ZABEZPEČTE SVOU FIREMNÍ SÍŤ S FIREWALLY NOVÉ GENERACE

NOVÉ SMĚRY VÝVOJE MĚNÍ UVAŽOVÁNÍ O BEZPEČNOSTI SÍTÍ

Přechod do cloudu a popularita práce z domova způsobuje, že firemní IT prostředí musí být nyní dostupné mnohem více způsoby, s mnohem více zařízeními a z různých míst. Koncoví uživatelé žádají širší možnosti přístupu k datům. To nutí organizace měnit uvažování o nastavení bezpečnosti svých sítí. Musí brát v úvahu cloudové prostředí, nové metody vývoje IT aplikací, používání přenosných mobilních zařízení, zapojení IoT, nutnost přístupu pro vzdálené pracovníky, propojení poboček a mnoho dalšího.

81% FIREM POUŽÍVÁ NĚKOLIK (PRŮMĚRNĚ 5) RŮZNÝCH TYPŮ SOUKROMÝCH, VEŘEJNÝCH NEBO HYBRIDNÍCH CLOUDŮ.

TRADIČNÍ OCHRANA VNITŘNÍ SÍTĚ UŽ NESTAČÍ

Požadavky na dostupnost firemních dat ze vzdálených prostředí s různými typy zařízení způsobily, že perimetr vnitřní sítě již téměř přestal existovat. Zaběhnuté bezpečnostní přístupy založené na důvěře v bezpečnost domácí sítě a kontrole provozu v ní dané kombinací portů a protokolů už pro dnešní síťové prostředí neposkytují dostatečnou ochranu.

FIREWALLY NOVÉ GENERACE PŘINÁŠEJÍ PROAKTIVNÍ OCHRANU

Z reaktivních zařízení v podobě tradičních firewallů, které podle předem nastavených pravidel kontrolují přístupy k interním zdrojům, se firewally nové generace staly proaktivními nástroji, které umožňují hloubkovou kontrolu veškerého provozu včetně šifrované komunikace, a to vše nejen na urovni síťového provozu, ale i na úrovni aplikací, uživatelů a obsahu přenášených dat. Umožňují tak předcházet známým i neznámým hrozbám, ještě než nastanou.

VYUŽITÍ STROJOVÉHO UČENÍ ZVYŠUJE EFEKTIVITU

Původní úsilí o maximální efektivitu v podobě zkracování času reakce na zjištěné bezpečnostní incidenty a času na povolování nově přidaných zařízení nebo změny nastavení bezpečnostních politik se dnes přetavuje do podoby automatizovaných doporučení bezpečnostních politik. Firewally nové generace využívají strojového učení a analytiku k vyhodnocení velkého objemu dat z různých zdrojů. Dokáží oddělit žádoucí síťový provoz od toho nežádoucího. Umožňují organizacím vidět a zabezpečit vše – včetně IoT – a zároveň pomáhají omezovat chyby a nedostatečnosti v nastavení.

STROJOVÉ UČENÍ POMŮŽE ODHALIT AŽ 95% POKROČILÝCH SKRYTÝCH HROZEB

CO OD NÁS MŮŽETE OČEKÁVAT:

Zajistíme nasazení pokročilé **ochrany firemní sítě** pomocí **firewallů nové generace** od předního světového poskytovatele řešení pro kybernetickou bezpečnost.

KLÍČOVÉ FUNKCE:

- **KONTROLA PROVOZU NA APLIKAČNÍ VRSTVĚ A VYUŽITÍ STROJOVÉHO UČENÍ**

Next Generation Firewally (NGFW) monitorují a řídí veškerý síťový provoz na aplikační vrstvě modelu ISO/OSI, rozeznávají aplikace v tomto provozu obsažené a jsou schopny detekovat a zastavit známé i neznámé hrozby v reálném čase, stejně jako ochránit uživatele před nákazou či ztrátou uživatelských přihlašovacích údajů. Mají implementovány prvky strojového učení, které je schopno v reálném čase zastavit skutečné zero-day útoky. Tato činnost žádným způsobem neovlivňuje uživatelskou přívětivost (UX).

- **VARIABILNÍ FORMA INSTALACE**

NGFW je možné provozovat jako HW zařízení libovolné velikosti a kapacity, virtuální firewally umístěné v privátních či veřejných cloudech, nebo v prostředí kontejnerů. Ve všech variantách je totožný operační systém a shodné funkce. Takže bez ohledu na zvolený typ platformy je poskytována stejně spolehlivá ochrana a stejný set funkcionalit.

- **PŘÍDAVNÉ SUBSCRIPCE**
  - Threat prevention (TP)
  - DNS security
  - URL filtering
  - Wildfire
  - Global Protect
  - SD-WAN
  - AutoFocus
  - IoT Security
  - Data Loss Prevention (DLP)
  - SaaS Security Inline
  - Nadstavbové VirtualSystems (kontexty)
  - Centrální management

ODBORNÁ SPOLUPRÁCE:

Naši experti Vám rádi pomohou s:

- návrhem či revizí celkové bezpečnostní koncepce
- výběrem optimálního řešení na míru Vašim potřebám
- přípravou Best Practice Assessment a návrhem optimálního využití dostupných bezpečnostních funkcí
- implementací celého řešení
- integrací na další systémy
- správou a úpravou pravidel pro minimalizaci plochy pro útok

VE VÝSLEDKU ZÍSKÁTE...

Pokročilou bezpečnostní technologii se schopností detekce i neznámých útoků

Hloubkovou kontrolu provozu, vizibilitu, včetně například podkladů pro optimalizaci využití přípojné kapacity

Provozní efektivitu, zjednodušení bezpečnostní infrastruktury, přístup přes jedinou konzoli

PROČ BYSTE SI MĚLI VYBRAT PRÁVĚ NAŠE ŘEŠENÍ.

Námi nabízená technologie se nepřetržitě už desátým rokem umisťuje na nejvyšší pozici **Leadera** v přehledu **Magic Quadrant for Network Firewalls** společnosti **Gartner**.

Pro poskytování našeho řešení máme vysokou kvalifikaci. **Thein Security** je držitelem nejvyšší dodavatelské certifikace **Diamond Innovator** a zároveň je jediným **autorizovaným servisním centrem** pro ČR a SR.

Disponujeme týmem **expertů s dlouholetými zkušenostmi.** Od roku **2010** patříme k průkopníkům kybernetické bezpečnosti se zaměřením na **prevenci úniku citlivých dat**, obrany proti **sofistikovaným útokům**, detekce neznámého **malwaru** a aktivní ochrany proti **útokům DDoS**. Dodáváme služby a technologie do **hybridních prostředí** (on prem / cloud) a specializujeme se na **Zero Trust přístup.**

STANEME SE VAŠÍM PARTNEREM PRO OBLAST KYBERNETICKÉ BEZPEČNOSTI.

Pro více informací o Zabezpečení firemních sítí a Firewallech nové generace kontaktujte naše obchodní zástupce na obchod.security@thein.eu nebo navštivte naše webové stránky.

Thein Security s.r.o., Pikrtova 1737/1a, 140 00 Praha 4 – Nusle, e-mail: info.security@thein.eu
Společnost vedená u Městského soudu v Praze oddíl C, značka 109813, IČO: 27415546, DIČ: CZ27415546