MostWare.

Zero Trust: jouw persoonlijke bodyguard op het internet

MostWare.

Managementsamenvatting

Zero Trust is een nieuwe manier van beveiligen. Een manier die aansluit bij de wijze waarop we vandaag de dag werken en leven. Flexibel, mobiel en altijd online. Traditionele beveiligingsmethodes zijn niet langer toereikend. Cybercriminelen maken gebruik van zwakke punten in de beveiliging die ontstaan doordat medewerkers steeds vaker vanaf verschillende locaties en met diverse apparaten bedrijfsnetwerken benaderen. Eenmaal binnen kan zo'n hacker relatief eenvoudig verder binnendringen in het netwerk en onherstelbare schade aanrichten. De manier om hiermee om te gaan is niet door het fort nog verder te versterken, maar door de controles op wie, wanneer en op welke manier naar binnen wil, te verscherpen. We controleren dus op identiteit, apparaat, applicaties en dataverkeer. Dat is de kern van Zero Trust. 'Vertrouw niemand, controleer alles.'

In dit artikel vertellen we meer over deze beveiligingsprincipes en hoe je een robuuste Zero Trust strategie opbouwt die past bij je organisatie. Ook vertellen we je welke technische componenten je daarbij nodig hebt en wat MostWare hierin kan betekenen.

MostWare.

Inhoudsopgave

Hoe veilig werk jij?	04
Een micro-firewall om elke gebruiker	05
Het fundament werd al gelegd in 2004	06
In 5 stappen aan de slag met Zero Trust	06
De impact van Zero Trust op jouw organisatie	09
Security Operation Centre (SOC)	10
Over MostWare	11

MostWare.

Hoe veilig werk jij?

Het moderne werken via de cloud biedt veel voordelen. Deelnemen aan een vergadering op je thuiswerkdag bijvoorbeeld of nog snel even een offerte bijwerken terwijl je bij een klant bent. Maar hoe zit het met de beveiliging? Maak jij altijd gebruik van een veilige verbinding als je inlogt op het bedrijfsnetwerk? Ook als je onderweg met spoed een document nodig hebt? Of wat te denken van die zakenrelatie die op bezoek is, en via zijn laptop zo in jullie bedrijfsnetwerk kan komen? Situaties die niet geheel ondenkbaar zijn, maar tegelijkertijd wel een enorm veiligheidsrisico met zich meebrengen.
Kortom, deze nieuwe manier van werken vraagt ook om een nieuwe manier van beveiligen. Een manier die uitgaat van het principe 'vertrouw niemand, controleer alles'. In de praktijk komt deze Zero Trust filosofie erop neer dat – voordat je als gebruiker toegang krijgt tot bepaalde applicaties, documenten of bestanden – jouw identiteit, apparaat én toegangsverzoek geverifieerd worden. Op deze manier wordt een hacker die toegang probeert te krijgen met gestolen inloggegevens op een onbekend apparaat geblokkeerd, net als een geverifieerde gebruiker die een betrouwbaar apparaat gebruikt maar probeert toegang te krijgen tot gegevens die hij niet mag zien. We verleggen hiermee de focus van toegangscontrole van je netwerk naar slimme controles die kijken naar de hele context. Deze holistische benadering van beveiliging zorgt ervoor dat je als organisatie meer grip krijgt op wat er binnen jouw IT-omgeving gebeurt. Of het nu gaat om inlogpogingen van buitenaf of het online gedrag van eigen medewerkers.

