřetržitého napájení celého systému. Obsahuje hlavní a záložní napájecí zdroje, o změně stavu napájení by měla jednotka informovat obsluhu.

2.5 Monitorování telefonních hovorů

Bez telefonu, ať už mobilního či klasické pevné linky, si obtížně můžeme představit fungování jakékoli společnosti. Telefonní spojení nám zajišťuje komunikaci nejen mezi dodavateli a odběrateli, ale také mezi samotnými zaměstnanci. Přes telefon je dnes řešena převážná většina obchodních záležitostí. Proto s příchodem moderních technologií u firem stoupá potřeba tyto hovory monitorovat, u velkých společností mající svá call centra, helpdesky nebo asistenční linky je monitoring těchto linek samozřejmostí již řadu let. Telefon, lze používat ovšem i jinak než k výkonu povolání a to k vyřizování soukromých hovorů. Tyto hovory nemusejí být vždy ze strany zaměstnance činěny tzv. „na černo“, mnoho zaměstnavatelů poskytuje svým zaměstnancům mobilní telefon i pro soukromé účely s tím, že zaměstnanec si svou část účtu uhradí sám. Toto řešení je legislativně čisté i z hlediska správy daní. Tyto hovory lze jednoduše za pomocí volacích předčíslí evidovat a automaticky vyhodnocovat jako soukromé s následnou úhradou přesné částky k platbě, samozřejmě se k nim musí daný zaměstnanec navolením speciální předvolby přiznat. Pomocí monitoringu lze také odhalit již zmíněné hovory „na černo“, už jen to že zaměstnanec uskutečnil hovor v sobotu před půlnocí, může být vodítko, že se nejednalo o vyřizování obchodní schůzky.

Telefonní hovory lze monitorovat několika různými způsoby. První variantou je zaznamenání pouze ID volaného s vazbou na volajícího účastníka, čas a datum hovoru, délku hovoru. Tato metoda je zpravidla využívána ke statistice hovorů. Dle telefonního čísla lze většinou s použití databáze adres a kontaktů vyhledat kam daný zaměstnanec telefonoval a zda se jednalo o hovor pracovní či soukromý. Tuto variantu nám může zajistit také náš telefonní operátor poskytnutím podrobného výpisu volání, kde je detailně uvedeno které číslo, kdy, kam a jak dlouho telefonovalo.

Druhá varianta zahrnuje monitoring výše uvedených dat a navíc samotného záznamu hovoru. Tato varianta vyžaduje sofistikovanější pobočkové ústředny s vyššími technickými požadavky, většinou se jedná o zařízení s pořizovací cenou převyšující 50 tis Kč.

Nahrávání telefonních hovorů je dnes nutným standardem nejen na krizových linkách, kde je nahrávání povinností, ale i u kontaktních center, kde pomáhá zvýšit efektivitu pracovníků a zkvalitňovat poskytované služby. Supervizor má u ruky nezkreslené výsledky práce jednotlivých operátorů, které můžou upozornit na chyby ve vedení rozhovoru. Řeší sporné situace při stížnostech klientů. Během hovoru není potřeba zdržovat se

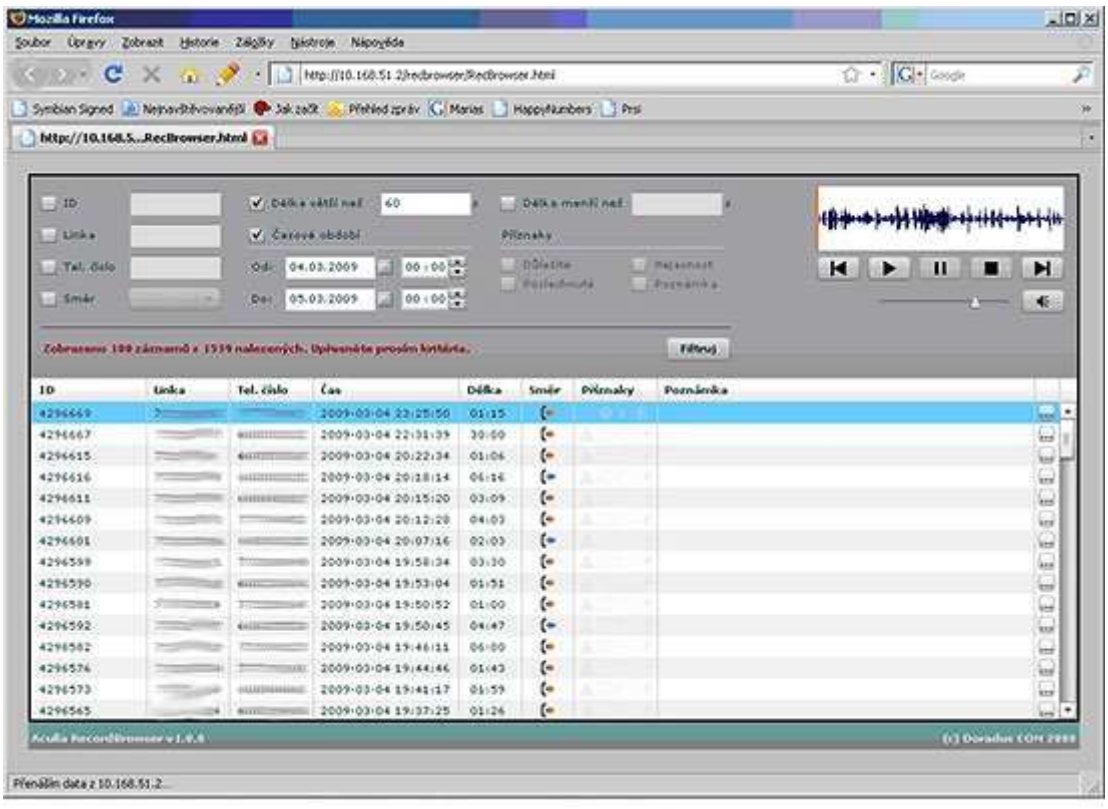
poznámkami, cítíte-li že hovor obsahuje příliš informací, jednoduše stisknete tlačítko na telefonu a hovor se nahraje od začátku. Může sloužit jako záznam z porad provozovaných pomocí telekonference [12]. Přístup k nahrávkám je většinou dostupný přes web klienta. K nahrávkám lze přistupovat pomocí víceúrovňových přístupů, např. každé oddělení může přistupovat pouze k jim určeným nahrávkám, supervizor a vedoucí pracovníci pak ke všem.

K zavedení monitoringu na pracovišti potřebujeme telefonní pobočkovou ústřednu. Vybírat lze z pobočkových ústředen analogových, digitálních a IP ústředen. Nejpoužívanější ústředny jsou dnes typu IP. Pobočková ústředna nám sdružuje vstupní linky např. PSTN, ISDN, VoIP (SIP, IAX), GSM a dále zpracovává příchozí a odchozí hovory. Tyto hovory přesměrovává, třídí, přepojuje, nahrává. K dalším doplňkovým funkcím lze zařadit možnost přidělování práv jednotlivým účastníkům, můžeme přesně definovat, na které telefonní čísla lze volat nebo vymezit oblast (vnitřní síť, stát, Evropa, svět, určité předvolby) a také kdy lze volat např. pouze v pracovní době. Dále můžeme sledovat a zaznamenávat veškerý telefonní provoz společnosti, a to kdo, kam, kdy, jak dlouho a za kolik telefonoval. Pobočková ústředna vytváří vnitřní sít účastníků, a šetří nám čas i peníze tím, že tito účastníci mezi sebou telefonují bez dalších poplatků. IP pobočkové ústředny a brány (gateway) mohou přinést výraznou úsporu financí, neboť tyto ústředny dokážou posunout hranice společnosti kamkoli na světě. VoIP ústředny jsou zapojeny do místních rozvodů sítě LAN a pomocí směrování na IP adresu a port jsou pak připojeni jednotlivý účastníci.

Obr. 8 Pobočková ústředna Faster IPBX-F400 s možností nahrávání

(Převzato: http://www.faster.cz/index.php/lang-cz/hlasove-sluzby-brno/pobokove-ustedny)

Pro rozsáhlejší systémy používané hlavně u společností mající vlastní call centra je pak navíc použit aplikační server a samostatná záznamová jednotka. Předpokládá se zde využití funkce hlasového automatu, který zákazníka nasměruje přesně tam, kde je třeba, aby byl jeho požadavek vyřízen co nejdříve, popř. automaticky odpoví na základě tónové volby zákazníka za pomocí předem nahraných hlasových informací. Možnost nastavit nahrávání jen reálné komunikace s operátorem, nebo také nahrávání po aktivaci operátorem např. při uzavírání smluv, reklamacích atd. Dokonalý on-line monitoring veškerého telefonního provozu a všech procesů v call centru, kde je k dispozici plný přehled o okamžitém zaplňování kanálů používaných telefonních linek a aktuálním stav přihlášených telefonních operátorů. Datový model využívá SQL server, kde jsou data bezpečně uložena pro sledované statistické přehledy o provozu. Rozdělení dle typu monitorování na odposlech a záznam. Je zde možná integrace do CRM, kde ihned po identifikaci účastníka můžeme v databázi dohledat potřebné informace a dále s ní pracovat.



Obr. 9 Webové rozhraní supervizora

(Převzato: http://www.doradus.cz/call-centrum.html)

Obory využití

- Záchranné a bezpečnostní sbory (záchranky, hasiči, policie, horská služba…)
- Finanční instituce a společnosti (banky, pojišťovny, makléři, obchodníci s cennými papíry…)
- Bezpečnostní agentury
- Cestovní ruch (cestovní kanceláře a agentury, hotely, restaurace…)
- Dispečinky (logistické firmy, letecké společnosti, taxislužby…)
- Obchodní oddělení firem
- Call centra
- Zákaznické linky a linky technické podpory
- A další

Proč nahrávat

- Zákonná nařízení
- Zpětná analýza stěžejní telefonické komunikace
- Hlídání a zvyšování kvality poskytovaných služeb
- Tréninky komunikativnosti pracovníků a jejich profesionalizace
- Odhalování podvodných a nekorektních volání
- Zamezení úniku informací

Podporované technologie

- Analogové státní linky
- ISDN2 (BRI)
- ISDN30
- VoIP
- Mobilní telefony s operačními systémy
- GSM brány (analogové i ISDN) a mobility extension
- Vnitřní analogové pobočky
- Systémové digitální pobočky
- VoIP pobočky

Podporované kodeky

- G.711, G.723, G.729, G.722

Formát zvukových souborů

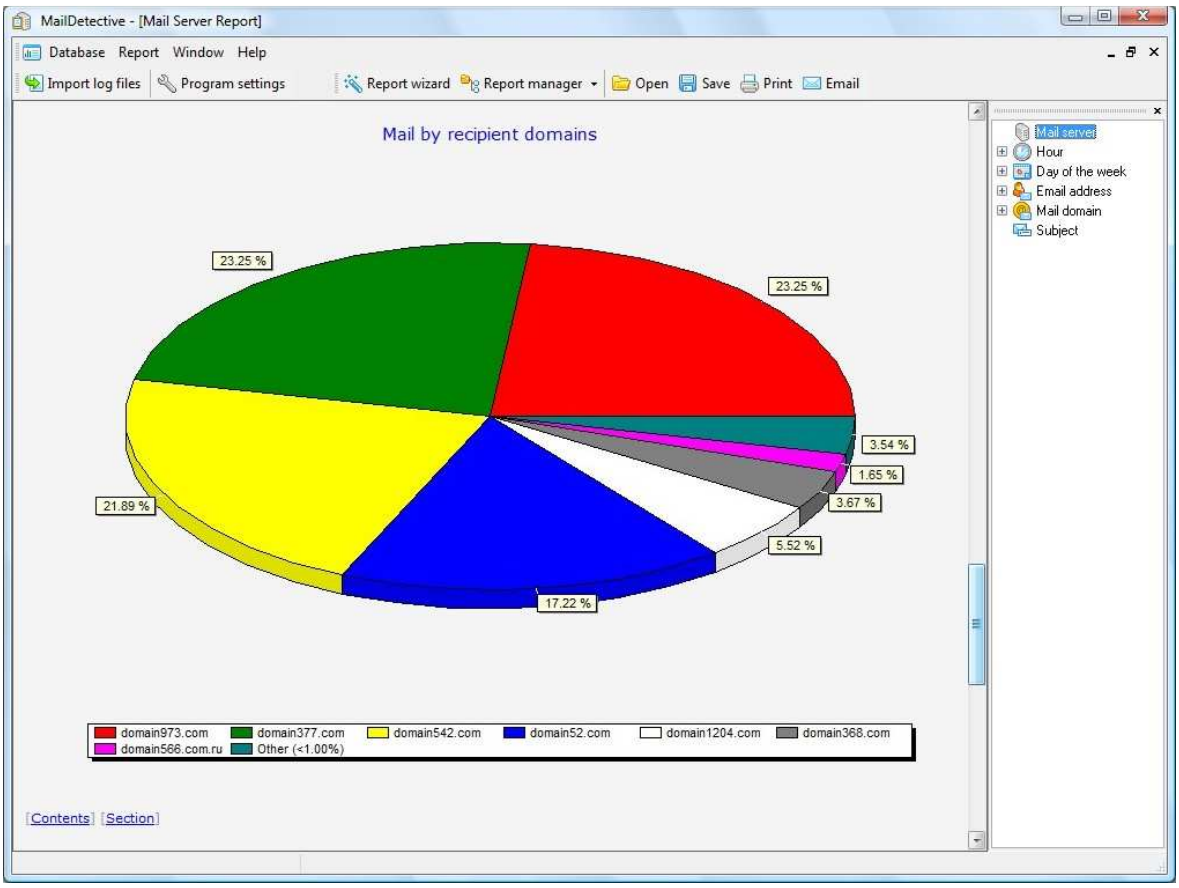
- MP3 (standardně)
- GSM
- WAV [13]

2.6 Emailová pošta

S mohutným rozvojem internetu v roce 1995 se nese i rozvoj komunikace po síti a to především pomocí emailové pošty, která postupně nahrazuje poštu klasickou. Stejně jako telefon i tento prostředek je využíván ke komunikaci s obchodními partnery. Pokud je zaměstnanci zneužíván nad rámec nařízení zaměstnavatele, může ukrojit notnou část pracovní doby zaměstnanců. Emailová adresa je ve své podstatě velice podobná adrese poštovní, která směřuje do určité schránky. Některými zaměstnavateli jsou využívány pouze obecné adresy typu info@xyz.cz, obchod@xyz.cz, sklad@xyz.cz, což je z hlediska ochrany práv příslušného uživatele adresy výhodnější, neboť je zcela zřejmě, že adresa nepatří konkrétní osobě, nýbrž společnosti.

K realizaci monitoringu je třeba vycházet z použité metody správy příchozí a odchozí pošty, kde malé společnosti obvykle řeší přístup do emailových schránek zaměstnanců pomocí protokolu POP3 nebo IMAP, v tomto případě je pošta uložena na serveru poskytovatele serverhostingu a následně předávána pomocí těchto protokolů do PC uživatele s nainstalovaným emailovým klientem. Máme zde na výběr z několika variant monitoringu. První a nejjednodušší je v nastavení dané emailové schránky využít možnosti přeposílání kopií zpráv na námi určenou adresu, čímž získáme přehled o veškerých přijatých zprávách. Druhou variantou je přihlášení se pomocí webového rozhraní poskytovatele do dané schránky. Abychom po přihlášení viděli i starší emailové zprávy, je třeba u emailového klienta uživatele nastavit ponechávání zpráv na serveru. Toto řešení není však příliš vhodné, neboť z důvodu omezeného poskytovaného diskového prostoru má každá ze schránek přidělenu svou kvótu, která limituje počet uložených zpráv na tomto serveru. Odchozí poštu lze u této varianty monitoringu kontrolovat nastavením vlastního serveru SMTP, který nám zajistí přeposílání veškeré komunikace na určenou adresu. Další možností je přesměrování pošty pomocí nastavení pravidel emailového klienta na PC uživatele. Střední a velké společnosti se povětšinou ubírají směrem stavby svého vlastního poštovního serveru. Jedná se o HW se serverovým operačním systémem a instalovaným vhodným softwarovým produktem, jako je např. MS Exchange Server, Kerio MailServer,

Merak Mail Server aj. Tyto servery nám zajišťují nejen odesílání a příjem, ale také nepřeberné množství funkcí jako třeba archivaci, sdílení emailů, kontaktů, kalendáře i poznámek, antispamovou a antivirovou kontrolu a mnohé další. Příchozí pošta je zde tříděna a ukládána do databáze, kontrola nad došlými i odeslanými zprávami zaměstnanců je pak pro pověřené vedoucí pracovníky hračkou. Máme-li obavu z toho, že pomocí e-mailu uniknou z naší společnosti cenná data, můžeme si nechat v rámci průchozích zpráv (včetně jejich příloh nejen ve formátu Microsoft Office) vyhledávat konkrétní frázi (např. „zápis z porady“) a pokud je taková zpráva identifikována, předat ji zodpovědnému pracovníkovi ke schválení či zamítnutí, nebo ji rovnou zamítnout a nedoručit. Pokud chceme monitorování pojmout spíše statisticky, je možné doinstalovat na náš poštovní server software, umožňující vizualizaci toku elektronické pošty, odhad poměru osobní a služební korespondence a odhalení zneužívání pošty, mezi takové patří třeba softwarový produkt MailDetective společnosti ADVSoft.



Obr. 10 Grafické zobrazení odeslané pošty dle příjemců

(Převzato: http://www.advsoft.info/products/maildetective)

2.7 Monitorování firemního PC

Převážná většina zaměstnanců používá ke své každodenní práci PC (personal computer) v překladu osobní počítač. Tento počítač je obvykle využíván, jak nám slovo osobní napovídá, jednotlivcem. Někteří zaměstnanci tráví za počítačem celou svou pracovní dobu a míra měřitelnosti vykonané práce není tak snadno zjistitelná jako řekněme třeba u dělníka, který vyrábí boty. U dělníka máme kalkulací vypočten počet výrobků, které je schopen za směnu vyrobit a pokud je výsledné číslo výrazněji nižší, víme ihned, že plnění výrobního plánu bylo něčím narušeno. U pracovníka za počítačem lze jen těžko počítáním úderů do klávesnice či kliknutí myší odhalit míru jeho pracovitosti. K základním prostředkům sloužícím k průkaznému monitoringu patří přihlašování uživatelů pomocí svých uživatelských jmen a hesel ke svým předem definovaným uživatelským účtům, jen tak lze vyloučit tvrzení zaměstnance, že to nebyl právě on, kdo v dané chvíli u počítače seděl. Těmto uživatelům jsou pak administrátorem přidělována práva, co na PC smí a co naopak nesmějí vykonávat. K monitorování počítačů lze na internetu nalézt nespočetné množství softwarových produktů, mnohé z nich jsou dokonce zcela zdarma pro nekomerční využití. Jednodušší programy zvládají monitorovat pouze některé určité činnosti popsané níže, jiné ucelené a velmi propracované produkty nám nabídnou kompletní řešení monitorování stovek počítačů v síti s přehledným výstupem včetně grafického zobrazení.

2.7.1 Odposlech sítě, vzdálená plocha

Pokud se nacházíme na stejné síti LAN jako počítač uživatele, kterého chceme monitorovat lze využít software pro odposlech na síti. Principielně je metoda odposlechu síťové komunikace založena na zachytávání paketů síťového protokolu. Díky odposlechu na úrovni protokolu TCP získáváme celou řadu přesných časových údajů, popisujících komunikaci mezi uživatelským prohlížečem a webovým serverem. Známe přesný čas přenosu požadované stránky (včetně všech jejích objektů) ze serveru do prohlížeče uživatele a rovněž čas přenosu uživatelských požadavků v opačném směru. Díky tomu přesně určíme, kolik času strávil uživatel nad obsahem stránky a kolik čekáním na její zobrazení.

Vzdálená plocha byla původně vyvinuta pro pomoc správcům sítě se vzdáleným ovládáním PC. Při použití této varianty nemusí tedy k jednotlivým uživatelům fyzicky

chodit, ale vše mohou vyřešit z pohodlí své kanceláře či domova, nebo třeba z dovolené na druhém konci světa. Využít ji lze však i k monitorování zaměstnanců.

Vzdálená plocha využívá služby TS (Terminal Services) běžící na serverovém i klientském operačním systému, používající Remote Desktop Protocol (RDP) a Remote Procedure Call (RPC). Služba TS využívá standardně port 3389, spojení je šifrováno. Jako klient slouží Remote Desktop Connection (RDC). Vzdálenou plochu je možné najít ve většině operačních systémů od Microsoft Windows 7 přes Mac OS X až po serverové operační systémy jako například nejnovější Microsoft Windows Server 8, obsahují ji také operační systémy Linux. U společnosti Microsoft nalezneme klientskou část pod položkou „připojení ke vzdálené ploše“. K připojení se pomocí vzdálené plochy můžeme také využít z mnohé z desítek alternativních produktů, jako například tightVNC, realVNC, TeamViewer, LogMeIn. Připojit se ke vzdálené ploše lze také s použitím chytrých mobilních telefonů, získáme tak přehled o monitorovaných počítačích kdekoli v terénu. Nevýhodou monitoringu pomocí vzdálené plochy je sledování pouze v reálném čase bez možnosti záznamu.

Obr. 11 Wyse PocketCloud Remote Desktop klient pro mobilní telefon iPhone

(Převzato: http://www.macworld.co.uk/ipad-iphone/reviews/?reviewid=3219929)

2.7.2 Zamezení přístupu k vybraným webovým stránkám

Funguje na bázi jakéhosi filtru, přes který procházejí požadavky uživatelů s žádostí o přístup k požadované stránce, filtr dále rozhodne na základě bezpečnostní politiky, zda obsah tj. přístup ke stránce povolí nebo zakáže. Omezení přístupu může být přednastaveno například formou kategorií webů mající stejné zaměření (např. hry, diskusní fóra, e-shopy) a definicemi přístupových práv jednotlivých uživatelů či skupin. Například státní správa povoluje zaměstnancům přístup na web z kategorie státní správy, ale odepře přístup na sociální sítě, či stránky obsahující warez a freemailové servery.

Použití webového filtru by však nemělo omezovat zaměstnance při práci. Klíčová je pro filtr především kvalita a aktuálnost databáze. Výhodu zde mají výrobci webových filtrů, kteří se zaměřují přímo na cílové prostředí (např. Česká republika) a kromě automatizovaných nástrojů mají např. i týmy tuzemských kategorizátorů, kteří webové stránky posuzují.

2.7.3 Keylogger

Softwarový nebo hardwarový nástroj sloužící primárně k zaznamenávání sledu stisknutých kláves na monitorovaném počítači. Lze jím sledovat veškeré aktivity uživatele a z výsledných log souborů si pak jednoduše poskládáme, co bylo v danou chvíli na počítači prováděno. Dokáže zaznamenat tajné hesla uživatelů bez ohledu na zabezpečený přenos dat, zaznamenávat snímky obrazovky v přesně definovaných intervalech, zaznamenat počet a druh spuštěných aplikací a také logovat informace o navštívených webových stránkách, tyto shromážděné informace je program schopen odeslat emailem např. každý den v určitou hodinu.

Tento nástroj je zařazen do kategorie špionážních, jeho použití bývá často utajeno a při neoprávněném použití může způsobit velké škody. V softwarové variantě běží jako skrytý proces a běžný uživatel jej může při odborné instalaci jen stěží odhalit. Další variantou je keylogger hardwarový, představme si jej jako mezičlánek mezi klávesnicí a počítačem velikosti flash disku, je zcela nezávislý, nezjistitelný antivirem, s vlastní interní pamětí, pro zjištění obsahu je nutné jej z monitorovaného PC vyjmout a přečíst obsah paměti.

2.7.4 Legálnost instalovaného software

V době stoupající softwarové kriminality a stále častějších kontrol ze strany protipirátských organizací by mělo být v zájmu každého zaměstnavatele legálnost

instalovaného software pečlivě hlídat. Jen stěží představitelná je situace kdy pracovník IT obchází stovky klientských stanic a kontroluje legálnost software. Tento problém je zpravidla řešen přidělováním práv jednotlivým uživatelům. Uživatelé se ke svému uživatelskému účtu přihlašují svým jedinečným jménem a heslem. Tento účet potažmo uživatel má práva značně omezena od práv administrátora. Je tak možno zakázat instalaci veškerých programů a omezit nastavování hlavních částí systému. Při nutnosti instalace software je pak třeba požádat administrátora, který pokud uzná vhodnost dané aplikace, nainstaluje software přímo na klientskou stanici či pomocí vzdálené plochy.

2.7.5 Únik a zneužití dat

Firemní informace, které jsou mnohdy svěřeny do rukou zaměstnanců, jsou často velmi cenné a jejich zneužití by společnosti mohlo způsobit značné škody. Zabezpečení dat by proto mělo být prioritou IT. Firmy obvykle investují nemalé částky do zabezpečení dat pomocí kvalitních firewall a antivirových programů, neuvědomují si ovšem, že hlavním nebezpečím pro firemní data jsou právě jejich vlastní zaměstnanci. Pokud jsou ve firmách využívány informační systémy, u kterých jsou strukturovaná data zapisována do databází, pomocí práv uživatelů pečlivě rozdělováno kdo má ke kterým informacím přístup a každý přístup k datům je logován, pak můžeme říci, že toto řešení je relativně bezpečné. Ne všechny data lze však mít v informačním systému, často jsou používány dokumenty typu Word a Excel, firemní data kolují uvnitř firmy a často i mimo ni. Tím dochází tak k vysokému riziku zneužití. Hlavní zásadou kvalitního zabezpečení dat na přenosných médiích je jejich šifrování, které nás ochrání od neúmyslného úniku dat, např. ztrátou flash disku či CD/DVD nosiče.

