Monitorování zaměstnanců je legální!

Úřad na ochranu osobních údajů prostřednictvím zákona 101 nutí firmy, aby povolovaly zaměstnancům vyřizování soukromých záležitostí v pracovní době. Pracovníci Úřadu se svými stanovisky snaží omezit práva zaměstnavatelů, aby s péčí řádného hospodáře provozovali podnikání a dosahovali zisků. Neměl by vzniknout Úřad na ochranu firemních dat? V něm by měl zaměstnavatel oporu, pokud by chtěl mít přehled o využívání vlastních informací a prostředků IT.

Ochrana soukromí a osobních dat je jedním z úkolů bezpečnostního manažera (CISO). Nicméně jeho prioritou by také měla být ochrana dat zaměstnavatele. Mezi činnosti CISO patří sledování událostí, které se dějí v rámci informačního systému. Monitoring je jedním ze základních požadavků ISO 27001 (A10.10), sběr a vyhodnocování událostí je zdrojem pro měření bezpečnosti (viz ISO 27004). Proč však Úřad na ochranu osobních údajů vydává stanoviska [1], která brání v naplňování bezpečnostních standardů a nejlepších praktik?

Na začátek jednoduchý příklad. Jsem zaměstnanec. Mám k dispozici služební auto, sekretářku, notebook, mobil a kancelář. Vše patří mému zaměstnavateli (kromě té sekretářky, tu jen platí) a jeho prostředky mohu neomezeně využívat, ale...

1. Soukromě jezdit autem mohu jen v souladu s legislativními předpisy a na mé náklady.

2. Sekretářku nemohu poslat se soukromým dopisem na poštu nebo na víkendový nákup.

3. Na notebook nemohu instalovat své hry, ukládat stažené MP3 a filmy a půjčovat ho doma dětem.

4. Soukromé hovory sice řeším služebním telefonem, ale oficiálně to povoleno není.

Lze předpokládat, že v jiných firmách panuje obdobná kultura. Zaměstnanci mají k dispozici řadu firemních prostředků, které mohou a musí využívat pro pracovní účely. České zákony v některých případech upravují soukromé použití firemního majetku, např. je povinné platit daň za soukromé cesty služebním autem. Na firemním notebooku je možné mít pouze legální obsah a software s licencí na zaměstnavatele. Úřad na ochranu osobních údajů však nepřípustně rozšiřuje práva zaměstnanců na soukromé využívání firemních prostředků a zaměstnavatelům znemožňuje kontrolu využívání pracovní doby.

Legální monitoring pohybu zaměstnanců

Úřad (zatím) nemá nic proti monitoringu aut pomocí GPS nebo služby SherlogTrace. Oběma způsoby lze přesně určit, kde se fyzicky auto (a tedy i zaměstnanec) nachází. Lze detailně analyzovat jeho cestu od jednoho zákazníka k druhému. Zastavil se na hodinu na oběd? OK, v pořádku. Zajel si ve 14,00 nakoupit do Makra? To asi nebude v souladu s pracovním řádem.

Za předpokladu, že auto je přiřazeno pouze jednomu konkrétnímu řidiči, je možné po celou pracovní dobu sledovat jeho fyzický pohyb. Jak je tedy možné, že jeho virtuální pohyb po informačním systému sledovat nelze? Když lze postihnout zaměstnance za to, že strávil hodinu pracovní doby soukromým nákupem v Tescu, proč není možné zjistit jeho „zastávku“ na Alza.cz, kde si hodinu vybíral televizi do ložnice? Nebo jsou data o fyzickém pohybu zaměstnance získaná pomocí GPS osobními údaji? Milý Úřade, jaké je tvé stanovisko?

Problém je však někde jinde. Když se začal rozšiřovat Internet a e-mail, nikdo nedokázal odhadnout podíl firemní a soukromé komunikace. Nikdo nestanovil základní pravidla pro soukromé a firemní využívání. Je to logické, protože taková pravidla stanovit nešla, a je otázkou, zda nyní stanovit jdou. Když dnes zaměstnanec dostane firemní auto, musí jít povinně (ze zákona) na školení, podepsat, že

ho bude-nebude využívat pro soukromé účely a je srozuměn s tím, že nepovolená soukromá cesta bude ihned zjištěna díky monitorování GPS. Lze toto aplikovat i na firemní notebook?

