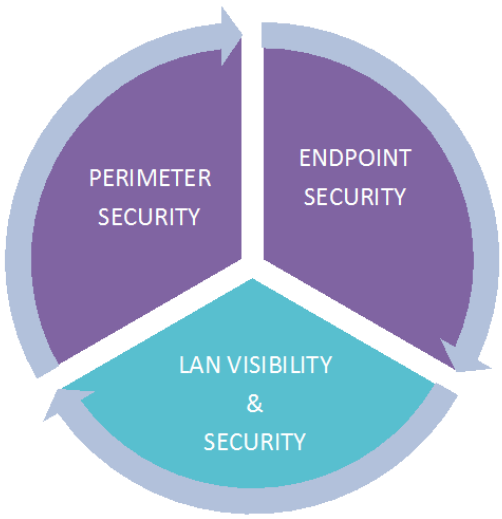
Bezpečná a efektivní IT infrastruktura

Účel dokumentu

Složitost IT infrastruktury s moderní dobou vzrůstá. Neustále jsou nasazovány nové produkty a využívány nové služby. Narůstá také množství hrozeb narušujících bezpečnost počítačových sítí. Na špici těchto hrozeb jsou sofistikované, na míru vytvořené útoky, které jsou schopny překonat tradiční řešení pro ochranu perimetru počítačové sítě. Po překonání bezpečnostních mechanizmů snadno infiltrují interní síť organizace, uvnitř které jsou možnosti obrany minimální. Přitom drtivá většina organizací je čím dál více závislá na počítačové síti a informačních technologiích. Infekce nebo ztráta dat na jedné stanici či několikahodinový výpadek sítě je velmi nepříjemnou záležitostí. Úspěšný útok na IT infrastrukturu nebo dlouhodobý výpadek celé počítačové sítě může být likvidační pro celou organizaci.

Tento dokument popisuje:

- Hlavní výzvy v oblasti efektivní správy počítačové sítě a kompletní ochrany před kybernetickými hrozbami
- Řešení pro bezpečnou a efektivní IT infrastrukturu



Obrázek 1: Technologie pro kompletní zabezpečení sítě

Výzva

Prvním krokem k bezpečné infrastruktuře je ochrana sítě na jejím perimetru. Blokovat nežádoucí provoz pouze pomocí pevně nastavených pravidel na firewallu již není dostatečné. Je nutné detekovat moderní hrozby, kontrolovat procházející data na aplikační úrovni, odhalovat známý malware a útoky tak, aby byla vnitřní síť před těmito útoky co nejlépe ochráněna. Moderní řešení pro ochranu perimetru musí být v reálném čase schopno rozpoznat a blokovat desetitisíce verzí škodlivého kódu při neustálé aktualizaci databáze známých hrozeb tak, aby byly schopny zachytit co nejvíce nových hrozeb a snížit riziko úniku citlivých dat organizace.

Druhým a nezbytným krokem je monitorování provozu lokální datové sítě tak, aby bylo možné reagovat na útoky, které perimetr překonají nebo jsou způsobeny přímo interními uživateli sítě (zaměstnanci, hosté, kteří získají přístup k síti). Pokročilé hrozby jsou totiž vytvářeny tak, aby nebyly snadno odhalitelné, a ochranu na perimetru sítě často překonají nebo se do sítě dostanou jinou cestou než přes perimetr. Poté se mohou volně šířit sítí a působit v ní tak, že je běžné bezpečnostní nástroje považují za legitimní chování. Díky skrytému působení pak mohou bez odhalení dlouhodobě sledovat citlivá data nebo osoby. Přestože se řešení na ochranu perimetru sítě stále zdokonalují, není v této situaci otázkou jak napadení sítě vyloučit, ale jak toto napadení odhalit co nejdříve. Příkladem za všechny je průmyslový špionážní malware, který byl odhalen v roce 2012. Jeho cílem je krádež technických výkresů a průmyslových designů a jejich odeslání na servery umístěné v Číně. Tento malware je známý pod jménem ACAD/Medre.A a na čínské servery odeslal několik desítek tisíc dokumentů AutoCAD.

Důležitým předpokladem pro zajištění bezpečnosti sítě je také její řádná správa. Ta se v dnešní době neobejde bez kompletní viditelnosti do síťového provozu napříč infrastrukturou, schopnosti rychlého a efektivního odstraňování problémů, či automatické detekce provozních problémů a anomálií v síti. Moderní řešení pro efektivní a bezpečnou síť musí tedy být nástrojem jak pro bezpečnostní, tak pro síťové oddělení a musí umožnit rychlou a kvalitní výměnu informací o incidentech v síti mezi těmito dvěma světy.

Posledním stupněm je kontrola každé z koncových stanic proti přítomnosti nežádoucího software. Proto využíváme antivirové programy.