Mnohem vyšší riziko firmám však hrozí při úmyslném vynášení citlivých dat zaměstnancem. Často se stává, že nespokojený bývalý zaměstnanec si vezme sebou něco na přilepšenou. Plány, projekty, technické výkresy, statistiky, analýzy a mnohé další citlivé data se můžou rázem ocitnout u konkurence. K předcházení takovým situacím slouží systémy pro prevenci úniku dat (označované jako Data Leak Prevention nebo Data Loss Prevention, zkráceně DLP). Jde o softwarová řešení, která pomáhají v prvé řadě definovat, co jsou to citlivá data a jak je třeba s nimi zacházet, dále pak vynucují uplatňování nastavených pravidel. K řízení citlivých dat je třeba v prvé řadě tyto data rozpoznat. To lze třeba účinně provést pomocí definování citlivých dat pomocí klíčových slov (např. slovo

„důvěrné“), algoritmů (rodná čísla, čísla účtů, …), seznamů (jména a adresy zákazníků) nebo šablon dokumentů (vzory smluv, interních směrnic apod.).

Další úlohou DLP systému je data vyhledat. Nejčastěji se kontroluje síťový provoz (mail, web, FTP apod.), koncové stanice (data uložená na lokálním disku) a síťová úložiště. Na stanicích je možné detekovat také např. uložení dat na flashdisk, odeslání na tiskárnu nebo třeba zkopírování do schránky.

Nejdůležitější částí je vyhodnocení a zpracování incidentů. Incident může vyvolat jak jediný dokument odesílaný mailem mimo firmu, tak sofistikovaná sekvence událostí. Nastavená pravidla určují, jak se systém k datům zachová – zda jen pasivně sleduje a monitoruje jejich pohyb, nebo je ihned blokuje. Nabízí se zde řada kombinací, odeslání citlivých dat je například povoleno, jen pokud jsou data zašifrována. Vyhodnocení pravidel se může odehrát z pohledu uživatele transparentně, nebo je naopak upozorněn na potenciální rizika, a navíc ještě třeba vyzván k uvedení důvodu, k čemu data potřebuje.

Nezbytný je samozřejmě také kvalitní reporting. DLP systému bychom měli jeho úlohu co nejvíce usnadnit správným nastavením základní bezpečnostní infrastruktury – například omezit možnost používání USB flashdisků, nastavit pravidla pro používání internetu, zejména freemailů, sociálních sítí apod. nebo zavést pro ty nejdůležitější dokumenty šifrovací technologie.

2.7.6 Monitoring tiskových úloh

Monitorovat můžeme všechny tiskové výstupy, jako jsou tisky, kopírování, faxy i výstupy z multifunkčních zařízení. Výsledky monitoringu poslouží nejen k analýze tiskového prostředí, ale jsou také důležitou informací pro detailní rozúčtování nákladů na tisk. Z výstupů monitoringu lze získat také informace o pokrytí papíru barvou, tyto data můžeme využít nejen pro výpočet nákladů a případné rozúčtování, ale také pro výpočty předpokládaných spotřeb toneru. Další možností je odhad spotřeby toneru (barvy) pro rozsáhlejší úlohy na základě analýzy tiskových parametrů a pokrytí jednotlivých listů.

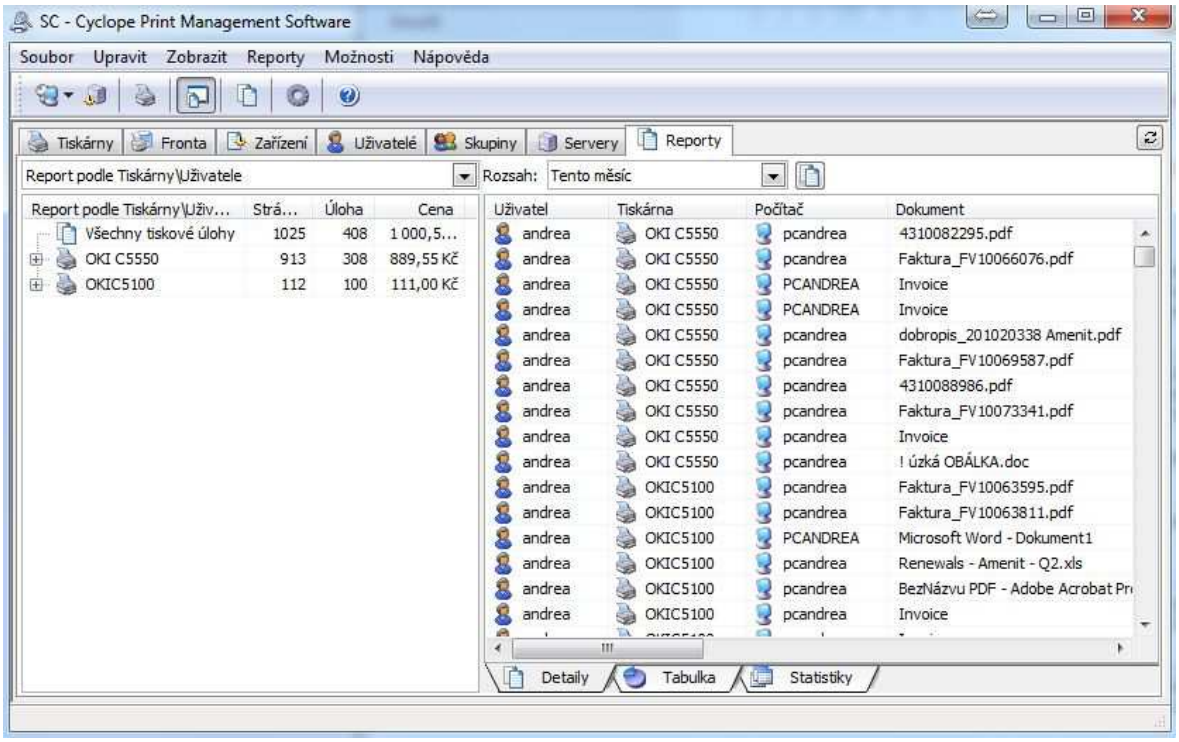
Výstupy z monitoringu (obr. 12) zahrnují počet stran, formát tisku, typ tisku – barevný, černobílý, pokrytí stránky, použitý papír, identifikace zadavatele tisku, lze odlišit i tisky a kopie. Na jejich základě je možné vytvořit libovolné požadované výstupy za zvolené období. Náklady je možné rozúčtovat na uživatele nebo skupiny uživatelů (oddělení, střediska), lze použít i členění na projekty. Je-li to účelné, je možné zohlednit i skutečné

pokrytí stránky barvou. V ceně lze zohlednit nejen množství a kvalitu tisku, ale i prioritu zpracování.

V případě požadavku zákazníka je možná i integrace accountingu tiskových nákladů do informačního systém.

K úspoře nákladů přispívá i stanovení denního, týdenního či měsíčního limitu tisku pro skupiny uživatelů nebo jednotlivé uživatele nebo nutnost autorizace uživatele u kopírky.

Bezpečnost tisku je zajištěna funkcemi odloženého (zabezpečeného) tisku nebo funkcí follow-me (následný tisk, tisk z libovolné tiskárny). V obou případech se dokument fyzicky vytiskne až po autorizaci zadavatele tisku na tiskovém terminálu. Autorizace je možná pomocí PIN, magnetickou nebo čipovou kartou, využitelnou i jinde, např. v docházkovém systému [16].



Obr. 12 Zobrazení tiskových výstupů dle uživatelů v síti

(Převzato: http://www.cyclope-series.cz/Stranky/monitorovani-tiskaren.aspx)

2.7.7 Ekonomie a ekologie provozu kancelářské techniky

Podíl celkové spotřeby elektrické energie výpočetní a kancelářskou technikou překračuje dle studie [15] hranici 20 %. Nejen nákupem energeticky úsporné techniky lze tuto hranici výrazně snížit. Z průzkumů vyplývá, že více než 30 % zaměstnanců po skončení pracovní

směny svůj osobní počítač nechává zapnutý, někteří z nich dokonce i přes víkend. Tento nešvar zaměstnavatelé často řeší vydáním směrnice o nutnosti vypnutí PC po skončení pracovní doby, ne vždy je však dodržována. Kontrola v síti LAN může probíhat například použitím příkazu ping. K automatizaci a zjednodušení poslouží jednoduchý *.bat soubor obsahující příkaz „ping nazevpc -n 1“ který nám vytvoří log soubor se zápisem vypnutých a zapnutých PC uživatelů, jeho spouštění pak můžeme naplánovat pomocí úkolového manažeru v nočních hodinách.

2.8 Lokalizace pomocí GPS

Jedná se o primárně vojenský globální družicový polohový systém, poskytující zdarma část svých služeb i civilním uživatelům, jehož provoz zajišťuje Ministerstvo obrany USA. Díky GPS lze určit dříve neznámou polohu, přesný čas a rychlost pohybu kdekoliv a kdykoliv na Zemi (tj. i nad jejím povrchem) při splnění podmínky přímé viditelnosti přijímače na alespoň čtyři družice tohoto systému.

V současné době se GPS využívá v širokém spektru oborů lidské činnosti a na jeho provoz se ročně vynakládá přibližně 600 až 900 milionů (v letech 2006-2008) amerických dolarů z rozpočtu USA [27]. Rozmach technologie GPS nám přinesl 1. květen roku 2000 – do této doby byla přesnost určení horizontální polohy pro civilní sféru uměle omezována na přibližně 100 metrů, nově lze počítat s přesností okolo 10 metrů.

2.8.1 Monitorování vozidel

V dnešní době již každá firma disponuje automobilem, ať už se jedná o osobní vůz, dodávku, nákladní vozidlo nebo pracovní stroj. Služební automobil dnes patří k běžné výbavě řady zaměstnanců. S provozem vozidla je spojena řada povinností, je nutno platit povinné ručení, silniční daň. Pokud firma nevyužívá možnosti uplatnit paušální výdaj na spotřebované pohonné hmoty a parkovné, tak je ze zákona povinna u každého vozidla vést knihu jízd.

Monitorovací systémy vozidel nám v dnešní době nabízejí spojení monitoringu pro potřeby zápisu elektronické knihy jízd, z toho vyplývající zpětné rekonstrukce jízd, monitorování čerpání pohonných hmot a v případě nejmodernějších systémů jsou nám schopny zprostředkovat současně informaci o dopravní nehodě vozidla či jeho odcizení. Systémy pracují zpravidla na bázi Client-Server aplikace, kde serverovou částí rozumíme webový server.

Monitorování vozidel přináší zaměstnavateli značnou úsporu. Díky tomu může kontrolovat jednotlivé neoprávněné jízdy zaměstnance, překračování povolených rychlostních limitů. Zaměstnanec se pak chová mnohem zodpovědněji, pokud ví, že jeho jízda vozidlem není anonymní. Zneužívání firemních vozidel pro soukromé účely je tímto zásadně potlačeno.

Dnešní systémy pro monitorování vozidel nám nabízejí také jeho střežení a případné dohledání v případě krádeže. Jízdy může provádět pouze oprávněná osoba, pokud dojde k situaci, že by se vozidlo pokusila řídit jiná osoba, toto vozidlo ihned odešle skrze mobilní síť informaci dispečinku, který je následně schopen pohotově zajistit fyzické vyhledání zcizeného vozidla.

2.8.2 Monitorování osob – osobní sledovací jednotky

V případě monitorování osob je stejně, jako u monitorování vozidel využíváno technologie GPS. Tento způsob monitoringu je využíván u osob, které mají pracovní činnost převážně v terénu. V dnešní době probíhá asi nejrozsáhlejší nasazování těchto zařízení například u pracovníků České Pošty. Hlavním cílem projektu České Pošty je zavedení technologie off-line monitoringu listovních doručovatelů po celém území České republiky. Jako další využití pošta vidí geomarketing či užitečná data při projednávání reklamací na kvalitu doručování (sporná tvrzení zda doručovatel objekt navštívil či nikoli) [26].

Dalším odvětvím, kde je využíváno monitorování osob pomocí systému GPS, jsou bezpečnostní agentury. Systém se využívá nejčastěji pro monitorování strážných při kontrolních obchůzkách. Systém přenáší on-line pomocí GSM komunikátoru aktuální polohu do monitorovacího systému klienta. Agentura má takto dokonalý přehled o práci zaměstnanců, zda je prováděna v souladu s vnitřními předpisy. Systémy často umožňují i přivolání pomoci v naléhavých případech, dále pak můžou obsahovat i oboustrannou hlasovou komunikaci.

Komerčně dostupné systémy pro sledování polohy pracovníků dokážou zjišťovat přesnou polohu objektu, avšak neumožňují zjistit stav monitorovaného pracovníka. Tato informace je však často velmi důležitá pro vyhodnocení závažnosti případné krizové situace a pro identifikaci z nich plynoucích problémů. V současné době přicházejí na trh speciální přístroje, tzv. osobní sledovací mobilní jednotky, které kladou důraz na sledování třetí prostorové „Z“ souřadnice. Tyto jednotky umožňují díky přesnému měření hodnoty „Z“ souřadnice identifikovat pád a konsekventní zranění hlídaného pracovníka – což je skutečně přínosné například když pracovník operuje v těžko přístupném lesním porostu ap.

Při zjištění události typu pád nebo nehybnost se automaticky aktivuje tzv. tlačítko mrtvého muže, a pokud pracovník v časovém limitu nepotvrdí svůj stav (stisknutím příslušného tlačítka), na dohledovém pracovišti nebo u zodpovědného pracovníka (bezpečnostní dozor) je spuštěn poplach. Vyšší třídy přístrojů dovolují měřit i tlak okolního vzduchu, teplotu okolí, náhlou změnu a nehybnost pracovníka, což je užitečná vlastnost u pracovníků pomáhajících např. při likvidaci lesních požárů.

II. PRAKTICKÁ ČÁST

3 NÁVRH PŘIMĚŘENÉ MÍRY KONTROLY NA PRACOVIŠTÍCH

Kontrola zaměstnanců na pracovišti vychází z nutnosti zajistit co největší bezpečnost majetku, zaměstnanců a v neposlední řadě efektivitu práce jednotlivých zaměstnanců. Je však nutné stanovit správnou míru kontroly. Při nedostatečné míře kontroly zaměstnanec často neodvádí svou práci naplno, při vysoké míře kontroly je zaměstnanec pod trvalým tlakem, dopadá na něj stres a může se tak postupem času projevit jeho psychické vyčerpání.

Kamerový systém nesmí zasahovat do soukromí, může být využit k ochraně majetku i osob a v případě splnění zákonných podmínek také ke kontrole plnění pracovních povinností zaměstnanců. Zde je nutno opravdu pečlivě zvážit, zda je nasazení kamerového systému v souladu s právními předpisy a etickými normami. Je nutné zaměstnance seznámit s umístěním kamer, případně přímo s kamerovými záběry. Nepřípustné je například umístění kamer na toalety či místa určená k odpočinku. Obávaným problémem může být zneužití dat. Pro ochranu těchto dat je třeba vymezit práva pro přístup, prohlížení by měli mít umožněny pouze zodpovědné osoby.

Docházkový, přístupový a vjezdový systém bývá zaměstnanci hodnocen spíše kladně. Přináší jim určitý komfort v přístupu do důležitých zón, umožňuje jim pohodlnou evidenci pracovní doby. Je ale důležité zajistit kontrolu, zda systém nebývá zneužit. U systémů pracujících na základě vyhodnocování biometrických prvků může však nastat problém se získáváním přístupových oprávnění jednotlivých zaměstnanců, například otisku prstů. V těchto případech je třeba zaměstnancům řádně vysvětlit, že získaná data nebude možné zneužít. Při zadávání otisku prstů je získán pouze matematický model, ze kterého nelze zpětně otisk prstu vygenerovat a zneužít.

U výpočetní techniky je vhodné případným problémům předcházet, ideální je povolit pouze ty nástroje, které jsou k výkonu povolání nezbytné. Vhodné je také filtrování obsahu internetových stránek, případně přímo zamezit přístup na ty servery, které spadají do okruhu činnosti určených k soukromým činnostem.

Využití satelitního sledování vozidel může přinést zaměstnavateli značné úspory, ať už opět po stránce bezpečnostní, nebo po stránce efektivnosti využívání vozidel.

Vzhledem k specifičnosti požadavků různých typů pracovišť a nemožnosti navrhnout univerzální sledovací systém, jsem se rozhodl včlenit do práce návrh monitorovacího systému pro konkrétní společnost. Tento systém bude podrobně popsán v následujících kapitolách.

3.1 Posouzení stavu objektu a personální stránky společnosti

Společnost PENTA, spol. s r.o. vlastní výrobní halu ve které provádí svou činnost, zabývá se pogumováním válců a lisováním technické pryže. Zaměstnanci pracují v 3směnném provozu (24 hod. po-pá), aktuální počet zaměstnanců je 14. Ranní směna provádí pogumování a lisování, odpolední a noční směna pak jen lisování na vulkanizačních lisech. Firma vyrábí pryžové výrobky převážně pro automobilový průmysl. Výrobní hala má rozlohu cca 500 m^2, dvě kanceláře a sociální zázemí. Společnost sídlí ve starší budově, nedaleko bývalého areálu SVIT, venkovní prostory v celkové rozloze cca 200 m^2 slouží jako parkoviště, skladovací prostor a samozřejmě jako místo určené k nakládce a vykládce.

3.2 Návrh monitorovacího systému v závislosti na požadavcích

Prvním krokem návrhu monitorovacího systému byla analýza požadavků a představ ke zřízení systému.

Kamerový systém bude instalován především z důvodu bezpečnostního monitorování prostor. Vedení společnosti však chce mít také možnost zpětné kontroly monitorovaných prostor včetně on-line přístupu ke kamerám. Kamerový systém bude veřejný, všichni zaměstnanci budou tedy znát polohu a rozsah záběru jednotlivých kamer, které budou značnou mírou přispívat současně k zajištění bezpečnosti na pracovišti.

Docházkový systém bude pořízen z důvodu splnění legislativních povinností zaměstnavatele, agenda docházky nyní probíhá jednoduchým způsobem zápisu do docházkové knihy. Systémem bude monitorována přítomnost zaměstnanců, a tím bude prokazatelněji zpracována agenda přesčasů. Každý zaměstnanec bude mít možnost kdykoliv si zjistit stav odpracovaných hodin v průběhu měsíce.

Systém kontroly vjezdu umožní všem oprávněným pracovníkům ovládat vjezdovou bránu a bude propojen se systémem docházkovým.

Systém kontroly vstupu bude taktéž propojen s docházkovým systémem. Bude zajišťovat vstup oprávněných osob do zabezpečených prostor a evidenci těchto vstupů.

Lokalizace vozidel pomocí GPS bude zajišťovat dokonalý přehled o pohybu firemních vozidel, o jejich využívání a navíc odpadne zdlouhavé vedení tištěných knih jízd.

Bezpečnostní systém bude zajišťovat ochranu sídla firmy, které tím bude chráněno před vloupáním a bude také přispívat k zajištění bezpečnosti zaměstnanců a jejich majetku.

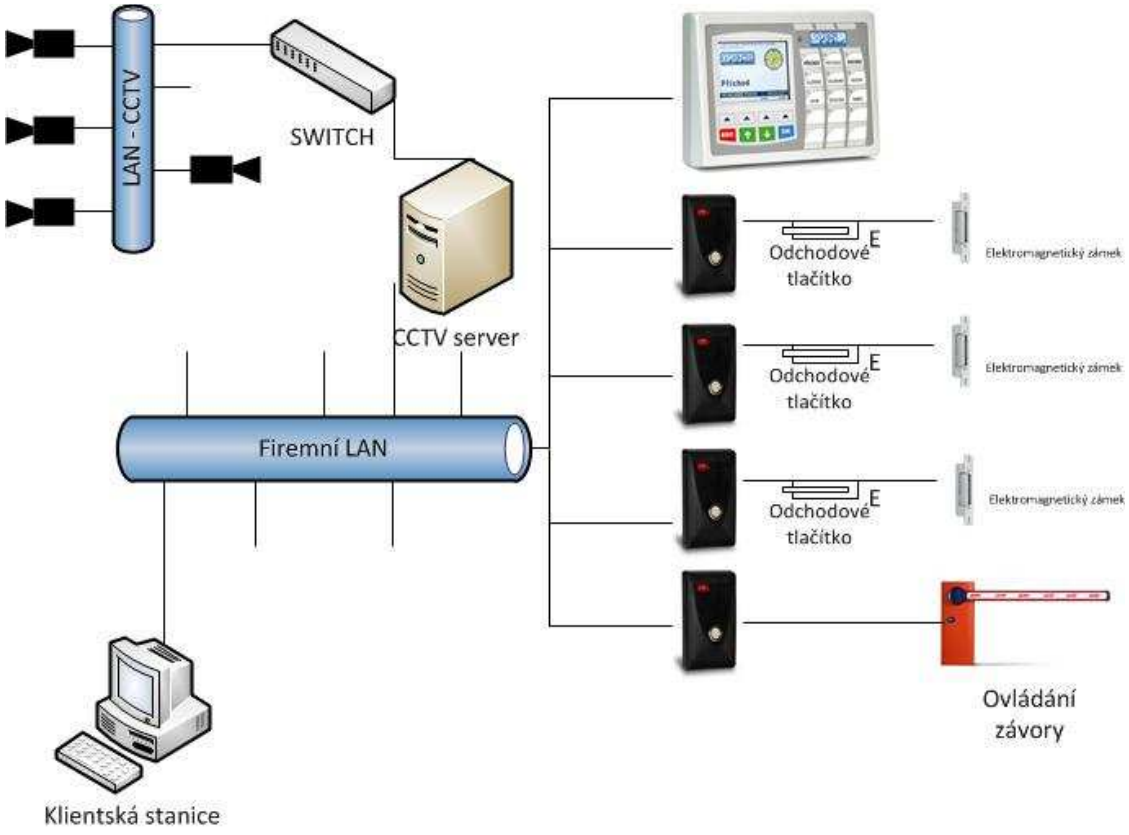
Hlavním požadavkem bylo spolehlivé a jednoduché ovládání všech systémů. Pracovníci budou pro všechny úkony používat pouze jedinou kartu, díky ní mohou ovládat docházku, vstupní systém, firemní vozidla a budou mít možnost ovládat i systém zabezpečovací.

Jako hlavní identifikační médium byl zvolen RFID bezkontaktní čip typu EM4102 125kHz (obr. 13). Tyto čipy jsou velmi často využívány pro účely docházkových a přístupových systémů díky své nízké ceně a vysoké spolehlivosti. Identifikační médium se dodává buď ve formě karet, nebo jako plastové přívěšky.

Obr. 13 RFID identifikační média

(Převzato: http://www.acsline.cz/cs/identifikacni-media)

Požadavkem firmy PENTA je tak kompletní monitorovací a bezpečnostní systém, který zabezpečí pracoviště a současně přinese zjednodušení úkonů spojených s vstupem, vjezdem, docházkou a využívání vozidel firmy. Návrh systémy by měl být proveden s důrazem na kvalitu, spolehlivost, nenáročnou obsluhu a rozšiřitelnost v případě potřeby.



Obr. 14 Schéma propojení kamerového a docházkového systému

(Převzato: vlastní tvorba)

Veškeré komponenty docházkového a kamerového systému jsou opatřeny komunikátorem přes TCP/IP protokol. V návrhu systému je počítáno s využitím stávající počítačové sítě, pro zařízení s vysokým datovým tokem bude vybudována samostatná počítačová síť.

CCTV server bude sloužit jako oddělovací prvek zmíněných LAN. Nově budovaná LAN bude určena pro IP kamery, které budou propojeny přes switch k CCTV serveru. Zde bude probíhat přenos dat z kamer do záznamového zařízení. Pro stávající počet kamer je dostačující síť LAN o přenosové rychlosti 100 Mbit/s. Z důvodu možného budoucího rozšíření je však doporučeno použití kabeláže typu Cat6.

Druhá síťová karta, která je obsažena v CCTV serveru bude sloužit pro propojení se stávající sítí LAN, a budou zde přenášena pouze data při přístupu k zaznamenaným datům.

Do firemní sítě LAN budou dále zapojeny přístupové jednotky a přístupový terminál. V klientské stanici bude probíhat prohlížení a zpracování dat z terminálů. Odchodové tlačítka a propojení mezi přístupovým terminálem a elektromagnetickým zámkem případně závory jsou napojena přímo do přístupového terminálu, zde se již nepřenáší žádná data, ale dochází pouze k sepnutí či k elektrickému impulzu pro ovládané zařízení.

