Bechtle Security Kompas

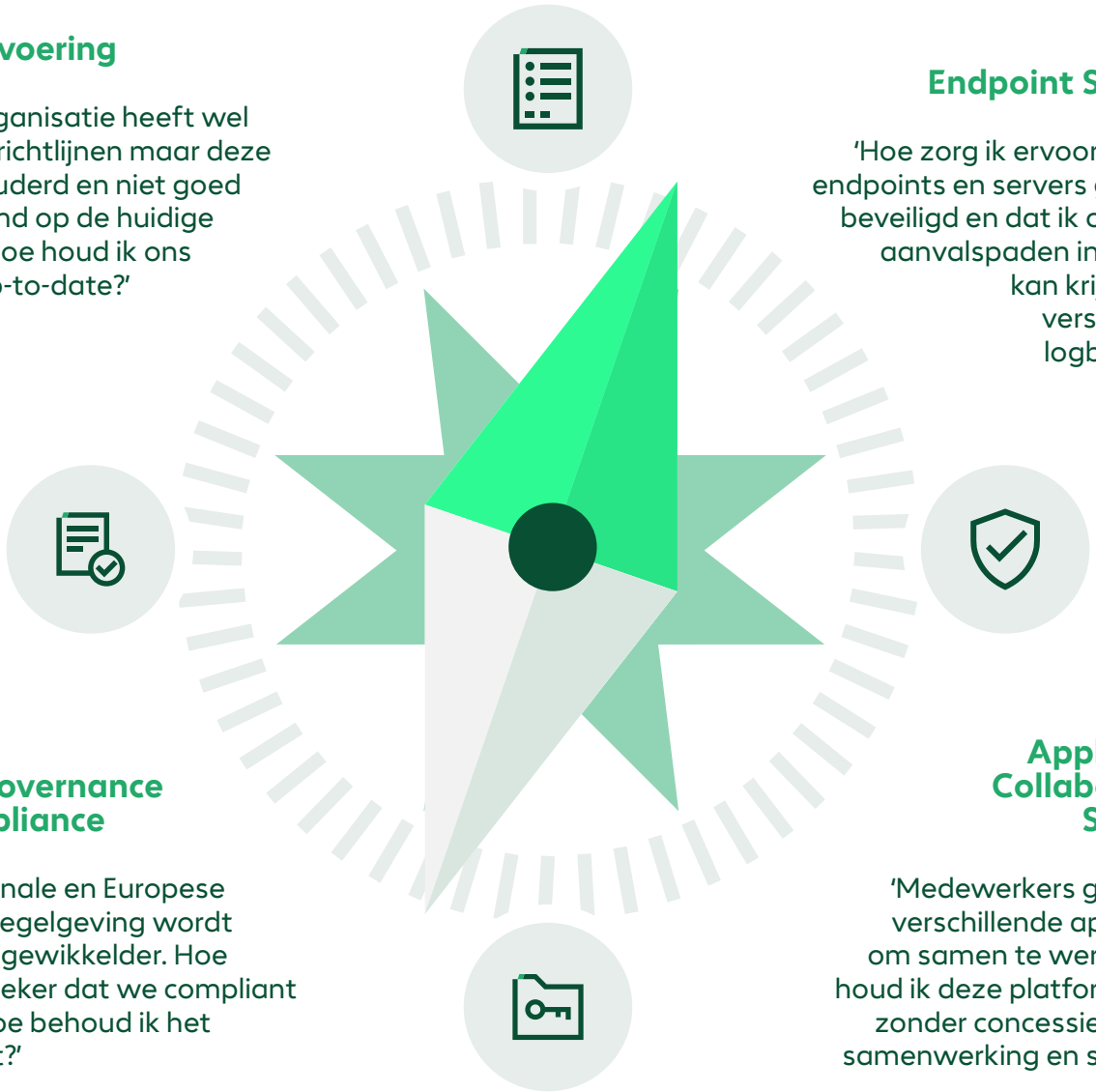
Herken jij jezelf in deze security-dilemma's?

Beleidsvoering

'Onze organisatie heeft wel security-richtlijnen maar deze zijn verouderd en niet goed afgestemd op de huidige risico's. Hoe houd ik ons beleid up-to-date?'

XDR & Endpoint Security

'Hoe zorg ik ervoor dat mijn endpoints en servers goed zijn beveiligd en dat ik complexe aanvalspaden inzichtelijk kan krijgen met verschillende logbronnen?'



Data Governance & Compliance

'De nationale en Europese wet- en regelgeving wordt steeds ingewikkelder. Hoe weet ik zeker dat we compliant zijn en hoe behoud ik het overzicht?'

Application Collaboration Security

'Medewerkers gebruiken verschillende applicaties om samen te werken. Hoe houd ik deze platforms veilig zonder concessies aan de samenwerking en snelheid?'

De zeven richtingen van het Bechtle Security Kompas

De vier security-dilemma's op de vorige pagina zijn natuurlijk niet de enige uitdagingen die jou bezighouden. Met het Bechtle Security Kompas willen we je helpen om alle uiteenlopende dillema's aan te pakken. In het kompas hebben wij die onderverdeeld in zeven richtpunten.