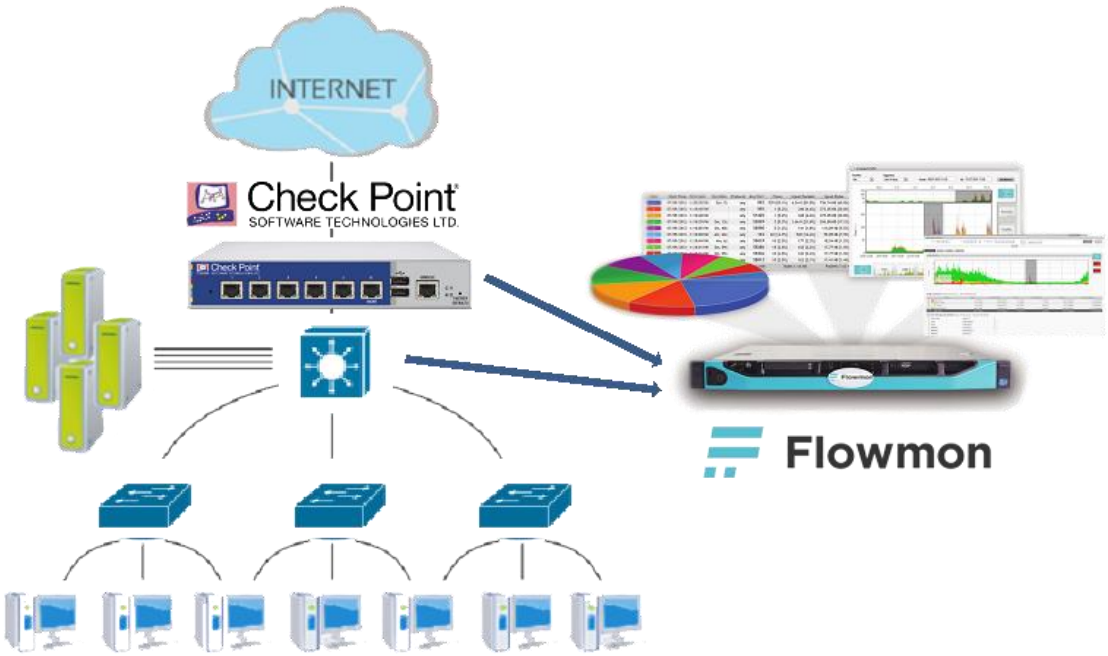
Architektura řešení

Řešení pro bezpečnou a efektivní IT infrastrukturu kombinuje níže uvedené prvky pro zajištění ochrany sítě na perimetru i uvnitř sítě a monitorování sítě pro provozní účely:

- Ochranu sítě na perimetru zajišťuje špičkový firewall společnosti Check Point se schopností automaticky detekovat a blokovat známé hrozby a s možností generovat záznamy o komunikaci na perimetru sítě. Check Point je analytickou společností Gartner uváděn jako leader v oblasti firewallů po období šestnácti let.
- Viditelnost do interní sítě prostřednictvím monitorování síťového provozu zajišťuje řešení Flowmon společnosti Flowmon Networks podporující Cisco standardy Netflow v5, v9, NBAR2 ale i obecné protokoly IPFIX či sFlow. Díky vlastním sondám a kompatibilitě se širokým okruhem síťových prvků je řešení možné nasadit do libovolné infrastruktury zákazníka.
- Automatickou detekci incidentů v interní síti provádí systém Flowmon ADS (Anomaly Detection System), který je součástí řešení Flowmon. Pro přesnější a efektivnější analýzu hrozeb používá Flowmon ADS také informace

o komunikaci na perimetru sítě zaslané z firewallu Check Point. Řešení Flowmon je pravidelně identifikováno ve zprávách analytické společnosti Gartner mezi top světovými řešeními v oblasti monitorování provozu a detekce pokročilých hrozeb.

- Ochranu koncových stanic proti známým hrozbám, které se dostaly na stanici pomocí překonání ochrany sítě na perimetru nebo jiným způsobem zajišťuje Check Point Endpoint Security. Zároveň Check Point Endpoint Security poskytuje možnost šifrování koncových stanic a přenosných médií, jako ochranu proti úniku dat v případě ztráty zařízení.



Obrázek 2: Komponenty řešení pro ochranu sítě proti pokročilým kybernetickým hrozbám

Díky tomuto ucelenému řešení získává zákazník jak ochranu před známými hrozbami na perimetru sítě a koncových stanicích, tak schopnost detekovat hrozby, které jsou aktivní uvnitř sítě organizace. Zároveň detailní viditelnost do síťového provozu poskytuje přehled o provozních problémech, anomáliích v síťovém provozu, či výskytu podezřelých aktivit v síti, které typicky předcházejí úspěšným útokům. Díky získávání dodatečných informací o provozu na perimetru sítě z firewallu Check Point je v řešení Flowmon možné snadněji a přesněji určit rozsah a důležitost případného bezpečnostního incidentu.

