Firewall

Firewall funguje jako kontrolní stanoviště na hranici sítě. Na základě sady definovaných pravidel rozhoduje o tom, zda daný datový paket propustí, nebo jej zablokuje. Chrání tak počítače před útoky zvenčí a zároveň může bránit škodlivému softwaru v odesílání dat zevnitř ven.

1. Typy firewallů podle provedení

- **Hardwarový (Síťový):** Samostatné zařízení umístěné mezi routerem a internetem. Chrání celou síť najednou. Často bývá součástí moderních routerů.
- **Softwarový (Hostitelský):** Program běžící přímo v operačním systému (např. Windows Firewall). Chrání pouze ten konkrétní počítač, na kterém je nainstalován.

2. Generace a technologie filtrování

Technologie firewallů se postupem času vyvíjela od jednoduché kontroly adres až po hloubkovou analýzu obsahu:

- **Paketové filtry (1. generace):** Kontrolují pouze základní informace v hlavičce paketu – IP adresu odesílatele/příjemce a číslo portu. Jsou velmi rychlé, ale snadno oklamatalné.
- **Stavové filtrování (Stateful Inspection):** Pamatují si stav navázaných spojení. Nepouští dovnitř pakety, které nejsou odpovědí na požadavek, jenž vyšel zevnitř sítě.
- **Aplikační brány (Proxy firewally):** Pracují na nejvyšší vrstvě. Dokáží analyzovat obsah konkrétních protokolů (např. HTTP, FTP) a blokovat například konkrétní webové stránky nebo škodlivé skripty.
- **Next-Generation Firewall (NGFW):** Moderní firewally, které kombinují vše výše uvedené s funkcemi jako IDS/IPS (detekce průniků), antivirovou kontrolou a analýzou šifrovaného provozu.

3. Pravidla firewallu (ACL)

Firewall pracuje na principu **Access Control Lists**. Pravidlo typicky vypadá takto:

> *„Pokud paket přichází z IP 1.2.3.4 a směřuje na port 80, Povolit. Všechno ostatní Zakázat.“*

Většina moderních firewallů používá strategii **Implicit Deny** – co není výslovně povoleno, to je automaticky zablokováno.

4. Porty: Dveře do vašeho počítače

Firewall často mluví o portech. Představte si je jako očíslované dveře:

- **Port 80/443:** Standardní provoz pro webové stránky (HTTP/HTTPS).

- **Port 25:** E-maily (SMTP).
- **Port 22:** Vzdálená správa (SSH).

Pokud firewall tyto „dveře“ zavře, nikdo se přes ně dovnitř nedostane.

5. Omezení firewallu

Firewall není všemocný. Neochrání vás například před:

- **Sociálním inženýrstvím:** Pokud uživatel sám dobrovolně prozradí heslo útočníkovi.
- **Fyzickým přístupem:** Pokud útočník přijde k počítači a vloží do něj infikované USB.
- **Špatně nastavenými pravidly:** Firewall je jen tak chytrý, jak jej administrátor nastaví.

> **Zajímavost:** Název pochází ze stavebnictví, kde „firewall“ označuje nehořlavou stěnu, která má zabránit šíření požáru mezi sousedními budovami. V IT má zabránit šíření „digitálního požáru“ (virů a útoků) do vaší sítě.

Zpět na Bezpečnost