Pokud dostane zaměstnanec auto s povolením využívat je pro soukromé účely, strhává se mu část ze mzdy. Stát si tedy uvědomuje, že může vybírat daň za soukromé využívání firemních prostředků. Kdy přijde stát na to, že by měl danit i soukromé používání firemního notebooku? Úřad ve svých stanoviscích explicitně uznává soukromé využívání firemních prostředků IT, proto ke zdanění není daleko.

(Ne)legální monitorování e-mailů

Ochraně zaměstnanecké e-mailové komunikace se detailně věnuje stanovisko 2/2009 [2] Úřadu, kde je uvedeno: *„Soukromý e-mail zaměstnance smí zaměstnavatel na základě oprávnění daných mu novým zákoníkem práce otevřít a přečíst pouze výjimečně, v zájmu ochrany svých práv, především jestliže je zřejmé, že se jedná o pracovní e-mail, tj. lze-li tento závěr učinit na základě údajů uvedených v hlavičce, a jestliže je pravděpodobné, že z objektivních důvodů, jako je dlouhodobá nemoc zaměstnance, by k jejímu vyřízení zaměstnancem mohlo dojít natolik pozdě, že by zaměstnavatel mohl utrpět újmu na svých právech.“*

Co to je „soukromý e-mail zaměstnance“? E-mailový účet vytvořený na poštovním serveru zaměstnavatele reprezentovaný e-mailovou adresou s firemní doménou nemůže být považován za soukromý. Zaměstnavatel má tady objektivní důvod předpokládat, že všechna data uložená na jeho poštovním serveru jsou firemní. A má také plné právo všechna uložená data analyzovat, zda se mezi nimi nenachází nelegální obsah. Shodný názor mají i renomovaní právníci pro oblast práva IT, viz Box 1.

A jak má zaměstnavatel poznat, že je obsah e-mailu soukromý, když není běžně oprávněn si přečíst ani záhlaví? I když ve výše uvedené citaci Úřad čtení hlavičky nezakazuje, v jiném odstavci stanoviska 2/2009 Úřad uvádí rozpor, kdy je záhlaví e-mailu možné přečíst pouze ve výjimečných případech: „Zaměstnavatel není oprávněn sledovat, monitorovat a zpracovávat obsah korespondence svých zaměstnanců. Zaměstnavatel případně smí u svých zaměstnanců pouze sledovat počet došlých a odeslaných e-mailů, případně (tj. zejména vznikne-li podezření ze zneužití pracovních prostředků, resp. využití k jiným než pracovním účelům) včetně hlavičky, tj. komu píší a od koho je dostávají.“ Inspektoři Úřadu musí být velmi zkušení bezpečnostní manažeři, když dokážou odhadnout zneužití pracovních prostředků pouze ze statistiky došlých a odeslaných zpráv.

Úřad se také ve stanovisku 2/2009 odkazuje na listovní tajemství a analogii e-mailu a papírové pošty. Zákon č. 29/2000 Sb., O poštovních službách v § 5 odst. 7 uvádí [3]: *„Je-li v poštovní adrese uvedena na prvém místě právnická osoba a na druhém místě fyzická osoba, za adresáta se považuje právnická osoba. Je-li v poštovní adrese uvedeno na prvém místě jméno a příjmení fyzické osoby a na druhém místě označení právnické osoby, za adresáta se považuje fyzická osoba s tím, že poštovní zásilka nebo poštovní poukaz má být dodán prostřednictvím této právnické osoby. Je-li v poštovní adrese namísto jména a příjmení určité fyzické osoby uvedena pouze její funkce v právnické osobě, za adresáta se považuje právnická osoba.“*

Analogicky však toto opatření nelze aplikovat na e-mail, protože ten svou strukturou může být pouze jednořádkový a vždy je na prvním místě jméno. Pokud kdokoli píše e-mail na firemní adresu, nemá možnost se rozhodnout, zda ho pošle jako soukromý (jmeno@firma.com) nebo firemní (firma@jmeno.com). Nelze ani využít pozice ve firmě. Kdo si může pamatovat, že zrovna Pepa Vopršálek je pracovnik27callcentrum2kolin@telefon.cz?

