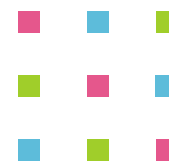
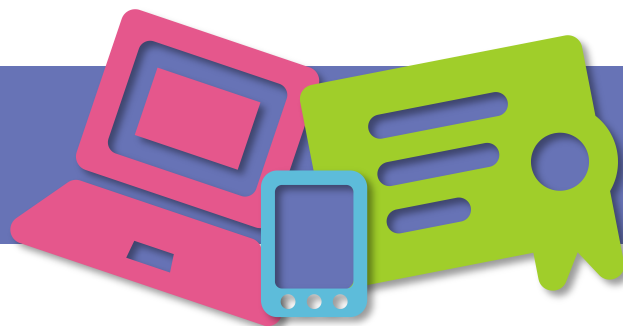


SECURITY 2014



22. ročník konference o bezpečnosti v ICT



BYOD – podmínky a konsekvence jejich provozu u podnikatele

Tomáš Roubík

Advokátní kancelář Roubík & spol.



Fenomén BYOD

- proč BYOD (**B**ring **Y**our **O**wn **D**evice)
 - zavedení elektronických pracovních prostředků ve vlastnictví pracovníka do procesů u podnikatele tak, aby jej vlastník zařízení - pracovník - mohl používat při práci pro podnikatele
 - cílem takového postupu je zpravidla
 - subj. zvýšení komfortu pracovníka při práci
 - úspory nákladů podnikatele



Slovníček pojmů

- BYOD pro účely této prezentace znamená jak mobilní zařízení tak i notebook, nebo PC
- pracovník = zaměstnanec nebo kontraktor,
- podnikatel = zaměstnavatel nebo objednavatel
- NOZ – nový občanský zákoník – tj. zákon č. 89/2012 Sb.
- OS – operační systém
- SW – software, pro mobilní BYOD častěji spíše aplikace
- Licence – výčet oprávnění k užití příslušného software



Pravidla pro používání BYOD - I

Vytvoření interních podmínek a standardů pro používání BYOD zařízení:

- závazek k dodržování pravidel pro užívání BYOD
- kontrola přístupu k BYOD zařízení (vynucení používání jednoduchého, nebo i sofistikované hesla)
- zavedení "time-out" – tedy ukončení činnosti u nepoužívaného zařízení
- používání zabezpečených (šifrovaných) komunikačních kanálů, úložišť dat a i aplikací, které s daty pracují
- používání antivirů a firewall
- povinnost včasné aktualizace používaného OS a SW
- vytvoření jednotlivých druhů BYOD zařízení - vyloučení některých činností pro jednotlivé druhy BYOD zařízení tak, aby bylo možno eliminovat/minimalizovat škody, jejichž vznik nelze adekvátně vyloučit jiným postupem



Pravidla pro používání BYOD - II

- souhlas vlastníka BYOD ke kontrole a zásahům podnikatele do BYOD včetně souhlasu ke zpracování os. údajů (pro případnou evidenci mimo BYOD v databázi podnikatele)
- souhlas ve vztahu k autorským právům, vytvořeným pracovníkem za pomoci BYOD zařízení
- vymáhání těchto podmínek podnikatelem
 - školení – často nazývané tzv. awareness program
 - fyzická kontrola při zahájení používání zařízení
 - vzdálená kontrola
 - evidence kontrolních úkonů
 - monitoring alespoň počtu a druhů BYOD zařízení u podnikatele
- možnost odesílání reportů o stavu zabezpečení každého zařízení
- umístění stránek nápovědy a stránek s často kladenými otázkami (FAQ) na firemní intranet

- kompenzace hodnoty BYOD zařízení podnikatelem
 - pracovník dostává kompenzaci za to, že dodržuje dohodnutá pravidla
 - nedodržování pravidel pak může mít vliv na výši kompenzace
 - výše kompenzace musí být adekvátní pořizovací hodnotě (nesmí ji v součtu překročit)
 - právně i psychologicky zavazující prvek