"Vertrouw niemand, controleer alles"

Een micro-firewall om elke gebruiker

Conventionele beveiligingsstrategieën gaan ervan uit dat alle gegevens die binnen het beveiligde bedrijfsnetwerk staan, beschermd zijn. Tot zo'n vijf jaar geleden was dit in de meeste gevallen ook zo. Een intelligente firewall zorgde ervoor dat het dataverkeer van en naar je netwerk gemonitord en gecontroleerd werd. Aanvallen konden zo opgespoord en geblokkeerd worden. Maar klikte een medewerker op een phishing-link of werd een wachtwoord gestolen, dan had je een probleem. En bij deze risico's is het niet gebleven. Doordat steeds meer applicaties en toepassingen buiten het bedrijfsnetwerk, in de cloud, gehost worden, is het een stuk complexer geworden om al het dataverkeer te monitoren en beveiligen. Tel daarbij op dat de gemiddelde medewerker niet meer veertig uur per week achter een desktop op kantoor zit, maar werkt vanaf verschillende locaties met diverse mobiele apparaten en je begrijpt dat de traditionele beveiligingsmethodes niet langer toereikend zijn.

Met Zero Trust laten we dit inmiddels valse gevoel van veiligheid los en creëren we als het ware een micro-firewall om iedere medewerker of gebruiker. Door middel van controle op identiteit, apparaat en handelingen bescherm je alle applicaties, diensten en middelen die buiten het bereik van het bedrijfsnetwerk liggen. Zo kan een medewerker zich vrij bewegen in de digitale wereld en profiteren van alle voordelen die de cloud en het moderne werken bieden, terwijl tegelijkertijd de bedrijfsgegevens optimaal beveiligd zijn.

Maak je daarnaast ook nog gebruik van een lokaal netwerk? Dan beveilig je deze uiteraard nog steeds met een intelligente firewall. Deze dubbele strategie zorgt ervoor dat je bedrijfsinformatie op alle niveaus veilig is.

MostWare.

Het fundament werd al gelegd in 2004

Het concept van Zero Trust is niet nieuw. Al in 2004 introduceerde Jericho Forum, een internationaal samenwerkingsverband op het gebied van IT-beveiliging, de term. Deze beveiligingsexperts begrepen aan het begin van deze eeuw al dat het concept van een veilige, afgeschermde digitale omgeving niet langer houdbaar was. Daarmee legden zij de basis voor deze hedendaagse beveiligingsstrategie. Inmiddels heeft Microsoft de Zero Trust aanpak volledig omarmd en een breed spectrum aan toepassingen en producten ontwikkeld, die ons in staat stellen om flexibel én veilig op het internet te bewegen. Werken via de cloud wordt hiermee niet alleen leuker en beter, maar ook veiliger.

In 5 stappen aan de slag met Zero Trust

Om Zero Trust succesvol toe te passen binnen je organisatie zijn er een aantal zaken van belang. Om ervoor te zorgen dat je niets over het hoofd ziet, hebben we bij MostWare een vijfstappenplan richting Zero Trust ontwikkeld. Deze stappen hebben betrekking op de informatie die verzameld wordt op het moment dat iemand probeert in te loggen, de beleidsregels die je wilt hierop wilt toepassen én de daadwerkelijke handhaving van deze regels.

1 Zorg voor een sterke identiteitsverificatie

De eerste check die je uitvoert wanneer iemand probeert toegang te krijgen tot bepaalde applicaties of informatie, is het verifiëren van zijn of haar identiteit. Met andere woorden: 'ben jij wel wie je zegt dat je bent?' Dit kun je doen door middel van een gebruikersnaam en wachtwoord, maar deze kunnen relatief eenvoudig onderschept worden tegenwoordig. Sterker nog, maar liefst 81% van de datadiefstallen ontstaat doordat een wachtwoord van een medewerker achterhaald is. Dit risico kun je ondervangen door het instellen van multifactor identificatie. Deze vorm van authenticatie combineert twee of drie van de volgende controlemethodes:

- Iets dat je **kent**, doorgaans een wachtwoord
- Iets dat je **hebt**, een vertrouwd apparaat zoals een telefoon waarop je een melding voor goedkeuring ontvangt
- Iets dat je **bent**, in de vorm van biometrische ken merken zoals gezichtsherkenning of je vingerafdruk

Door gebruik te maken van Microsoft Azure Active Directory kun je deze identiteitsverificatie eenvoudig inrichten. Naast multifactor identificatiemogelijkheden, biedt het namelijk ook een gebruiksvriendelijke eenmalige aanmeldingsmogelijkheid (single sign-on) en constante controle door middel van slimme analyses. Mocht er een bedreiging gedetecteerd worden nadat iemand al ingelogd is, dan kan er alsnog actie worden ondernomen.