1. Beleidsvoering

2. Identity & Access

3. Data Governance & Compliance

4. Application collaboration

5. Cloud computing

6. XDR & Endpoints

7. Secure Edge (Network)

Waarom we een kompas als hulpmiddel gebruiken?

Omdat wij merken dat iedere organisatie zijn eigen prioriteiten heeft. Aanvalspaden lopen soms via kwetsbare endpoints, terwijl in andere gevallen misconfiguraties in de cloud leiden tot data breaches. Met het Bechtle Security Kompas kunnen we jouw volledige security-situatie analyseren en gericht inschatten waar voor jou de grootste beveiligingsrisico's liggen. Om een goed beeld te krijgen, starten we met een scan van jouw IT-omgeving.

1. Beleidsvoering

We beginnen met de NIS2 readiness check. Als jouw organisatie wordt gezien als 'essentieel' of 'belangrijk', moet je aan de NIS2 voldoen. Maar ook als jij producten of diensten levert aan organisaties die onder de NIS2 vallen, kunnen zij eisen stellen aan jouw beveiligingsbeleid. Volgens deze Europese richtlijn ben je dan verplicht om security-risico's in kaart te brengen en passende maatregelen te nemen. Maar waar sta je nu en waar begin je? We helpen je om binnen één uur antwoord daarop te krijgen door samen een gerichte vragenlijst door te nemen.

Scans die we o.a. kunnen uitvoeren: *NIS2 readiness check, Data risk assessment.*

2. Identity & Access

Aanvallers breken niet in, ze loggen in: ze misleiden jouw medewerkers om toegang te krijgen. In deze situatie is traditionele cybersecurity is niet langer voldoende. De meeste aanvallen zijn gericht op credentials en authenticatie-tokens. Met de Identity & Access-assessments krijg je een goed beeld welke credentials op straat liggen en in welke mate aanvallers jouw credentials kunnen stelen.

Scans die we o.a. kunnen uitvoeren: *Tenant check, Attack surface check, Data risk assessment, Email risk assessment, Threat protection engagement workshop.*

3. Data Governance & Compliance

Data governance en compliance zijn essentieel om data effectief te beheren, risico's te minimaliseren en boetes te vermijden. Zo loop je het risico op sancties als je niet aan regelgeving voldoet zoals de AVG en NIS2. De Bechtle security-consultants helpen je deze risico's te identificeren en een governancebeleid op te stellen, zodat jouw data voortaan consistent en correct verwerkt wordt.

Scans die we o.a. kunnen uitvoeren: *Tenant check, Data risk assessment, Data governance workshop.*

4. Application collaboration

OneDrive, SharePoint, Teams en Exchange Online zijn onmisbaar om remote te kunnen werken. Dat weten aanvallers ook. Hoe zorg je ervoor dat jouw medewerkers optimaal gebruik kunnen maken van collaboration software, zonder dat gevoelige data in verkeerde handen valt? Met de Application Collaboration-assessments brengen we de gevaren in kaart en adviseren hoe medewerkers productief en toch veilig kunnen werken.

Scans die we o.a. kunnen uitvoeren: *Tenant check, Data risk assessment, Email risk assessment.*

5. Cloud computing

Cloud computing biedt flexibiliteit en schaalbaarheid, maar brengt ook gedeelde verantwoordelijkheid met zich mee. Cloud providers beveiligen de infrastructuur, maar jij bent zelf verantwoordelijk voor de databeveiliging en gebruikersconfiguratie. De Bechtle security-professionals helpen je om de risico's in kaart te brengen. Bijvoorbeeld rond het toegangsbeheer, de dataclassificatie en configuratie. Zo kan jij alles uit jouw cloud halen.

6. XDR & Endpoints

Phishing, ransomware en datalekken – jouw IT-omgeving wordt vanuit alle hoeken bedreigd. Wij helpen je om op de hoogte te blijven van de laatste cybersecurity-bedreigingen met Microsoft Defender XDR. Daarmee krijg je inzicht in jouw cybersecurity van alle endpoints in het netwerk. Daarnaast kun je hiermee e-mail & collaboration, identity, cloudapplicaties en vulnerability management aan elkaar koppelen voor een totaaloverzicht. Ook kun je checken of medewerkers zich wel aan het security-beleid houden, bijvoorbeeld op het gebied van wachtwoordgebruik en het delen van gevoelige informatie.

Diensten die we o.a. kunnen uitvoeren: *Threat Protection Engagement Workshop*.

7. Secure Edge (Network)

Jouw personeel logt vanaf verschillende locaties in op het bedrijfsnetwerk. Maar hoe veilig zijn die verbindingen? Wij helpen je om alle apparaten, systemen en netwerken die verbinding maken grondig te controleren. Zodat onbevoegden geen toegang krijgen tot jouw bedrijfsnetwerk en medewerkers juist wel overal op een veilige manier kunnen inloggen, of dat nu thuis, op kantoor of onderweg is.

Hoe presteert jouw organisatie op de 7 punten van het Security Kompas?

Ontdek het met de Bechtle Security Scan en verbeter jouw IT-beveiliging in 6 stappen!

Lees verder

bechtle