# Návrhy zabezpečení informačních systémů proti průnikům přes RDP, SSH a MS VPN (RAS)

**Kontrola, zda nedošlo ke kompromitaci systému**

- Kontrola přítomnosti neznámých lokálních účtů a profilů na serveru
- Kontrola přítomnosti webového prohlížeče (nejčastěji portable verze Google Chrome, ale může se lišit)
- Kontrola logu úspěšného vzdáleného připojení k serveru via RDP
- Kontrola zadních vrátek – zda nejsou otevřeny nelegitimní porty, zda neběží nelegitimní služby
- Kontrola běžících procesů, zda neběží nelegitimní procesy (s tím souvisí i kontrola výkonu serverů – zda nějaký nelegitimní proces/služba nespotřebovává velké množství prostředků serveru)
- Kontrola nainstalovaných programů
- Kontrola zapnutého antivirového řešení (útočník často vypíná antivirový program)
- Kontrola přítomnosti podezřelých .exe souborů ve složce C:\windows\system32 (např. 122334455.exe)

**Zabezpečení Remote Desktop Protocol**

- Zakázat připojení pomocí RDP z WAN, povolit pouze z LAN
- Pro připojení do LAN používat VPN (ne MS VPN RAS)
- Pomocí firewallu omezit zdrojovou adresu, ze které je možné se přihlásit na RDP
- Používat RDP over SSL
- Zapnout logování nejen úspěšného přihlášení, ale i neúspěšných pokusů o přihlášení na cílovém stroji
- používat Network Level Authentication (NLA) – pouze na Windows Server 2008 a vyšší
- nastavit RDP tak, aby naslouchal na jiném portu než na standardním 3389

**Účty**

- používat opravdu silná hesla

- nastavit rozumnou lock-out politiku pro zamykání účtů
- nepoužívat defaultní účet Administrator, vytvořit jiného privilegovaného uživatele s jiným jménem (hůře uhádnutelným než Administrator nebo admin)

**Zabezpečení SSH**

- Zakázat přihlášení uživatele root přes SSH
- Používat RSA autentizaci (RSA klíče se „silnou“ passphrase)
- Omezit zdrojovou adresu, ze které je možné se přihlásit na SSH
- Zakázat X11 forwarding

**Obecné zásady**

- Důsledně dbát na včasné aktualizace systémů
- Důsledně zálohovat systémy a zálohy nemít online připojené k provozním systémům (využít možností zálohovacího SW nebo odpojovat pomocí skriptu) – ochrana před ransomware, který je použit v druhé fázi útoku