ON2IT ZERO TRUST INNOVATORS

Een allesomvattend Zero Trust product bestaat niet

Tegenwoordig is het moeilijk om in het IT-security landschap de term 'Zero Trust' te ontwijken. Leveranciers (met name hun marketingafdelingen) gebruiken de term te pas en te onpas in de hoop wat mee te pikken van de populariteit van de term en de noodzaak voor bedrijven om security serieus te nemen.

Auteur: Rob Maas

Rob Maas is Lead Architect bij ON2IT en officieel Forrester Zero Trust Strategist. Rob is gespecialiseerd in het praktisch implementeren van Zero Trust bij bedrijven.

Zero Trust	**Microsegmentatie**
Continious Compliance	**SaaS**
DAAS	**Shadow-IT**
CMDB	**GDPR**
IT-security	**Zero Trust Risk Map**

Vrijwel elke fabrikant claimt het ultieme Zero Trust product in hun portfolio te hebben, waarmee implementatie en beheer van een volledige Zero Trust omgeving een eitje wordt. Helaas bestaat een allesomvattend product voor Zero Trust niet en het zal er ook nooit komen.

Zero Trust is een strategie en deze strategie schrijft geen producten voor. Een strategie geeft duiding over de richting waarin een bedrijf moet bewegen. Hierbij geeft Zero Trust een aantal handvatten. De meest bekende is 'Never trust, Always verify', maar ook 'Design from inside-out'. Hoe vervolgens invulling wordt gegeven aan deze strategie is aan de gebruiker. Het omarmen en toepassen van Zero Trust in een organisatie is dan ook een kwestie van de juiste mensen (stakeholders) en het gebruik van de juiste hulpmiddelen.

Wat moet ik beschermen?

De basis van Zero Trust ligt bij de vraag: ''Wat zijn mijn bezittingen (DAAS') en waar ben ik voor verantwoordelijk?'' Als je immers niet weet wat je bezit dan kun je dit ook niet beschermen. Het is daarom essentieel om inzicht te hebben in wat de IT-omgeving allemaal omvat. Vergeet hierbij zeker niet de veelal bestaande 'shadow-IT' in de vorm van cloud-producten zoals Evernote, Trello, Slack, etc.

Deze inventarisatie is het absolute startpunt waarbij meerdere producten kunnen helpen, echter vaak ook met hun eigen specifieke doelgebied. Uiteindelijk is dit een exercitie die nog grotendeels door mensen moet worden uitgevoerd, wellicht gesteund door hulpmiddelen.

Ook hier geldt dat deze systemen slechts een hulpmiddel zijn en dat het definiëren van relaties en de daadwerkelijke risico's uiteindelijk mensenwerk blijft.

Tenslotte moeten de resultaten uit de inventarisatie overzichtelijk worden verwerkt. Het loont om hier voldoende tijd aan te besteden en te starten met het up-to-date brengen van een Configuration Management Database (CMDB) voor de security. Vergelijk dit met hoe bedrijven hun financiële administratie zorgvuldig bijhouden, zo hoort dit ook te gebeuren met IT-systemen. Deze administratie vormt de basis voor een gezonde en veilige IT-omgeving.

Welke risico's lopen mijn bezittingen

Wanneer inzichtelijk is wat de IT-omgeving allemaal omvat, is het belangrijk om te duiden welke risico's gepaard gaan met de bezittingen. Steeds vaker zal dit niet alleen vanuit het perspectief van het bedrijf zijn, bijv. intellectueel eigendom, maar ook gestuurd worden vanuit wet- en regelgeving zoals de GDPR. Bovendien eisen andere stakeholders zoals klanten, toeleveranciers en gebruikers steeds vaker dat security op orde is. Er komen tegenwoordig meer en meer kritische vragen, bijv. in de vorm van aanbestedingen. Het op orde hebben van IT-security kan dan ook gebruikt worden als verkoopargument en om vertrouwen te bevorderen.

Door de risicovolle kenmerken (bijv. CIA/BIV ratings, type data; PII) te beschrijven in de CMDB ontstaat er een prioriteitenlijst. Daarna is het zaak om (micro) segmenten te creëren; een segment kan worden gezien als een veiligheids-zone die één of meerdere 'bezittingen' bevat. Ter illustratie; als er data met een hoog risicoprofiel door meerdere systemen loopt, kan je ervoor kiezen om een segment te creëren waarin al deze systemen worden gestopt.

Vervolgens moet je bepalen welke maatregelen je moet nemen om het risico te verkleinen, inzicht te verschaffen en te kunnen rapporteren op dit segmentniveau. Deze maatregelen kunnen erg uiteenlopen, van ''Wie/wat mag er bij dit segment komen (wie mag er de veiligheidszone betreden)?'' tot ''Aan welke eisen moet ik voldoen om onderdeel te mogen zijn van dit segment (bijv. 'endpoint protectie' moet actief zijn)?'' Ook hier geldt dat wet- en regelgeving kan helpen of zelfs dwingen. Vaak zijn er voor verschillende industrieën voorschriften over hoe om te gaan met bepaalde data/systemen.

