Hoe goed is jouw organisatie beschermd tegen digitale dreigingen?

Doorloop deze beslisboom en kom erachter hoe het gesteld is met de security binnen jouw oranisatie

Hoe veilig is de toegang tot het eigen bedrijfsnetwerk?

Heeft jouw organisatie een hybride omgeving? Dus een combinatie van on-premises en cloud?

JA

Dient een gebruiker zijn wachtwoord apart te wijzigen of -resetten voor zowel de lokale AD als de Azure AD? En moet dit altijd via de IT-beheerder aangevraagd worden?

JA

Heeft jouw organisatie een veiligheidsbeleid als het gaat om wie, wanneer, waar en vanaf welk apparaat toegang heeft tot (gevoelige) bedrijfsdata?

NEE

NEE

Ga door naar bescherming voor e-mail, SharePoint, OneDrive en Teams.

JA

Entra ID P1

Ga door naar het volgende thema!

NEE

Is jouw organisatie voorbereid tegen het toenemend aantal cyberaanvallen per e-mail, SharePoint, OneDrive en Teams?

Ben je goed beveiligd tegen een cyberaanval wanneer een medewerker op een verdachte link klikt of bijlage opent in een email?

JA

.. en wanneer een medewerker dit doet in in SharePoint, OneDrive of Teams?

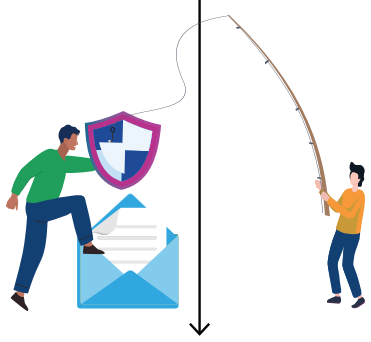
JA

... en wanneer een medewerker een verdachte e-mail ontvangt van een zogenaamd be-trouwbare afzender (Impersonation)?

JA

Ga door naar beheer en beveilig mobiele apparaten.

NEE



NEE

Defender for Office 365 Plan 1

Ga door naar het volgende thema!

NEE

Kan jouw organisatie de veiligheid van bedrijfsdata nog garanderen met de wildgroei aan mobiele apparaten?

Heeft jouw organisatie een overzicht van zakelijke apps op mobiele apparaten?

JA

Worden alle mobiele apparaten centraal beheerd en kunnen (security) updates, patches en software eenvoudig gepusht worden?

JA

Zijn de zakelijke apps, met jouw bedrijfsdata, op deze apparaten goed beveiligd? Dus dat je moeite moet doen om deze te openen?

JA

Ga door naar beheer en beveilig documenten met gevoeldige data.

NEE

Intune

Ga door naar het volgende thema!

NEE

Hoe zorgt jouw organisatie ervoor dat documenten en e-mails met gevoelige (bedrijfs)informatie niet bij verkeerde personen terecht komen?

Versturen jullie regelmatig documenten en e-mails met gevoelige persoons- of bedrijfsgegevens?

JA

Is de kans minimaal dat dit soort gegevens in verkeerde handen terechtkomt?

JA

Weet jouw organisatie waar documenten (met gevoelige informatie) zich bevinden?

JA

NEE

Ga door naar beheer en beveilig jouw apparaten.

NEE

Information Protection Plan 1

Ga door naar het volgende thema!

NEE

Zijn de apparaten binnen jouw organisatie goed beveiligd tegen ransomware, malware, phishing en andere hedendaagse bedreigingen?

Detecteert jouw organisatie proactief mogelijke beveiligings-problemen die een hoog risico voor je bedrijf vormen?

JA

Heeft jouw organisatie een security-oplossing voor bedreigingen van malware- en virusaanvallen op je apparaten en in de cloud?

JA

Heeft jouw organisatie tools die aanvallen herkennen en reageren op geavanceerde bedreigingen en deze ook verwijderen?

JA

Is het met jullie huidige security-oplossingen mogelijk om cyberaanvallen te analyseren en te herstellen?

JA

Bekijk de achterkant.

NEE

NEE

Defender for Business

Ga door naar het volgende thema!

NEE

NEE

BEN JIJ BENIEUWD HOE GOED JIJ NU DAADWERKELIJK BESCHERMD BENT?

DE MICROSOFT OPLOSSINGEN

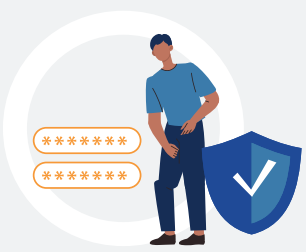
Kwam je uit op 1 oplossing?
Dan kun je deze los toevoegen aan je huidige Microsoft 365 of Exchange Online abonnement of je kunt de Microsoft 365 Business Premium suite overwegen.

Kwam je uit op 2 of meerdere oplossingen?
Dan adviseren wij de **Microsoft 365 Business Premium suite**. Deze bevat al deze oplossingen en is daarmee DE moderne werkplek voor je medewerkers om altijd en overal productief, maar vooral veilig te kunnen werken.

Het beschermt niet alleen tegen de hedendaagse (cyber)bedreigingen, maar met deze werkplek ben je ook AI-ready en dus helemaal klaar voor de toekomst!

Kwam je op geen enkele oplossingen uit?
Chapeau, dan heb je de beveiliging voor jouw organisatie goed op orde!

8 REDENEN WAAROM ORGANISATIES VOOR MICROSOFT 365 BUSINESS PREMIUM KIEZEN

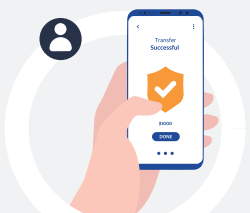


Gedoe met wachtwoorden?
Een hybride omgeving? Een wachtwoordwijziging of reset in de Azure AD wordt tevens gesynchroniseerd met de on-premise AD DS-omgeving.
Entra ID P1

Veilig e-mailen
Bescherm je organisatie tegen verdachte e-mails in de vorm van o.a. ransomware, CEO-fraude, Social Engineering en phishing.
Defender for Office 365 Plan 1

Slimme toegangscontroles
Door een veiligheidsbeleid kan een organisatie de juiste toegangscontroles toepassen. Hierdoor kunnen gegevens altijd en op iedere locatie veilig worden geraadpleegd door gebruikers.
Conditional Access

Mobile Device Management
Mobile Device Management is de oplossing tegen de wildgroei aan mobiele apparaten. Het biedt centraal beheer, bescherming van zakelijke/ gevoelige data en maakt applicaties eenvoudig beschikbaar.
Intune



Eenvoudige configuratie
Er zijn geen image of handmatige instellingen nodig voor nieuwe apparaten, voordat ze aan gebruikers worden gegeven. Hardwareleveranciers kunnen ze direct naar je medewerkers verzenden.
Windows Autopilot

Bescherm je data
Krijg grip op documenten met gevoelige data die ook extern gedeeld worden.
Information Protection

Shared Computer Activation
Gebruik Office/Microsoft 365 Apps binnen een RDS-omgeving.
Shared computer activation for Microsoft 365 Apps

Optimale beveiliging
Beveilig je apparaten tegen ransomware, malware, phishing en andere bedreigingen.
Microsoft Defender for Business

Wil jij ook een veilige moderne werkplek voor jouw organisatie?

Neem contact op met Delta-N!

Delta N B.V.
Laan van Waalhaven 450
2497 GR Den Haag

085 - 487 52 00
info@delta-n.nl

Microsoft Solutions Partner