Obr. 15 Schéma bezpečnostního systému

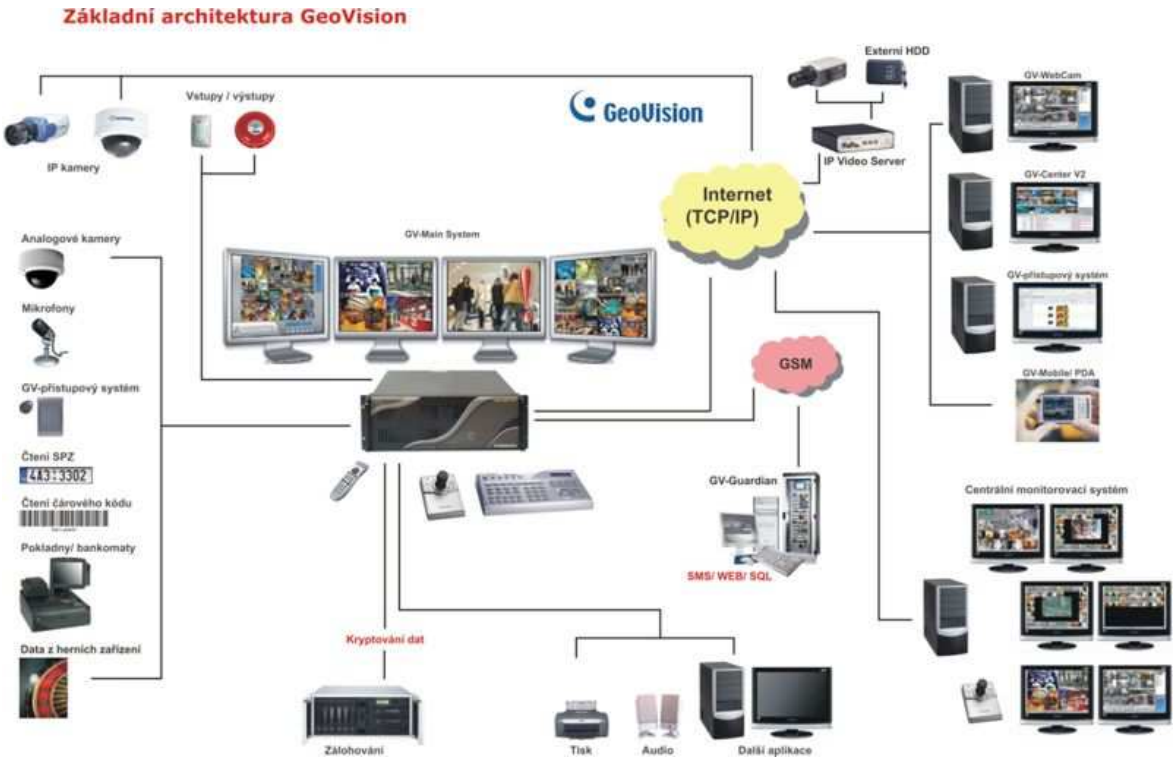
(Převzato: vlastní tvorba)

3.3 Kamerový systém

Úkolem kamerového systému je monitorovat prostor před sídlem společnosti, výrobní prostory a vstupní chodbu. Hlavním požadavkem je dostatečné rozlišení použitých kamer.

Při návrhu byla zvažována jak varianta s analogovými kamerami, digitální záznamovým zařízením a také varianta založená na IP technologii. Vzhledem k požadavku na kamery s vyšším rozlišením byla zvolena IP technologie.

Navrhnutým systémem CCTV je produkt GEOVISION. Jedná se o komplexní systém, jehož základem je software GeoVision. Portfolio obsahuje všechny nutné komponenty pro integraci jak IP kamer, tak i analogových kamer. Umožňuje síťovou správu, ukládání a prohlížení záznamů z kamer. Při použití IP kamer GeoVision je tento software dodáván zdarma ve verzi až pro 32 videokanálů, což bude společnosti nadmíru dostačovat.



Obr. 16 Základní architektura GeoVision

(Převzato: http://www.geo-vision.cz)

Pro účely firmy PENTA, spol. s r.o. bude kamerový systém složen z řídícího počítače, lokální sítě LAN a IP kamer. V budoucnu bude možno tento systém jednoduše rozšiřitelný.

Systém bude zálohovaný pomocí UPS zdroje, aby v případě výpadku el. energie byl stále funkční.

3.3.1 Kamery

V první fázi návrhu byla provedena podrobná obhlídka objektu a proběhlo vytipování vhodných míst pro umístění kamer.

V kamerovém systému bude využito 3 různých typů kamer.

Venkovní kamera

Venkovní kamera budou sloužit pro monitorování venkovních prostor a místa vjezdu do firmy. Budou použita kamera GeoVision GV-BX320D-E. Tato kamera o rozlišení 3Mpix je ve venkovním odolném krytu s integrovaným IR přísvitem. Kamera je dodávána s objektivem 2.8mm-6mm.

Obr. 17 Kamera GeoVision GV-BX320D-E

(Převzato: http://www.geo-vision.cz/e-shop/gv-ip-kamery-c29/geovision-bx320d-e-i351)

Kamera pro monitorování provozu

Pro monitorování provozu bude využita stropní kamera GeoVision GV-FE421D. Jedná se o 4MPix unikátní stropní kameru, která umožní kompletní bezeztrátové vykrytí zvoleného prostoru z jediného bodu. Kamerou pořízený hemisférický obraz je pomocí software GeoVision převeden do běžného zobrazení, s možností využití virtuálních PTZ funkcí. Fisheye kamera pak funguje jako otočná kamera (ovšem bez jakýchkoli mechanických částí), díky megapixelovému rozlišení i s možností smysluplného využití digitálního zoomu.

Obr. 18 Kamera GeoVision GV-FE421D

(Převzato: http://www.geo-vision.cz/e-shop/gv-ip-kamery-c29/geovision-fe421d-i13)

Kamera pro monitorování chodby a vstupu

V systému budou použity dvě kamery GeoVision GV-FD220D. Jedná se o 2Mpix kameru ve vnitřním provedení s IR přísvitem a 2.7-9 mm DC objektivem. Tato kamera bude monitorovat vstupní vnitřní prostory u docházkového terminálu a chodbu.

3.3.2 HW a SW vybavení, LAN

Pro účely provozu záznamového software bude sloužit počítačový server. Jedná se o počítač s čtyřjádrovým procesorem, data budou ukládána na dva pevné disky s kapacitou 1 TB, tento server bude mít dvě síťové karty a bude vyhrazen pouze pro účely kamerového systému.

Z důvodu vysokého datového toku IP kamer bude pro kamerový systém vybudována oddělená počítačová síť. Jednotlivé kamery a první síťová karta serveru bude připojena k aktivnímu prvku – tím bude vytvořena samostatná LAN pro kamerový systém. Přes druhou síťovou kartu bude server komunikovat s místní firemní sítí LAN.

Na serveru bude nainstalována aplikace GeoVision GV-Recording Server, která bude zajišťovat záznam z kamer. Pro prohlížení záznamů a on-line přenosu z kamer bude sloužit aplikace GV-MultiView.

3.4 Docházkový systém vstupu a vjezdu

Docházkový systém, systém vstupu a vjezdu byl zvolen od firmy ESTELAR s.r.o.

Elektronický identifikační systém ACS-line je moderní a výkonný nástroj pro elektronické získávání a zpracování provozních dat. Ucelený systém nebo jeho dílčí části dokážou pokrýt potřeby firem a institucí všech velikostí a oblastí působnosti. Systém ACS-line

aplikuje nejmodernějších technologie pro identifikaci osob, výrobků a materiálu, což umožňuje maximální automatizaci a efektivní řízení lidských zdrojů.

Systém ACS-line je ucelený soubor hardwarových komponentů a softwarového vybavení pro zajištění nejrůznějších činností. Jednotlivé systémy vzájemně spolupracují, včetně sdílení společných dat. Ve větších instalacích je možné přímé propojení na podnikový informační systém, který sloučí získaná data s ostatní agendou. Dílčí sestavy lze využít také samostatně s možností postupného rozšiřování.

3.4.1 Docházkový terminál

Docházkový terminál (obr. 19) byl zvolen tak, aby umožňoval připojení přes TCP/IP protokol, ovládání docházkového systému bude pomocí RFID karet nebo přívěšků.

Zaměstnanci budou na tomto terminálu registrovat příchody a odchody. Identifikaci budou provádět přidělenou kartou. Pro zamezení identifikace s cizí kartou bude na toto místo směrovat kamera, v případě pochybností je možné dohledat záznam z kamerového systému.

Obr. 19 Docházkový terminál KT600B-TCP

(Převzato: http://www.acsline.cz/cs/kt600b-tcp-dochazkovy-terminal-bezkontaktni-2)

Na terminálu může zaměstnanec kromě příchodu/odchodu zvolit i jinou operaci, například služební jízda, nemoc, dovolená apod. V terminálu lze nadefinovat jakoukoli další operaci.

Terminál bude umístěn u vchodu do firmy a bude sloužit zároveň jako přístupový terminál do firmy. Zařízení bude ovládat i elektromagnetický zámek vstupních dveří, v případě identifikace oprávněné osoby tento zámek sepne a umožní jejich otevření.

3.4.2 Přístupový systém

K zamezení pohybu neoprávněných osob budou elektromagnetickým zámkem opatřeny i dveře do kanceláří a na hlavní pracoviště. U těchto dveří budou umístěny přístupové jednotky AL20-TCP a snímací jednotky bezkontaktních čipů EDK4. Dále bude tato jednotka použita i pro venkovní závoru a bude tak obsluhovat i vjezdový systém.

Obr. 20 Přístupová jednotka AL20 a čtečka EDK4 v antivandal provedení

(Převzato: www.estelar.cz)

Přístupová jednotka AL20-TCP (obr. 20) je řídící jednotka pro ovládání dvou jednostranných nebo jednoho oboustranného vstupu. Dveřní zámky jsou ovládány pomocí relé, volitelně lze i sledovat stav dveří (zavřeno/otevřeno). Jednotky jsou připojené přes protokol TCP/IP do sítě LAN a jsou spravovány s docházkovým softwarem. Mají vlastní off-line paměť, historie průchodů se ukládá a docházkovým softwarem jsou poté průchody vyčteny.

Čtečka EDK4 (obr. 20) slouží pro bezkontaktní snímání čipů, provedení je vhodné i do náročných provozů včetně venkovního umístění.

3.4.3 Softwarové a hardwarové vybavení

Systém je navržen tak, aby bylo možné využít stávající LAN. Všechny jednotky a terminály komunikují přes protokol TCP/IP. Obsluhu obstarává software ACS-LINE.

Docházkový systém ACS-line slouží pro evidenci a vyhodnocení docházky, přípravu podkladů pro mzdy, sledování přítomnosti na pracovišti a pohybu zaměstnance v průběhu pracovní doby. Umožňuje práci s daty (dle oprávnění), jejich editaci, korekci a schvalování. Obsahuje velké množství tiskových sestav, umožňuje i exporty dat do mzdových systémů.

Každý ze zaměstnanců obdrží osobní identifikační médium. ID médium se přiřazuje na kartě zaměstnance spolu s dalšími osobními údaji a předpisy pracovního režimu. V

programu se definuje všechen připojený hardware a jeho vlastnosti. Pro každý terminál můžete nadefinovat až 50 různých operací pro průchod terminálem (příchod do práce, odchod k lékaři, odchod na služební cestu, odchod na jiné pracoviště, aj.). Pro každou operaci lze definovat chování při dalším automatizovaném zpracování, způsob započtu a zobrazení v přehledových sestavách. Každému pracovníkovi je přiřazen kalendář, podle kterého je mu počítán fond pracovní doby a následné přesčasy. Program obsahuje předdefinované státní svátky, které jsou pak automaticky započítány do výsledků pracovníka. Načítání dat z terminálů se provádí ručně v případě potřeby nebo jej lze jako další funkce programu přednastavit automaticky v plánovači úloh. Výsledný algoritmus pro výpočet odpracované doby je dán individuálním nastavením dle potřeby podniku.

Zpracovaná data o docházce program přehledně graficky zobrazí s možností manuální úpravy. Do již zpracovaných dat bude možno vkládat nebo upravovat operace. V případě chyby je tak možné vložit docházku dle kalendáře. Veškeré provedené změny jsou zvýrazněny tak, aby ruční úprava dat byla zřetelně označena. U upravených údajů je také označeno, kdo změnu provedl. Nastavením přístupových práv můžete editaci docházky omezit pouze pro osoby, které mají právo docházku upravovat. Pro tisk výsledků je předdefinováno mnoho formulářů tiskových sestav a další lze uživatelsky definovat.

Obr. 21 Princip funkce docházkového software

(Převzato: http://www.acsline.cz/media/image/sch_princip-prace-dochazka.jpg)

Software bude nainstalovaný na počítači, na kterém se vede mzdové účetnictví. Přístup bude zabezpečen heslem. K počítači bude připojen i personifikátor RD3B – ten bude sloužit k načítání karet do systému a jejich přiřazování danému zaměstnanci.

Obr. 22 Personifikátor RD3B

(Převzato: http://www.acsline.cz/cs/personifikatory)

Celý docházkový systém je navržen tak, aby jeho funkčnost byla zajištěna i při vypnutém počítači s docházkovým softwarem. Data jsou ukládána v jednotkách a až následně jsou vyčítána. Vyčítání lze provádět ručně, nebo automaticky dle nastavení.

Licence docházkového software je dodávána dle počtu zaměstnanců – pro účely firmy PENTA, spol. s r.o. byla zvolena varianta ADS25 - docházkový a přístupový software do 25 osob, lokální instalace.

3.5 Lokalizace vozidel pomocí GPS

Návrh řešení lokalizace vozidel pomocí GPS vychází z aktuálních potřeb firmy PENTA, spol. s r.o. Společnost vlastní 5 osobních vozidel, z nichž 2 jsou současně využívány také pro soukromé účely.

Základní požadavky na možnosti systém byly:

- Vedení elektronické knihy jízd
- Možnost on-line lokalizace vozidla na mapách přes webový prohlížeč
- Zpětné dohledání jednotlivých jízd
- Evidence pohonných hmot
- Evidence zaměstnanců, kteří vozidlo využívali
- Možnost střežení vozidla

V ČR je nabídka poskytovatelů služeb lokalizace vozidel pomocí GPS velmi široká. Na trhu existuje široká nabídka výrobků různých kvalit. K poskytování těchto služeb je také možno využít některou z množství firem, které umožňují lokalizaci vozidel a vedení knihy jízd. Z těchto firem jsou to například:

- *Vodafone Auto manažer,* http://www.vodafone.cz/zivnostnici-a-male-firmy/reseni-pro-firmy/sluzby-a-reseni/vodafone-auto-manazer/
- *GPS Dozor*, http://www.gpsdozor.cz/popis_systemu_sledovani_vozidel.html

- *LOKÁTORY.CZ*, http://www.lokatory.cz/
- *CarNet, http://www.sledovaniaut.cz/produkty/monitorovaci-system-carnet_5.html*
- *LogisCarE*, http://www.online-sledovani.cz/
- *GX SOLUTIONS*, http://www.gxsolutions.cz/

Po provedeném průzkumu trhu byla zvolena technologie ONI systém od firmy NAM s.r.o.

Jedná se o českého výrobce, jehož produkty využívá například Policie, záchranná služba, bohaté zkušeností mají i se sledováním vozidel na známé Barum Rallye.

3.5.1 Služby ONI systém

Technologie ONI systém je založena na 3 produktech. Jedná se o produkty ONI Sledování, ONI Sledování plus a ONI Střežení. V následující tabulce je porovnání funkcí jednotlivých variant.

Tab. 1 Tabulka přehledu vlastností ONI systém

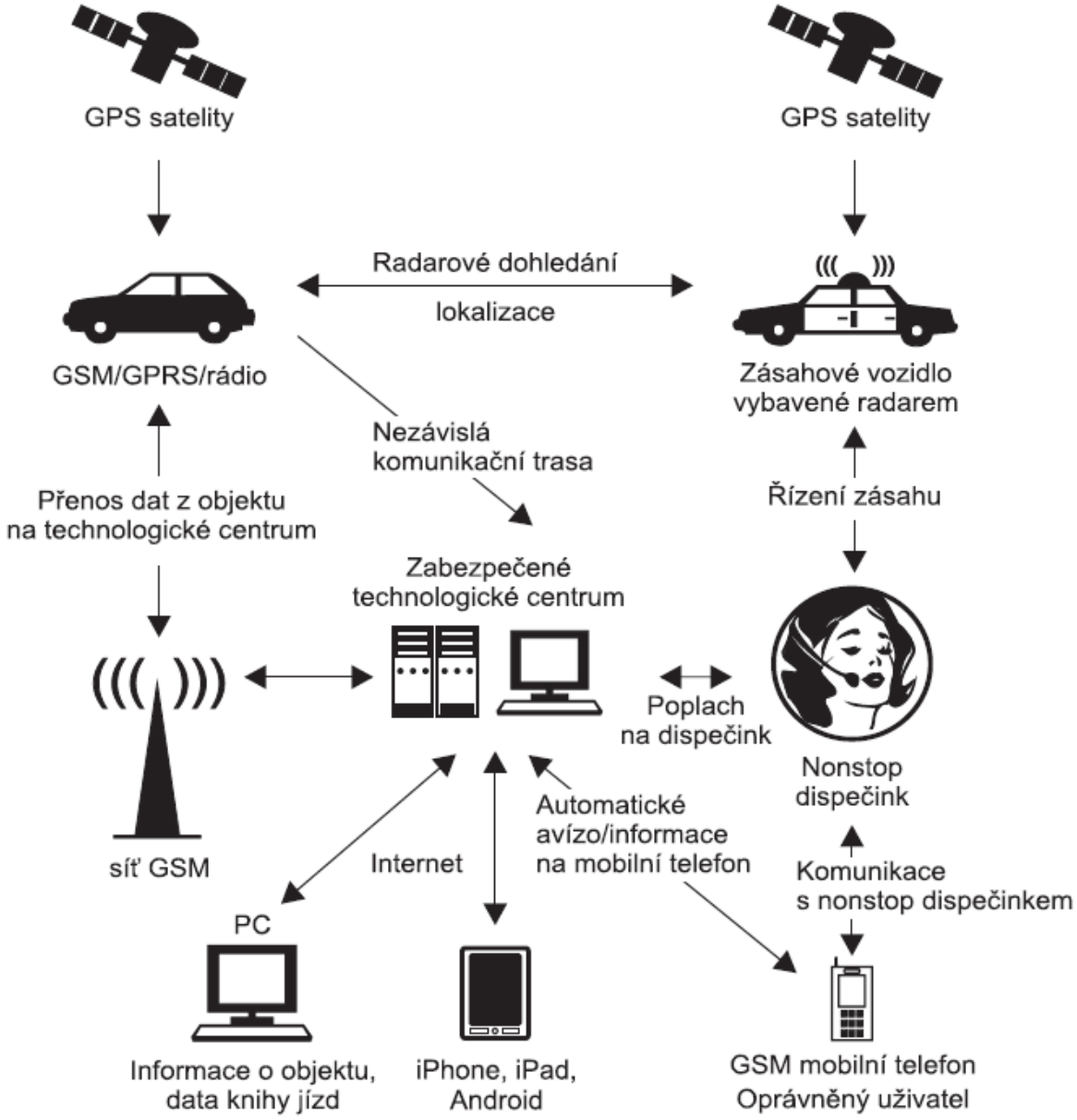
(Převzato: http://www.onisystem.cz/produkty)

Funkce	ONI Sledování	ONI Sledování plus	ONI střežení
Sledování vozu	☑	☑	☑
Kniha jízd	☑	☑	☑
Zpracování cestovních příkazů	☑	☑	☑
Aktivní monitoring	☑	☑	☑
Sleva na pojištění	☑	☑	☑
SMS o odtahu		☑	☑
SMS o krádeži		☑	☑
SMS o havárii		☑	☑
Radarové dohledání			☑
Identifikace řidiče	☑		☑
Napojení na PCO			☑
Docházkový systém	☑		☑
Funkčnost v zahraničí	☑	☑	☑
Výkazy o provozu vozidel	☑	☑	☑
Záznam trasy	☑	☑	☑
Kontrola dodržování rychlosti	☑	☑	☑

Pro účely společnosti PENTA, spol. s r.o. byly zvoleny varianty ONI Sledování a ONI střežení z důvodu přítomnosti funkce Identifikace řidiče. Tato funkce zajišťuje to, aby každé jízdě byl přiřazen konkrétní řidič, který vozidlo v danou dobu používal. Tento parametr se přenáší i do elektronické knihy jízd.

Princip funkce je založen na neustálém sbírání polohy vozidla pomocí čipu GPS, tyto informace jsou ukládány do vnitřní paměti jednotky. Dále se v jednotce shromažďují údaje o stavu vozidla a údaje ze čtečky karet. V pravidelném intervalu jsou tyto údaje vyslány přes GPRS modem do technologického centra. Odtud je možné údaje získat pomocí software knihy jízd nebo pomocí webového prohlížeče. U služby ONI Střežení se odesílání dat provádí každých 20 sekund, u služby ONI Sledování je tento interval volitelný, pohybuje se od 20 sekund do 5 minut v závislosti na použitém tarifu. Standardně se u služby ONI sledování využívá tarif o intervalu 5 minut.

Při využití služby ONI Střežení je nutná funkce identifikace řidiče. Pokud se oprávněný řidič „přihlásí“ do vozidla pomocí čtečky a RFID karty, může vozidlo nastartovat a využívat jej. Pokud se pokusí vozidlo využít neoprávněný uživatel nebo dojde ke krádeži kol, celého vozidla či k poškození vozidla na parkovišti, je vyslán poplach na technologické centrum. Operátor technologického centra informuje oprávněné osoby nebo zajistí zásah bezpečnostní agentury a ta vozidlo dohledá.



Obr. 23 Princip fungování služby

(Převzato: http://www.onisystem.cz)

3.5.2 Hardware

Hlavním stavebním prvkem systému je řídící a vyhodnocovací jednotka. Tato jednotka se dodává ve více provedeních, záleží na zvolené službě ONI systém.

Do vozidel, která využívá vedení společnosti, bude použita jednotka ONI Střežení. Jedná se o vozidla s vyšší pořizovací cenou a tímto způsobem bude zajištěno jejich zabezpečení

proti krádeži. Do ostatních vozidel bude využita jednotka ONI Sledování, primárním účelem bude zde sledování jízd a uživatelů vozidla.

Obě varianty podporují připojení čtečky RFID karet. Tímto se budou uživatelé identifikovat při používání vozidla.

Volitelně lze systém osadit i sledováním stavu PHM, bohužel se však jedná o nákladné rozšíření, pro účely firmy bylo toto vyhodnoceno jako neekonomické z důvodu vysoké pořizovací ceny (cca 20 tis Kč na jedno vozidlo).

Montáž všech jednotek bude skrytá, zařízení bude mít skrytou i anténu GPS/GSM.

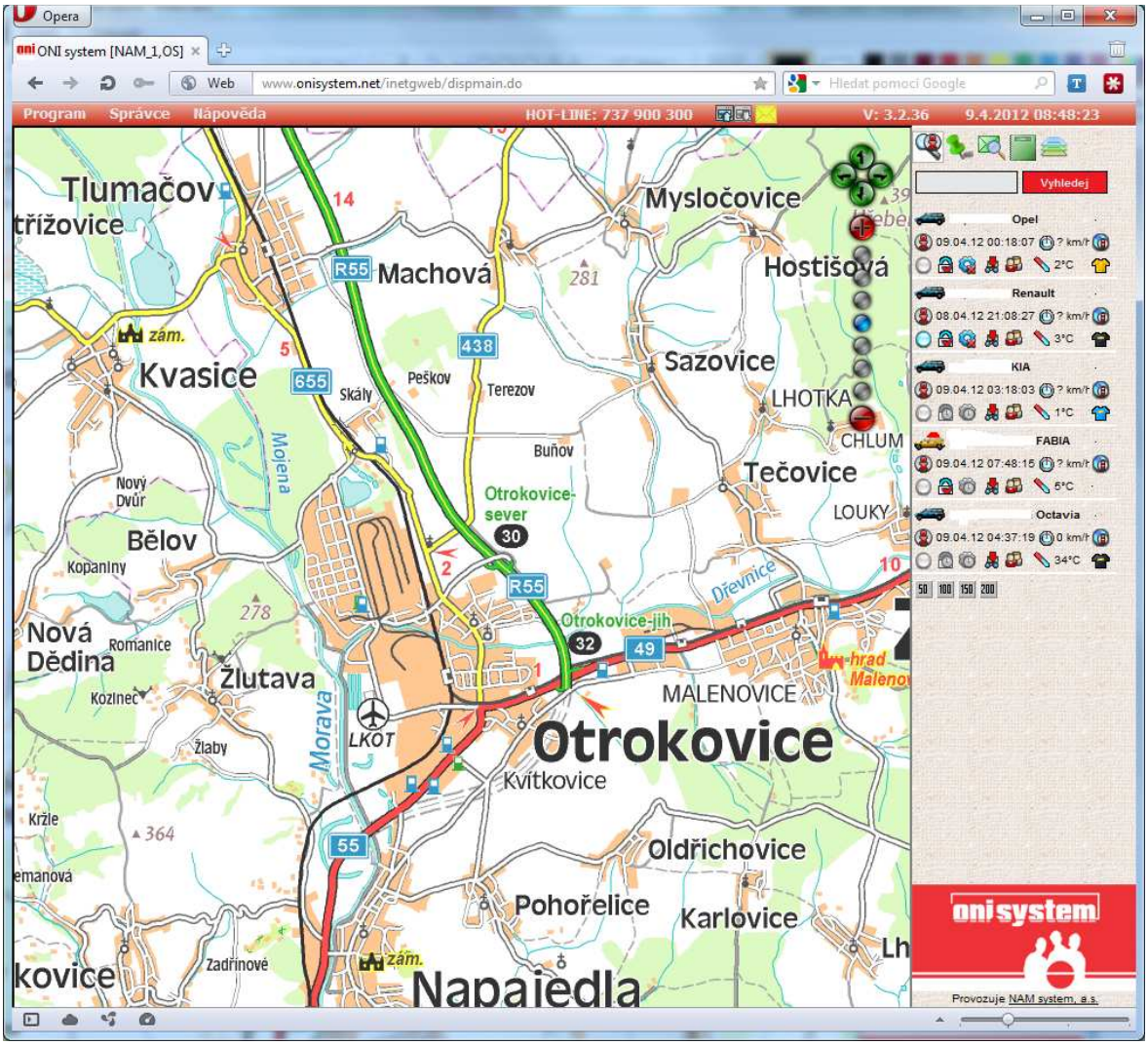
Všechny jednotky obsahují akcelerační čidlo, díky němu umí vyhodnotit například havárii vozidla nebo jeho odtažení. Služba ONI Sledování tyto údaje pouze shromažďuje, služba ONI střežení tyto údaje aktivně monitoruje a předává do technologického centra.

