UPOZORNĚNÍ K PŘESMĚROVÁNÍ PORTŮ

(Port Forwarding)

Přesměrování portů umožňuje zpřístupnit zařízení umístěná v lokální síti zákazníka (např. IP kamery, servery, řídicí jednotky, NAS apod.) přímo z veřejné internetové sítě.

V praxi to znamená, že tato zařízení mohou být dostupná odkudkoliv z internetu. Aktivací této funkce dochází ke **zvýšení bezpečnostních rizik**, která je nutné vzít v úvahu.

1. **Bezpečnostní rizika**
    - Zařízení zpřístupněná prostřednictvím přesměrování portů jsou trvale dostupná z veřejné sítě a mohou být cílem
        - automatizovaných skenů
        - pokusů o neoprávněný přístup
        - zneužití známých nebo dosud neopravených bezpečnostních zranitelností
    - Nesprávná konfigurace nebo neaktuální software může vést zejména k
        - neoprávněnému přístupu k zařízení nebo datům
        - narušení funkčnosti sítě
        - zneužití zařízení k útokům na jiné systémy v síti internetu
2. **Odpovědnost zákazníka**

    V případě aktivního přesměrování portů

    - nese **plnou odpovědnost za provoz, zabezpečení a správnou konfiguraci zpřístupněných zařízení zákazník**
    - zákazník je povinen zejména
        - udržovat zařízení, firmware a software v aktuálním stavu
        - používat odpovídající autentizační a bezpečnostní mechanismy
        - zajistit, aby zpřístupněné služby neohrožovaly bezpečnost sítě

    Poskytovatel připojení **nenese odpovědnost za škody vzniklé v důsledku zneužití zařízení zpřístupněných prostřednictvím přesměrování portů**.
3. **Opatření při ohrožení bezpečnosti sítě**

    V případě, že bude zjištěno, že z přípojky zákazníka dochází k

    - útokům na jiné systémy nebo sítě
    - šíření škodlivého provozu
    - jinému jednání, které ohrožuje bezpečnost, stabilitu nebo integritu sítě

    vyhrazuje si poskytovatel právo **dočasně omezit nebo zablokovat provoz přípojky**, a to **bez předchozího upozornění**, do doby odstranění problému a zajištění nápravy ze strany zákazníka.

    Obnovení plného provozu je podmíněno prokazatelným odstraněním příčiny bezpečnostního incidentu.
4. **Doporučená bezpečnostní opatření**

    Pokud je přesměrování portů nezbytné, doporučuje se

    - **omezit přístup pouze na konkrétní zdrojové IP adresy**
    - **minimalizovat počet otevřených portů a zpřístupněných služeb**
    - **pravidelně kontrolovat stav zařízení a síťový provoz**

    Dále doporučujeme zvážit využití pokročilých bezpečnostních služeb, které nabízíme:

    - **FlowCutter – bezpečnostní monitoring sítě**
        - informace o provozu a aktivitách ve vnitřní síti
        - pohled útočníků na perimetr z internetu
        - denní report otevřených portů směrem do internetu
        - týdenní report zranitelností (vulnerability scan)
        - automatické detekce útoků a anomálií
    - **Pokročilé firewallové ochrany (NGFW)**
        - Sophos XG
        - FortiGate
        - Ubiquiti UniFi Cloud Gateway
        - další řešení pro zvýšení bezpečnosti perimetru
5. **Alternativní řešení**

    V řadě případů lze přímé přesměrování portů nahradit bezpečnějšími řešeními, například:

    - přístupem prostřednictvím VPN
    - využitím cloudových služeb výrobce zařízení
    - zabezpečenými tunely nebo centrální správou přístupu
    - reverzní proxy nebo bezpečnostní bránou
    - Zero Trust síťovým přístupem (ZTNA)
        - Sophos ZTNA
        - FortiGate ZTNA
        - Cloudflare Zero Trust
        - OpenZiti
        - Pritunl Zero
        - další kompatibilní ZTNA řešení
6. **Kontakt pro další dotazy**

    Pokud máte jakékoliv dotazy, nebo máte o některé nabízené bezpečnostní služby zájem, můžete nás kontaktovat na:

    - **E-mail:** mail@netair.cz
    - **Telefon:** +420 488 572 050