ENJOY SAFER TECHNOLOGY™

RDP - dobrý sluha může být i zlý pán

Pandemie COVID-19 radikálně změnila povahu každodenní práce. Velká část zaměstnanců vykonávala svou práci z domova pomocí vzdáleného přístupu. Trend home office však představuje velkou příležitost pro kybernetické útočníky.

Před pandemií:

Drtivá většina zaměstnanců pracovala v kanceláři.

Infrastruktura byla pod dohledem a kontrolou IT oddělení.

Během a po pandemii:

Většinová část „kancelářské" práce je vykonávána z domácího prostředí.

Zaměstnanci přistupují k firemním systémům a citlivým datům prostřednictvím protokolu RDP (Remote Desktop Protocol).

VPN

Ačkoli je správa dat na firemním serveru výrazně bezpečnější pomocí VPN, obzvláště pokud je pojištěna dvoufaktorovou autentizací, **RDP i přes řadu rizik využívá velký počet firem.**

V případě využívání RDP je nutné dbát na správné nastavení.

3389

Zásadní problém je otevření portu 3389 do internetu.

Nezabezpečený port 3389 je nejběžnější – nejčastěji jde o Windows Server s otevřeným vzdáleným přístupem.

Díky častým chybám v nastavení se RDP se stalo populárním vektorem útoku.

Během pandemie byl zaznamenán výrazně vyšší počet ESET klientů, u kterých byly útoky či pokusy o útok evidovány. **V porovnání s letošním lednem se na konci června jednalo o 112 % nárůst.**

Doporučení pro nastavení RDP:

Omezení přístupu k RDP z internetu.

Použití silných hesel, která mají potenciál předcházet slovníkovému útoku.

Dvoufaktorová autentizace v rámci přihlášení.

3389

Omezení na firewallu externí připojení k místním zařízení přes port 3389.

Pravidelně aktualizovaný software na všech koncových stanicích.

46

Limitovaný počet neplatných přihlášení – pokud by RDP čelilo slovníkovému útoku, tak se po určitém počtu pokusů zařízení zamkne.