5 největších bezpečnostních IT rizik při práci z domu či v terénu

Brno, 21. února 2013

Práci z domu či z terénu, neboli home či mobile office, využívá mnoho firem. Ušetří díky tomu peníze i čas zaměstnanců. Ne všechny společnosti si ovšem uvědomují, že je to práce s citlivými interními daty mimo prostředí firmy. A že tedy hrozí jejich zneužití nebo odcizení. Přinášíme vám přehled pěti rad, jak zabránit nejrizikovější situacím.

Pozor na soukromé počítače a notebooky
Největší riziko pro firmu představuje situace, kdy zaměstnanec využívá k práci své vlastní vybavení. Tedy svůj počítač, notebook, tablet, mobilní telefon či USB disk. Tato zařízení jsou pak zcela mimo kontrolu firmy. „*Uložená a zpracovávaná vnitrofiremní data leží v případě home office mimo chráněné prostředí firmy. V jakémkoliv množství a jakkoliv dlouho. Paměťové disky mají dost velkou kapacitu, a dokud na nich nedochází místo, tak se z nich maže jen minimum*," uvedl Martin Hanzal, výkonný ředitel společnosti SODATSW, která vyvinula nový šifrovací produkt AreaGuard Neo. Obrovské riziko představuje i fakt, že přístupové heslo nebo USB disk sdílí více lidí. Například rodič a dítě. „*Známe případy, kdy pubertální dítě zveřejnilo citlivá data na Facebooku. Proto radím, aby firmy dovolily zaměstnancům s vlastním vybavením přístup jen přes terminálový server. Pak se citlivá data na soukromá zařízení nedají stahovat*," doporučil Hanzal.

Důležitost centrálně řízené bezpečnostní politiky
Nejčastějším mobilním zařízením, na kterém zaměstnanci pracují, jsou notebooky. A firmy často dělají tu chybu, že na těchto zařízeních zanedbávají doménovou politiku, tedy centrální řízení bezpečnostní politiky organizace. Právě ta zajistí požadované bezpečnostní nastavení na všechny tyto notebooky. Jedná se především o řízení přístupových práv, antivirovou ochranu, správnou funkci firewallu. A také o nastavení šifrování, monitoringu práce s vnitrofiremními daty a další důležité bezpečnostní prvky, které jsou běžné uvnitř organizace. Navíc je nutné zajistit bezpečný přístup do vnitřní sítě organizace pomocí VPN, tedy virtuální privátní sítě. Díky tomu může zaměstnanec kdekoli pracovat úplně stejným způsobem, jako když sedí v kanceláři.

Uživatelský účet přístupová práva
To, že řadoví zaměstnanci mají nastavená administrátorská práva na notebooku, je další velmi častá chyba. Notebook se tím totiž zcela vymyká kontrole. Zaměstnanci také často používají příliš jednoduchá či snadno odhalitelná hesla. Tento problém se ale dá odstranit příslušností v doméně. Dalším rizikem je, že pod uživatelským účtem zaměstnance mohou s počítačem pracovat také rodinní příslušníci – nejčastěji děti. Je proto dobré mít na notebooku ještě druhý uživatelský účet s omezenými přístupovými právy k lokálně uloženým vnitrofiremním datům. Pod tímto účtem není možné přistoupit do vnitřní sítě a mohou ho tedy využít právě rodinní příslušníci. Tento účet může použít i oprávněný uživatel v případě, že se připojuje v nebezpečném prostředí, jako je třeba veřejná wi-fi síť, na internet.

Šifrování bez nároků
Každé zařízení s citlivými daty, které zaměstnanec vynáší mimo společnost, musí používat šifrování citlivých dat organizace. V praxi nejúčinnější ochranou je šifrování uživatelského profilu. Ten totiž obsahuje soubory s citlivými firemními daty a veškerou mailovou korespondenci včetně kontaktů, kalendáře a úkolů. Šifrování celého profilu zajistí, že data jsou kdekoliv přístupná pouze jejich oprávněnému uživateli, a nikdo je nemůže zneužít ani při ztrátě či odcizení notebooku. Současně to na zaměstnance neklade žádné další nároky. Pokud je notebook v doméně, pak zůstává uživateli pouze jedna autentizace – nutná znalost jediného přístupového hesla. A správa IT má přesně pod kontrolou, jestli jsou všechna data v bezpečí. Podobně je zapotřebí použít šifrování také pro všechna data, která se přenáší přes USB flashky a externí disky.

Do mobilů jen část pošty
Tablety a mobily jsou velkým bezpečnostním rizikem pro všechny firmy, které přemýšlí nad ochranou svých dat. Nástroje pro jejich správu jsou zatím velmi omezené, cenově nedostupné a navíc nepohodlné. Proto jedinou účinnou ochranou je na tato zařízení žádná citlivá data neukládat. A použít je pouze k lokálnímu uložení části pošty. „*Tato zařízení obecně slouží spíše k náhledu na data. Ovšem i k tomu doporučuji použít přístup přes terminálový server. Je také dobré proškolit uživatele a vytvořit směrnici pro použití tabletů a mobilů. Směrnice například určí, že zařízení musí chránit přístupové heslo, které je potřeba vždy zadat po více než pěti minutách nečinnosti uživatele*," doporučil Martin Hanzal ze společnosti SODATSW. Je dobré také zapnout vnitřní šifrování paměti a vyhýbat se ukládání nebo dlouhodobému uložení citlivých dat organizace.

SODATSW spol. s r.o.

SODATSW spol. s r.o. je výrobce a dodavatel originálních řešení určených pro správu a bezpečnost pracovních stanic. Profesionální ochraně dat a monitoringu činností na počítačích se věnuje již od roku 1993. Šifrování dat společnosti SODATSW využívá například Ministerstvo vnitra ČR, Ministerstvo obrany ČR, Ministerstvo školství, mládeže a tělovýchovy či Ministerstvo financí ČR. Data pomáhá chránit i dalším orgánům státní správy a samosprávy, školám, zdravotnickým zařízením stejně tak jako bankám a malým i velkým firmám. Jen v České republice chrání technologie SODATSW více než 50.000 počítačů.

SODATSW disponuje certifikátem Microsoft Partner. Společnost úspěšně absolvovala certifikační audit systému kvality mezinárodního standardu ISO 9001:2009 pro systém managementu kvality vývoje, technické podpory a implementace a zároveň ISO/IEC 27001:2006 pro systém managementu bezpečnosti informací. SODATSW získal také osvědčení podnikatele od NBÚ pro seznamování se s utajovanými informacemi do stupně utajení Důvěrné. Od podzimu 2011 je členem poradní skupiny NIAG Cyber Defence při vedení NATO v Bruselu.

Kontakty

Martin Hanzal
výkonný ředitel SODATSW spol. s.r.o.
Horní 32, 639 00 Brno
Tel: +420 602 702 780
e-mail: martin@sodatsw.cz
www.sodatsw.cz