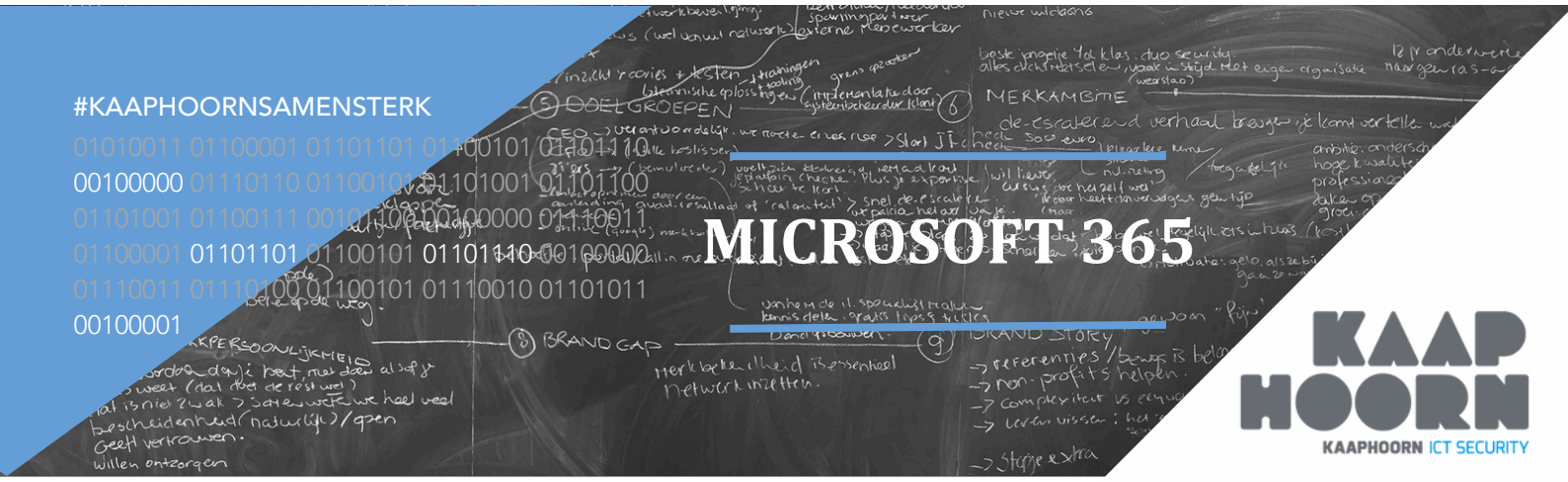

Microsoft 365

Veel bedrijven die de overstap maken naar Microsoft 365 beseffen niet dat veel van de beveiligingsmaatregelen, die in hun lokale Exchange-omgeving werden toegepast, niet standaard actief zijn in de Microsoft-omgeving. Ons onderzoek naar Microsoft 365 focust op de aanbevolen beveiligingsinstellingen die organisaties zouden moeten implementeren om hun Office 365-tenant veilig te configureren en te gebruiken.

Aanvalsoppervlak

Onder Attack Surface Reduction (ASR) verstaan we het verkleinen en verminderen van het aanvalsoppervlak van een omgeving, applicatie of website. Dit wordt vaak bereikt door het uitvoeren van best practices of door bepaalde functies in te schakelen of uit te schakelen. Door ASR toe te passen, verkleinen we de kans op het onbedoeld delen of lekken van informatie of data, en implementeren we vaak laagdrempelige maatregelen.

Vragen?

Twijfelt u of uw omgeving wel veilig is of vraagt u zich af wat wij voor u kunnen betekenen? Neem vrijblijvend contact op kasperdewaard@kaaphoorn.net of bel op 0229 799 800.

1 GOED

Essentiele cyberhygiëne en vertegenwoordigt de minimumstandaard voor informatiebeveiliging voor alle ondernemingen.

2 BETER

Aanvullende stappen. Kwetsbaar voor geavanceerde aanvallen weerbaar voor veelvoorkomende aanvallen en dreigingen.

3 BESTE

Be in control. De organisatie gaat strategisch om met security en bestand tegen geavanceerde aanvallen.

DOEL

Een nulmeting is natuurlijk nooit een doel op zich. Zie het als een start punt.

- Het doel van de Microsoft 365-audit is om inzicht te krijgen in de basisbeveiliging van Office 365-instellingen. Microsoft maakt onderscheid tussen 'goed', 'beter' en 'beste', afhankelijk van onder andere de licenties die een klant gebruikt. Onze rapportage vormt het ideale vertrekpunt voor het ontwikkelen van een veilig IT-beleid en een digitale strategie.

RAPPORTAGE

U ontvang binnen enkele werkdagen een volledig adviesrapport met concrete aanbevelingen en adviezen.

- Na afloop van ons onderzoek ontvangt u een adviesrapport dat we samen met u zullen doornemen. In dit rapport worden aanbevelingen opgenomen voor het optimaliseren van de beveiliging van uw Microsoft 365-omgeving.

HARDENING

Tijdens de Microsoft 365-audit controleren en adviseren we over aanvullende beveiligingsmaatregelen op het gebied van Attack Surface Reduction (ASR) en Identity & Access Management (IAM). We beoordelen de aanbevolen instellingen en best practices die aangeven hoe identiteiten, gebruikt voor authenticatie tegen Office 365-services, beveiligd kunnen worden. Deze richtlijnen zijn van toepassing op zowel gebruikers met als zonder beheerdersrechten. We beschrijven specifieke instellingen voor Office 365-applicaties om de service beter te beveiligen. Door onze adviezen te implementeren, wordt de Office 365-tenant veiliger gemaakt en het beveiligingsniveau van de organisatie verhoogd.

"Dankzij hun expertise is onze Microsoft 365-omgeving nu sterker en veiliger dan ooit. Ze hebben niet alleen de deuren gesloten voor bedreigingen, maar ons ook de tools gegeven om voorop te blijven in de strijd tegen cybercriminaliteit."

Stephan Dekker, Kaap Hoorn Accountants & Belasting Adviseurs

Een veilige omgeving begint met een 360-graden aanpak.

Over ons

We doen allemaal dat wat we het beste kunnen en voor ons is dat cyber security. Daarmee dragen wij ons steentje bij aan een prettigere en veiligere samenleving. Samen staan we sterk.

Contactgegevens

We leren u graag kennen om samen te bepalen wat we voor u kunnen betekenen. Voor een vrijblijvende kennismaking, bel of mail ons.

Telefoon: 0229 799 800
E-mail: kasperdewaard@kaaphoorn.net