

## Fyzické zabezpečení bezdrátových sítí

Během hledání relevantních informací o tomto tématu jsem byl nemile překvapen jejich nedostatkem. V naprosté většině případů, i v napohled kvalitních dokumentech, nebyla zmíněna ani základní fyzická opatření bezdrátových vysílačů. To je možné opomenout snad jen v případě, že zřizujeme bezdrátovou síť pro domácnost. Zde je jasné, že se jedná o soukromé, uzamčené prostory, do kterých mají přístup pouze členové rodiny a případné návštěvy. I tato informace by ovšem měla být v textu explicitně zmíněna.

Cílem těchto opatření je zabránit neautorizovaným osobám v použití bezdrátových zařízení k získání přístupu k síťovým zdrojům a komunikaci. Dobrým doporučením je dbát na zabezpečení všech mobilních zařízení, kde si uživatelé často nechávají uložená hesla a může dojít k jejich ztrátě nebo odcizení. Vzhledem k velkým důsledkům útoku v případě přímého přístupu k bezdrátovým vysílačům a k dostupnosti levných, ale účinných metod fyzické ochrany bych doporučil věnovat těmto zabezpečením zvýšenou pozornost. Očividným rizikem je možnost resetovat přístupový bod na tovární nastavení, které často není šifrované a k přístupu vyžaduje heslo, které lze najít na internetu. Druhým nebezpečím je, že se útočník připojí do fyzického portu, čímž obejde zabezpečení bezdrátové sítě. Možností ochrany je hned několik.

1. Namontování přístupového bodu (AP) na strop nebo zeď, kam není možné se lehce dostat nebo je umístíte do zabezpečených míst jako jsou uzamykatelné skříňky či serverovny.
2. Použití AP odolné proti neoprávněné manipulaci (tamper-proof). Obvykle bývají zabezpečené zámky nebo šrouby, které znemožňují jeho otevření, připojení dalších kabelů, jeho resetování a jeho přemístění např. LN2600 Rugged Security Router.
3. Jako další fyzické opatření lze brát omezení dosahu signálu tak, aby pokrýval pouze určený prostor a nešířil se např. mimo sídlo firmy. Tímto zabráníme možnosti odposlechu bezdrátové komunikace někým kdo není zaměstnancem a nemůže být vpuštěn do budovy.
4. Veškeré kapesní počítače zabezpečte silným heslem a použijte PSK šifrování.
5. Zapněte automatické zamykání kapesních počítačů po určité časové prodlevě a nastavte vyžadování hesla po zapnutí.
6. Používejte monitorovací systém pro kontrolu zda všechna zařízení fungují správně, žádné nechybí, nebo žádné nepřebývá.

Při zřizování podnikové bezdrátové sítě je nutné mít na paměti, že nezabezpečujete síť pouze před útočníky zvenčí, ale i před zaměstnanci. Dle průzkumu společnosti Symantec byl v roce 2011 nejčastějším zlodějem dat současný zaměstnanec firmy, muž ve věku 37 let, zastávající pozici programátora, vědce nebo inženýra.

Maceček Miroslav  
396328

### Zdroje:

<http://www.symantec.com/connect/blogs/insider-data-theft-when-good-employees-go-bad>  
<http://www.verizonenterprise.com/DBIR/2013/>

Wireles Special Interest group. PCI DSS Wireless Guidelines, 2011