



Redakční otázky k tématu "VZDÁLENÝ PŘÍSTUP – RIZIKA PODNIKOVÉ MOBILITY"
na ICT SECURITY

Comguard – Vymezte zdroje přístupné vzdáleně!

Autor odpovědí:

Mgr. Marian Lysák, Senior Security Consultant, COMGUARD a.s.

1) Jsou dnešní technologie již plně připravené na zajištění bezpečnosti při zachování plné mobility?

Dnešní technologie dostupné na IT trhu ušly dlouhou cestu k tomu, aby splňovaly požadavky dnešních dnů na zajištění bezpečnosti mobilních uživatelů. Další vývoj a ještě delší cesta je čeká v budoucnu, ale již dnes splňují technologie základní požadavky, které jsou na ně kladeny. Uživatelé se připojují do firemních a jiných sítí na potřebné zdroje bezpečným šifrovaným kanálem, který se ustanoví mezi klientským softwarem a zařízením / branou pro vzdálený vstup do sítě. Kromě tohoto kanálu, který zajišťuje utajení, dnešní technologie podporují ověření identity uživatele na základě využití PKI struktur a dvoufaktorové autentizace. Ještě, než je uživateli zpřístupněn zdroj v síti, obvykle prochází hloubkovou kontrolou i samotné zařízení, ze kterého uživatel inicioval spojení. Pokud se ustanoví bezpečný kanál, je ověřena identita uživatele a přístupový bod je úspěšně prověřen, pak dostane uživatel k dispozici požadované zdroje v cílové síti na základě své autorizace. Kromě toho další komunikace může být kontrolována mechanismy, které detekují únik dat, případně další nežádoucí provoz, který je tímto spojením generován. Příkladem může být SSL VPN brána NeoAccel, která provádí kontrolu nejen koncových stanic, ale i plnění bezpečnostní politiky organizace. Tj. například možné vymezení zdrojů, ke kterým má uživatel vzdálený přístup. Výrobce považuje tuto funkcionality kontroly plnění bezpečnostní politiky natolik důležitou, že jako jeden z mála nevyžaduje žádné speciální příplatky.

2) Jak nejlépe v oblasti mobilní bezpečnosti eliminovat tzv. lidský faktor?

Tato otázka ihned nabízí odpověď ve smyslu, že s lidským faktorem lze do jisté míry bojovat, ale nelze jej úplně potlačit. Je to pravdivé tvrzení. Vezmeme-li téměř automatický provoz v atomových elektrárnách nebo funkci autopilota v nadzvukových letadlech dojdeme k přesvědčení, že ačkoliv zmiňované obsahuje hodně automatických prvků, lidský faktor tam hraje velmi důležitou úlohu a že jej nelze úplně eliminovat. U přístupů mobilních uživatelů je situace stejná. Hodně bezpečnostních záležitostí lze vyřešit za samotného uživatele, aniž by o tom věděl, ale vždy přijde na řadu akce samotného uživatele, něco, co musí zmáčknout anebo vyplnit. V tomto momentě přichází ke slovu lidský faktor, který je, jak už jsme uvedli, nevyzpytatelný. Jak moc je toto potlačeno, má vliv na zatížení administrace bezpečnostních prvků, které do této komunikace vstupují. Hodně technologií směřuje řešení problematických situací na samotné uživatele pomocí self-desků apod. tak, aby si problémy uživatelé pokud možno vyřešili sami a nezatěžovali drahou pracovní sílu administrace. O lidském faktoru se lze bavit i v souvislosti s únikem informací, ať už vědomým nebo nevědomým



zapříčiněním dotyčným uživatelem. Na takové situace existují zbraně, které jsem částečně popsal v odpovědi na předchozí otázku.

3) Jak vynutit bezpečnost u zařízení, ke kterým není přímý fyzický přístup?

V této problematice se dostáváme na práh rozlišení mezi fyzickou bezpečností (zamčené dveře, přístupové kódy, bezpečnost budovy ...) a bezpečností systémů na softwarové úrovni (firewally, antiviry, ips sondy ...). Vynutit bezpečnost u zařízení, ke kterým není přímý fyzický přístup lze právě jen na té druhé úrovni. Pokud přímý fyzický přístup neexistuje a je možné docílit i fyzické bezpečnosti např. z důvodu, že organizace, která provádí softwarové zabezpečení je jiná, než ta, co provádí fyzické zabezpečení, pak celá skládanka dává smysl a oba prvky zabezpečení jsou splněny.

4) Je důležité při současném stavu technologií rozlišovat mezi mobilními a nemobilními řešeními?

Pokud směřujeme k tomu, že rozlišujeme mezi uživateli, kteří jsou připojeni do sítě bezdrátově a uživatele, kteří jsou připojeni drátově, pak mezi tím v dnešní době rozlišovat stále musíme. Rozsah bezpečnostních pravidel uplatněných na obě skupiny není stejný. Tato situace plyne z použitých protokolů v obou případech. Skupina protokolů bezdrátových přístupů je mladší. Stále prochází vývojem a změny v bezpečnostních prvcích jsou vždy s novou verzí přínosem. S ohledem na obsah komunikace je na dané organizaci a její vyhodnocení rizik, kterou z metod je ještě únosné použít a kterou již nelze použít pro velké riziko narušení komunikace a následujících ztrát.

5) Představuje příchod systému Windows 7 s novými možnostmi (jako např. DirectAccess) výrazné zvýšení bezpečnosti mobilních systémů?

Pokud za mobilní systémy budeme považovat přenosné počítače uživatelů, pak určitě každá nová verze Microsoft Windows přinesla podstatné změny, které měly pozitivní vliv na zabezpečení systému a síťové komunikace. Služba DirectAccess, která je podporovaná na systémech Windows 7 a serverech Windows Server 2008 R2 je jistě zajímavá. V řeči výrobce přináší přístup mobilních uživatelů na zdroje vzdálených sítí bez použití spojení VPN, což by mělo mít za následek eliminace administrátorského času a také větší zabezpečení. Administrátoři by v tomto případě měli mít mobilní uživatele více pod kontrolou, podobně, jako uživatele, kteří jsou přímo v dané síti. Slova VPN ve spojení s protokolem IPv6-over-IPsec, který je součástí této komunikace, bych se ale nebránil. Jestli technologie opravdu přinese deklarované možnosti, ukáže až čas, který ji prověří. Dnešní doba ale zažívá boom technologií pro vzdálené připojení SSL VPN, které odstraňují potíže protokolu IPsec. Příkladem může být opět firma NeoAccel, která nabízí řešení bezpečného vzdáleného připojení se všemi vymoženostmi, které jsou dostupné na technologickém trhu.