IT doupě

# Jak funguje Internet – LAN security

Ahoj a vítám vás u dalšího dílu. Pokud jste zatím tyto články četli a některým z nich i porozuměli, máte zřejmě docela dobrou představu o tom, „Jak funguje Internet“. Veškeré protokoly, hesla, nebo šifrování jsou vám ovšem k ničemu, pokud útočník získá k zařízení fyzický přístup. Stačí jeden port switche a dokáže probourat celou síť. Jak to dělá a jak tomu ideálně zabránit? To bude téma dnešního dílu.

Začněme zlehka. Není špatný nápad nastavit na zařízeních hesla a vypnout všechny nepoužívané porty. Tímto eliminujeme drtivou většinu všech možných útoků. No jo, ale co připojené porty? Aby útočník nenahradil některé z vašich počítačů svým riced Kali linux Thinkpadem, musí se i tyto porty zabezpečit. Dobrým způsobem je pamatovat si MAC adresy připojených zařízení a pokud se najednou neshodují, port buď natvrdo vypnout nebo alespoň blokovat všechen jeho provoz. Tohle dnes umí většina switchů na trhu.

A otevíráme králičí noru (zase). Pokud totiž zjistíme whitelistnutou MAC adresu, není tak těžké ji zkopírovat a vložit do našeho framu. Pak potřebujeme těžší kalibr – protokol 802.1x neboli něco, co zvládá AAA (authentication, authorization and accounting – kdo je to, jaká má práva a všechno zaznamenat). Nejčastěji se používá centralizovaný RADIUS server a takto zabezpečená síť nepustí žádné zařízení dovnitř do té doby, dokud se neprokáže platnými údaji (ideálně certifikátem, o bezpečnosti hesel víme všichni svoje). Takto můžeme zabezpečit i všechny routery a switche a rázem máme naprosto bezpečnou síť… téměř.

Síť je bezpečná jen tolik jako její nejslabší článek. Tím jsou samozřejmě myšleni uživatelé. Proti social engineeringu sice moc zbraní neexistuje, nicméně můžeme alespoň zablokovat podvodné weby (například YouTube a Google mapy) a emaily, a to přímo serverem, kterým budou muset všechny tyto pakety projít. V extrémních případech se dá dokonce udělat whitelist povolených webů, ale riskovat demonstrace zaměstnanců, kteří nebudou mít přístup na novinky.cz, asi nikdo nechce. Spoustu lidí dnes pracuje z domova, a proto je důležité umožnit připojení pouze přes šifrovanou VPN a zabránit tak vyzrazení informací napůl cesty.

Nakonec je ještě nutné zabezpečit samotné klienty. I tady můžete RADIUS použít pro jakoukoliv authentikaci, nicméně uživatel, ať už legitimní či nikoliv, má zde mnohem volnější ruce. Může smazat systém a nahradit ho svým. Může použít Gobbler a rezervovat všechny adresy v DHCP. Může se díky ARP vydávat za default gateway. Může ze sebe udělat DHCP server a nabízet falešné ínformace. Může ze sebe udělat switch, připojit se na DTP trunk a volně přecházet mezi VLAN. Může zneužít Native VLAN a udělat to samé co v předchozím kroku. Může ze sebe udělat Root Bridge. Může… asi chápete, kam tím mířím. A i přesto, že se všem zmíněným problémům dá různými způsoby předejít, stačí chyba konfigurace nebo nová zranitelnost a někdo se špatnými úmysly si cestu skrz vždy najde.

Ne vždy to musí skončit takto negativně. Pokud vás zabezpečení sítě zajímá stejně jako mě, kromě CCNA 2 si můžete zkusit i CyberOps Associate, který naše škola nabízí zdarma a pomůže vám s pochopením kyberbezpečnosti, dalšího z oborů, který AI ještě chvíli dominovat nebude. Snad jste se dnes něco nového dozvěděli a do dalšího měsíce Informatice Zdar!

Jan Dlabaja, 3L