"81% van de datadiefstallen ontstaat doordat een wachtwoord van een medewerker achterhaald is"

2 Stel de betrouwbaarheid van apparaten vast

De volgende stap heeft betrekking op de betrouwbaarheid van het apparaat waarmee ingelogd wordt. Zo kan het zijn dat een laptop of mobiele telefoon van een medewerker is gestolen of zonder medeweten is besmet met malware, gehackt is of is gebruikt bij cybercriminaliteit. Door gebruik te maken van slimme technologie zoals Microsoft Intune in combinatie met Microsoft Defender Advanced Threat Protection wordt belangrijke informatie over de gebruikte apparaten geregistreerd en wordt de status continu in de gaten gehouden. Zo kun je vaststellen of een apparaat:

- Het juiste besturingssysteem gebruikt
- Geregistreerd is voor bedrijfsmatig gebruik
- Zwakke plekken in de beveiliging vertoont
- Mogelijk gecompromitteerd is

Deze laatste check gebeurt op basis van een waarschijnlijkheidsanalyse. Wanneer een apparaat bijvoorbeeld gebruikt wordt vanuit het buitenland terwijl de betreffende medewerker daar nooit geweest is, dan is de kans dat het niet pluis is vrij groot. Dit is ook het geval wanneer uit security databases blijkt dat het apparaat betrokken is geweest bij een cyberaanval of als er opeens midden in de nacht ingelogd wordt terwijl de medewerker zelf op één oor ligt.

3 Definieer slimme beleidsregels

Dit is misschien wel de belangrijkste stap als het gaat om Zero Trust. Op basis van identiteit- en apparaatcontrole heb je nu veel informatie verzameld over een gebruiker die wil inloggen. Vervolgens moet je bepalen onder welke voorwaarden hij of zij toegang krijgt. Deze voorwaarden leg je vast in beleidsregels. Zo kun je bepalen of iemand:

- Toegang krijgt
- Geen toegang krijgt
- Beperkte toegang krijgt
- Aanvullende verificatiehandelingen moet uitvoeren

Voorbeelden van beleidsregels zijn:

'Onze medewerkers gebruiken iPhones, dus als iemand probeert in te loggen met een Android apparaat dan wordt de toegang geweigerd.'

'Als een gebruiker vanaf een bepaalde geografische locatie probeert in te loggen, dan wordt gevraagd om een extra verificatie.'

'Als een ingelogde gebruiker meer dan 20 bestanden verwijderd, dan wordt deze persoon automatisch uitgelogd met het verzoek contact op te nemen met een security (SOC) medewerker.'

'Als een gebruiker inlogt vanaf een onbekend apparaat, dan krijgt degene geen toegang tot bedrijfskritische applicaties of informatie.'

Op deze manier zijn er nog veel meer beleidsregels te bedenken die passen bij de werkwijze van jouw organisatie. Bovendien is het niet noodzakelijk om direct een uitgebreid scala aan regels op te stellen. Als organisatie kun je er bijvoorbeeld ook voor kiezen om te starten met het alleen toestaan van inlogpogingen vanaf kantoor of vanuit Nederland. Vervolgens kun je gaandeweg nieuwe beleidsregels toevoegen die passen bij de manier waarop jij en je collega's werken. Aan jou om te bepalen of deze marge voor jouw doelstelling acceptabel is.