3.5.3 Software

Ke každé službě ONI systému je bezplatně dodávána licence programu SPZ 2012 ONI Profesional. Tato licence opravňuje využívat program SPZ 2012 ONI Profesional pro všechna vozidla, která jsou registrována ve službě ONI.

SPZ 2012 ONI Profesional je ucelený systém, sloužící k evidenci a zpracování veškerých údajů, souvisejících s provozem vozidel, který najde využití nejen při evidenci jízd, ale například při správě autoparku (kontroly termínů, garančních prohlídek), v účtárně (cestovní náhrady, silniční daň), při sledování veškerých nákladů na provoz vozového parku, při zpracování elektronicky dodávaných přehledů transakcí firmami CCS, Benzina, OMV, Shell a dalších. Kniha jízd SPZ 2012 ONI Profesional je plně v souladu s platnou legislativou České republiky a pokrývá veškeré potřeby firmy jak ve vztahu k finančním úřadům, tak z hlediska nezbytného kompletního přehledu o vozovém parku.

Aktuální polohy vozidel, informace o jízdách a administraci služeb ONI umožňuje zobrazit webová aplikace (obr. 24).



Obr. 24 Webová aplikace ONI systém

(Převzato: http://www.onisystem.cz/produkty)

K přístupu do webové aplikace ONI systém lze využít jakýkoliv počítač s připojením na internet. Pro bezchybnou funkčnost je doporučen prohlížeč Internet Explorer, avšak pracuje i v prohlížečích jiných. Připojení se k systému bude možné také pomocí vybraných mobilních telefonů s operačním systémem Android či iPhone OS.

3.6 Bezpečností systém

V rámci provozu firmy PENTA, spol. s r.o. byl navrhnut současně i poplachový zabezpečovací a tísňový systém. Tento systém bude zajišťovat jak ochranu majetku tak i samotných zaměstnanců.

3.6.1 Ochrana proti vniknutí nepovolaných osob

Základem poplachového zabezpečovacího a tísňového systému je zabezpečovací ústředna Digiplex Evo192. Ústředny DIGIPLEX EVO 48/192 jsou určeny pro střední a velké objekty do maximálního počtu 192 zón a 8 podsystémů. Jde o plně adresovatelný sběrnicový systém, do kterého lze zařadit až 254 sběrnicových modulů (klávesnice, bezdrátová nadstavba, expandery, PGM výstupy, doplňkové zdroje, posilovač sběrnice, hlasová nadstavba) i samostatné sběrnicové detektory BUS.

Vedle klasických NC zón s výstupem relé (připojené na vstupy ústředen, expanderů nebo klávesnic) a zón tvořených sběrnicovými detektory (PIR vnitřní i venkovní, magnetický kontakt, detektor tříštění skla, stropní detektor) lze tvořit i bezdrátové zóny připojením k bezdrátové nadstavbě.

Obr. 25 Set zabezpečovací ústředny Digiplex Evo192

(Zdroj: http://www.variant.cz/zbozi/0702-179-evo192-box-s-40-k641)

Systém bude ovládán pomocí klávesnice a bezkontaktních identifikačních medií a bude napojen na PPC (poplachové přijímací centrum).

Ochranu proti vniknutí nepovolaných osob budou tvořit PIR detektory a detektory tříštění skla. Detektory tříštění skla budou umístěny u všech prosklených oken. Detektory PIR budou zajišťovat kanceláře a všechna místa, odkud by pachatel mohl vniknout do objektu.

Na vnějším plášti budovy bude umístěna zálohovaná siréna.

Deaktivaci systému bude prováděna na klávesnici umístěné u hlavního vstupu. Tato klávesnice obsahuje i čtečku RFID médií, zaměstnanci mohou tento systém ovládat stejným ID médiem, které je určeno pro ovládání docházkového systému.

V případě poplachu bude spuštěna siréna a poplachová zpráva bude přenesena na PPC (poplachové přijímací centrum) bezpečnostní agentury.

Obr. 26 Pohybový detektor Digigard 55

(Převzato: http://eurosat.cz/425-digigard-55.html)

3.6.2 Ochrana proti požáru

Do systému PZTS budou zapojeny také opticko-kouřové detektory SD-325AR. V případě požáru bude poplachová zpráva přenesena na PPC bezpečnostní agentury.

Obr. 27 Opticko-kouřový detektor SD-325AR

(Převzato: http://eurosat.cz/2690-sd-325ar.html)

3.6.3 Detektor mrtvého muže

Vzhledem k 24hodinovému provozu a případům, kdy bývá počet zaměstnanců na pracovišti často, obzvláště v nočních hodinách, omezen, byl navržen i systém obsahující „detektor mrtvého muže“. Tento systém přináší zaměstnancům ochranu a možnost

přivolání pomoci v nebezpečných situacích. Důvodem návrhu tohoto systému je např. možnost výskytu toxických zplodin při nedodržení technologických postupů u některých vulkanizací nebo možný úraz z důvodu nesprávného postupu při obsluze strojů, všechny tyto eventuelní situace mohou ohrozit život a zdraví pracovníka.

Jedná se o dvou tlačítkový tísňový kapesní vysílač, který umožňuje detekci pádu, obsahuje také ochranu proti vytržení. Toto zařízení umožňuje vysílat signál v případech, kdy se zaměstnanec ocitne v nouzi nebo například v bezvědomí. Zařízení detekuje úhel naklonění, při detekci naklonění je vydán předpoplachový zvukový signál. Pokud na něj zaměstnanec nezareaguje, je vyslán signál pádu. Ovladač má na sobě umístěné tlačítka, pomocí kterých lze zařízení otestovat a hlavně je zde přítomno tlačítko nouze. Po stisknutí tlačítka je vyslán signál pro přivolání pomoci.

Zařízení se skládá z kapesního vysílače MDT 122 a bezdrátového přijímače. Přijímač je zapojen do ústředny PZTS.

Signály jsou dále přenášeny na poplachové přijímací centrum bezpečnostní agentury.

Obr. 28 Detektor mrtvého muže SpiderAlert MDT-122 S

(Převzato: http://www.visonictech.com/Emergancy-Call-Man-Down-Transmitter-SpiderAlert.html)

Zařízení nijak nesleduje geografickou polohu zaměstnance, při použití v rozsáhlejších budovách je rozlišení přibližné polohy prováděno pomocí rozmístění více přijímačů. Pro podmínky firmy PENTA, spol. s r.o. je dostačující pouze jeden přijímač. Hlavní myšlenkou je přivolání pomoci, dohledání osoby již nebude v relativně malé budově problém.

3.7 Analýza monitorovacího a bezpečnostního systému

Všechny navržené systémy sbírají data a bude prováděna jejich archivace. Tyto data budou sloužit jako prvek ochrany pracoviště a zaměstnanců, bude tak možno dohledat sporné případy. Je samozřejmě nutné zabezpečit, aby tyto data nebyla zneužita.

Pro zaměstnavatele může systém přinést optimalizaci nákladů, měl by zvýšit pracovní morálku zaměstnanců. Vedení bude mít větší přehled o chodu firmy. Zároveň dojde k ulehčení vedení povinné evidence a legislativy.

Důležitým krokem při realizaci je podrobné seznámení zaměstnanců s novým bezpečnostním systémem. Zejména kamerový systém může vyvolávat určité averze.

Navrhnutý bezpečnostní systém poskytuje naprostý přehled o pohybu zaměstnanců či nepovolaných osob, je možné jej i vzdáleně dohlížet přes internet.

4 POSOUZENÍ MONITORINGU Z PRÁVNÍHO A ETICKÉHO HLEDISKA

Pokud se rozhodneme pro aplikaci některých prvků monitoringu, je třeba si uvědomit následující. Přes to, že náš vztah k monitorovanému je pracovněprávní, jedná se o mnohdy o výrazný zásah do soukromí zaměstnance. Soukromí je skutečně v naší civilizaci považováno za hodnotu, která má i v právním řádu mnoha států dlouhou historii. Jen stručně a na okraj připomenu: Začíná v Anglii už roku 1361 tzv. the Justice of the Peace Act, v roce 1776 je regulován přístup k soukromým záznamům ve Švédsku, roku 1858 dochází k zákazu zveřejňovat soukromé záležitosti ve Francii, roku 1889 zakazuje Norsko zveřejňování informací týkajících se osobních a domácích záležitostí; samozřejmě největší posun v chápání práva na soukromí přichází ve 20. století po druhé světové válce, když Spojené národy roku 1948 vyhlašují Všeobecnou deklaraci lidských práv. Při posuzování vhodnosti a vymezení míry přiměřenosti monitoringu je třeba se řídit nejen zákonem, ale také brát v potaz etické hledisko věci, pomoci v rozhodování nám může také studium reálných soudních kauz. Při hledání hranice vhodnosti monitoringu bychom se měli v první řadě řídit tím, že zaměstnanci jsou především lidé a ne stroje, u kterých za své peníze požadujeme 100 % pracovní nasazení za každých okolností. Při nasazování jakéhokoli formy monitoringu bych vždy doporučoval o tomto zaměstnance náležitě informovat, neboť dle mého názoru, již tento fakt samotný bude zaměstnance nutit k vyšším pracovním výkonům.

4.1 Právní náhled na věc

Problematika monitoringu zaměstnanců je z hlediska práva dosti složitá a rozsáhlá, znění zákonů, které se této problematiky týkají, si ne vždy lze jednoduše vyložit. V některých případech je tak opravdu obtížně určitelné, co je dle zákona povoleno a co nikoli, také názory právníků se různí. V následujících řádcích se pokusím tuto problematiku zhodnotit.

Zaměstnanecké právo nám mimo jiné ošetřuje Zákon č. 262/2006 Sb., zákoník práce, dále jen ZP, z něhož je pro oblast monitorování na pracovišti nejpodstatnější §316. Odstavce 1 až 3 ustanovení § 316 zákoníku práce, které uvádějí, že zaměstnanci nesmějí bez souhlasu zaměstnavatele užívat pro svou osobní potřebu výrobní a pracovní prostředky zaměstnavatele, včetně výpočetní techniky ani jeho telekomunikační zařízení. Tyto prostředky je zaměstnanec povinen používat zásadně k výkonu práce a v jeho souvislosti

(§ 316 odst. 1 ZP), pokud neexistuje mezi stranami dohoda jiná. V případě neoprávněného používání pracovních pomůcek k osobní potřebě, by tak docházelo k neoprávněnému obohacování na úkor zaměstnavatele, tento čin však nelze trestat finančními postihy, jedná se ale o porušování povinností dle § 52 písm. g) ZP. Zaměstnavatelé jsou oprávněni přiměřeným způsobem dodržování těchto příkazů kontrolovat (§ 316 odst. 1 ZP). Otázkou tedy není, zda lze kontrolu provádět, ale co se vlastně skrývá pod slovem přiměřená kontrola. § 316 ZP tak dle mého názoru legalizuje kontrolu těchto prostředků, ke kterým pak není třeba souhlasu zaměstnance, ovšem stanovuje povinnost informovat o rozsahu a způsobu, jakým je kontrola prováděna.

Pokud však není zaměstnavatelem prováděna činnost zvláštní povahy, pak by prostředky jmenované v § 316 odst. 2 ZP, nebylo možné použít. Vzhledem k tomu, že použití těchto prostředků zákon přímo zakazuje, tak ani souhlas zaměstnance samotného, že s touto kontrolou souhlasí, byť přes nezanedbatelnost základních práva a svobod, považujeme za irelevantní, neboť by to bylo v rozporu s § 19 odst. 1 ZP. Z hlediska zvláštní povahy činnosti je třeba poznamenat, že tato nebyla prozatím přesně definována a dokonce ani vyšší soudy v ČR dosud nerozhodovaly žádný případ stanovující měřítka, na jejichž základě by bylo možno tento pojem rozklíčovat. Obecně je však uvažováno to, že se jedná především o činnosti, u nichž je třeba chránit informace (ochrana obchodního tajemství, činnosti pracující s různými stupni utajování a zvláštních režimů, počítačové firmy), nebo o činnosti, kde je sledování zaměstnanců nutné pro ochranu zdraví osob (např. nebezpečné tovární provozy, policejní služebny, vězeňské služby), a také činnosti, kde je třeba sledování nasadit z důvodu ochrany majetku zaměstnavatele (banky, čerpací stanice). Za legitimní důvod použití prostředků monitoringu je dle literatury [25], považována také ochrana majetku zaměstnance.

Ze zákona tedy vyplývá, že pokud však lze kontrolu provádět jinými než speciálními monitorovacími prostředky, pak je užití speciálních monitorovacích prostředků protiprávní. Z výše uvedeného si můžeme dovodit, že monitorovací systémy jako jsou odposlech, záznam telefonních hovorů, kontrola obsahu elektronické či listovní pošty adresované zaměstnanci, tedy zákon nedefinuje jako přiměřený způsob kontroly.

Pokud jsou zaměstnavatelem k monitorování nasazeny některé z výše uvedených monitorovacích prvků, je třeba rozlišovat mezi monitoringem a monitoringem s uchováváním dat, každá úprava totiž podléhá odlišnému režimu. Samotný monitoring bez následného ukládání dat zákon povoluje, za předpokladu, že zaměstnanec byl s rozsahem

kontroly předem, popřípadě ihned po zavedení monitoringu obeznámen. Za obeznámení se pak předpokládá např. podpis pracovní smlouvy či v případě nasazení monitoringu v průběhu pracovněprávního vztahu to, že zaměstnanec nepodá výpověď. Monitoring v reálném čase pak současně nesmí narušovat integritu osobnosti zaměstnance.

Pokud je však na pracovišti nasazen typ monitoringu s následným uchováním dat, pak se dle § 5 odst. 2 ZOOÚ jedná o zpracování osobních údajů a o takovémto jednání je pak třeba informovat Úřad pro ochranu osobních údajů a také získat od subjektu údajů (zaměstnance) výslovný souhlas. Dle zákona o ochraně osobních údajů nese právní odpovědnost za osobní údaje získané z kamerového systému zejména správce. Za správce je považován ten, kdo určuje účel a prostředky zpracování osobních údajů § 4 odst. j) ZOOÚ. Správce může na základě pověření určit k této činnosti zpracovatele, pokud zákon tuto možnost nevylučuje § 4 odst. k). Přesto, že správce na základě určitého právního úkonu určí zpracovatele osobních údajů, nevyvazuje se z mnoha povinností, které jsou dány zákonem. Zákon na ochranu osobních údajů mnohé nejzákladnější povinnosti stanovuje pouze správci. Těmito nejzákladnějšími povinnostmi jsou zejména: oznamovací neboli registrační povinnost dle § 16, práva a povinnosti při zpracování osobních údajů dle § 5, poučení subjektů údajů dle § 11. Jiná ustanovení zákona dávají povinnost správci i zpracovateli, a to zejména při zabezpečení osobních údajů dle § 13. Každý, kdo má povinnost provést oznamovací povinnost o zpracování osobních údajů, a tuto si nesplní, se vystavuje riziku postihu za přestupek dle ustanovení § 44 odst. 2, písm. i) s pokutou až do výše 1 milionu korun.

Pokud by však byly naplněny podmínky ustanovení § 316 odst. 2 ZP, takovéto zpracování by teoreticky mohlo spadat do výjimky dle ust. § 5 odst. 2 písm. e) ZOOÚ. V tomto případě není souhlas subjektu třeba, avšak zaměstnanec musí být o zaváděných monitorovacích prvcích přesto informován. Za informování zaměstnance je dle mého názoru možno považovat informaci o rozsahu a způsobu kontroly, jakým je kontrola prováděna. Uvažujme případ, kdy zaměstnavatel uvede do provozu monitorovací kamerový systém dle ust. § 5 odst. 2 písm. e) ZOOÚ, v tomto případě se dle mého názoru za informování zaměstnanců dá považovat opatření dveří samolepkou informující zaměstnance o probíhajícím monitoringu kamerovým systémem, neboť lze předpokládat, že zaměstnanec těmito dveřmi vchází na pracoviště a vstupem do monitorovaných prostor se tak stává informován.

V případě využití kamerového systému je třeba posoudit, zda se jedná o oprávněné sledování za účelem ochrany zájmů zaměstnavatele či o narušení soukromí zaměstnanců a kontrolou jejich pracovní výkonnosti. Dle literatury [25] by totiž monitorovací kamerový systém neměl sloužit k mapování pracovní výkonnosti zaměstnance, neboť k tomuto účelu je zaměstnavatelem zaměstnán především vedoucí pracovník, v případě využívání tohoto kamerového systému k tomuto účelu by se jednalo o porušení zákona, pokud by zde opět neexistoval důvod dle § 316 odst. 2.

V případě monitorování telefonních hovorů je, dle stanoviska ÚOOÚ 2/2009 [28], třeba obsah komunikace veškerých hovorů považovat za zaměstnavateli utajený i v případě, že se rozhovor týká jeho zájmů. Ovšem obecné údaje, jako jsou třeba délka telefonního hovoru, ID volaného je dle ustanovení § 316 odst. 1 ZP zaměstnavatelem možné monitorovat.

U emailových adres se má za to, že pokud tato adresa obsahuje identifikátor zaměstnance (zpravidla jméno a příjmení, který daného zaměstnance identifikuje), je třeba s nimi nakládat stejným způsobem jako v případě výše uvedeném. Jiná situace však nastává tehdy, pokud emailová adresa obsahuje před znakem @ pouze obecnou informaci (např. info, sklad, uctarna aj.), v takovém případě je možné tuto schránku plně monitorovat.

Absurdním se stává názor o nemožnosti monitoringu emailové pošty zaměstnance, v případě, pokud by zaměstnanec např. rozesílal z firemního e-mailu bez povolení a vědomí svého zaměstnavatele spamovou elektronickou poštu. Zaměstnanec by tím vedle pracovně právních předpisů porušil i ust. § 93 ZoEK 127/2005 Sb., který zakazuje zneužití elektronické adresy odesílatele, což znamená, řečeno slovy zákona, že „použít adresu elektronické pošty pro odeslání zprávy nebo zpráv třetím osobám bez souhlasu držitele této adresy elektronické pošty je zakázáno.“ Zaměstnanec by se tak též dopouštěl přestupku dle ust. § 120 odst. 1 písm. g) a h) ZoEK, a za takový přestupek je možno uložit pokutu až 100.000,- Kč. Mnohem závažnější však je, že pokud by takový zaměstnanec rozesílal spamovou poštu, a zaměstnavatel by neměl účinný systém kontroly v této oblasti, nastala by velmi nebezpečná situace pro zaměstnavatele, protože by neměl jak prokázat exces, a také protiprávní jednání svého zaměstnance, resp. ani by o něm nevěděl, ačkoliv by v každém případě zaměstnavatel odpovídal za správní delikt rozesílání spamové elektronické pošty z firemního e-mailu ust. § 118 odst. 1 písm. j) ZoEK. Možná pokuta za takový delikt zaměstnavateli právnické osobě nebo podnikající fyzické osobě je značná - až do 10 % z výnosů dosažených za poslední ukončený kalendářní rok, a je pro zaměstnavatele jen

malou útěchou, že nejvýše může činit taková pokuta 10.000.000,- Kč ust. § 118 odst. 11 ZoEK.

Na monitorování práce s počítačem se dle mého názoru ustanovení § 316 odst. 1 ZP nevztahuje, jelikož tento způsob kontroly není ve výčtu prostředků uveden, počítač je tedy možno plně monitorovat, je však nad míru vhodné o tomto zaměstnance informovat.

V případě využití prostředků pro monitorování vozidel GPS, je jejich použití zpravidla v souladu se zákony, a to v případech, pokud se jedná o sledování vozidla za účelem zjištění jeho polohy pro případ zcizení tohoto vozidla. Primárně totiž tento systém neslouží k zjištění polohy zaměstnance, ale ke zjištění polohy vozidla. Pokud se bude jednat ze strany zaměstnavatele také o sledování trasy "soukromých" jízd pravděpodobně se bude dopouštět porušení povinnosti stanovené v § 5 odst. 1 písm. d) ZOOÚ, tedy shromažďovat osobní údaje odpovídající pouze stanovenému účelu a v rozsahu nezbytném pro naplnění stanového účelu. K tomuto porušování by však docházelo pouze v případě, že by zaměstnanec nebyl zaměstnavatelem obeznámen o tom, že toto vozidlo má instalován sledovací systém GPS, neboť v případě, že je zaměstnanec o tomto faktu informován, je zcela na něm, zda toto vozidlo zaměstnavatele k soukromé cestě použije či nikoliv.

4.2 Etický náhled na věc

V následujících řádcích se pokusím jednotlivé části monitorovacích systémů zhodnotit z etického hlediska. Pro zjištění toho, jak se na otázky ve věci monitoringu dívají lidé v České republice, jsem vytvořil dotazník, který je přílohou této diplomové práce. Výsledky provedeného průzkumu jsou zevrubně popsány v kapitole 4.3.

4.2.1 Etika

Co to vlastně je Etika? Mnozí z nás si představí pod tímto pojmem to, že bychom se k sobě měli chovat hezky a důstojně, jak by se od občana civilizovaného evropského demokratického státu očekávalo. Ano, etika je vlastně takový koordinátor chování každého jedince, říká nám, co můžeme a co bychom neměli. Tyto obecné pravidla nejsou nikde celistvě napsány, sestávají se totiž z mnoha různých regulátorů chování lidí, právních norem či třeba státních nařízení. Etické chování je však často zaměňováno se našimi přáními, osobními zájmy a pod rouškou dodržování lidských práv či etického chování se pak dožadujeme splnění našich požadavků. Etika hraje zcela jistě velmi významnou roli v komunikaci, mezilidských vztazích a je nepostradatelná v každém profesním chování a

jednání. Etika je velmi obtížně definovatelná, k jejímu upřesnění vytvářejí dnešní společnosti vlastní etický kodex, kde se každý člen konkrétní společnosti dozví, co je tolerováno a co už je za hranicí etiky. Etický kodex může být závazný, tzn. podepsán každým zaměstnancem společnosti nebo nezávazný a pak je jeho dodržování dobrovolné. Jejich užití je typické v lékařských, právnických, novinářských nebo učitelských profesích. V následujících řádcích se pokusím vyjádřit svůj názor k problematice monitorování zaměstnanců z etického hlediska.

4.2.2 Posouzení monitoringu z hlediska etiky

Aby bylo monitorování etické, musí být jeho důvod zcela legitimní a toto sledování musí být veřejné, v žádném případě se nesmí jednat o skrytý monitoring. Prostředky monitoringu musejí jednoznačně odpovídat našemu cíli, měla by existovat důvodná možnost, že toto monitorování dopomůže k odhalení určitého nepatřičného chování, kterému předcházelo naše podezření, či tomuto chování zabrání. Dále je nutno stanovit k jakému účelu bude výstupní materiál použit, jak bude s daty nakládáno a komu bude tento úkol svěřen. Důležité je také rozdělení stejnou měrou, nelze rozlišovat zaměstnance dle rasy, barvy pleti, pohlaví, sexuální orientace, jazyka, víry a náboženství, politického nebo jiného smýšlení, členství nebo činnosti v politických stranách nebo politických hnutích, odborových organizacích a jiných sdruženích, národnosti, etnického nebo sociálního původu, majetku, rodu, zdravotního stavu, věku, manželského a rodinného stavu nebo povinností k rodině. Měli bychom se vyvarovat rozdělení pracovních skupin, tzn. ne sledovat jedno oddělení a druhé ne. Informace shromážděné pro jeden účel nesmějí být použity pro účel jiný. Nesmíme také zapomenout na pečlivé zabezpečení získaných dat a to nejen elektronicky, ale také personálně, vhodné je pověření dalšího zaměstnance, který bude kontrolovat dohledové oddělení či daného zaměstnance, který je monitoringem primárně pověřen. Monitorované zaměstnance je třeba předem řádně seznámit s účelem a adekvátností monitoringu. Při vhodném objasnění situace budou zaměstnanci schopni pochopit mnohem lépe to, proč je vlastně chceme sledovat. Je třeba zaměstnance ujistit, že v žádném případě nebude narušeno jejich soukromí a nebudou porušena jejich osobní práva. Vždy bychom se měli snažit nedovolenému chování na pracovišti předcházet pomocí dostupných nástrojů či prostředků, než později nasazovat monitoring zaměstnanců. Chceme-li, aby zaměstnanec věnoval celou svou osobnost ve prospěch zaměstnání a hlavně svého zaměstnavatele, kterému má přinášet zisky, je třeba, aby jeho osobnost tohoto zaměstnance byla v pracovních vztazích náležitě respektována.

