Bechtle security scan

Cyberdreigingen worden steeds geavanceerder en de regelgeving strenger. Zorg dat jouw organisatie niet alleen voldoet aan de security-eisen, maar ook risico's actief beheerst.

Met de Bechtle security scan krijg je een volledige, merkonafhankelijke evaluatie van je IT-omgeving en helder inzicht in waar je het beste kunt investeren. Dit doen we aan de hand van zes assessments.

In zes stappen naar een veiligere IT-omgeving

Kun jij al deze vragen met vertrouwen beantwoorden?

NIS2 readiness check
Is jouw organisatie klaar voor de nieuwe wetgeving?

Tenant check
Kan jouw Microsoft 365 tenant naar een hoger niveau getild worden?

Attack surface check
Zijn er kwetsbaarheden in jouw systeem die aanvallers kunnen uitbuiten?

Email risk assessment
Beschermt jouw e-mail security oplossing jouw medewerkers voldoende?

Data risk assessment
Staat jouw gevoelige data achter slot en grendel?

DMARC-analyse
Kan er misbruik worden gemaakt van jouw e-mail domein?

Shortread: Bechtle security scan

Assessments

Afhankelijk van jouw IT-omgeving duurt de scan tussen de 2 en 4 weken. In deze periode verzamelen we gegevens over je IT-omgeving en bereiden we de rapportage voor.

NIS2 readiness check

1 uur

We beginnen met de NIS2 readiness check. De Europese wetgeving vereist namelijk dat organisaties risico's beoordelen en passende maatregelen nemen. We beginnen met een bondig en doelgericht interview waarbij we samen in kaart brengen welke maatregelen op het gebied van processen, menselijk handelen en technologie al zijn genomen. Deze basis risico-inventarisatie geeft je een helder beeld van de huidige stand van zaken.

Tenant check

1 week

De Tenant check voeren we uit in jouw Microsoft 365-omgeving. We krijgen toegang tot jouw Microsoft-configuratie en voeren een grondige scan uit op kwetsbaarheden, misconfiguraties en licentie-optimalisatie. We evalueren Entra ID, Intune en Defender en geven gericht advies over de status van je tenant.

Attack surface check

3 dagen

De Attack surface check biedt een volledig overzicht van jouw externe aanvalsoppervlak. We scannen jouw externe IP-adressen op kwetsbaarheden en misconfiguraties, en geven inzicht in subdomeinen, gelekte wachtwoorden en eventuele vermeldingen van jouw organisatie op het dark web.

Email risk assessment

3 dagen

We combineren de Attack surface check met de Email risk assessment. Hier maken we verbinding met jouw Microsoft 365-omgeving en geven we een second opinion over je e-mailbeveiliging. Dit assessment helpt te identificeren of phishing, spam of malware jouw huidige e-mailfilters hebben omzeild.

Data risk assessment

3 dagen

Het Data risk assessment biedt inzichten in datarisico's binnen OneDrive, SharePoint en Teams door snel gevoelige en overshared content te identificeren en te prioriteren. Deze beoordeling stelt ons in staat om permissies te ontdekken en mogelijk ongewenste toegang tot kritieke informatie te vinden.

DMARC-analyse

2 weken

We voeren ook een DMARC-analyse uit. Als er verbeteringen nodig zijn, vragen we je om je DNS-record tijdelijk aan te passen om te controleren op malafide spoofing van je e-maildomein. Dit proces duurt maximaal twee weken, waarna we de bevindingen met je delen.

Shortread: Bechtle security scan

Het resultaat

Jij ontvangt uitgebreide rapport met al onze bevindingen inclusief advies voor vervolgstappen. Deze zullen we samen met jou doornemen tijdens een adviesgesprek.

We geven je dan ook gericht advies over eventuele vervolgstappen die jij kunt nemen om jouw security te versterken. Denk hierbij aan interviews die naast techniek ook de processen en het beleid binnen jouw organisatie bekijken.

Starten met de Bechtle security scan

De Bechtle security scan is een grondige analyse van jouw IT-omgeving, waarbij we open poorten, kwetsbaarheden en beveiligingsrisico's detecteren zodat jij je organisatie beter kunt beschermen.

Wil je meer informatie over de Bechtle security scan, of wil je direct een afspraak inplannen? Neem dan via onderstaande button contact met ons op.

Neem contact op

bechtle ARP