4 Pas de beleidsregels toe

Voor het toepassen van de beleidsregels heb je tools nodig die je helpen om gegevens en applicaties te beschermen en het beleid te handhaven. Geavanceerde tools die je in staat stellen om:

- Per inlogpoging het risico te berekenen
- Voorwaardelijke toegang te realiseren
- De toegang op documentniveau in te stellen
- Data in cloudapplicaties te beschermen

MostWare kan je helpen bij configureren van de juiste veiligheidsproducten op basis van Microsoft Azure Active Directory. Zo creëren we een Security Operation Centre van waaruit niet alleen bedreigingen gedetecteerd en geëlimineerd worden, maar waar we ook beveiligingsinformatie verzamelen om zo met slimme inzichten je organisatie nóg veiliger te maken.

5 Blijf alle handelingen proactief monitoren

De laatste stap sluit perfect aan bij het motto 'vertrouw niemand, controleer alles'. Volgens dit principe blijf je namelijk continu controleren op verdachte activiteiten. Ook hierbij spelen de opgestelde beleidsregels een belangrijke rol. Dankzij deze regels hoef je niet letterlijk bij elke medewerker over de schouder te kijken, maar kun je wel direct actie ondernemen wanneer een bedreiging gesignaleerd wordt. Het is bijvoorbeeld logisch dat een applicatiebeheerder softwareaanpassingen moet kunnen uitvoeren, maar een beleidsregel kan zijn dit alleen mag gebeuren in een afgeschermd deel van het netwerk. Wanneer dit toch in een 'live-omgeving' gebeurt, dan zullen alle spreekwoordelijke alarmbellen meteen afgaan.

Daarnaast heeft het constant monitoren ook betrekking op het steeds nauwkeuriger maken van de voorspelling of een bepaalde inlogpoging of handeling al dan niet legitiem is. Dit gebeurt op basis van machine learning technologie. Door vals positieve meldingen eruit te filteren, leert het systeem steeds beter wat een bedreiging is en wat niet.

Daarnaast zijn er wereldwijd gigantische hoeveelheden bedreigingsinformatie en beveiligingsgegevens beschikbaar, waar de beveiligingstechnologie van Microsoft van kan profiteren. Op die manier kun je het Zero Trust-beleid binnen jouw organisatie steeds beter afstemmen op de werkelijkheid.

MostWare.

De impact van Zero Trust op jouw organisatie

Zero Trust is zo ontworpen dat de impact op de digitale bedrijfsveiligheid enorm is. Tegelijkertijd is de impact op de belasting van je netwerk en medewerkers zo klein mogelijk. Met deze aanpak verdeel je namelijk je netwerk, applicaties, gebruikers en data als het ware in verschillende segmenten. Op basis van deze segmentatie pas je beveiligingsmaatregelen toe die overeenkomen met de functie van de gebruiker en de gevoeligheid van de informatie. Je kunt er dus op vertrouwen dat iedere medewerker, klant of samenwerkingspartner het juiste toegangsniveau krijgt binnen de digitale omgeving. Waarmee niet alleen je beveiliging optimaal is, maar ook de productiviteit verbetert. Iedere gebruiker beschikt immers exact over die informatie en toepassingen die hij of zij nodig heeft om goed te kunnen functioneren. Bovendien zorgt deze gesegmenteerde aanpak ervoor dat een eventueel veiligheidsincident invloed heeft op slechts een deel van het netwerk en niet op het volledige netwerk.

Voor medewerkers geldt dat zij gebruik zullen moeten gaan maken van multifactor identificatie bij het inloggen. Dit betekent dat er naast het invoeren van een gebruikersnaam en wachtwoord altijd een extra handeling moet worden uitgevoerd. Dit kan even wennen zijn. Bij MostWare begeleiden we medewerkers daarom bij het instellen en in gebruik nemen van deze vorm van identificatie. Dankzij de single sign-on mogelijkheid hoeven zij bovendien maar eenmaal in te loggen, waarna ze toegang hebben tot alle relevante applicaties en bestanden.

