Řízení služeb zabezpečení – IPS/IDS router

Sítě jsou soustavně vystavovány novým hrozbám a sofistikovaným útokům, které se pomocí tradičních metod stále obtížněji identifikují a odrážejí. Pokročilé evazivní techniky („Advanced evasion techniques“, AET) například skrývají útoky na datové proudy tak, že obcházejí ochranné mechanismy, jako jsou např. systémy prevence průniků. Detekce takovýchto útoků a obrana proti nim vyžadují nejmodernější aktivní ochranu.

Systém prevence průniku (Intrusion Prevention Systems, IPS), také známý jako systém pro detekci a prevenci průniku (Intrusion Detection and Prevention Systems, IDPS), je **zařízení pro počítačovou bezpečnost, které monitoruje síť a/nebo aktivity operačního systému na škodlivou činnost**. Hlavní funkce IPS systémů jsou identifikace škodlivé činnosti, zaznamenávání informací o jejím průběhu, následném blokování této činnosti a také její nahlašování.

IPS systémy jsou považovány za rozšíření IDS systémů, protože monitorují jak provoz na síti, tak i aktivity operačního systému, které by mohly vést k narušení bezpečnosti. Hlavní rozdíl oproti IDS systémům je, že systém IPS je zařazen přímo do síťové cesty (in-line), a tak může aktivně předcházet, případně blokovat detekovaný nežádoucí a nebezpečný provoz na síti. Konkrétněji, IPS může provádět takové akce jako vyvolání poplachu, filtrování škodlivých paketů, násilné resetování spojení a/nebo blokování provozu z podezřelé IP adresy. Všechny tyto úkony často provádí ve spolupráci s firewallem.

IPS také umí opravit chybný cyklický redundantní součet (CRC), defragmentovat proudy paketů, předcházet problémům s řazením TCP paketů, a čistit nežádoucí přenos včetně nastavení síťové vrstvy.

Klíčové vlastnosti

- Inspekce šifrovaného provozu SSL/TLS v reálném čase jako **prevence útoků a úniků dat**.
- **Ochrana sítě proti nastupujícím hrozbám a malwaru**, včetně těch maskovaných sofistikovanými AET, které dokážou oklamat většinu nových firewallů.
- Zajištění včasné reakce v řádu minut, ne hodin. Instrukce k **aktualizacím stovek fyzických i virtuálních lokací** po celém světě prostřednictvím jediného kliknutí.

Základem úspěchu společnosti je vysoce dostupná síť vybavená ochranou proti proměnlivým hrozbám, bez ohledu na její velikost. Problém mnohých společností spočívá v nedostatku odborných znalostí nebo vnitropodnikových zdrojů. Stejně tak je to i s potřebným HW, SW vybavením, které je potřeba správně konfigurovat, udržovat a reagovat na aktuální hrozby. Náš tým certifikovaných techniků je vždy k dispozici.

Doporučené zařízení:

UniFi Dream Machine Pro

UniFi Dream Machine Pro je velice výkonné zařízení se 4jádrovým CPU, má 4 GB RAM a všechny užitečné a potřebné funkce vkládá do malé elegantní krabičky. Určitě stojí za zmínku také managovatelný 8portový gigabitový switch s podporou VLAN. USG je Unify Security Gateway neboli Router s pokročilými funkcemi IDS/IPS, DPI, Endpoint Scanning a další. Wifi systém Unifi je prostě All-in-one, neboli vše v jednom. Operační systém je Linux – ten zajišťuje velké možnosti přizpůsobení daným požadavkům.

Klíčové vlastnosti:

- komplexní řešení sítě v kancelářích a společnostech
- velice výkonné zařízení s 4jádrovým CPU a 4 GB RAM
- all-in-one zařízení
- snadné zapojení Plug&Play
- uniFi Protect software slouží pro kamery, 3,5“ slot pro HDD nahrávání z kamer
- automatická QoS Top prioritizace (volání, videopřenosy)
- VPN Server
- uniFi Controller umožňuje vzdálený přístup s mobilní aplikací
- lze použít jako kontrolér pro WiFi AP UNIFI

Ing. Filip Lang | filip.lang@ictnwt.cz | +420 724 707 417 **ictnwt.cz**