Úřad se snaží ve svém stanovisku nazvat osobními údaji téměř vše, co je spojeno s elektronickou komunikací. Dokonce samotná e-mailová adresa je podle něj osobním údajem: *„Ačkoliv e-mailová adresa patří zaměstnavateli, je-li složena ze jména a příjmení zaměstnance, např. Jan.Svoboda@doména.cz, je e-mail na ni doručený soukromou elektronickou poštou a taková e-mailová adresa je sama o sobě vždy osobním údajem.“* (citace ze stanoviska 2/2009)

Zde je však rozpor se samotnou definicí pojmu osobní údaj, viz § 4 odst. a) zákona 101/2000 Sb.: *„Osobním údajem je jakákoli informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu.“*

Opravdu lze podle e-mailu identifikovat konkrétní osobu? Ve velkých společnostech jsou běžné e-mailové adresy Josef.Novak1@firma.cz nebo Josef.Novak2@firma.cz nebo Josef.Novak3@firma.cz. A jak je to s e-mailem novak@firma.cz? Rozhodně lze pochybovat, že podle e-mailu, který je tvořen pouze na základě příjmení, je jednoznačně možné identifikovat konkrétního člověka. Je velmi pravděpodobné, že jestli je e-mail ve tvaru novak@firma.cz, je v dané firmě pouze jeden kon-

Slovo právníka – JUDr. Tomáš Sokol **BOX 1**

Celé je to poněkud šaškárna už teď. Pokud bez souhlasu zaměstnavatele nesmí zaměstnanec používat jeho počítač pro osobní potřebu, včetně osobní elektronické korespondence, pak to taky smí zaměstnavatel kontrolovat. Což zákoník práce připouští. V tom případě ale nelze brát ohled na soukromou korespondenci, neboť zaměstnavatel má zákonný důvod předpokládat, že v jeho počítači žádná takové není.

http://blog.aktualne.centrum.cz/blogy/tomas-sokol.php?itemid=8821

krétní, jednoznačně určitelný pan Novák. Pokud je však e-mailová adresa osobním údajem, pak jakékoli uvedení jména anebo příjmení je osobním údajem. Dojde snad Úřad tak daleko, že zruší jmenovky na schránkách a zvoncích? Podle nich lze úplně stejnou logikou také jednoznačně určit subjekt údajů. Musí majitel mobilu, kde jsou v adresáři uvedené všechny kontakty na osobu, podávat na Úřad oznámení o zpracování osobních údajů?

Monitorování přístupu na web

Úřad ve stanovisku 2/2009 také uvádí, že zaměstnavatel nesmí sledovat používání webových stránek zaměstnanci: *„Sledovat používání webových stránek zaměstnanci pro účely zaměstnavatele tedy možné není, pokud nejsou splněny zákonem stanovené podmínky, tj. závažný důvod spočívající ve zvláštní povaze činnosti zaměstnavatele. Pod tím si lze představit např. mezinárodní bankovní převody nebo dozor nad prací vězňů.“*

I když lze věřit ve vysokou kompetentnost pracovníků Úřadu, není možné toto stanovisko nepovažovat za přehnané. Logování přístupů na web společně s ID uživatele a IP adresou konkrétní pracovní stanice je standardní funkcí každého firewalu a proxy. Podle vyjádření Úřadu však hrozí pokuta 10 000 000 Kč všem organizacím, které mají takto připojený systém na Internet.

Úřad se ve svém stanovisku opírá o směrnici Evropského parlamentu a Rady 2002/58/ES, která mluví o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací. Ve stanovisku 2/2009 Úřad za směrnice cituje část článku 26: *„...údaje o účastnících, které jsou zpracovávány v rámci sítí elektronických komunikací pro navázání spojení a přenos informací, obsahují informace o soukromém životě fyzických osob a dotýkají se práva na ochranu jejich korespondence nebo se dotýkají oprávněných zájmů právnických osob. Takové údaje je možno uchovávat pouze v rozsahu, který je nezbytný pro poskytování služby pro účely účtování a platby za propojení, a to po omezenou dobu.“*

Pokud si ale pozorný čtenář přečte celý článek 26, pochopí, že Úřad vytrhává z kontextu věty, které se mu do jeho stanoviska hodí. Doplnění citace zní: *„Jakékoli další zpracování takových údajů, které by poskytovatel veřejně dostupných služeb elektronických komunikací chtěl provádět pro potřeby marketingu služeb elektronických komunikací nebo pro poskytování služeb s přidanou hodnotou, je přípustné pouze za předpokladu...“* Úřad tedy ve svém stanovisku úspěšně zamlčuje, že celá směrnice je o ochraně soukromí, kterou musí zajistit poskytovatel veřejně dostupných služeb elektronických komunikací, a tím zaměstnavatel pro své zaměstnance není (dokonce i v případě, že zaměstnavatel je ISP).