Kamerové systémy

Použití kamer či kamerového systému v bankách, obchodech, nebo na benzinové stanici je zcela jistě v souladu s etickými normami, neboť se prokazatelně jedná o zabezpečení majetku těmito prostředky před případnou krádeží či poškozením. Jiná situace nastává tehdy, je-li kamerový systém použit ke sledování prostor, ve kterých je osobami předpokládáno soukromí a to například v šatnách, sprchách, umývárnách na toaletách či ve zkušebních kabinkách prodejny. Neetické bude také nepochybně sledování administrativních pracovníků v kancelářích, kde je riziko ztráty a poškození majetku minimální. Ke sledování pracovních výkonů těchto administrativních pracovníků bude vhodné použít jiných monitorovacích nástrojů. Aby byla splněna podmínka etičnosti, je vždy třeba obeznámit sledované vhodnou formou o tom, že jejich soukromí je ve sledovaném prostoru narušeno.

Odposlouchávací zařízení prostor

Použití této metody monitoringu je obecně považováno za neetické a to bez ohledu na to zda je skryté či veřejné. O výjimku by se mohlo jednat v případě záznamu z porady za souhlasu všech zúčastněných, kde je vysoký předpoklad toho, že se nebude jednat o soukromých záležitostech a údaje na poradě zmíněné nebudou mít charakter osobních údajů jednotlivce.

Kontrola vstupu a vjezdu, docházkové systémy

Kontrola tohoto charakteru je obecně vnímána jako přípustná, obzvláště pokud se jedná o zaměstnance. Je vlastně jakýmsi ekvivalentem „píchacích hodin“ a slouží k vyhodnocení doby strávené v zaměstnání. Zaměstnanec se takto vlastně prokazuje, že vstupuje, popř. vjíždí na místo, které je v majetku zaměstnavatele a začíná svou pracovní dobu, což nahrazuje fyzickou ostrahu objektu.

Monitorování přítomnosti osob v zabezpečených prostorách

Sledování prostor pomocí PZTS je ryze bezpečnostním prvkem, jeho zneužití v neprospěch zaměstnance není prakticky možné, jedná se tedy opět o prvek monitoringu, jenž je v souladu s etickými normami.

Monitorování telefonních hovorů

Zde záleží na charakteru společnosti využívající monitoring hovorů, bude-li se jednat o složky IZS je monitoring zcela na místě, jinak tomu bude v případě monitorování

pracovníků zabývajících se stavební činností. Tento způsob monitoringu je hojně využíván v call centrech velkých společností pod záminkou zkvalitňování služeb, ne vždy však slouží pouze k tomuto účelu. Volající strana je sice ve většině případů upozorněna na probíhající monitoring, ovšem pokud chce svůj problém vyřešit, nemá na výběr jinak, než s monitoringem souhlasit a v hovoru pokračovat, ne vždy se tedy jedná o etický přístup. Při použití tohoto monitorovacího systému je nutno brát v potaz případy, kdy je zaměstnancům povoleno využívat své mobilní telefony současně pro soukromé účely po pracovní době, byť za úhradu poměrné části účtu, v tomto případě by měl být monitorovací systém nastaven tak, aby byl aktivní pouze po dobu pracovní doby, nebo by mělo být zaměstnanci umožněno tento systém deaktivovat. Jako eticky přiměřené bych ve většině případů doporučil monitorovat pouze ID volaného a délku hovoru.

Monitorování emailové pošty

Zde je nutné přihlédnout k charakteru zasílaných zpráv, kontrola emailových zpráv zaměstnanců je jistě etická pouze za předpokladu, že se jedná o zprávy zaslané výhradně z firemní schránky zaměstnance a mající formu pracovní, nikoli soukromou. Zde je na zaměstnavateli jakým způsobem vymezí používání jeho emailových schránek, pokud zaměstnavatel nenařídí použití pouze k pracovním účelům, pak je možné takto monitorovat pouze hlavičky zpráv nikoli celý text (tělo) zprávy. Monitorování soukromých emailových zpráv je z hlediska etiky zcela nepřípustné i za předpokladu, jednalo-li by se o zprávu zaslanou zaměstnancem v pracovní době.

Monitorování firemního PC

Vzhledem k tomu, že počítač lze využít i jinak než k pracovním účelům, je třeba opět stanovit rozsah jeho použití, pokud je zaměstnancům používání PC k osobním účelům v pracovní době povoleno, byť jen v malé míře, není vhodné tyto počítače sledovat v plném rozsahu. Určitě bych nedoporučoval sledování a shromažďování dat zadaných prostřednictvím klávesnice, neboť by se mohlo jednat o shromažďování osobních nebo soukromých údajů zaměstnance. Vezměme třeba příklad zaměstnance, který zapomněl z domu odeslat platbu za elektřinu a využil by k tomuto účelu a se souhlasem zaměstnavatele jeho pracovní prostředek, v tomto případě počítač. Za tohoto předpokladu by zaměstnavatel získal přístupové údaje k bankovnímu účtu zaměstnance, takovéto jednání by nebylo za prvé etické a za druhé by sebou neslo vysoké bezpečnostní riziko zneužití. Za etické je možné dle mého názoru považovat monitorování doby strávené

prohlížením internetu a adres navštívených stránek, názvy a doba činnosti aplikací, obsah pevných disků počítače a externích nosičů dat.

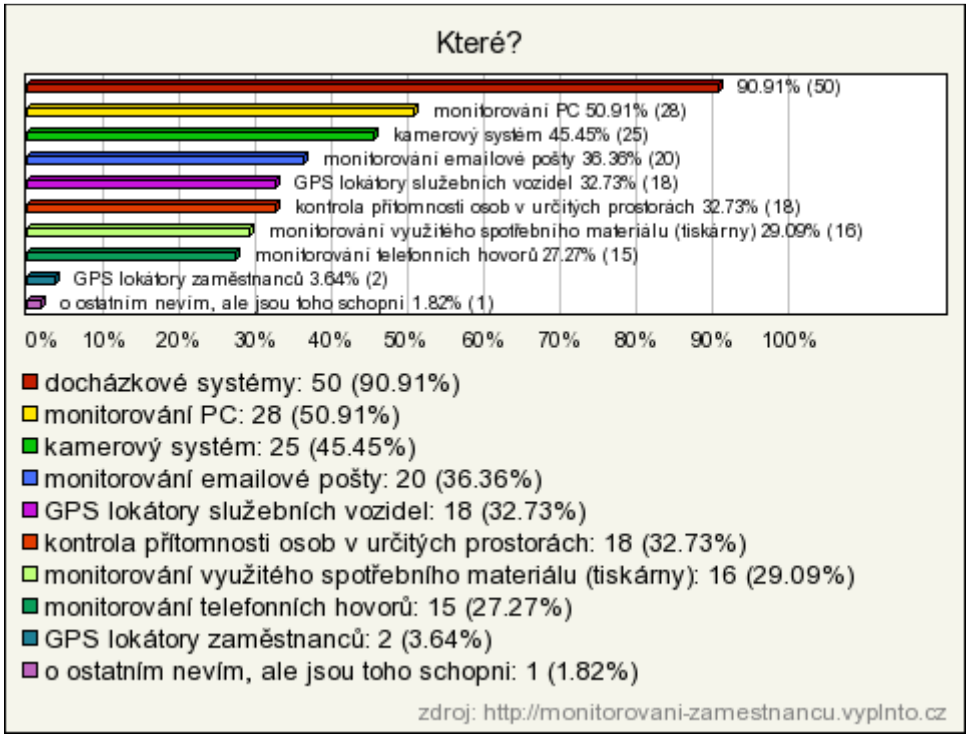
Monitorování pomocí GPS

Sledování polohy zaměstnance je možno považovat za etické za předpokladu, že slouží k zajištění jeho bezpečnosti nebo bezpečnosti majetku zaměstnavatele. Typickým příkladem může být například lokace pracovníků při těžbě dřeva, kde systémy GPS slouží v kombinaci s detektorem mrtvého muže k zajištění bezpečnosti zaměstnanců při výkonu povolání. Zaměstnavatel nebo vedoucí pracovník tak může pohotově reagovat na vzniklou situaci a zachránit zaměstnanci dokonce i život. Jako etické můžeme brát také GPS sledování kufru peněz přepravovaného do banky, nebo dnes často používané GPS lokátory vozidel. U sledovaných vozidel pomocí systému GPS je na místě umožnit zaměstnanci dočasné vyřazení systému z provozu v případě, že vozidlo je v souladu s legislativními předpisy a na náklady zaměstnance schváleno k užívání k osobním účelům.

4.3 Výsledky provedeného průzkumu

Ke zjištění stavu veřejného mínění týkajícího se sledování zaměstnanců jsem vytvořil dotazník, který je přílohou této diplomové práce. Dotazník obsahuje 29 otázek, některé z nich větvící se v závislosti na dané odpovědi. Na tento dotazník odpovědělo 118 respondentů, z nichž bylo 53,39 % mužů, zbývající část tvořili ženy. Převážná většina respondentů byla ve věku 20-35 let, středoškolsky a vysokoškolsky vzdělaných. Z průzkumu vyplívá, že 51,69 % dotázaných považuje monitorování zaměstnanců za etické a tedy přijatelné, mnozí z nich s určitými výhradami. Respondenti, kteří nepovažují monitorování za etické, tak odpovídají převážně z důvodu možného pocitu neustálého sledování a narušení jejich soukromí. Ti dotázaní, kteří odpovídali na otázku „Myslíte si, že je morální a etické monitorovat činnost zaměstnanců“ ANO, dále v dotazníku vyzdvihnuli, že je pro ně přijatelné monitorovat pomocí docházkových systémů (88,98%), EZS (60,17%), GPS vozidel (50,85%) a monitorování využitého spotřebního materiálů (44,07%), ostatní prvky monitorování jako jsou monitorování PC, emailu, telefonu, GPS osob a také použití kamerového systému na pracovišti je pro ně příliš invazivní. Na otázku zdali by se mohlo stát, že by dotázaní byli monitoringem v zaměstnání nějakým způsobem negativně ovlivněni, odpovídalo více než 60 % dotázaných, že ano a to opět z důvodu zásahu do soukromí, pocitu sledování, nervozity a také snížené pracovní výkonnosti. Nutno podotknout, že nadpoloviční většina dotázaných byla v době průzkumu v pozici

zaměstnance pracujícího jako řadový pracovník nebo střední management. 73,61 % těchto zaměstnanců odpovědělo, že jejich zaměstnavatel užívá některých prvků monitoringu ke sledování jejich činnosti. V následujícím grafu je znázorněn podíl použitých prvků monitoringu.



Obr. 29 Podíl používaných monitorovacích prvků

(Převzato: http://monitorovani-zamestnancu.vyplnto.cz)

Z výše uvedeného (obr. 29) tak vyplívá, že zaměstnavatelé využívají nejhojněji docházkové systémy, které však zaměstnancům zpravidla nevadí. Avšak výčet následujících používaných systémů monitoringu, jako je PC monitorování, kamerové systémy a dokonce kontrola emailové pošty zaměstnanců, by zaměstnanci raději na pracovišti oželeli. Velice překvapivé je zjištění, že více než 70 % zaměstnavatelů se ke sledování svých zaměstnanců uchýlilo bez předchozího souhlasu jich samotných, pouze něco nad 20 % respondentů v průzkumu odpovídalo, že po nich byl vyžadován podepsaný souhlas, a po 7 % souhlas ústní. S ohledem na výše uvedené je opět překvapením, že 80 % jejich zaměstnanců i přesto považuje monitoring jejich pracoviště za oprávněný. Otázka číslo 17 „Jsou Vašim zaměstnavatelem tolerovány některé z následujících činností (v pracovní době)?“ vypovídá o tom, že skoro polovina zaměstnavatelů je tolerantní vůči svým zaměstnancům a povoluje jim v přiměřené míře užívat pracovních prostředků pro soukromé účely, můžeme se jen domnívat, že tito zaměstnanci tolerance svého

zaměstnavatele nezneužívají. Ve spojení s používáním firemního PC, zaměstnavatelé nejvíce tolerují využívání internetového prohlížeče k nepracovním účelům, více než 73 %, skoro stejná část zaměstnanců si myslí, že používání firemních prostředků k soukromým účelům by mělo být povoleno. Pouze 22,22 % zaměstnanců odpovídá, že v zaměstnání výhradně pracují a soukromé záležitosti si řeší po pracovní době.

Sečteno podtrženo, dotazovaní zaměstnanci se problematice monitoringu stavějí více méně kladně, jsou ochotni tolerovat monitorování na pracovišti, avšak průzkum říká, že jsou velice citliví na své soukromí, které musí být samozřejmě i na pracovišti zaměstnavatelem plně respektováno. Chápou svého zaměstnavatele, že má jistě své důvody, proč monitoring nasazuje, můžeme jen hádat proč tomu tak je, zda kvůli nim samotným či jejich spolupracovníkům. Průzkum vypovídá o tom, že zaměstnanci chtějí, aby jejich zaměstnavatel do jisté míry toleroval soukromé činnosti na pracovišti, a věřím, že by se mu za tento ústupek odvděčili vyšší pracovní výkonností.

ZÁVĚR

Cílem této práce bylo uceleně zhodnotit problematiku monitorování zaměstnanců a pracoviště, a to jak po stránce technické, tak po stránce etické a právní. Výstupem tohoto zhodnocení je navržení přiměřené míry kontroly na pracovišti a to se zacílením na konkrétní společnost.

Práce krok po kroku provádí čtenáře touto problematikou. V teoretické části je popsán význam monitorování a jsou podrobně rozebrány možné formy monitorování a technické prostředky k tomuto účelu sloužící.

V praktické části jsem se v prvé řadě pokusil navrhnout přiměřenou míru monitoringu na pracovištích. Vzhledem k individuálnosti jednotlivých společností a jejich rozdílným potřebám, jsem se rozhodnul podrobněji zaměřit na návrh řešení monitoringu pro konkrétní společnost, a to společnost PENTA, spol. s r.o. Tato společnost byla při tvorbě této práce mým pracovištěm, tudíž jsem znal konkrétní potřeby a slabé stránky společnosti a byl jsem schopen objektivně posoudit stav dané společnosti.

V této práci je navržen komplexní monitorovací systém sloužící především k ochraně zaměstnanců a majetku zaměstnavatele, ale je také přínosem pro zjednodušení některých činností.

Docházkový systém zpřehlední evidenci pracovní doby zaměstnanců a zjednoduší činnosti spojené se zpracováním mezd.

Přístupový systém zabezpečí vstup a vjezd zaměstnanců do vybraných prostor společnosti, avšak pouze těm z nich, kteří mají k tomuto patřičné oprávnění. Dojde tak ke zjednodušení činnosti spojené s přístupem při použití jedinečné přístupové karty, stejná karta bude sloužit také k ovládání docházkového systému.

Součástí návrhu monitorovacího systému je také kamerový systém se záznamem. Tento systém poslouží k účinnému sledování vybraných prostor a dopomůže, v případě potřeby, vedení firmy ke zpětnému náhledu na určitou činnost na konkrétním místě. Kamery budou sledovat i prostory, ve kterých je umístěn docházkový terminál, na základě záznamu bude pak možné dohledat případné neoprávněné činnosti spjaté se vstupem zaměstnanců na pracoviště.

Dalším prvkem navrženého monitorovacího systému je poplachový zabezpečovací a tísňový systém, který bude chránit majetek zaměstnavatele a také zaměstnance samotné.

První část navrženého systému bude zabezpečovat neoprávněný přístup do střežených prostor a bude zajišťovat také ochranu v případě vzniku požáru. Další část poslouží k ochraně zaměstnanců na pracovišti za použití detektorů „mrtvého muže“ jenž budou v případě ohrožení zaměstnance o tomto informovat. PZTS bude přímo propojen s poplachovým přijímacím centrem, pracovníci bezpečnostní agentury tak budou moci pohotově reagovat na nastalou situaci.

Posledním prvkem navrženého monitorovacího systému je monitorovací systém vozidel, tento bude přispívat k ochraně vozidel v případě krádeže, ale pomůže také zjednodušit vedení agendy jízd.

Vytvořený návrh obsažený v této práci dopomohl společnosti PENTA, spol. s r.o. k dosažení optimálních podmínek zabezpečení a monitorování provozu pracoviště a byl pro ni v konečném důsledku velkým přínosem, neboť tento návrh je již nyní ve fázi realizace.

Posledním bodem praktické části je posouzení jednotlivých monitorovacích prostředků z hlediska právního a etického. Pokusil jsem se zde zhodnotit tuto eticky rozporuplnou, mnohdy právně nejasnou problematiku a doporučit tak čtenáři možné způsoby a podmínky provozu monitorovacího systému. Ke zjištění stavu veřejného mínění byl mnou proveden průzkum formou dotazníku zveřejněného na internetu a výsledky tohoto průzkumy byly v této práci zhodnoceny.

ZÁVĚR V ANGLIČTINĚ

The focus of this study was to evaluate comprehensively the issue of monitoring of employees and the workplace, in terms of technique and from the view of ethics and law. The outcome of this evaluation is to propose an adequate degree of monitoring in the workplace in general terms and for a target company too.

This thesis is intended to walk the reader through the topic step by step. The theoretical part describes the importance of monitoring and analyzes the possible forms of monitoring and technical means used for this purpose in detail.

The practical part is primarily an attempt to propose a reasonable level of monitoring in the workplace. Due to the individuality of company and the different needs, I decided to focus on the proposed solution specific society monitoring, and PENTA, ltd. At the same time this company was my workplace, so I knew the specific needs and weaknesses of the company and I was able to objectively assess the status of the company.

The thesis suggests complex monitoring systems which are primarily used to protect employees and assets of the company. As well as simplifies certain work tasks.

The time clock would make the employees work schedule more transparent and help with payroll processing.

Access control system secures the entry and exit of employees to the selected company premises. This will simplify actions related to access using a unique access card. The same card will also control the attendance system.

Part of the monitoring design is video recording system. This system will provide effective monitoring of selected areas and will help to give feedback to the company management. The cameras will monitor important places included the place where time clock is located. Then it will be possible to trace any unauthorized activity related to the entry of employees in the workplace.

Another part of the designed monitoring system is a warning system which will protect the property of the employer and the employees themselves. The first part of the proposed solution will prevent unauthorized access to the guarded areas and will also provide protection in case of fire. Another part will protect employees in the workplace using the. “Spider Alert Man Down Transmitter”, to inform security about possible injury. Intrusion

and Hold-up Alarm System will be directly connected to the alarm receiving center, security agency personnel will be able to respond promptly to the situation.

The last part of the proposed solution is a GPS vehicle monitoring system. This will contribute to the protect vehicles against a possible theft, as well as help to simplify the record keeping of road trips.

The suggested solution for PENTA, ltd. will help to achieve optimal conditions of security and traffic monitoring. Finally it will be of great benefit as it is currently being proven.

The last focus of practical part is the assessment is from the view of ethics and law. I have tried to analyze topics that are ethically unclear and not legally defined. I recommend several possible solutions. To understand the public opinion there was an internet survey, and the results were evaluated in this thesis.

SEZNAM POUŽITÉ LITERATURY

[1] LUKÁŠ, Luděk et al. *Bezpečnostní technologie, systémy a management I.* Zlín: Radim Bačuvčík – VeRBuM, 2011. ISBN 978-80-87500-05-7.

[2] KINDL, Jiří. *Projektování bezpečnostních systémů I.* 2. vydání. Zlín: UTB, 2007. ISBN 978-80-7318-554-1.

[3] KŘEČEK, Stanislav. *Příručka zabezpečovací techniky.* 3. vydání. Blatná: Cricetus – Ing. Stanislav Křeček, 2006. ISBN 80-902938-2-4.

[4] LOVEČEK, T. a NAGY, P. *Bezpečnostné systémy – Kamerové bezpečnostné systémy*. Žilina: EDIS vydavatelstvo, 2008. ISBN 978-80-8070-893-1.

[5] ČESKO. Zákon č. 2/1993 ze dne 16. prosince 1992 Usnesení předsednictva České národní rady o vyhlášení LISTINY ZÁKLADNÍCH PRÁV A SVOBOD jako součásti ústavního pořádku České republiky. In: *Sbírka zákonů České republiky*. 1992, částka 1, s. 17-24. Dostupný také z: http://aplikace.mvcr.cz/archiv2008/sbirka/1993/sb01-93.pdf.

[6] ČESKO. Zákon č. 262/2006 ze dne 21. dubna 2006 Zákoník práce. In: *Sbírka zákonů České republiky*. 2006, částka 84, s. 3146-3241. Dostupný také z: http://aplikace.mvcr.cz/archiv2008/sbirka/1993/sb01-93.pdf.

[7] ŠTEFKA, Vladislav. *Právní řád I.* 2. vydání. Zlín: UTB, 2009. ISBN 978-80-7318-805-4.

[8] MiCoS SOFTWARE. *Sledování zaměstnanců a monitoring pc* [online]. ©2009-2011 [cit. 2012-01-26]. Dostupné z: http://www.monitorovat-pc.cz/.

[9] ČSN ISO 690. *Informace a dokumentace – Pravidla pro bibliografické odkazy a citace informačních zdrojů*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2011. Třídící znak 01 0197.

[10] KRBKOVÁ, Lenka. *Návrh řešení problému kontroly zaměstnanců* [online]. Brno, 2009. 132 s. Diplomová práce. Vysoké učení technické v Brně. Dostupné z WWW: http://www.vutbr.cz/www_base/zav_prace_soubor_verejne.php?file_id=14055.

[11] Informace o možnostech odposlechu Vaší společnosti. *Specialisté na ochranu proti odposlechu* [online]. 2011. vyd. 2011 [cit. 2012-05-01]. Dostupné z: http://www.triangulace.cz/informace-o-zpusobech-uniku-informaci-diky-odposlechu/.

[12] Monitoring hovorů. *CIT.CZ, spol. s r.o. - komunikujte s CITem* [online]. 2011 [cit. 2012-05-01]. Dostupné z: http://www.cit.cz/Products.aspx?pid=7.

[13] Nahrávání hovorů | Doradus - computer telephony. *Úvodní stránka | Doradus - computer telephony* [online]. 2010 [cit. 2012-05-01]. Dostupné z: http://www.doradus.cz/nahravani-hovoru.html.

[14] ČESKO. Vyhláška č. 28/2001 ze dne 10. ledna 2001 Ministerstva dopravy a spojů. In: *Sbírka zákonů České republiky*. 2001, částka 10, s. 411-412. Dostupný také z: http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=3588.

[15] ROZMAN, J. a ČÍŽEK, M. *Ekonomický provoz osobních počítačů, studie* [online]. Dostupné z: http://zeleneuradovani.cz/content/File/poc_stud.pdf.

[16] Služby - Controlling a monitoring tisků - TA. *Triumph-Adler* [online]. 2008 [cit. 2012-05-01]. Dostupné z: http://www.ta.cz/sluzby/controling-a-monitoring-tisku.html

[17] ČSN EN 50133-1. *Poplachové systémy: Systémy kontroly vstupů pro použití v bezpečnostních aplikacích - Část 1: Systémové požadavky.* Praha: Český normalizační institut. 2001. 28 s.

[18] ČSN EN 50133-2-1. *Poplachové systémy - Systémy kontroly vstupů pro použití v bezpečnostních aplikacích - Část 2-1: Všeobecné požadavky na komponenty* Praha: Český normalizační institut. 2001. 12 s.

[19] ČSN EN 50133-7. *Poplachové systémy - Systémy kontroly vstupů pro použití v bezpečnostních aplikacích - Část 7: Pokyny pro aplikace.* Praha: Český normalizační institut. 2000. 16 s.

[20] Může zaměstnavatel číst e-mailovou poštu svých zaměstnanců?: Archiv novinek. WEBCONSULT.CZ. *Advokátní kancelář Vyroubal Krajhanzl Školout, s.r.o.* [online]. 2006 [cit. 2012-05-01]. Dostupné z: http://www.akvks.cz/cz/novinky/archiv-novinek/muze-zamestnavatel-cist-e-mailovou-postu-svych-zamestnancu.html.

[21] ČESKO. Zákon č. 101/2000 ze dne 4. dubna 2000 o ochraně osobních údajů a změně některých zákonů. In: *Sbírka zákonů České republiky*. 2000, částka 32, s. 1521-1532. Dostupný také z: http://aplikace.mvcr.cz/archiv2008/sbirka/2000/sb032-00.pdf.

[22] KOPECKÝ, D. *Monitorování zaměstnanců (výsledky průzkumu)*, 2012. [online]. Dostupné z: http://monitorovani-zamestnancu.vyplnto.cz.

