

Fyzická bezpečnost bezdrátových počítačových sítí

V poslední době nastává rozvoj bezdrátových sítí. Může za to jednoduchost spojená s mobilitou a rostoucí počet malých zařízení, která už se k fyzickému kabelu ani nepřipojí a přesto ke své činnosti potřebují internet. Ve spojitosti s tímto rozšířením bezdrátových sítí však přichází bezpečnostní rizika, která u fyzických sítí nebyla. Pokud je však někdo aktivně řeší, často pak zapomíná na rizika související s drátovými sítěmi, které ty bezdrátové rozšiřují. Právě těmito riziky se bude zabývat můj text.

Bezpečnost pro uživatele Připojením k síti přes kabel získáváme pocit bezpečnosti. Myslíme si, že na rozdíl od bezdrátové komunikace, nás nikdo nemůže odposlouchávat, takže můžeme si nedávat pozor na používání HTTPS pro autentizaci a šifrování webových služeb. Toto je však nebezpečné podcenění situace. Pokud nemáme fyzicky přehled, odkud kam ethernetový kabel vede, může se stát, že naší komunikaci může odposlouchávat někdo zapojením nějakého svého uzlu do sítě před nás. Pokud by měl útočník větší motivaci a menší možnost ovlivnit fyzicky síť, může odposlouchávat pomocí citlivého měření elektrických signálů, které se v kabelu šíří⁽¹⁾. Tomuto problému ještě napomáhá, že u drátové komunikace se mnohem méně chrání bezpečnost. V bezdrátových sítích už je dnes standardem šifrované WPA, drátovou komunikaci šifruje málokdo. I autentizace uživatele je u bezdrátových sítí komplexnější, příkladem může být i naše fakultní síť. Pro autentizaci na WiFi máme možnost volby wlan_fi, nebo Eduroam (fi), přičemž Eduroam má autentizaci pomocí PEAP, při připojení do sítě fyzicky potřebujete provést jen přihlášení na fadmin (čímž jsme na úrovni wlan_fi, tedy v situaci, kdy je po autentizování jedinou kontrolou ICMP vázané na MAC adresu, která lze změnit).

Bezpečnost z pohledu správce Právě snadná autentizace je největší riziko pro síť z pohledu správce. Zatímco konfiguraci přes WiFi naštěstí už někteří výrobci domácích síťových prvků zakazují z výroby, správa s fyzickým připojením není (alespoň u základních zařízení) problém. Až v enterprise sféře lze síťové prvky konfigurovat jedinečně pomocí konfiguračního portu (ať už přes ethernet, nebo seriový port). Pak se zase musí dbát na to, aby se do místnosti s těmito zařízeními nedostal nepovolaný člověk. Kromě možnosti přímé konfigurace by měl možnost provést i tovární reset.

Navrhovaná řešení pro uživatele Bezpečnost z pohledu uživatele se zvýší s lepší informovaností. Pokud bude znát možnosti odposlouchávání a zároveň mu řekneme, že se tomu vyvaruje používáním HTTPS, pak by jej to mohlo vést například k používání rozšíření do prohlížeče HTTPS Everywhere. Obecně se může řídit i dalšími radami pro používání nezabezpečené bezdrátové sítě, alespoň v případě, že drátovou síť, ke které se připojuje, nezná. Na druhou stranu to však nemá smysl přehánět a přemýšlet o routeru, který by podporoval šifrování, pro domácí síť.

Navrhovaná řešení pro správce sítě Konstruktor sítě by měl myslet i na fyzické zabezpečení sítě. Je hezké, že vymyslíme perfektně zabezpečenou bezdrátovou síť, ale

útočník bude mít možnost se do sítě připojit ethernetovým kabelem, který visí ze zdi. Proto by už při návrhu infrastruktury mělo být dbáno na ochranu síťových prvků. Umístění routeru na strop do výšky 3 metry ochrání před většinou potenciálních útočníků, ale pokud by někdo měl opravdovou motivaci se k takovému routeru dostat, tak bez jiných bezpečnostních opatření pro něj nebude pouhá výška omezením. Pokud by hrozilo, že motivace pro odposlouchávání je opravdu veliká, pak se dá uvažovat i nad zavedením šifrování pro drátovou komunikaci. Každopádně je nutné rizika znát a zvážit, jakou hodnotu má tajnost přenášených dat po síti.

Závěr Tento text je docela protichůdný proti tématu, zdali vůbec používat bezdrátovou síť. Bezdrátové sítě podpořily vývoj v zabezpečení, používané protokoly pro šifrování i autentizaci jsou dnes vyspělé, zatímco drátovou komunikaci považujeme naivně za bezpečnou. Většina útoků na bezdrátové sítě je vedena skrze špatné nastavení (režim WPS u WPA, slabé hesla). Stejně tak však špatné nastavení (i fyzické) může znamenat stejně výrazné chyby pro drátovou komunikaci. Bylo by hezké, kdyby se některé bezpečnostní prvky, které se používají pro bezdrátovou komunikaci rozšířily i do té drátové.

Zdroje

⁽¹⁾ Odposlouchávání signálů přenášených elektrickým vodičem

⁽²⁾ Zabezpečení WiFi