SONICWALL CLOUD APP SECURITY

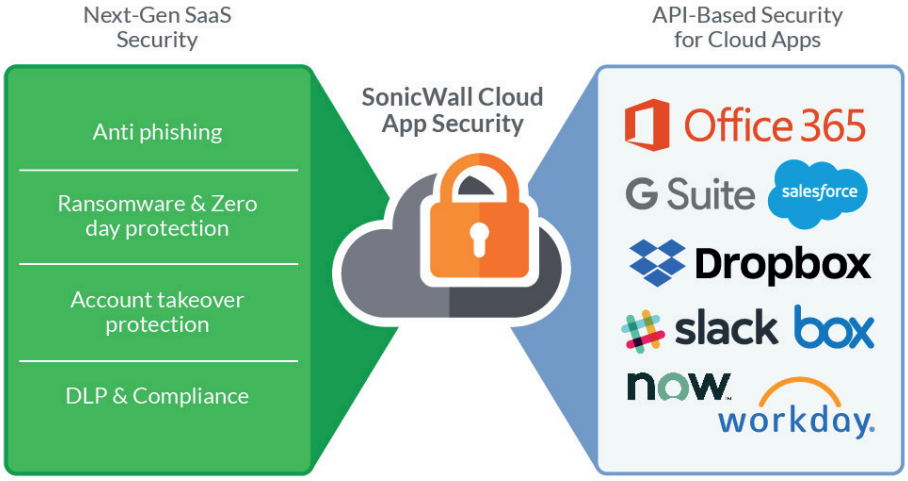
Is zakelijke e-mail in de cloud wel zo veilig?

Organisaties hebben bijna allemaal te maken met uitdagingen omtrent e-mail beheer. Niet vanwege de complexiteit, maar omdat het al vele jaren het belangrijkste toegangspunt (90%) is geworden voor cybercriminelen. Zij profiteren meestal van de onwetendheid en het misleiden van werknemers die uiteindelijk klikken waar ze niet zouden moeten klikken.

Het dreigingsniveau is inmiddels zo hoog dat steeds meer bedrijven hun e-mail naar de cloud verplaatsen in de hoop dat de beveiligingsmaatregelen die door bedrijven zoals Google of Microsoft worden toegepast, bedreigingen zullen stoppen. Het is zeer riskant om te zeggen dat deze maatregelen voldoende zijn, want hoewel e-mail is gemigreerd naar de cloud, is het zo dat nog steeds meer dan 70% van de aanvallen via e-mail geïnitieerd worden. Bovendien worden door cybercriminelen allerlei soorten verduisteringstechnieken toegepast die ervoor zorgen dat minstens 1 op de 10 verzonden kwaadaardige e-mails alle bescherming van deze e-mailproviders omzeilt. Hieraan toegevoegd is het feit dat een aanzienlijk percentage van de werknemers niet de nodige training heeft gehad om onderscheid te maken tuss en legitieme en niet-legitieme e-mails, verdachte links of bijlagen te herkennen, voorzorgsmaatregelen te nemen zoals het verifiëren van de URL of de bedrijfswebsite van de afzender, enzovoorts. Als gevolg hiervan, en wanneer het te laat is, ontdekken bedrijven soms dat de defensieve maatregelen van cloudproviders niet voldoende is.

Cloud App Security

De reactie van SonicWall is Cloud App Security. In een scenario waarin e-mailaanvallen niet alleen toenemen, maar ook geavanceerder zijn dan ooit, pleiten bedrijven als SonicWall ervoor dat een gelaagde aanpak de beste manier is om zich te verdedigen tegen onbekende en gerichte aanvallen. SonicWall Cloud App Security maakt gebruik van een meerlagig preventiesysteem dat aanvallen kan detecteren die zo complex zijn als gerichte phishing, zero-day-aanvallen, phishing-aanvallen of frauduleuze toe-eigening van Office 365- en G Suite-accounts.



Belangrijkste kenmerken:

- Antiphishing en sandboxing voor bijlagen en time-of-click URL-bescherming.
- Inkomende, uitgaande en interne e-mailscanner in Exchange Online en Gmail.
- Barrièrebescherming die ongeautoriseerd uploaden en delen van gevoelige bestanden naar OneDrive en Google Drive voorkomt.
- Bescherming tegen account-kaping, bedreigingen van binnenuit en gecompromitteerde inloggegevens.

Daarnaast biedt de oplossing van SonicWall uitgebreide SaaS-bescherming. Geautoriseerde cloudapplicaties worden beveiligd met dezelfde technologieën en de organisatie verkrijgt meer gedetailleerde inzichten en controle via native API-integraties. De combinatie met de Next Generation Firewalls van Sonicwall helpt ook om het gebruik van de altijd gevaarlijke en onbekende Shadow-IT te beteugelen.

Snel geïmplementeerd

Het activeren van SonicWall CAS oplossing neemt, ongeacht de omgeving, niet meer dan een paar minuten in beslag en is zeer prijscompetitief en transparant in te zetten als een aanvullende zeer effectieve beveiligingslaag. SonicWall CAS is daardoor een tool die het dagelijkse leven van bedrijven vergemakkelijkt, zodat zij zich geen zorgen hoeven te maken over een van de belangrijkste elementen van hun IT-infrastructuur en zo via ons distributiekanaal hun klanten één van de meest interessante beveiligingsoplossingen op de markt kan aanbieden. ■