[23] PALLA, Tomáš. Ochrana zaměstnanců před neoprávněným sledováním kamerovým systémem. *Právní rádce : měsíčník Hospodářských novin.* 2010, roč. 18, č. 1.

[24] BĚLINA, M. et al. *Pracovní právo*. 4. dopl. a přeprac. vydání. Praha : Nakladatelství C. H. Beck, 2010. 575 s.

[25] BĚLINA, M. et al. *Zákoník práce : komentář*. 2. vyd. Praha : Nakladatelství C. H. Beck, 2010. 1123 s.

[26] HRON, Michal. Na české pošťačky a pošťáky dohlíží GPS, má pomoci zkvalitnit služby. *Mobil.cz* [online]. 2012 [cit. 2012-05-01]. Dostupné z: http://mobil.idnes.cz/na-ceske-postacky-a-postaky-dohlizi-gps-ma-pomoci-zkvalitnit-sluzby-1gg-/mob_tech.aspx?c=A120309_152650_mob_tech_hro.

[27] *FY 2008 Presidential Budget Request for National Security Space Activities. George C. Marshall Institute* [online]. 2007 [cit. 2012-04-29]. Dostupný z WWW: http://www.marshall.org/pdf/materials/507.pdf.

[28] *Úřad pro ochranu osobních údajů : Názory úřadu : Stanoviska : Stanovisko č. 2/2009 – Ochrana soukromí zaměstnanců se zvláštním zřetelem k monitoringu pracoviště* [online]. 2009 [cit. 2012-05-01]. Dostupné z: http://www.uoou.cz/files/stanovisko_2009_2.pdf.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

3G	Třetí generace mobilních telefonů.
Aj.	A jiné
BNC	Bayonet Neill–Concelman.
BUS	Sběrnice
CCD	Charge-Coupled Device.
CCTV	Closed Circuit Television
CD	Compact Disc
CMOS	Complementary Metal–Oxide–Semiconductor
CPU	Central Processing Unit
CRM	Customer Relationship Management
CRT	Cathode Ray Tube
DLP	Data Loss Prevention
DVR	Digital Video Recorder
EZS	Elektronická Zabezpečovací Signalizace
FTP	File Transfer Protocol
GPRS	General Packet Radio Service
GPS	Global Positioning System
GSM	Global System for Mobile Communications
HD	High Definition
HW	Hardware
IAX	Inter-Asterisk eXchange
ID	Identity Document
IMAP	Internet Message Access Protocol
IP	Internet Protocol

ISDN	Integrated Services Digital Network
IT	Information Technology
IZS	Integrovaný Záchranný Systém
JPEG	Joint Photographic Experts Group
Kč	Česká koruna
LAN	Local Area Network
LCD	Liquid Crystal Display
LED	Light-Emitting Diode
MP3	MPEG Audio Layer III
MS	Microsoft
Např.	Například
NC	Normally Closed
NVR	Network Video Recorder
Odst.	Odstavec
OS	Operační Systém
PAL	Phase Alternating Line
PC	Personal Computer
PGM	Pragmatic General Multicast
PHM	Pohonné hmoty
PIR	Passive Infrared Sensor
Písm.	Písmeno
POP3	Post Office Protocol, version 3
Popř.	Popřípadě
PPC	Poplachové Přijímací Centrum
PTSN	public switched telephone network
PZS	Poplachový Zabezpečovací Systém

PZTS	Poplachový Zabezpečovací a Tísňový Systém
RDC	Remote Desktop Connection
RFID	Radio-Frequency Identification
RPC	Remote Procedure Call
Sb.	Sbírka zákonů
SIP	Session Initiation Protocol
SMTP	Simple Mail Transfer Protocol
SPZ	Státní Poznávací Značka
SQL	Structured Query Language
S-VHS	Super Video Home System
SW	Software
TB	TeraByte
TS	Terminal Service
ÚOOÚ	Úřad pro Ochranu Osobních Údajů
UMTS	Universal Mobile Telecommunications System
UPS	Uninterruptible Power Supply
USA	United States of America
USB	Universal Serial Bus
Ust.	Ustanovení
VHS	Video Home System
VOIP	Voice Over Internet Protocol
WAV	Waveform Audio File Format
WIFI	Wireless Local Area Network
ZoEK	Zákon o Elektronických Komunikacích
ZOOÚ	Zákon o Ochraně Osobních Údajů
ZP	Zákoník Práce

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: DOTAZNÍK

1. Jste žena nebo muž?

☐ muž ☐ žena

2. Jaký je váš věk?

☐ 0-20 ☐ 20-28 ☐ 28-35 ☐ 35-45 ☐ 45-55 ☐ 55 a více

3. Jaká je úroveň Vašeho nejvyššího dokončeného vzdělání?

☐ základní ☐ vyučen/a ☐ středoškolské ☐ VOŠ ☐ vysokoškolské

4. Myslíte si, že je etické a morální monitorovat činnosti zaměstnanců?

☐ ano ☐ ne

5. Z jakého důvodu?

☐ narušení soukromí ☐ pocit sledování ☐ je to v rozporu se zákonem ☐ vlastní odpověď:

6. Které prvky monitoringu jsou dle Vás morální a etické?

☐ docházkové systémy ☐ GPS lokátory služebních vozidel ☐ GPS lokátory zaměstnanců ☐ kamerový systém ☐ kontrola přítomnosti osob v určitých prostorách ☐ monitorování emailové pošty ☐ monitorování PC ☐ monitorování telefonních hovorů ☐ monitorování využitého spotřebního materiálu (tiskárny) ☐ vlastní odpověď:

7. Myslíte si, že by Vás použití monitoringu mohlo v zaměstnání negativně ovlivnit?

☐ ano ☐ ne

8. Jakým způsobem?

☐ pocitu neustálého sledování ☐ snížená pracovní výkonnost ☐ zásah do soukromí ☐ vlastní odpověď:

9. Jaká je váš současný stav? [větvení]

☐ student/ka ☐ zaměstnanec ☐ podnikatel/ka (bez zaměstnanců) ☐ podnikatel/ka (se zaměstnanci) ☐ nezaměstnaný/ná ☐ na mateřské dovolené ☐ důchodce

10. Na jaké pozici vykonáváte své povolání?

☐ řadový pracovník ☐ střední management ☐ vrcholový management ☐ jiná odpověď:

11. Co nejvíce vystihuje Vaši práci?

☐ administrativa ☐ obchodní činnost ☐ výrobní činnost ☐ personální činnost ☐ marketing ☐ management ☐ doprava ☐ jiná odpověď:

12. Využívá Váš zaměstnavatel některé prvky monitoringu na pracovišti? [větvení]

☐ ano ☐ ne

13. Které?

☐ docházkové systémy ☐ GPS lokátory služebních vozidel ☐ GPS lokátory zaměstnanců ☐ kamerový systém ☐ kontrola přítomnosti osob v určitých prostorách ☐ monitorování emailové pošty ☐ monitorování PC ☐ monitorování telefonních hovorů ☐ monitorování využitého spotřebního materiálu (tiskárny) ☐ vlastní odpověď:

14. Jak jste se o monitorování dozvěděl/a?

☐ z pracovní smlouvy ☐ ze směrnice, dodatku ☐ od kolegů ☐ osobním sdělením vedoucího pracovníka ☐ z nástěnky, nálepky na dveřích ☐ jinak

15. Byl po Vás požadován souhlas s monitorováním vaší osoby a činnosti?

☐ ano, písemně ☐ ano, ústně ☐ ne

16. Myslíte si, že monitoring ve Vaší společnosti je oprávněně zaveden?

☐ ano ☐ ne

17. Jsou Vaším zaměstnavatelem tolerovány některé z následujících činností (v pracovní době):

☐ soukromé emaily ☐ soukromé telefonické hovory ☐ soukromé cesty služebním vozidlem ☐ soukromé využívání PC ☐ vše povoleno v přiměřené míře ☐ vše zakázáno

18. Porušujete alespoň občas tento zákaz (pokud není, prosím neodpovídat)?

☐ ano ☐ ne

19. Jsou Vaším zaměstnavatelem tolerovány některé z následujících činností spojených s užíváním PC k osobním účelům:

☐ nákupy na internetu ☐ procházení internetu ☐ skype, ICQ, MSN, aj. ☐ sociální sítě (facebook, twitter, aj.) ☐ tisk pro soukromé účely ☐ hry ☐ vše zakázáno

20. Co si myslíte o využívání firemního PC, telefonu a vozidla k soukromým účelům (v pracovní době)?

☐ proč ne, dělá to každý ☐ v přiměřené míře by to mělo být povoleno ☐ rád/a bych, ale brání mi v tom monitoring ☐ v zaměstnání výhradně pracuji a soukromé záležitosti řeším po pracovní době ☐ jiná odpověď:

21. Využíváte ke sledování zaměstnanců některé prvky monitoringu? [větvení]

☐ ano ☐ ne

22. Které?

☐ docházkové systémy ☐ GPS lokátory služebních vozidel ☐ GPS lokátory zaměstnanců ☐ kamerový systém ☐ kontrola přítomnosti osob v určitých prostorách ☐ monitorování emailové pošty ☐ monitorování PC ☐ monitorování telefonních hovorů ☐ monitorování využitého spotřebního materiálu (tiskárny) ☐ vlastní odpověď:

23. Je pro Vás monitorování přínosem? [větvení]

☐ ano ☐ ne

24. V jakém směru je pro Vás monitorování přínosem?

☐ vyšší pracovní výkonnost ☐ úspora nákladů ☐ dodržování pracovní doby ☐ vyšší bezpečnost zaměstnanců ☐ ochrana citlivých dat ☐ Vlastní odpověď: ____

25. Zaznamenal/a jste někdy stížnosti ze strany zaměstnanců?

☐ ano ☐ ne

26. Myslíte si, že jsou Vámi používané metody monitoringu v souladu se zákonem?

☐ ano ☐ ne

27. Plánujete jejich zavedení? [větvení]

☐ ano ☐ ne

28. Které?

☐ docházkové systémy ☐ GPS lokátory služebních vozidel ☐ GPS lokátory zaměstnanců ☐ kamerový systém ☐ kontrola přítomnosti osob v určitých prostorách ☐ monitorování emailové pošty ☐ monitorování PC ☐ monitorování telefonních hovorů ☐ monitorování využitého spotřebního materiálu (tiskárny) ☐ vlastní odpověď:

29. Z jakého důvodu?

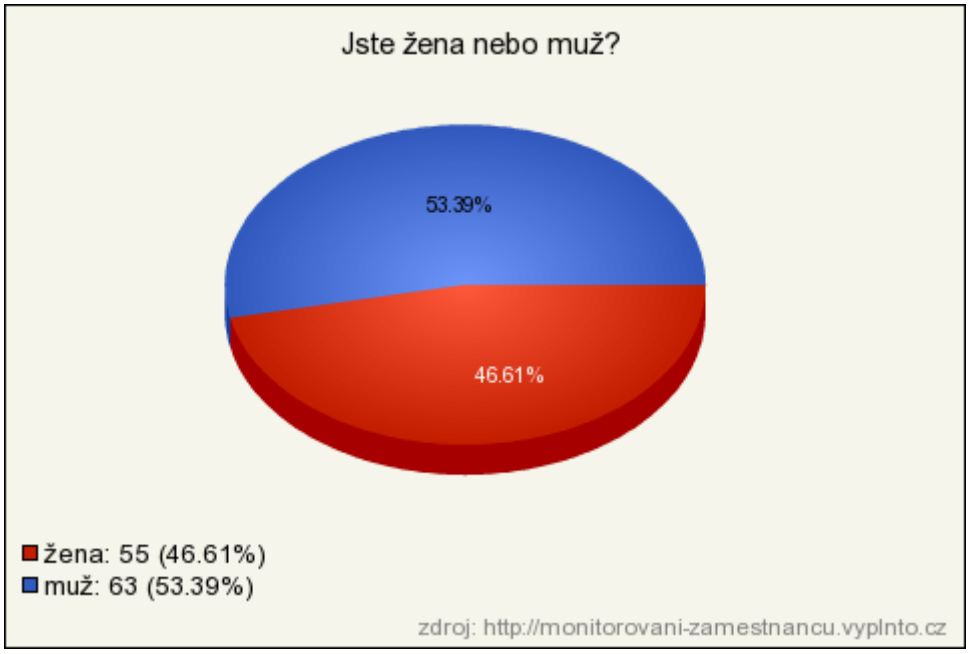
☐ nepotřebujeme naše zaměstnance monitorovat, vždy se chovají v souladu s nařízeními ☐ obáváme reakce zaměstnanců ☐ obáváme se rozporu se zákonem ☐ Vlastní odpověď: _____

PŘÍLOHA P II: VÝSLEDKY PRŮZKUMU

1. Jste žena nebo muž?

Povinná otázka, respondent musel zvolit jednu z nabízených odpovědí.

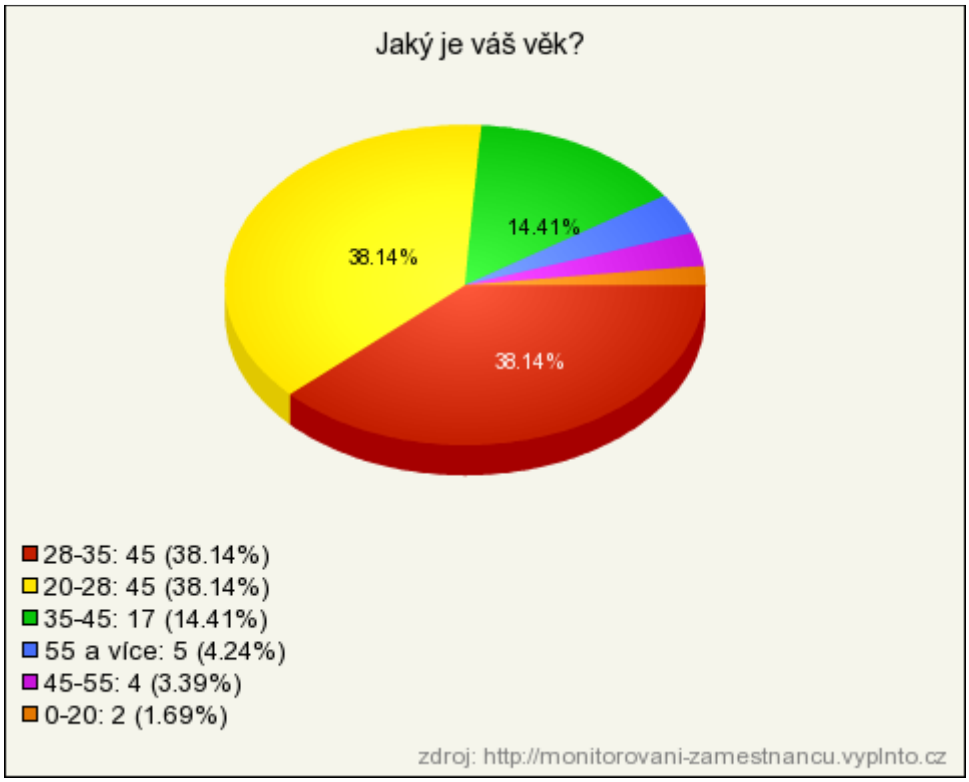
Odpověď	Počet	Lokálně	Globálně
muž	63	**53.39%**	53.39%
žena	55	**46.61%**	46.61%



2. Jaký je váš věk?

Povinná otázka, respondent musel zvolit jednu z nabízených odpovědí.

Odpověď	Počet	Lokálně	Globálně
28–35	45	**38.14%**	38.14%
20–28	45	**38.14%**	38.14%
35–45	17	**14.41%**	14.41%
55 a více	5	**4.24%**	4.24%
45–55	4	**3.39%**	3.39%
0–20	2	**1.69%**	1.69%



3. Jaká je úroveň Vašeho nejvyššího dokončeného vzdělání?

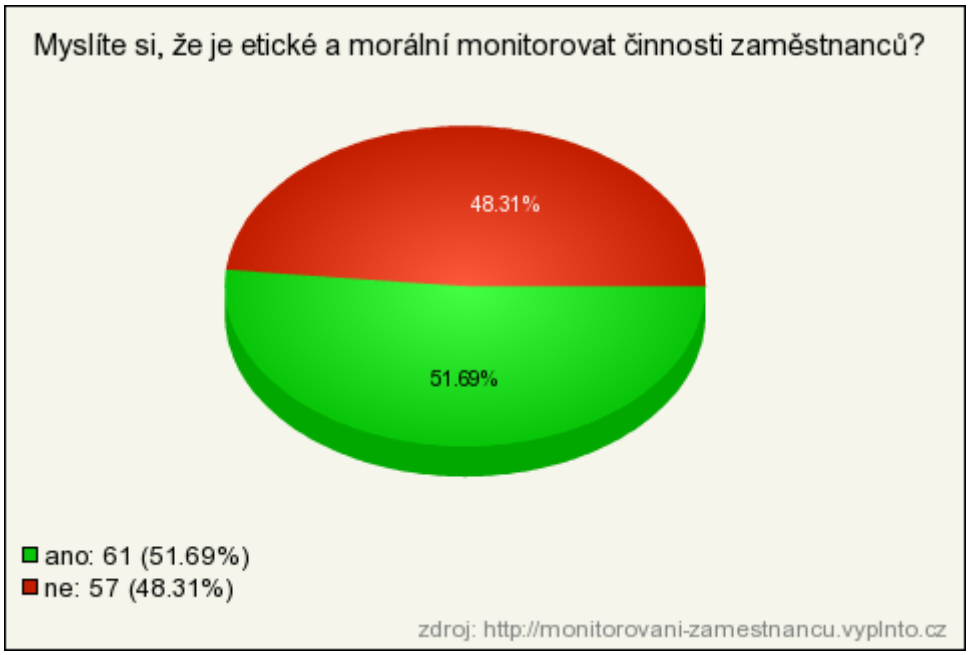
Povinná otázka, respondent musel zvolit jednu z nabízených odpovědí.

Odpověď	Počet	Lokálně	Globálně
středoškolské	58	**49.15%**	49.15%
vysokoškolské	50	**42.37%**	42.37%
VOŠ	4	**3.39%**	3.39%
základní	4	**3.39%**	3.39%
vyučen/a	2	**1.69%**	1.69%

4. Myslíte si, že je etické a morální monitorovat činnosti zaměstnanců?

*Povinná otázka, respondent musel zvolit jednu z nabízených odpovědí a podle toho se mu zobrazily další otázky [**ano** → otázka č. 6, **ne** → otázka č. 5].*

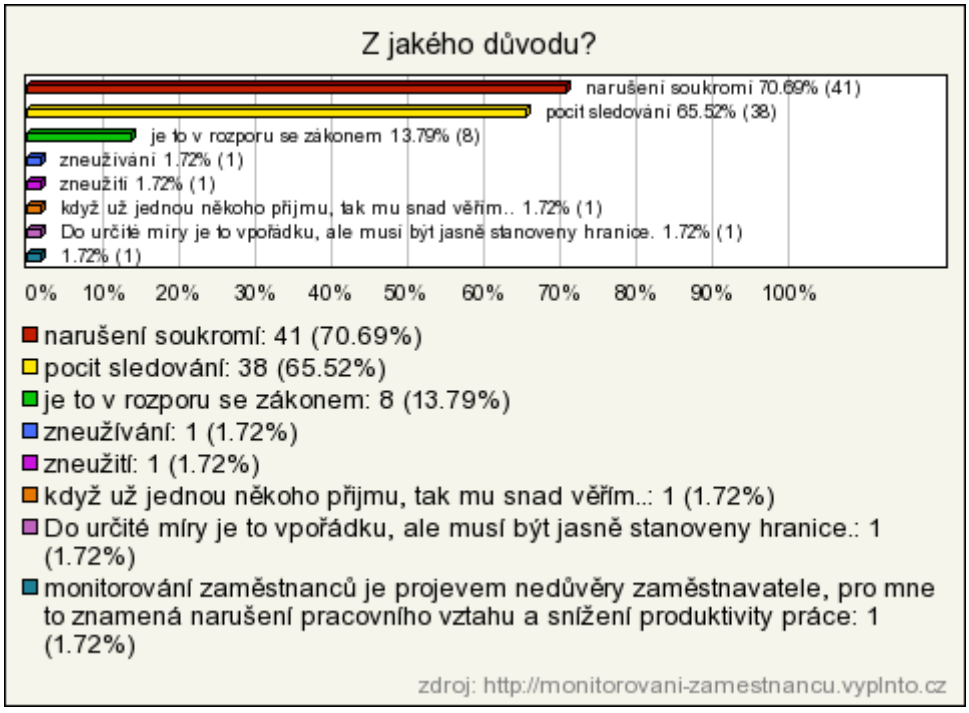
Odpověď	Počet	Lokálně	Globálně
ano	61	**51.69%**	51.69%
ne	57	**48.31%**	48.31%



5. Z jakého důvodu?

Povinná otázka, respondent musel zvolit alespoň některou z nabízených odpovědí nebo dopsat nějakou vlastní.

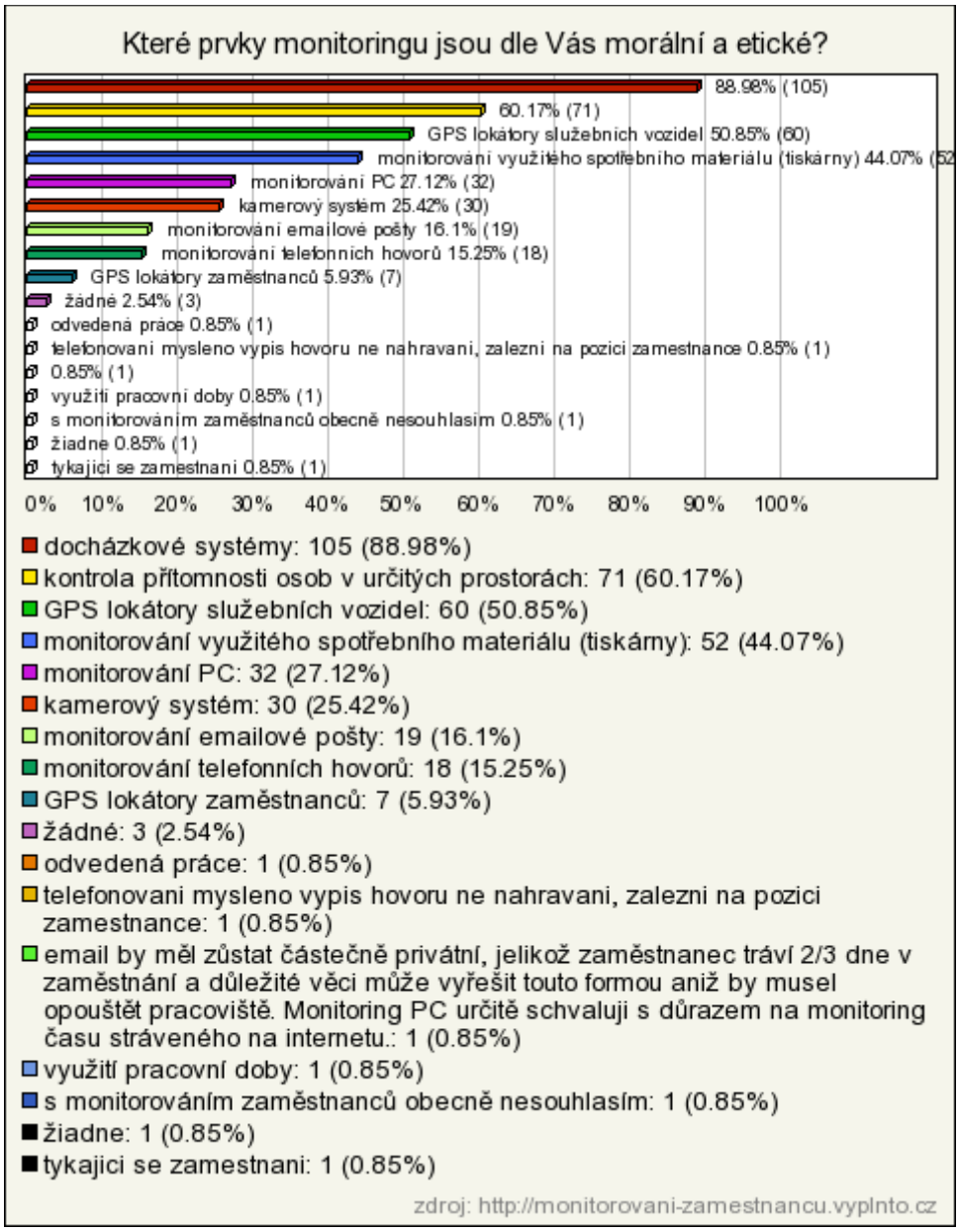
Odpověď	Počet	Lokálně	Globálně
narušení soukromí	41	**70.69%**	34.75%
pocit sledování	38	**65.52%**	32.2%
je to v rozporu se zákonem	8	**13.79%**	6.78%
zneužívání	1	**1.72%**	0.85%
zneužití	1	**1.72%**	0.85%
když už jednou někoho přijmu, tak mu snad věřím..	1	**1.72%**	0.85%
Do určité míry je to vpořádku, ale musí být jasně stanoveny hranice.	1	**1.72%**	0.85%
monitorování zaměstnanců je projevem nedůvěry zaměstnavatele, pro mne to znamená narušení pracovního vztahu a snížení produktivity práce	1	**1.72%**	0.85%



6. Které prvky monitoringu jsou dle Vás morální a etické?

Povinná otázka, respondent musel zvolit alespoň některou z nabízených odpovědí nebo dopsat nějakou vlastní.

