Traditionele netwerk controle is niet meer effectief

Iedereen is er zo langzamerhand van doordrongen dat een netwerk goed moet worden beveiligd. Onder ander door toename van gebruik van internet, Messaging, Wifi, VoIP en E-commerce toepassingen dwingen bedrijven, klanten en partners toegang te verschaffen tot netwerksystemen. Een goede beveiliging voor uw systemen is dus niet alleen noodzakelijk, maar tevens bedrijfskritisch. Immers als een hacker uw server heeft gekraakt kunnen uw gebruikers er niet meer mee werken. Dat kost geld! En niet te vergeten, men kan bij een dergelijke kraak uw belangrijke bedrijfsinformatie stelen. Dat kan u weer geld gaan kosten.

Beveiliging van netwerken heeft daarom de hoogste prioriteit. De traditionele Firewall classificeert verkeer en blokkeert deze of laat m door. De daaropvolgende IPS oplossingen werken met signatures en zijn gebaseerd op Poort scannen. Het resultaat hiervan is dat een aanval die ontwijkend en dynamisch is zoals geavanceerde Malware; via niet gecontroleerde poorten makkelijk het netwerk binnen kunnen dringen zonder gedetecteerd te worden.

De meest voorkomende bedreigingen die worden tegengehouden door een Intrusion Prevention systeem zijn Wormen, Denial of Service attacks en exploits. Het probleem in deze is dat een IPS niet alle IPS signatures aan boord heeft om te checken en sterker nog, niet op alle protocollen deze check doet. Een IPS probeert een signature set uit op specifiek verkeer gebaseerd op Poort niveau. Deze limitatie zorgt ervoor dat Malware of Exploits vaak op niet gecontroleerde Poorten binnen kunnen komen en dus niet gezien worden. Ook omdat er maar gekeken wordt naar veel voorkomende Malware signatures en niet die honderdduizend andere Malware aanvallen.

Veel organisaties hebben verschillende beveiligingsoplossingen op aanvulling van bestaande poort gebaseerde Firewalls, IPS, Proxy, Web- Content filter, Anti Virus en Applicatie specifieke bescherming. Zoals Instant Messaging controle of het blokken hiervan en ook Anti Spam is een onderdeel van de Security geworden.

Juist deze houtje-touwtje oplossingen zorgen voor veel andere problemen zoals:

- Niet alles wat gecontroleerd moet worden, wordt ook daadwerkelijk gecheckt omdat niet al het dataverkeer gevolgd kan worden, denk maar aan Wifi, VoIP, BYOD of uitgaand verkeer
- De verkregen informatie vaak moeilijk te interpreteren is, maar belangrijke context van verschillende gebeurtenissen vaak gemist wordt omdat de verschillende beveiliging-oplossingen alleen binnen hun specifieke regels en filters gaat kijken.
- Beveiligingsbeleid, toegangscontrole/authenticatie en onderzoekmogelijkheden vaak verspreidt zijn over verschillende devices en andere waardoor het erg moeilijk wordt om Security maatregelen te ontwikkelen en ook toe te passen.
- Omdat hetzelfde verkeer vaak door verschillende toepassingen wordt gescand zorgt dit voor hogere latency wat weer zorgt voor een trager netwerk.

Dus dat wat je niet checkt, kun je dus ook niet beschemen!