FORTINET veracomp

Fortinet a Veracomp

Ochrana proti pokročilým hrozbám aneb Pískoviště a nejen to

V dnešní době je již všeobecně známo, že bezpečnostní technologie jako „Intrusion Prevention System“, „Application Control“, „Anti-Malware“ a další jsou stavebním kamenem každé IT infrastruktury. Ale zároveň se již ví, že tato řešení je nutné doplnit, zejména v oblasti neznámého malwaru, o další řešení, která jsou v současnosti velmi často probírána.

Jde o tzv. sandboxy. Mnoho výrobců vstoupilo do tohoto segmentu trhu se svým produktem, jen aby neměli mezery ve svém produktovém portfoliu. Jiní dávají této problematice velkou váhu a snaží se přijít s takovým řešením, které by bylo co nejvíce efektivní a dokázalo skutečně ochránit společnost před co největší škálou pokročilých hrozeb. A jaký je přístup společnosti Fortinet?

Součinnost celého řešení

Společnost Fortinet si uvědomuje, že ochranu proti pokročilým hrozbám (dále jen ATP) nelze řešit jedním produktem, ale součinností více zařízení, která jako celek poskytují komplexní ochranu korporátní sítě. Díky možnostem ostatních produktů v produktovém portfoliu získává společnost Fortinet unikátní řešení, jak se s pokročilými hrozbami vypořádat. ATP by mělo být schopné zajistit následující tři úkony:

Prevence

Prvním krokem k ochraně podnikové sítě je cíleně zmenšovat riziko pomocí produktů, jako jsou next-generation firewally (FortiGate), mailové brány (FortiMail) nebo aplikace pro ochranu koncových zařízení (FortiClient). Zmíněné produkty využívají technik, jako je anti-malware, application control, web-filtering, anti-bot a další. Tyto technologie dokáží rozpoznat většinu hrozeb, které útočníci k pokusu o průnik do podnikové sítě využívají.

Anti-malware například dokáže kromě detekce a blokace virů a botnetových sítí také odhalit neznámé hrozby za použití společností Fortinet patentované technologie „Content Pattern Recognition Language“.

Detekce

Jádrem celého systému je produkt FortiSandbox, který slouží k detekci v danou chvíli neznámých hrozeb. K tomu využívá několik metod, jak dosáhnout co nejvyššího úspěchu.

Soubor, který se dostane k analýze do FortiSandboxu, nejprve projde antivirovou analýzou, která má úspěšnost v proaktivní i reaktivní detekci 95 %. Následně je proveden dotaz do cloudové sítě, která sdílí informace o právě detekovaných hrozbách. Tyto informace jsou získávány ze všech FortiSandbox zařízení po celém světě. Poté je provedena kódová emulace, která dokáže ve velmi krátkém čase odhadnout chování napsaného programu. Nakonec je spuštěn analyzovaný soubor v izolovaném virtuálním prostředí, kde je simulována práce uživatele tak, aby došlo k aktivování skrytého malwaru. Jde tedy o otevření souboru a další následné simulace uživatelské činnosti. Po aktivaci malwaru jsou zaznamenávány informace o kontaktování tzv. Command and Control centra, odesílání dat do internetu apod.

Nakonec je zpracován výstup, který určí, zda se skutečně jedná o dosud neznámou hrozbu, a informace o této hrozbě jsou následně sdíleny ostatním Fortinet produktům v síti, ale i všem ostatním produktům napojeným na cloudové služby společnosti Fortinet.

Mitigace – zmírnění dopadu

Jakmile dojde v předchozím kroku k odhalení neznámé hrozby, je zapotřebí okamžitě zabránit veškerým potenciálním škodám a jejímu dalšímu šíření. Infikované zařízení musí být okamžitě uloženo do karantény nebo zcela odpojeno od sítě. Následně ale musí být zajištěno, aby nebylo možné další šíření například za pomocí přenositelných USB disků, a právě v tuto chvíli přichází na řadu produkt pro zabezpečení koncových stanic FortiClient, který je také jedním z důležitých prvků ATP.

Co je to FortiSandbox

Ideální způsob nasazení tohoto zařízení, kdy je využito všech výhod kooperace mezi Fortinet produkty, je tzv. integrované nasazení. Díky přímé integraci mohou produkty FortiGate, FortiWeb, FortiMail a FortiClient napřímo odesílat soubory k hloubkové analýze do FortiSandboxu. Navíc může být FortiSandbox nasazen zcela samostatně, kdy jsou do něj odesílána data pomocí síťového TAPu nebo SPAN portu. Samozřejmostí je možnost provést analýzu vlastního souboru v tzv. režimu On-Demand. FortiSandbox je možné pořídit ve dvou fyzických provedeních nebo jako virtuální zařízení do prostředí VMware. Vlastnosti jednotlivých modelů jsou popsány v následující tabulce:

FortiSandbox	FSA-1000D	FSA-3000D	FSA-VM
VM Sandboxing (Files/ /Hour)	160	560	n/a
AV scanning (Files/ /Hour)	6 000	15 000	n/a
Number of VMs	8	28	2 (max. 52)
CPU#	1 × Quad Core	2 × 8 Core	4/unlimited
RAM size	32 GB	128 GB	8 BG/unlimited
Total network interfaces	8	8 (2 × 10 G included)	6
Local built-in storage	4 TB (max. 8 TB)	4 TB (max. 8 TB)	30 GB (max. 16 TB) 100 GB Recommended

Proč prodávat FortiSandbox:

- lokální zastoupení výrobce;
- TAC umístěné v Praze;
- technická podpora ze strany distributora i výrobce;
- registrace obchodních případů;
- potenciální obchodní případ u zákazníků s produkty podporujícími integraci s FortiSandboxem.

Argumenty pro koncového zákazníka:

- unikátní přístup pokrývající všechny důležité kroky ATP řešení;
- snadná integrace do stávajícího prostředí;
- real-time detekce a blokace;
- možnost zapůjčení DEMO zařízení.

Distribuce pro ČR:

X

Distribuce pro SR:

X

-fes-