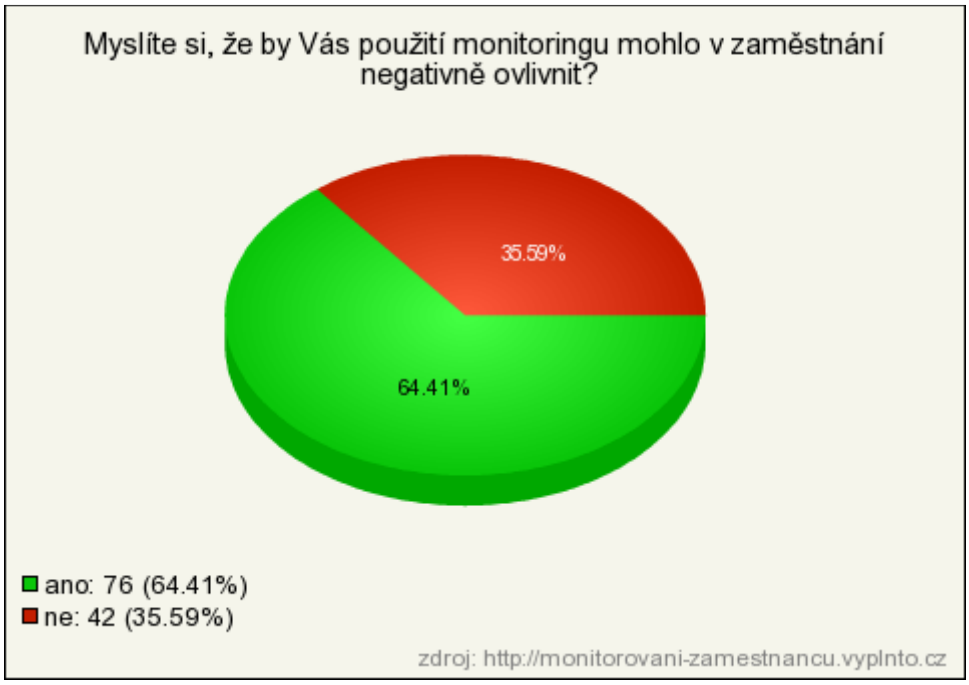
Odpověď	Počet	Lokálně	Globálně
docházkové systémy	105	88.98%	88.98%
kontrola přítomnosti osob v určitých prostorách	71	60.17%	60.17%
GPS lokátory služebních vozidel	60	50.85%	50.85%
monitorování využitého spotřebního materiálu (tiskárny)	52	44.07%	44.07%
monitorování PC	32	27.12%	27.12%
kamerový systém	30	25.42%	25.42%
monitorování emailové pošty	19	16.1%	16.1%
monitorování telefonních hovorů	18	15.25%	15.25%
GPS lokátory zaměstnanců	7	5.93%	5.93%
žádné	3	2.54%	2.54%
odvedená práce	1	0.85%	0.85%
telefonovani mysleno vypis hovoru ne nahravani, zalezni na pozici zamestnance	1	0.85%	0.85%
email by měl zůstat částečně privátní, jelikož zaměstnanec tráví 2/3 dne v zaměstnání a důležité věci může vyřešit touto formou aniž by musel opouštět pracoviště. Monitoring PC určitě schvaluji s důrazem na monitoring času stráveného na internetu.	1	0.85%	0.85%
využití pracovní doby	1	0.85%	0.85%
s monitorováním zaměstnanců obecně nesouhlasím	1	0.85%	0.85%
žiadne	1	0.85%	0.85%
tykajici se zamestnani	1	0.85%	0.85%



7. Myslíte si, že by Vás použití monitoringu mohlo v zaměstnání negativně ovlivnit?

*Povinná otázka, respondent musel zvolit jednu z nabízených odpovědí a podle toho se mu zobrazily další otázky [**ano** → otázka č. 8, **ne** → otázka č. 9].*

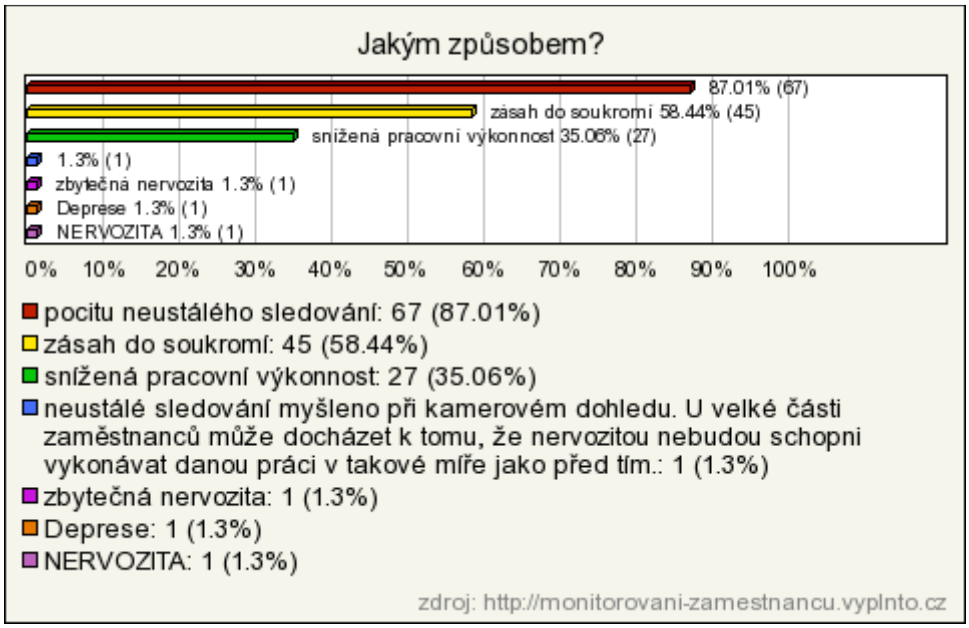
Odpověď	Počet	Lokálně	Globálně
ano	76	**64.41%**	64.41%
ne	42	**35.59%**	35.59%



8. Jakým způsobem?

Povinná otázka, respondent musel zvolit alespoň některou z nabízených odpovědí nebo dopsat nějakou vlastní.

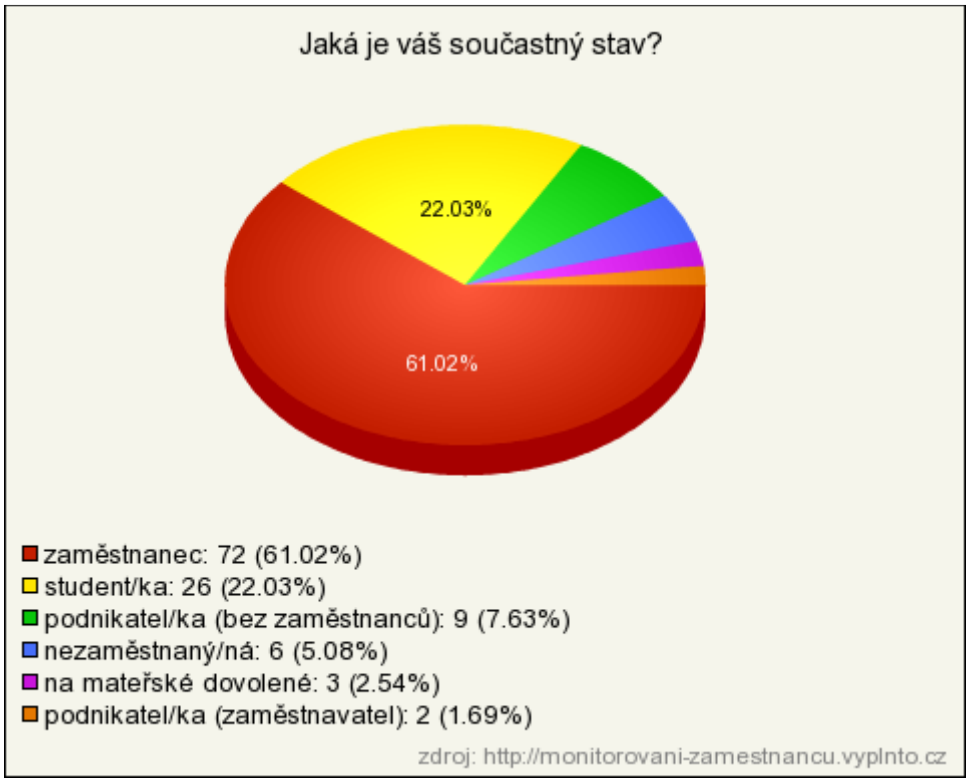
Odpověď	Počet	Lokálně	Globálně
pocitu neustálého sledování	67	**87.01%**	56.78%
zásah do soukromí	45	**58.44%**	38.14%
snížená pracovní výkonnost	27	**35.06%**	22.88%
neustálé sledování myšleno při kamerovém dohledu. U velké části zaměstnanců může docházet k tomu, že nervozitou nebudou schopni vykonávat danou práci v takové míře jako před tím.	1	**1.3%**	0.85%
zbytečná nervozita	1	**1.3%**	0.85%
Deprese	1	**1.3%**	0.85%
NERVOZITA	1	**1.3%**	0.85%



9. Jaká je váš současný stav?

*Povinná otázka, respondent musel zvolit jednu z nabízených odpovědí a podle toho se mu zobrazily další otázky [**student/ka** → konec dotazníku, **zaměstnanec** → otázka č.10, **podnikatel/ka (bez zaměstnanců)** → konec dotazníku, **podnikatel/ka (zaměstnavatel)** → otázka č. 21, **nezaměstnaný/ná** → konec dotazníku, **na mateřské dovolené** → konec dotazníku, **důchodce** → konec dotazníku].*

Odpověď	Počet	Lokálně	Globálně
zaměstnanec	72	**61.02%**	61.02%
student/ka	26	**22.03%**	22.03%
podnikatel/ka (bez zaměstnanců)	9	**7.63%**	7.63%
nezaměstnaný/ná	6	**5.08%**	5.08%
na mateřské dovolené	3	**2.54%**	2.54%
podnikatel/ka (zaměstnavatel)	2	**1.69%**	1.69%



10. Na jaké pozici vykonáváte své povolání?

Povinná otázka, respondent musel zvolit jednu z nabízených odpovědí nebo napsat odpověď vlastními slovy.

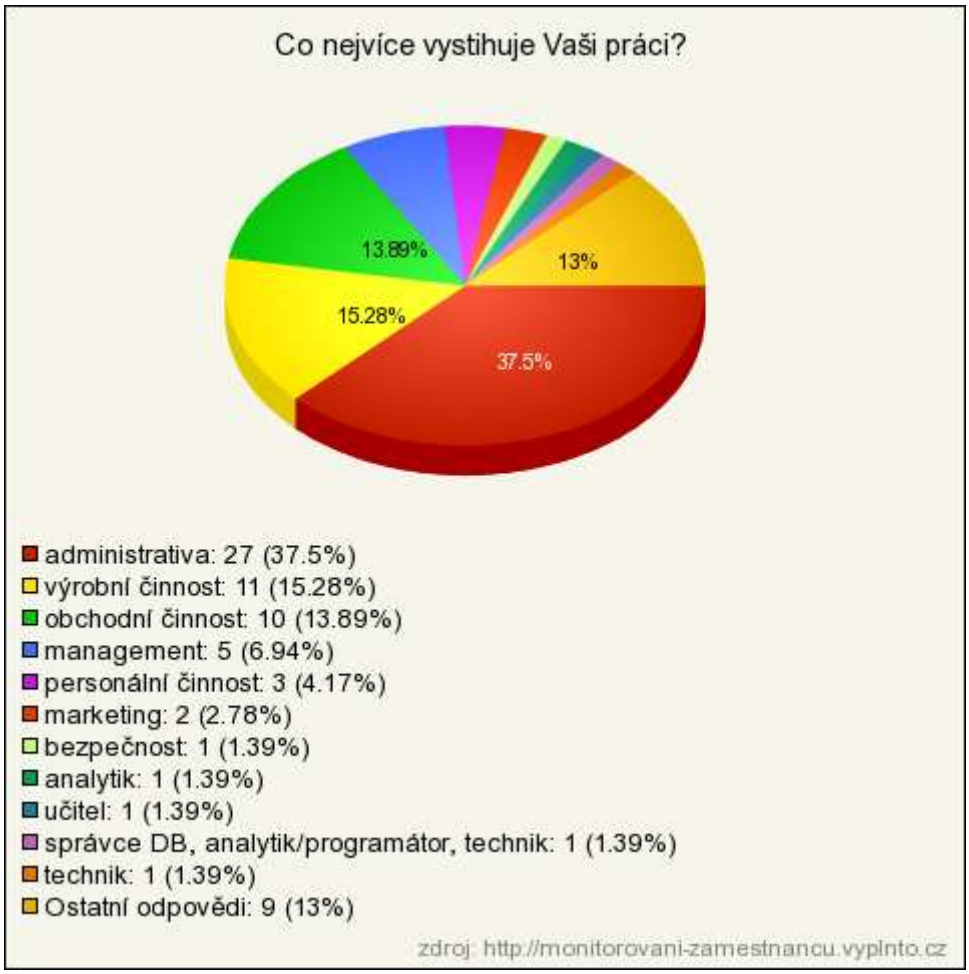
Odpověď	Počet	Lokálně	Globálně
řadový pracovník	43	**59.72%**	36.44%
střední management	24	**33.33%**	20.34%
vrcholový management	4	**5.56%**	3.39%
vedoucí pracovník	1	**1.39%**	0.85%

11. Co nejvíce vystihuje Vaši práci?

Povinná otázka, respondent musel zvolit jednu z nabízených odpovědí nebo napsat odpověď vlastními slovy.

Odpověď	Počet	Lokálně	Globálně
administrativa	27	**37.5%**	22.88%
výrobní činnost	11	**15.28%**	9.32%
obchodní činnost	10	**13.89%**	8.47%
management	5	**6.94%**	4.24%
personální činnost	3	**4.17%**	2.54%
marketing	2	**2.78%**	1.69%
bezpečnost	1	**1.39%**	0.85%
analytik	1	**1.39%**	0.85%
učitel	1	**1.39%**	0.85%
správce DB, analytik/programátor, technik	1	**1.39%**	0.85%
technik	1	**1.39%**	0.85%
školství	1	**1.39%**	0.85%

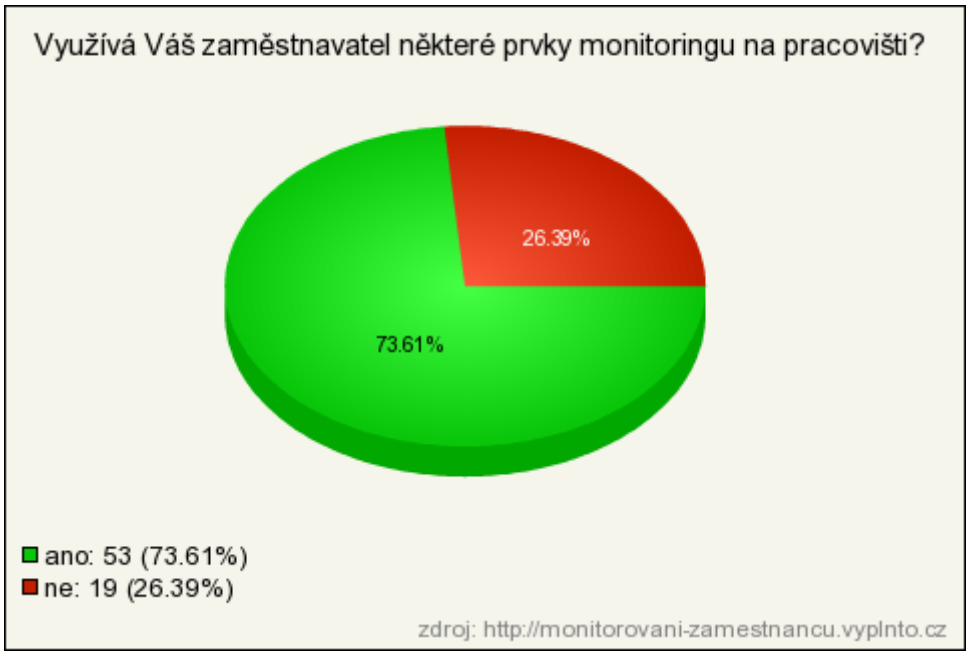
technicka pozice	1	1.39%	0.85%
právo	1	1.39%	0.85%
údržba IT	1	1.39%	0.85%
právní činnost	1	1.39%	0.85%
procesní inženýr	1	1.39%	0.85%
státní správa	1	1.39%	0.85%
Vývoj	1	1.39%	0.85%
zdravotnictví	1	1.39%	0.85%



12. Využívá Váš zaměstnavatel některé prvky monitoringu na pracovišti?

*Povinná otázka, respondent musel zvolit jednu z nabízených odpovědí a podle toho se mu zobrazily další otázky [**ano** → otázka č. 13, **ne** → otázka č. 17].*

Odpověď	Počet	Lokálně	Globálně
ano	53	**73.61%**	44.92%
ne	19	**26.39%**	16.1%

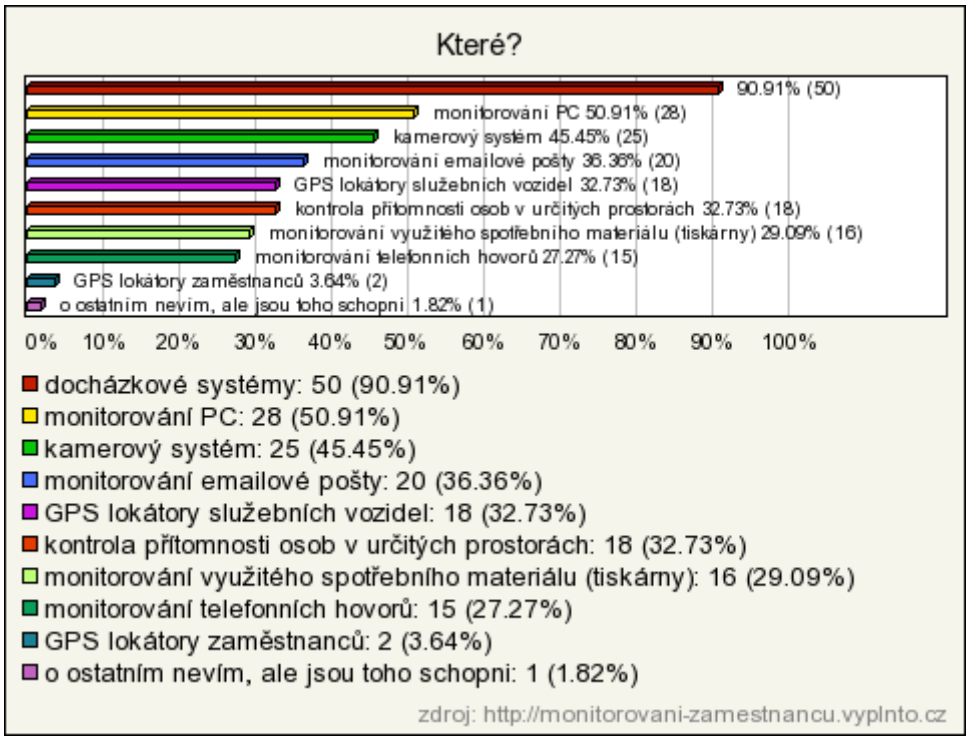


13. Které?

Povinná otázka, respondent musel zvolit alespoň některou z nabízených odpovědí nebo dopsat nějakou vlastní.

Odpověď	Počet	Lokálně	Globálně
docházkové systémy	50	**90.91%**	42.37%
monitorování PC	28	**50.91%**	23.73%
kamerový systém	25	**45.45%**	21.19%
monitorování emailové pošty	20	**36.36%**	16.95%
GPS lokátory služebních vozidel	18	**32.73%**	15.25%
kontrola přítomnosti osob v určitých prostorách	18	**32.73%**	15.25%

monitorování využitého spotřebního materiálu (tiskárny)	16	**29.09%**	13.56%
monitorování telefonních hovorů	15	**27.27%**	12.71%
GPS lokátory zaměstnanců	2	**3.64%**	1.69%
o ostatním nevím, ale jsou toho schopni	1	**1.82%**	0.85%

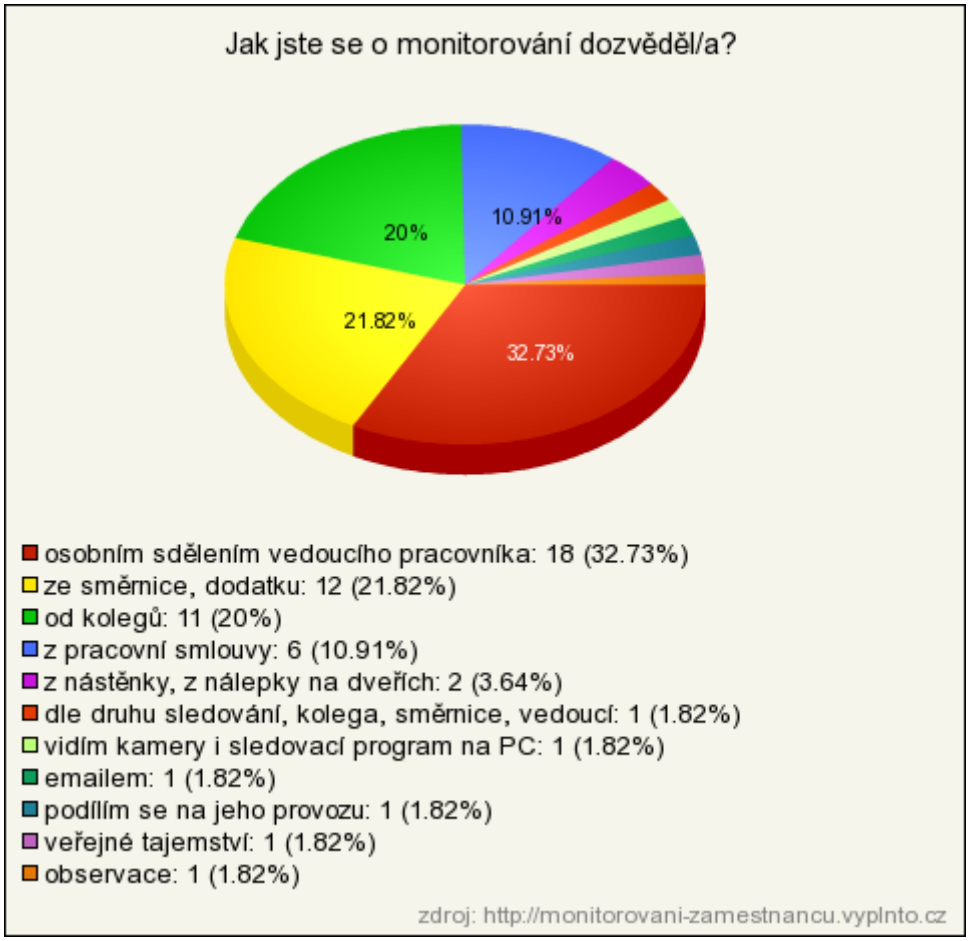


14. Jak jste se o monitorování dozvěděl/a?

Povinná otázka, respondent musel zvolit jednu z nabízených odpovědí nebo napsat odpověď vlastními slovy.

Odpověď	Počet	Lokálně	Globálně
osobním sdělením vedoucího pracovníka	18	**32.73%**	15.25%
ze směrnice, dodatku	12	**21.82%**	10.17%
od kolegů	11	**20%**	9.32%
z pracovní smlouvy	6	**10.91%**	5.08%
z nástěnky, z nálepky na dveřích	2	**3.64%**	1.69%
dle druhu sledování, kolega, směrnice, vedoucí	1	**1.82%**	0.85%
vidím kamery i sledovací program na PC	1	**1.82%**	0.85%

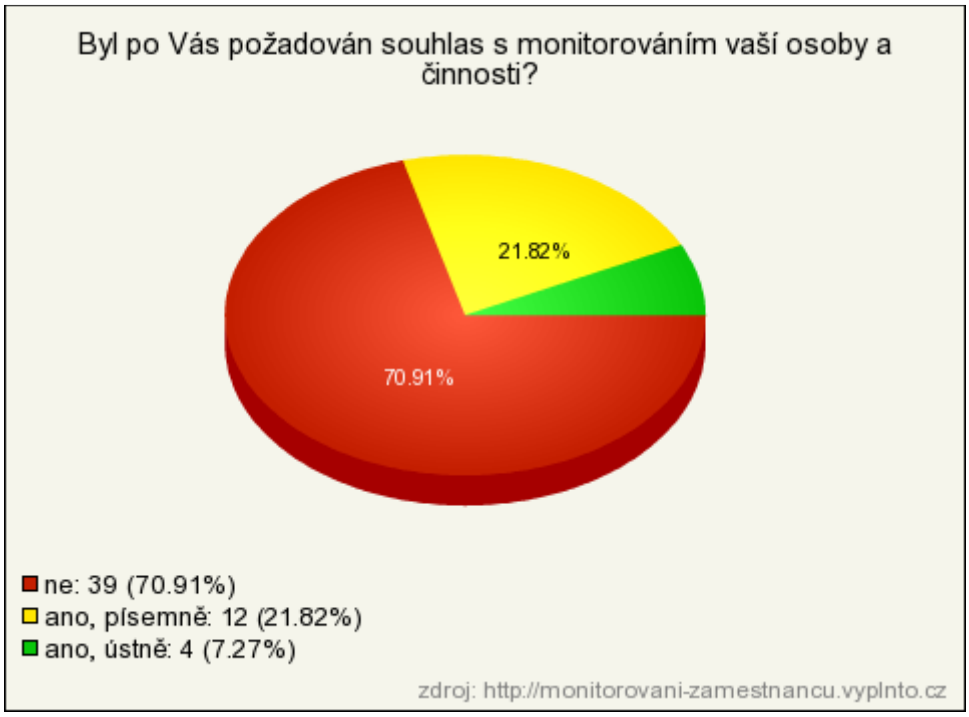
emailem	1	**1.82%**	0.85%
podílím se na jeho provozu	1	**1.82%**	0.85%
veřejné tajemství	1	**1.82%**	0.85%
observace	1	**1.82%**	0.85%



15. Byl po Vás požadován souhlas s monitorováním vaší osoby a činnosti?

Povinná otázka, respondent musel zvolit jednu z nabízených odpovědí.

