Microsoft


# Security in het MKB: Office 365

## Het veiligheidsniveau van Office 365

# Het veiligheidsniveau van Office 365

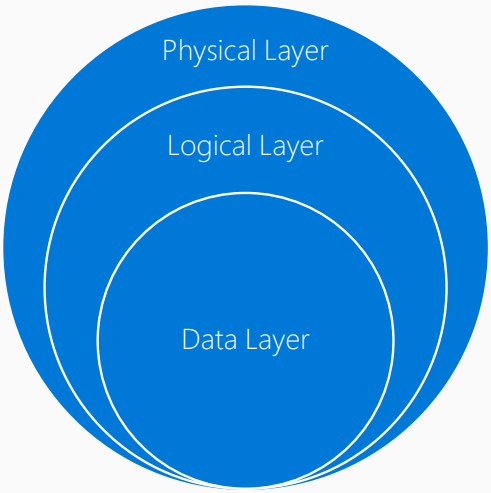
Bedrijven hebben behoefte aan services die hun medewerkers helpen om meer te kunnen doen vanaf vrijwel elke locatie, maar wel met een optimale beveiliging tegen doorlopend evoluerende bedreigingen. Office 365 voldoet aan beide vereisten met een streng beveiligd cloudgebaseerd productiviteitsplatform. Als jouw organisatie de overstap maakt naar cloudservices zoals Office 365, gaat naast de bestaande veiligheidsoverwegingen het vertrouwensaspect meespelen. Je wilt dat jouw serviceprovider veilig omgaat met de gegevens die je aan hem toevertrouwt.

"Je wilt dat jouw serviceprovider veilig omgaat met de gegevens die je aan hem toevertrouwt."

Microsoft is een erkende sectorleider op het gebied van cloudbeveiliging. Ons team heeft tientallen jaren ervaring met de ontwikkeling van zakelijke software en werkt onze services en toepassingen doorlopend bij, waardoor we een veilige cloudservice kunnen bieden die voldoet aan zware sectornormen.

Informatie over de beveiliging, privacy, naleving, transparantie en gebruikscontinuïteit van Office 365 is te vinden in het Office 365 Vertrouwenscentrum.

Het Office 365-platform biedt beveiliging op elk niveau, van toepassingsontwikkeling tot fysieke gegevenscentra en de toegang van eindgebruikers. Op het serviceniveau gebruiken we een diepteverdedigingsstrategie die je gegevens beschermt met meerdere beveiligingslagen (fysiek, logisch en data):




Bij een diepteverdedigingsstrategie zijn beveiligingen aanwezig in meerdere lagen van de service. Als één laag wordt doorbroken, zijn er compenserende maatregelen aanwezig die verzekeren dat de beveiliging gehandhaafd blijft. De strategie omvat ook tactieken voor het opsporen, voorkomen en verzwakken van aanvallen voordat deze plaatsvinden. Dit vereist doorlopende verbeteringen van de beveiligingsfuncties, inclusief:

- Scannen en herstellen van poorten
- Perimeterscans
- Beveiligingsupdates voor besturingssystemen
- Detectie en preventie van DdoS-aanvallen op netwerkniveau
- Meerstaps-authenticatie voor servicetoegang

Met betrekking tot mensen en processen omvat de inbreukpreventie:

- Controle van de toegang en acties van alle gebruikers/beheerders
- Geen vaste machtigingen voor beheerders
- Just-in-time toegang en tijdelijke, specifiek verleende machtigingen voor het verhelpen van problemen met de service
- Scheiding tussen de e-mailomgeving van medewerkers en de productieomgeving
- Verplichte achtergrondonderzoeken voor personen met hogere toegangsrechten. Deze onderzoeken omvatten uitgebreide controles en handmatige goedkeuringen.

Inbreukpreventie bestaat ook uit automatische verwijdering van overbodige accounts wanneer een medewerker het bedrijf verlaat, van groep verandert of het account niet gebruikt. Waar mogelijk wordt de mens vervangen door een geautomatiseerd, toolgebaseerd proces. Inclusief routinefuncties zoals implementatie, foutopsporing, diagnostische verzameling en het herstarten van services.

We blijven investeren in systeemautomatisering voor het opsporen van abnormaal en verdacht gedrag en een snelle aanpak van beveiligingsrisico's. We verbeteren ook doorlopend ons geautomatiseerde patchingsysteem, dat automatisch oplossingen genereert en implementeert voor problemen die door de beveiligingssystemen worden ontdekt. Dit draagt enorm bij aan de veiligheid en flexibiliteit van de service. We voeren periodieke penetratietests uit om doorlopende verbetering van incidentresponsprocedures mogelijk te maken. Deze interne tests helpen onze beveiligingsexperts bij de ontwikkeling van een methodisch, herhaalbaar en geoptimaliseerd responsproces.

# 1. Fysieke laag

## Fysieke laag - faciliteit

Klantgegevens worden opgeslagen in onze Office 365-gegevenscentra, die geografisch zijn gespreid zonder de voordelen van regionale opslag uit het oog te verliezen. Onze gegevenscentra zijn volledig ontworpen voor de bescherming van services en gegevens tegen schade door natuurrampen of onbevoegde toegang.

"De beveiliging van edgerouters maakt de detectie van aanvallen en tekenen van kwetsbaarheid in de netwerklaag mogelijk."