Hierdoor is deze manier van inloggen veilig én gebruiksvriendelijk. Maar hoe zit het met de implementatie van Zero Trust? Wat merken medewerkers en IT-beheerders daarvan? Dat hangt ervan af of je ervoor kiest om het zelf te doen of (deels) uit te besteden. Heb je een eigen IT-afdeling, dan kun je jouw cloudomgeving wellicht prima zelf beveiligen op basis van de Zero Trust strategie. Mits je beschikt over voldoende kennis en capaciteit om een eigen beveiligingscentrum in te richten op basis van de juiste technologieën, en incidenten te monitoren, analyseren en op te volgen.

Twijfel je hierover? Dan is het ook mogelijk om dit gedeeltelijk of volledig uit te besteden. Zo kunnen wij je bijvoorbeeld helpen met het inrichten en configureren van een beveiligingscentrum, waarna je het beheer en de opvolging van incidenten zelf doet. Uiteraard kunnen we ook de volledige Zero Trust beveiliging voor je uit handen nemen. Wanneer je ervoor kiest om dit uit te besteden aan MostWare dan zullen onze security specialisten de juiste licenties regelen, de software configureren en je helpen met het opstellen van de Zero Trust beleidsregels. Zo stomen we ook jouw organisatie klaar voor een nieuw niveau van veiligheid. Dit heeft verder geen impact op de bestaande IT-infrastructuur. De focus ligt op de digitale identiteit van medewerkers en eventuele externe gebruikers zoals klanten, partners en leveranciers. Er hoeft dus niets geïnstalleerd te worden op bestaande systemen. Wel is het belangrijk dat je als organisatie gebruik maakt van Microsoft 365. Heb je nog geen Microsoft 365 of alleen Office 365? Dan kunnen we je helpen de juiste licenties toe te voegen.

MostWare.

Security Operation Centre (SOC)

Het Security Operation Centre van MostWare kun je zien als het beveiligingshoofdkwartier van jouw organisatie. Vanuit hier houden wij jouw IT-omgeving 24/7 veilig. Dit doen we met de meest recente Microsoft veiligheidsproducten en de nieuwste inzichten. Ook verbeteren we indien nodig de opgestelde beleidsregels. De sleutelwoorden zijn hierbij: Protect, Detect en Respond.

Protect

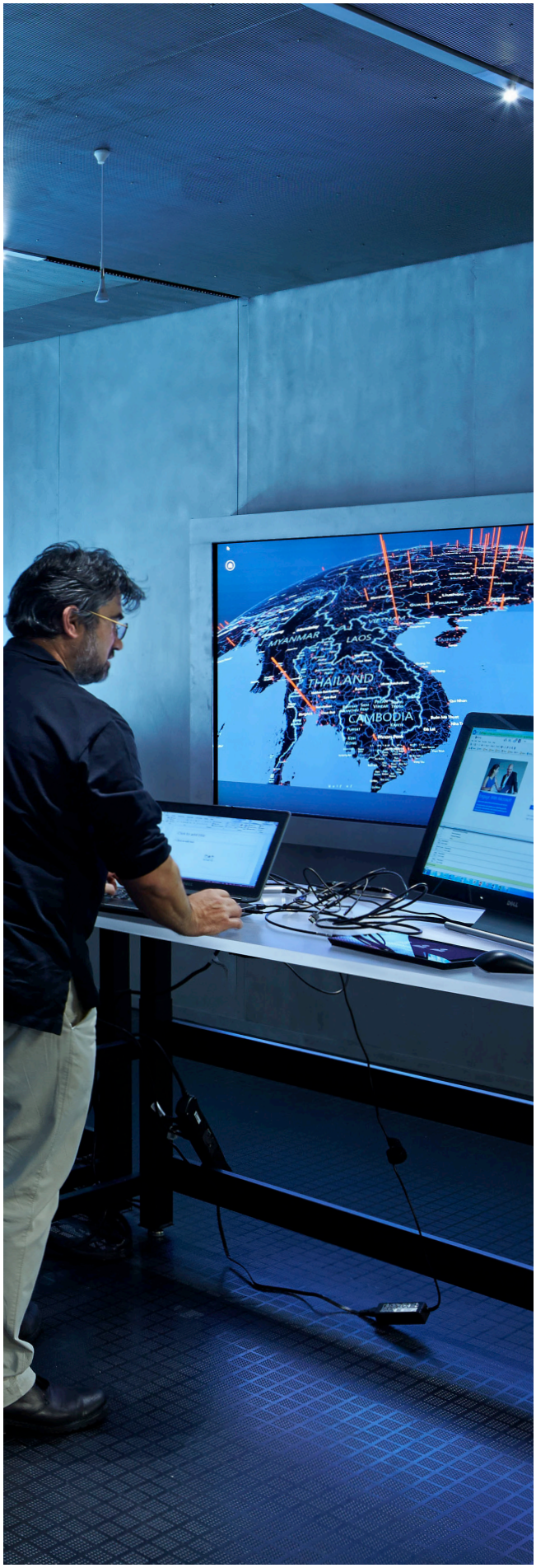
Voorkomen is altijd beter dan genezen. Daarom zijn we voortdurend bezig met het verbeteren van de beveiliging. Zo scherpen we de beleidsregels aan op basis van rapportages en worden de nieuwste security features toegepast op het Zero Trust beleid. Zo zorgen we voor een veilige inrichting.