Přínosy řešení

Řešení pro bezpečnou a efektivní IT infrastrukturu je zaměřeno na poskytnutí komplexní ochrany sítě před známými i sofistikovanými hrozbami a zajištění bezpečné a stabilní infrastruktury. Klíčové přínosy řešení pro bezpečnou a efektivní infrastrukturu jsou:

- Automatická ochrana proti známým hrozbám na perimetru sítě
- Detekce hrozeb ve vnitřní síti, pokud se jim do vnitřní sítě podaří proniknout
- Schopnost rozpoznat původní projevy hrozeb a jejich včasného zamezení
- Rychlé řešení incidentů v síti díky kompletní viditelnosti do síťového provozu
- Pravidelný reporting o stavu sítě, možnost plánování kapacit sítě
- Škálovatelné a cenově příznivé řešení zajišťující komplexní ochranu sítě

- Zjednodušení a automatizace náročného a drahého manuálního procesu vyšetřování incidentů
- Schopnost využít stávající prvky v síti jako zdroje dat (Cisco, Enterasys, HP, Huawei, Mikrotik, Nortel a další)
- Schopnost integrovat výstupy do jednoho dashboardu

Popis komponent řešení

Blokování známých hrozeb na perimetru sítě

Pokročilé Next Generation firewally společnosti Check Point obsahují specializované firewallové řešení, které detekují a zabraňují hrozby přicházejících z vnější sítě Internet (moduly IPS, DDoS, Anti-virus, Anti-bot, Emulace hrozeb ve virtuálním prostředí), řídí a zabezpečují odcházející interní provoz (moduly Application Control, URL Filtering, Anti-bot) a zároveň chrání organizaci před únikem citlivých dat (modul DLP). Díky těmto funkcím jsou Next Generation firewally společnosti Check Point schopny bez nutnosti zásahu obsluhy zachytit na perimetru sítě nežádoucí provoz a zásadním způsobem tak zvýšit zabezpečení sítě na jejím perimetru.

Firewally Check Point dále slouží jako generátory informací o síťovém provozu na perimetru pro řešení Flowmon.

Generování, evidence a analýza NetFlow dat za účelem kompletní viditelnosti do síťového provozu

Generování informací o provozu v interní síti zákazníka zajišťují stávající aktivní prvky v síti. V případě, že stávající infrastruktura neumožňuje NetFlow data generovat, je možné použít pro monitorování dedikovanou sondu Flowmon Probe, připojenou ke core switchům LAN. Pro generování NetFlow na perimetru slouží firewall Check Point. Tímto způsobem je možné evidovat informace o každém zrealizovaném spojení v síti.

Sběr, uchování a zpracování NetFlow zajišťuje řešení Flowmon společnosti Flowmon Networks. Pomocí Flowmon je možné tyto informace následně využít pro reporting, pro analýzu provozu, při řešení incidentů v síti nebo při plánování rozvoje sítě. Řešení Flowmon je schopno přijímat NetFlow z široké řady síťových prvků, mezi jinými také z firewallů Check Point a poskytuje kompletní viditelnost do síťového provozu.

Automatická detekce hrozeb a podezřelého chování ve vnitřní síti

Automatickou detekci hrozeb a anomálií v síťovém provozu zajišťuje modul Flowmon ADS (Anomaly Detection System) od společnosti Flowmon Networks založený na technologii Network Behavior Analysis (NBA). Jedná se bezpečnostní rozšíření Flowmon kolektoru, které využívá nasbíraná data o provozu v síti. Tato data automaticky zpracovává v reálném čase a poskytuje tak možnost okamžité ochrany proti probíhajícím hrozbám. Umožňuje také ukládání dlouhodobé historie informací o provozu v síti a poskytuje tak potřebnou důkazní evidenci či podklady pro forenzní analýzu i několik let zpětně.

Proč řešení pro bezpečnou a efektivní IT infrastrukturu?

Unikátní kombinace Next Generation firewallů Check Point se schopností automaticky detekovat a eliminovat hrozby na perimetru sítě se řešením Flowmon pro viditelnost do vnitřní sítě a automatickou detekci hrozeb představuje efektivní způsob, jak chránit svoji organizaci před pokročilými kybernetickými hrozbami a zároveň zajistit efektivní a stabilní IT infrastrukturu. Díky propojení obou řešení se zároveň snižují náklady na implementaci a zkracuje doba řešení incidentů v síti.

Více informací

Pro více informací prosím kontaktujte svého Check Point nebo Flowmon Networks partnera.

Check Point Worldwide Headquarters
5 Ha'Solelim Street
Tel Aviv 67897
Israel
www.checkpoint.com

Flowmon Networks, a.s.
U Vodárny 2965/2
616 00 Brno
Česká republika
www.flowmon.com