Zaměstnavatel může bez jakýchkoli obav před postihem Úřadu zaznamenávat všechny přístupy na všechny webové stránky ze všech firemních počítačů. Je zcela legální zaznamenávat události na proxy nebo firewallu a vyhodnocovat je, mj. i za účelem kontroly zaměstnanců a využívání pracovní doby. Log nemusí obsahovat ID uživatele (i když ID není osobní údaj), stačí zaznamenávat IP adresu, z níž jsou přístupy konány, a po vyhodnocení v potřebných případech spojit IP s konkrétním zaměstnancem.

Ano, lze legálně monitorovat e-maily

Zákoník práce v § 316 odst. 1 povoluje zaměstnavateli kontrolovat využívání firemních prostředků pro soukromé účely: *„Zaměstnanci nesmějí bez souhlasu zaměstnavatele užívat pro svou osobní potřebu výrobní a pracovní prostředky zaměstnavatele včetně výpočetní techniky ani jeho telekomunikační zařízení. Dodržování zákazu podle věty první je zaměstnavatel oprávněn přiměřeným způsobem kontrolovat.“*

Všechna data, která jsou uložena na zařízení zaměstnavatele, jsou v jeho vlastnictví, pokud smlouva nebo legislativní předpis nestanoví jinak. Není sporu v tom, že záznamy (logy) o aktivitě v systému jsou data, jejichž vlastníkem je zaměstnavatel. Rozsah záznamu o dané události je záležitostí nastavení nástroje pro log management, a pokud záznam neobsahuje osobní údaje, nelze na něj aplikovat zákon 101. V praxi tedy stačí, aby záznam o příchozím nebo odchozím e-mailu obsahoval celý obsah i hlavičku, kde však bude e-mailová adresa zaměstnance nahrazena anonymním identifikátorem. Tomuto se říká normalizace záznamů pro potřeby SIEM (Security Information and Event Management). Identifikátor bude možné zpětně spojit se jménem uživatele, ale přístup k této databázi bude přísně řízen a nemusí ho mít stejné osoby, jaké mají přístup k logům.

Analýza nad těmito logy (včetně obsahu e-mailů) může probíhat bez znalosti konkrétních osob a pouze v případech, kdy opravdu dochází k porušování pracovní smlouvy (tzn. že zaměstnanec nepracuje a řeší soukromou korespondenci), lze v jiném datovém zdroji (např. HR systém) identifikovat konkrétní osobu a zahájit např. disciplinární řízení.

Pokud chce zaměstnavatel monitorovat síťovou komunikaci svých zaměstnanců, musí je na to upozornit. Zákoník práce v § 316 odst. 3 dává zaměstnavateli povinnost přímo informovat zaměstnance o rozsahu monitorování a o způsobech jeho provádění. Ideálním místem, kde by takové upozornění mělo být uvedeno, je pracovní řád. Rozsah a způsob monitorování je také běžně uveden v řídicí bezpečnostní dokumentaci, ale zde to bude spíše z technického pohledu. Nicméně s bezpečnostní politikou by měli být prokazatelně seznámeni všichni zaměstnanci – uživatelé informačního systému.

Zaměstnavatel musí kontrolovat síťovou komunikaci

Nový zákoník práce v § 316 odst. 2 poněkud nešťastně zmiňuje, že zaměstnavatel

nemůže bez závažného důvodu kontrolovat elektronickou poštu: *„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.“* Škoda, že Úřad ve stanovisku necituje také první odstavec stejného paragrafu, kde zákoník práce zakazuje zaměstnancům *„...bez souhlasu zaměstnavatele užívat pro svou osobní potřebu výrobní a pracovní prostředky zaměstnavatele včetně výpočetní techniky ani jeho telekomunikační zařízení.“*

Otázkou zůstává, kdy má zaměstnavatel závažný důvod monitorovat e-maily. Je to ochrana vlastního majetku (data), sledování spotřeby pracovní doby nebo kontrola dodržování legislativy (např. autorský zákon). Pokud by zaměstnanec využíval firemní prostředky k rozesílání spamové pošty, a zaměstnavatel by neměl možnost efektivně kontrolovat komunikaci, mohl by se zaměstnavatel dostat do problémů, protože by neměl jak prokázat protiprávní jednání svého zaměstnance, resp. by o něm ani nevěděl. Bohužel pro zaměstnavatele by však v každém případě odpovídal za správní delikt rozesílání spamové elektronické pošty z firemního e-mailu (ust. § 118 odst. 1) písm. j) zákona o elektronických komunikacích). Možný postih pro zaměstnavatele je nemalý: až 10 % z výnosů dosažených za poslední ukončený kalendářní rok, nejvýše 10 000 000 Kč. Právní posouzení odpovědnosti zaměstnance nebo zaměstnavatele by bylo velmi složité a bez prováděné kontroly e-mailové komunikace by se zaměstnavatel mohl velmi jednoduše dostat do stavu důkazní nouze.