Detect

Dankzij automatische detectiemechanismen tonen intelligente dashboards continu de beveiligingsstatus. Worden er bijzonderheden of afwijkingen gedetecteerd, dan wordt er direct actie ondernomen. Door het systeem zelf én door onze security specialisten. Bovendien worden alle incidenten en mogelijke bedreigingen maandelijks gerapporteerd. Deze rapportages helpen ons vervolgens weer om het systeem nog beter te maken.

Respond

Uiteraard ondernemen we direct actie als zich een incident voordoet. Ons security team benadert de betrokken medewerker en helpt hem of haar de juiste stappen te nemen. We hebben uitgebreide draaiboeken klaarliggen voor de meest uiteenlopende incidenten, zodat we altijd adequaat kunnen reageren. Is het echt ernstig? Dan nemen we onmiddellijk contact op met jouw Security Officer om samen de juiste maatregelen te nemen.



MostWare.

Zero Trust: jouw persoonlijke bodyguard op het internet

Over de auteur Rogier Belt

Het beheer van Microsoft 365 kent voor Rogier geen geheimen. Nadat hij een brede kennis heeft ontwikkeld van Microsoft cloud-technologie is de doorontwikkeling van de Zero Touchmethodiek een logisch vervolg geweest. Rogier is in het bezit van alle relevante Microsoft certificeringen op gebied van security en met alle learnings uit het toepassen van Zero Touch op Microsoft-technologie en de oprichting van het SOC van MostWare is deze whitepaper ontstaan. Rogier deelt zijn kennis graag omdat hij iedereen een veilige werkomgeving gunt.

Rogier Belt

Over MostWare

Bij MostWare geloven we dat iedere organisatie toegang moet hebben tot de mooiste IT-oplossingen. Daarom delen wij al sinds 1990 graag onze kennis en kunde. Inspireren met IT noemen we dit. Dat doen we altijd vanuit het oogpunt van onze klant. Door verder te kijken dan de vraag die vandaag op tafel ligt. Daarbij zijn we niet bang om buiten de gebaande paden te treden. Zo vinden we oplossingen die ook morgen en in de toekomst nog aansluiten bij jouw bedrijfsvisie. Of je nu aan de slag wilt met Zero Trust, een moderne werkplek wilt creëren of meer wilt doen met slimme data, met gave technologieën maken we jouw werkdag leuker en beter.

Meer weten?

Hebben wij je nieuwsgierigheid gewekt en wil je graag weten hoe Zero Trust jouw organisatie veiliger kan laten werken? Neem dan gerust contact met ons op via 071-5791010.

MostWare.