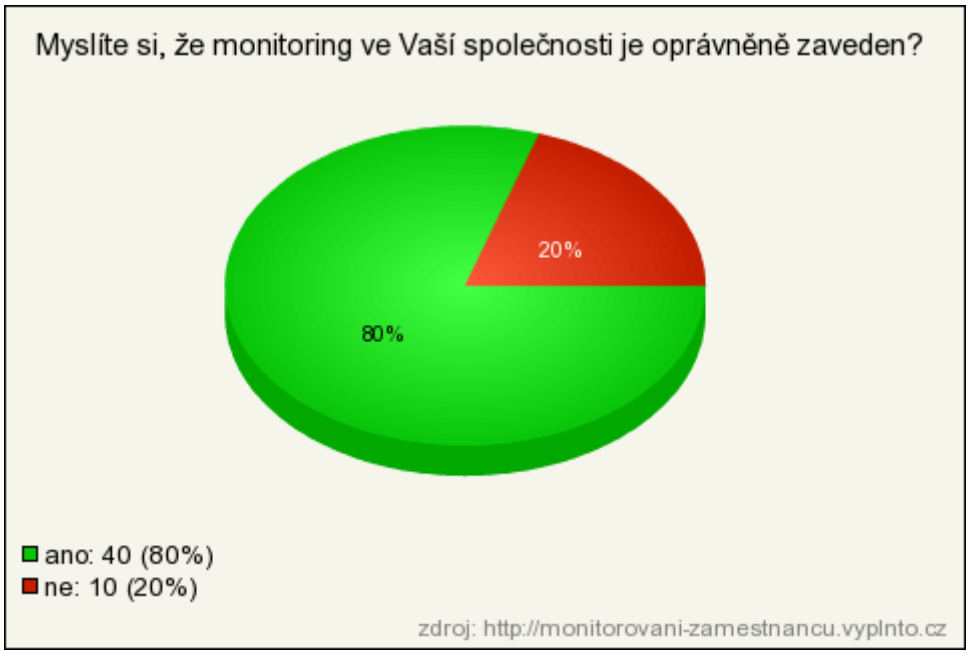
Odpověď	Počet	Lokálně	Globálně
ne	39	**70.91%**	33.05%
ano, písemně	12	**21.82%**	10.17%
ano, ústně	4	**7.27%**	3.39%



16. Myslíte si, že monitoring ve Vaší společnosti je oprávněně zaveden?

Nepovinná otázka, respondent se mohl rozhodnout mezi odpověďmi „ano" a „ne".

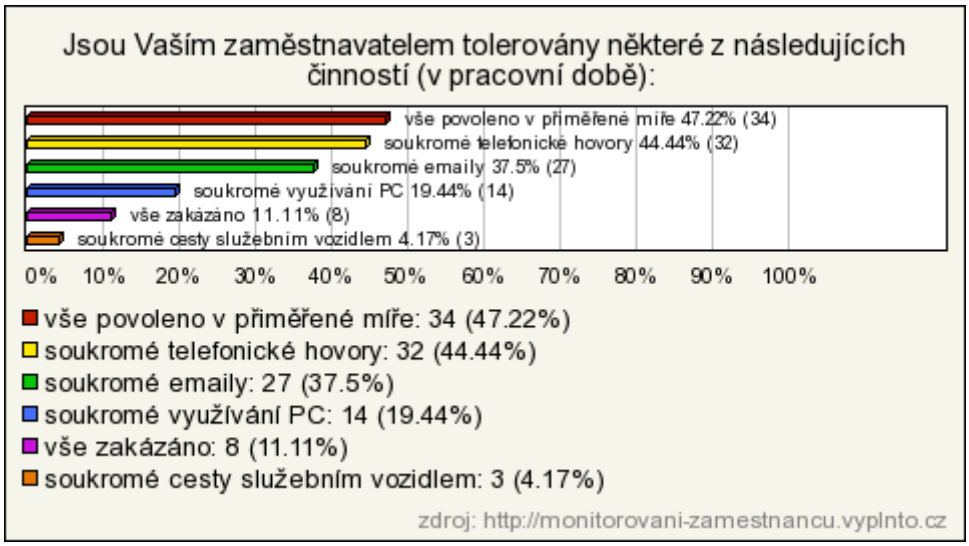
Odpověď	Počet	Lokálně	Globálně
ano	40	**80%**	33.9%
ne	10	**20%**	8.47%



17. Jsou Vaším zaměstnavatelem tolerovány některé z následujících činností (v pracovní době):

Povinná otázka, respondent musel zvolit alespoň některou z nabízených odpovědí.

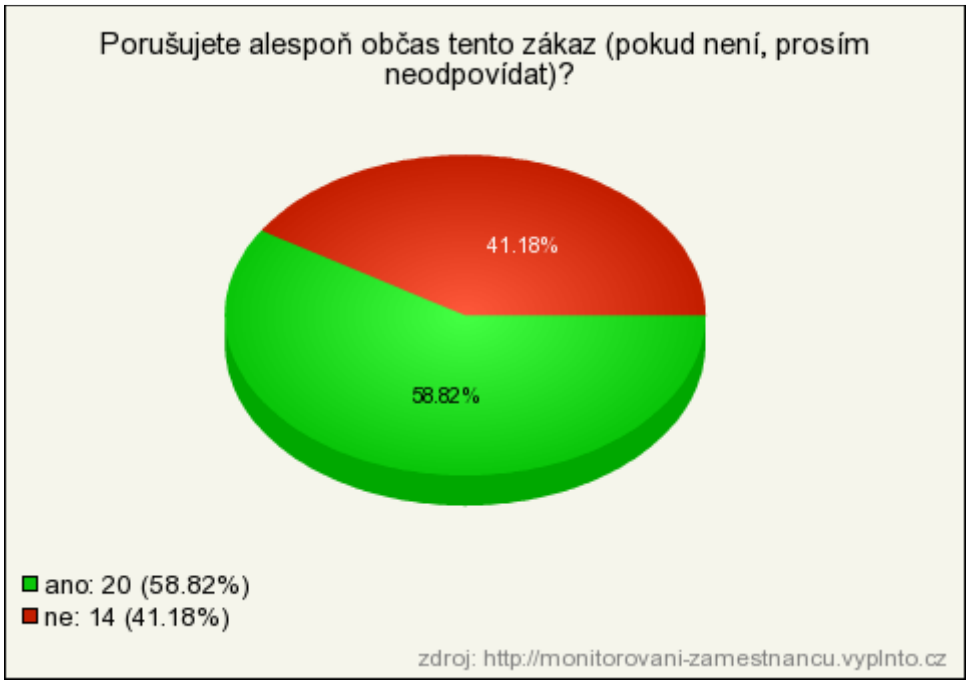
Odpověď	Počet	Lokálně	Globálně
vše povoleno v přiměřené míře	34	**47.22%**	28.81%
soukromé telefonické hovory	32	**44.44%**	27.12%
soukromé emaily	27	**37.5%**	22.88%
soukromé využívání PC	14	**19.44%**	11.86%
vše zakázáno	8	**11.11%**	6.78%
soukromé cesty služebním vozidlem	3	**4.17%**	2.54%



18. Porušujete alespoň občas tento zákaz (pokud není, prosím neodpovídat)?

Nepovinná otázka, respondent se mohl rozhodnout mezi odpověďmi „ano" a „ne".

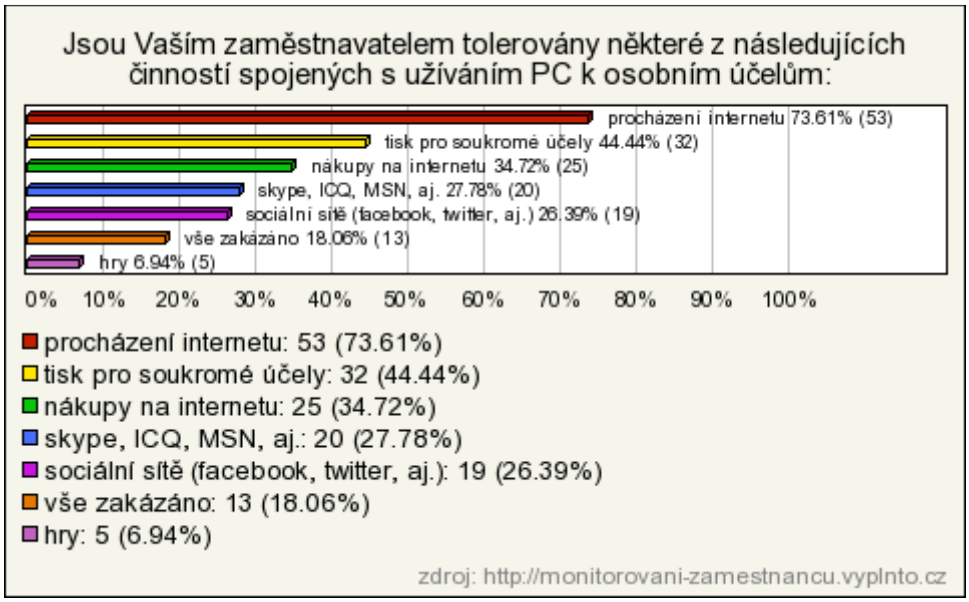
Odpověď	Počet	Lokálně	Globálně
ano	20	**58.82%**	16.95%
ne	14	**41.18%**	11.86%



19. Jsou Vaším zaměstnavatelem tolerovány některé z následujících činností spojených s užíváním PC k osobním účelům:

Povinná otázka, respondent musel zvolit alespoň některou z nabízených odpovědí.

Odpověď	Počet	Lokálně	Globálně
procházení internetu	53	**73.61%**	44.92%
tisk pro soukromé účely	32	**44.44%**	27.12%
nákupy na internetu	25	**34.72%**	21.19%
skype, ICQ, MSN, aj.	20	**27.78%**	16.95%
sociální sítě (facebook, twitter, aj.)	19	**26.39%**	16.1%
vše zakázáno	13	**18.06%**	11.02%
hry	5	**6.94%**	4.24%

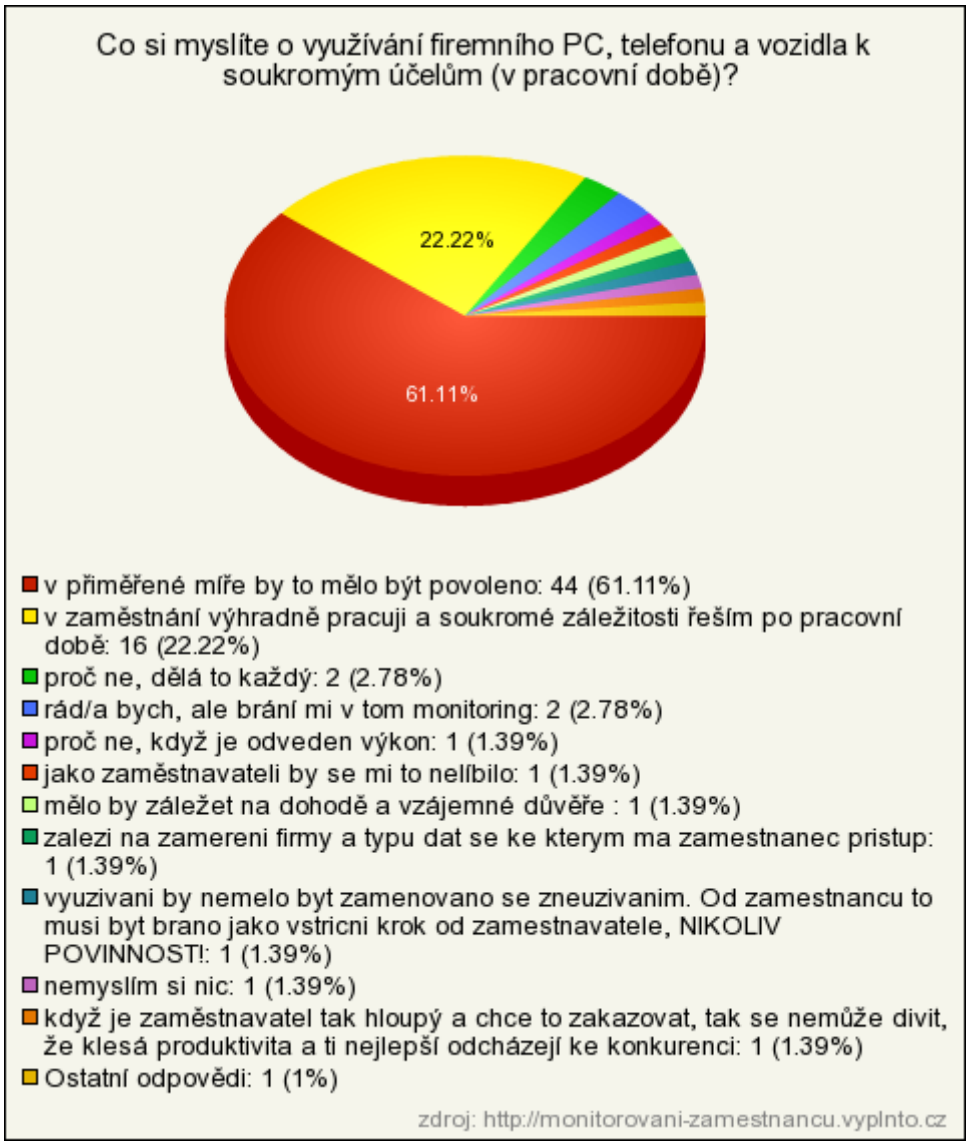


20. Co si myslíte o využívání firemního PC, telefonu a vozidla k soukromým účelům (v pracovní době)?

Povinná otázka, respondent musel zvolit jednu z nabízených odpovědí nebo napsat odpověď vlastními slovy.

Odpověď	Počet	Lokálně	Globálně
v přiměřené míře by to mělo být povoleno	44	**61.11%**	37.29%
v zaměstnání výhradně pracuji a soukromé záležitosti řeším po pracovní době	16	**22.22%**	13.56%
proč ne, dělá to každý	2	**2.78%**	1.69%
rád/a bych, ale brání mi v tom monitoring	2	**2.78%**	1.69%
proč ne, když je odveden výkon	1	**1.39%**	0.85%
jako zaměstnavateli by se mi to nelíbilo	1	**1.39%**	0.85%
mělo by záležet na dohodě a vzájemné důvěře	1	**1.39%**	0.85%
zalezi na zamereni firmy a typu dat se ke kterym ma zamestnanec pristup	1	**1.39%**	0.85%
vyuzivani by nemelo byt zamenovano se zneuzivanim. Od zamestnancu to musi byt brano jako vstricni krok od zamestnavatele, NIKOLIV POVINNOST!	1	**1.39%**	0.85%

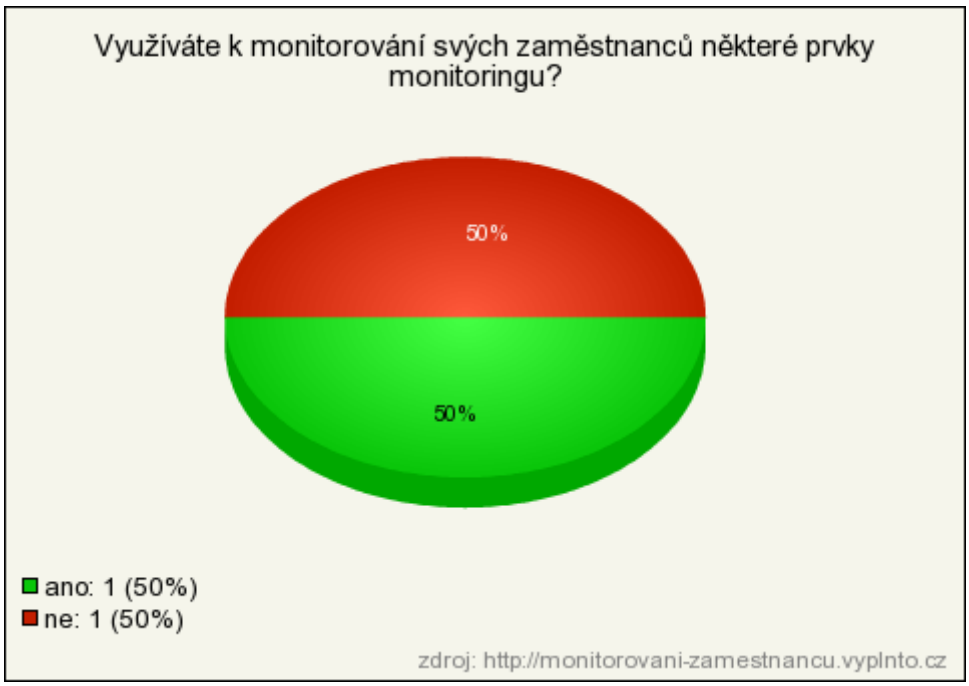
nemyslím si nic	1	**1.39%**	0.85%
když je zaměstnavatel tak hloupý a chce to zakazovat, tak se nemůže divit, že klesá produktivita a ti nejlepší odcházejí ke konkurenci	1	**1.39%**	0.85%
záleží na důvodu, proč využít služební PC, telefon nebo vozidlo k sourkomým účelům	1	**1.39%**	0.85%



21. Využíváte k monitorování svých zaměstnanců některé prvky monitoringu?

*Povinná otázka, respondent musel zvolit jednu z nabízených odpovědí a podle toho se mu zobrazily další otázky [**ano** → otázka č. 22, **ne** → otázka č. 27].*

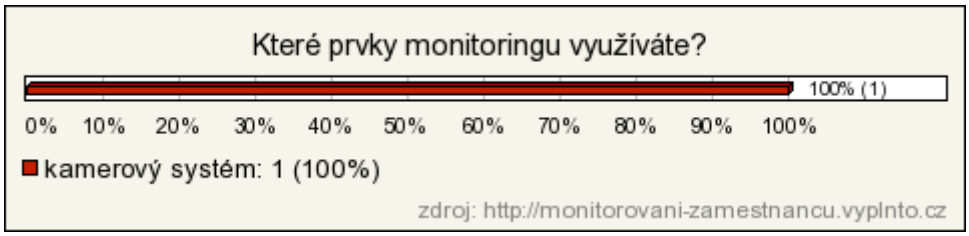
Odpověď	Počet	Lokálně	Globálně
ne	1	**50%**	0.85%
ano	1	**50%**	0.85%



22. Které prvky monitoringu využíváte?

Povinná otázka, respondent musel zvolit alespoň některou z nabízených odpovědí nebo dopsat nějakou vlastní.

Odpověď	Počet	Lokálně	Globálně
kamerový systém	1	**100%**	0.85%



23. Je pro Vás monitorování přínosem?

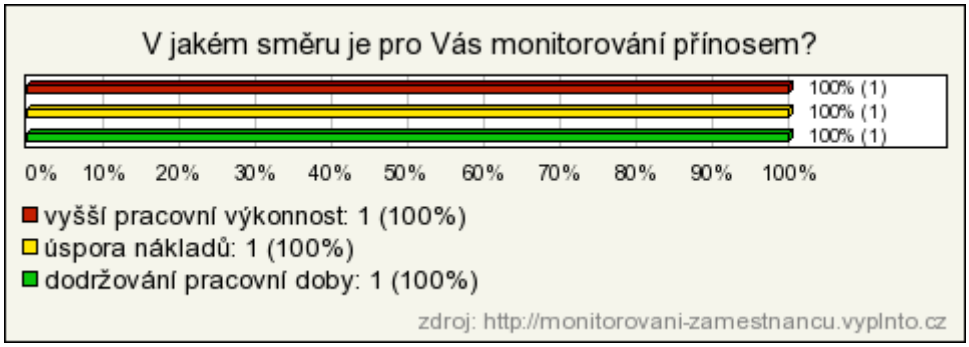
*Povinná otázka, respondent musel zvolit jednu z nabízených odpovědí a podle toho se mu zobrazily další otázky [**ano** → otázka č. 24, **ne** → otázka č. 25].*

Odpověď	Počet	Lokálně	Globálně
ano	1	**100%**	0.85%

24. V jakém směru je pro Vás monitorování přínosem?

Povinná otázka, respondent musel zvolit alespoň některou z nabízených odpovědí nebo dopsat nějakou vlastní.

Odpověď	Počet	Lokálně	Globálně
vyšší pracovní výkonnost	1	**100%**	0.85%
úspora nákladů	1	**100%**	0.85%
dodržování pracovní doby	1	**100%**	0.85%



25. Zaznamenal/a jste někdy stížnosti ze strany zaměstnanců?

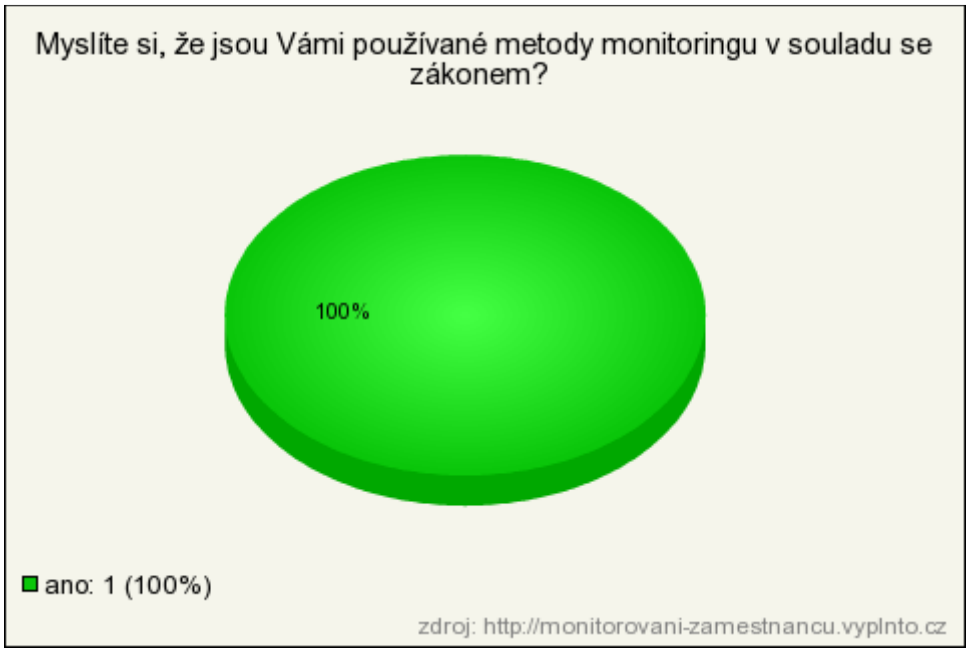
Povinná otázka, respondent se musel rozhodnout mezi odpověďmi „ano" a „ne".

Odpověď	Počet	Lokálně	Globálně
ne	1	**100%**	0.85%

26. Myslíte si, že jsou Vámi používané metody monitoringu v souladu se zákonem?

Nepovinná otázka, respondent se mohl rozhodnout mezi odpověďmi „ano" a „ne".

Odpověď	Počet	Lokálně	Globálně
ano	1	**100%**	0.85%



27. Plánujete jejich zavedení?

*Povinná otázka, respondent musel zvolit jednu z nabízených odpovědí a podle toho se mu zobrazily další otázky [**ano** → otázka č. 28, **ne** → otázka č. 29].*

Odpověď	Počet	Lokálně	Globálně
ne	1	**100%**	0.85%

28. Které?

Povinná otázka, respondent musel zvolit alespoň některou z nabízených odpovědí nebo dopsat nějakou vlastní.

Odpověď	Počet	Lokálně	Globálně
žádné odpovědi			

29. Z jakého důvodu?

Povinná otázka, respondent musel zvolit alespoň některou z nabízených odpovědí nebo dopsat nějakou vlastní.

Odpověď	Počet	Lokálně	Globálně
nepotřebujeme naše zaměstnance monitorovat, vždy se chovají v souladu s nařízeními	1	**100%**	0.85%