De toegang tot de klanttoepassingen en -services in gegevenscentra wordt 24/7 beperkt tot essentiële medewerkers op basis van hun rol. Voor de fysieke toegangscontroles worden meerdere identificatie- en beveiligingsprocessen gebruikt, waaronder badges, smartcards, biometrische scanners, beveiligingspersoneel op de locatie, doorlopende camerabewaking en tweestaps-authenticatie. De gegevenscentra worden bewaakt met behulp van bewegingssensors, camerasystemen en inbraakalarmen. Daarnaast omvat de beveiliging geautomatiseerde brandpreventie- en blussystemen en aardbevingsbestendige racks.

# 2. Logische laag

De logische beveiligingslaag bestaat uit maatregelen en processen waarmee hostmachines worden beveiligd. Dit geldt voor draaiende toepassingen en de werkzaamheden van de beheerders van deze machines en toepassingen.

"De meeste acties die beheerders op hosts en toepassingen uitvoeren zijn geautomatiseerd."

## Geautomatiseerde bewerkingen

De meeste acties die beheerders op hosts en toepassingen uitvoeren zijn geautomatiseerd, zodat menselijke tussenkomst tot een minimum wordt beperkt. Hierdoor wordt het risico van inconsistente configuraties of kwaadwillende activiteiten beperkt. Deze geautomatiseerde aanpak gaat door tot de implementatie van systemen in onze gegevenscentra.

## Beheerderstoegang tot gegevens

De beheerderstoegang tot Office 365 en jouw gegevens wordt streng bewaakt.
De belangrijkste elementen van dit proces zijn rolgebaseerde toegang en verlening van de minimaal vereiste machtigingen voor de uitvoering van specifieke taken. Deze principes worden gevolgd ongeacht of het gaat om fysieke (dus tot het gegevenscentrum of de servers) of logische toegang. Een goed voorbeeld is de Lockbox-procedure die beheerders moeten doorlopen bij een verzoek om aanvullende machtigingen.

## Toegangsbeheer vindt plaats op meerdere niveaus:

- Op medewerkersniveau, waar met achtergrondonderzoeken en streng accountbeheer wordt verzekerd dat alleen bevoegde personen een taak kunnen uitvoeren
- Rolgebaseerd toegangsbeheer
- Een Lockbox-procedure die de volgende elementen omvat:
  - Just-in-time accounts met strenge wachtwoordbeveiliging
  - Een beperkte toegangsduur
  - Toegang voor specifieke acties op basis van rol
- De servers voor de Office 365-service hebben een voorgedefinieerde set procedures die kunnen worden uitgevoerd met behulp van Applocker
- Controle en beoordeling van elke toegang

## Security Development Lifecycle

De Microsoft Security Development Lifecycle (SDL) is een uitgebreid veiligheids-waarborgproces voor elke fase van het ontwerp en de ontwikkeling en implementatie van onze software en services, inclusief Office 365. Door middel van ontwerpvereisten, kwetsbaarheidsanalyses en bedreigingsmodellering helpt het SDL ons om zwakke plekken te voorspellen, identificeren en verhelpen voordat een service de volledige BitLocker-productiecyclus doorloopt. De SDL wordt continu bijgewerkt met de meest actuele gegevens en beste werkmethoden om te verzekeren dat nieuwe services en software voor Office 365 vanaf dag één optimaal zijn beveiligd.

## Anti-malware, patching en configuratiebeheer

Het gebruik van anti-malwaretoepassingen vormt een belangrijk element van de beveiliging van jouw gegevens in Office 365. De software detecteert en verhindert het binnendringen van computervirussen en wormen in de servicesystemen. Geïnfecteerde systemen worden in quarantaine gezet om verdere schade te voorkomen totdat herstelmaatregelen worden getroffen. Anti-malwaretoepassingen bieden zowel preventie als detectie van kwaadwillende software. Onze standaard configuratievereisten voor servers, netwerkapparatuur en andere Microsoft-toepassingen zijn gedocumenteerd waar de normen het gebruik van een standaardpakket voorschrijven.  Deze pakketten worden vooraf getest en geconfigureerd met beveiligingsmaatregelen. Voor veranderingen in de productieomgeving zoals updates, hotfixes en patches wordt dezelfde standaard veranderingsbeheerprocedure gevolgd. Patches worden geïmplementeerd binnen de door de uitgever gespecificeerde tijdsperiode. Veranderingen worden vóór de implementatie beoordeeld op toepasselijkheid, risico en hulpbronvereisten door onze beoordelingsteams en de adviesraad (CAB).

# 3. Gegevenslaag

Office 365 is een schaalbare multi-tenantservice, wat inhoudt dat je gegevens worden bewaard op hardware die met andere klanten wordt gedeeld. We hebben Office 365 zodanig ontworpen dat meerdere klanten de service op een veilige manier kunnen gebruiken door middel van gegevensisolatie. De gegevensopslag en -verwerking voor elke gebruiker is gescheiden met behulp van Azure Active Directory en functies die specifiek zijn ontwikkeld voor het bouwen, beheren en beschermen van multi-tenantomgevingen. Azure Active Directory isoleert jouw gegevens door middel van beveiligingsgrenzen. Je gegevens worden beschermd, zodat ze niet door mede-tenants kunnen worden bekeken of geschonden.

Benieuwd hoeveel jij weet over beveiliging voor je bedrijf?

Doe nu de Digital Security Test