Zaměstnavatel může monitorovat a ukládat hlavičky i texty e-mailů, pokud důvodně předpokládá, že obsahují čistě firemní komunikaci, neboť tak to určují vnitřní organizační předpisy a pravidla, která zaměstnanec akceptoval. Podle platné legislativy je možné, a v některých případech nezbytné, takovouto komunikaci sledovat. A je spíše otázkou vkusu a etiky, kam až čtenář e-mailu zajde, když narazí na soukromé texty, viz rovněž další názor právníka v Boxu 2.

Není správné, aby zaměstnanec poslal soukromý papírový dopis na náklady zaměstnavatele a ještě k tomu zneužil jiných zaměstnanců, aby dopis odnesli na poštu. Stejně tak není možné explicitně povolovat soukromou elektronickou komunikaci realizovanou firemními prostředky na náklady zaměstnavatele. Zaměstnanci by neměli zneužívat benevolentnosti svých zaměstnavatelů. A pokud to dělají, měli by přijmout jím stanovené podmínky. Zaměstnavatel má plné právo sledovat všechny události v informačním systému a kontrolovat používání vlastních firemních prostředků.

Zůstává otevřená otázka, jak by rozhodl soud v případě, kdy jde o distribuci nelegálního obsahu. Do jaké míry by obstála výmluva zaměstnavatele na stanovisko Úřadu, že nemohl monitorovat e-maily zaměstnanců, kteří spamovali dětské porno? Jasno bude, až se takový případ dostane k soudu a ten pravomocně rozhodne. Do té doby nezbývá nic jiného, než komunikovat s pracovníky Úřadu a kontinuálně je vzdělávat v právních otázkách a nejlepších bezpečnostních praktikách.

Jan Mikulecký
mikulecky@rac.cz

Slovo právníka – Mgr. Tomáš Tyll **BOX 2**

Do říše pro zaměstnavatele potenciálně velice nebezpečných právních mýtů tedy nutno odkázat pověry o tom, že zaměstnavatel je povinen umožnit zaměstnancům na své náklady odesílání a přijímání jejich soukromé elektronické pošty, stejně jako názor, že zaměstnavatel nikdy a za žádných okolností nesmí kontrolovat firemní e-mail. Absurdnost posledně zmíněného názoru vynikne zvlášť v případě, pokud by zaměstnanec např. rozesílal z firemního e-mailu bez povolení a vědomí svého zaměstnavatele spamovou elektronickou poštu. Za prvé, zaměstnanec by tím vedle pracovně právních předpisů porušil i ust. § 93 zákona o elektronických komunikacích (zák. č. 127/2005 Sb., v platném znění), které 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) zákona o elektronických komunikacích. Za takový přestupek je možno uložit pokutu až 100 000 Kč.

http://www.akvks.cz/cz/novinky/archiv-novinek/muze-zamestnavatel-cist-e-mailovou-postu-svych-zamestnancu.html#1

Ing. Jan Mikulecký, Ph.D. CISM, CGEIT

Absolvent ČVUT Praha, od roku 1999 pracuje v RAC jako konzultant pro řízení rizik, ISMS, BCMS a penetrační testy. Člen komise ISACA CISM TES, rady ISACA ČR a redakční rady DSM.

POUŽITÉ ZDROJE

[1] Úřad na ochranu osobních údajů, *Stanoviska úřadu, 30/6/2010,* http://www.uoou.cz/uoou.aspx?menu=14&loc=329.
[2] Úřad na ochranu osobních údajů, *Stanovisko č. 2/2009, Ochrana soukromí zaměstnanců se zvláštním zřetelem k monitoringu pracoviště, únor 2009,* http://www.uoou.cz/files/stanovisko_2009_2.pdf.
[3] Program ZÁKON verze 4.0, *Vyhláška o základních službách držitele poštovní licence, 6/5/2010,* http://www.pravnipredpisy.cz/predpisy/ZAKONY/2004/286004/Sb_286004_——_.php.
[4] Úřad na ochranu osobních údajů, *zákon č. 101/2000 Sb., O ochraně osobních údajů, 4/4/2000,* http://www.uoou.cz/uoou.aspx?menu=4&submenu=5&loc=20.
[5] Úřední věstník L 201, *Směrnice Evropského parlamentu a Rady 2002/58/ES o soukromí a elektronických komunikacích 12/6/2002,* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:CS:HTML.