Zmapování procesů

- zmapování procesů, kde může dojít k vlivu BYOD na externí vztahy s cílem předcházení případným škodám
- zmapování procesů pro tvorbu interních pravidel (což je podstatné pro vytváření více skupin zařízení BYOD - s různými přístupovými oprávněními)
- vytvoření únikového plánu pro sebe i pro klienty pro případ zneužití nebo ztráty zařízení BYOD (např. vzdálené zablokování/smazání zařízení, smazání přístupových práv apod.)
- provádění pen. testů



Autorská práva - I

Autorská práva ve vztahu k zařízení BYOD a konsekvence pro podnikání

- tři okruhy
 - kompatibilita SW, nainstalovaném na BYOD zařízení, se systémy podnikatele
 - přístup k SW podnikatele za pomoci BYOD
 - kompatibilita SW, nainstalovaném na BYOD, se záměry (předmětem podnikání) podnikatele
- některé licence nemusí být kompatibilní se standardem u podnikatele, proto je potřeba dopředu vyjasnit, jakou licenci má SW na BYOD zařízení mít, aby bylo kompatibilní (např. není možné doménové nastavení apod.)
- řešerší obvyklého SW si ověřit vhodnost běžného SW v BYOD pro použití při podnikání (tj. aby použití pro business nebylo vyloučeno – což je např. případ licencí u software pro vzdělávání, který nelze používat ke komerčním činnostem – různé akademické licence apod.)
- v pravidlech vyloučit možnost, že SW, který není možné bez jiné licence používat pro podnikání, bude možné použít i v BYOD pracovníka



Autorská práva - II

- to samé by se týkalo vyloučení možnosti použít SW, který např. pracuje s různými typy volných licencí (GNU GPL licence, Creative Commons, Debian atd.), kde musíte dodržovat licenční podmínky, platné pro tento typ licencí
- zajistit si souhlas pracovníka s širokým využitím jím vytvořených autorských děl, pokud již není v jiné smluvní dokumentaci
- příklad z praxe: pokud např. budete vyžadovat, aby měl pracovník na svém BYOD zařízení antivir, případně jiný SW, je to možné, pokud to licenční podmínky původce toho SW připouští - což zpravidla ano, neboť licence jsou na zařízení a nikoli na vlastníka zařízení (samozřejmě vzniká otázka kontroly v případě auditu ze strany původce SW nebo nějaké kontrolní instituce)



Konsekvence

Možné konsekvence při nedodržení pravidel ve vztahu k podnikateli a ve vztahu k zákazníkům

- ve vztahu pracovník vůči podnikateli
 - porušení závazných pravidel, které je ve svém důsledku více či méně závažným porušením smlouvy mezi pracovníkem a podnikatelem
 - porušení mlčenlivosti
 - způsobení škody, které může být považováno za úmysl, tedy bez limitu
- ve vztahu podnikatele k zákazníkovi
 - porušení povinnosti k ochraně obchodního tajemství (§ 504 NOZ)
 - porušení ochrany důvěrných informací (smluvní)
 - porušení smlouvy se zákazníkem ve vztahu k dohodnutému způsobu přístupu k jeho datům
 - povinnost k náhradě škody
 - smluvní pokuty, pokud zajišťují povinnosti podnikatele vůči zákazníkovi
- konsekvence pro pracovníka - odstupňováno podle závažnosti porušení pravidel pracovníkem
 - krácení kompenzace
 - ztráta možnosti používat BYOD zařízení
 - ukončení smluvního vztahu s pracovníkem



Shrnutí na závěr

- Základem zavedení principu BYOD je pečlivá příprava a prevence. Následné nápravy při zanedbání přípravy jsou již bolestivé a nákladné.
- Chování pracovníků – ověřování skutečnosti, že vaši pracovníci dodržují pravidla pro užívání BYOD, je jednou z nejlepších bezpečnostních kontrol – a potvrzením vhodnosti BYOD koncepce.
- Shora uvedené postupy je také vhodné doplnit správnou komunikací s pracovníky, podporou managementu, včasnou reakcí a vysvětlením problémů a využívání praktických ukázek zneužití v rámci školení pracovníků.

Děkujeme za pozornost.

Tomáš Roubík

AK Roubík & spol.

tomas.roubik@akroubik.com