Ook voor de bovenstaande actie geldt dat er meerdere producten zijn die inzicht kunnen verschaffen in de relaties van systemen en kwetsbaarheden. Maar ook hier geldt dat deze systemen slechts een hulpmiddel zijn en dat het definiëren van relaties en de daadwerkelijke risico's uiteindelijk mensenwerk blijft.

Door de segmenten vast te leggen en goed te beschrijven ontstaat er een duidelijk overzicht van de omgeving:

- welke risicovolle kenmerken zijn van toepassing op het segment?
- hoe relevant is het segment?
- wie is er verantwoordelijk voor dit segment, etc.?

Deze vastlegging wordt ook wel een ‘Zero Trust Risk Map’ genoemd.

De keuze van de producten die nodig zijn om Zero Trust daadwerkelijk te implementeren hangt samen met de gekozen beveiligingsmaatregelen en de eventuele concessies die gedaan worden door het niet toepassen van bepaalde beveiligingsmaatregelen.

Implementatie

Nu we eenmaal duidelijk hebben wat we moeten beschermen en aan welke eisen deze bescherming moet voldoen, kunnen we beginnen met het daadwerkelijk implementeren van maatregelen. In veel gevallen zijn er al meerdere producten aanwezig die we kunnen gebruiken voor de implementatie van de Zero Trust Risk Map. Soms is het zelfs niets meer dan de figuurlijke schakelaars aan of uit zetten, met name voor SaaS applicaties.

De keuze van de producten die nodig zijn om Zero Trust daadwerkelijk te implementeren hangt samen met de gekozen beveiligingsmaatregelen en de eventuele concessies die gedaan worden door het niet toepassen van bepaalde beveiligingsmaatregelen, oftewel te kiezen voor een geaccepteerd risico.[2]

Na de implementatie is het belangrijk om te monitoren en te acteren op eventuele security incidenten in de omgeving, waarbij uiteraard een incident in een segment met een hoge risico classificatie een hogere prioriteit krijgt. Het is daarom van groot belang dat de security-monitoring en gekoppelde ticketing-systemen dit onderscheid snel kunnen maken, zodat de juiste prioriteit aan een incident gegeven kan worden. Op deze manier kan een security incident meteen de bijbehorende en gepaste aandacht krijgen.

Tevens is het belangrijk om met enige regelmaat te controleren of geïmplementeerde beveiligingsmaatregelen nog steeds actief zijn, waarbij er actie ondernomen wordt als dit niet het geval is, gezien het risico op een security incident dan toeneemt. Deze werkwijze wordt Continuous Compliance genoemd en is vanuit wet- en regelgeving steeds vaker een eis.

Conclusie

De verschillende stappen om vanuit de Zero Trust strategie tot een tactisch model te komen en dit vervolgens te implementeren, vereisen allemaal verschillende hulpmiddelen, maar bovenal de juiste mensen/stakeholders.

Het is belangrijk dat alle vergaarde informatie op elkaar aansluit en dat er een duidelijk overzicht komt van wat we bezitten, wie waarvoor verantwoordelijk[3] is, welke risico's hiermee gepaard gaan en hoe we deze risico's willen verkleinen.

Na implementatie van verschillende security maatregelen is het van belang dat informatie die deze systemen genereren aansluit op hetgeen wat ze beschermen. Op deze manier kan de juiste prioriteit en opvolging aan (security) incidenten worden gegeven.

Met de juiste inrichting kan er tevens gerapporteerd worden hoe de omgeving of hoe een segment ervoor staat. Zijn er segmenten die meer risico's lopen dan verwacht en waar extra security maatregelen een uitkomst bieden? Of loont het om het segment op te splitsen in meerdere microsegmenten. Kortom, er ontstaat een mogelijkheid om niet alleen inzicht te hebben in de huidige (security) staat van de omgeving, maar ook om deze continue te verbeteren middels continuous improvement.

Om bovenstaande te kunnen realiseren is het van essentieel belang dat de juiste mensen/ specialisten met deze informatie aan de slag gaan om te verzekeren dat het juist geïnterpreteerd en geanalyseerd wordt.

Er kan gekozen worden om deze competentie zelf te borgen, door te investeren in de juiste mensen en kennis. Uiteraard kan deze taak ook uitbesteed worden aan een extern Security Operations Center (SOC).

ON2IT

ON2IT heeft ruimschoots ervaring met het helpen en inrichten van Zero Trust bij klantomgevingen en heeft dan ook verschillende producten en diensten om dit gehele proces te ondersteunen:

Readiness Assessment;

In welke mate is de organisatie klaar voor Zero Trust?

Fitness Assessment;

In welke mate zijn we in staat Zero Trust daadwerkelijk te implementeren?

Progress Monitor;

Hoe ver zijn we met het implementeren van Zero Trust en wat is de kwaliteit?

De ON2IT Portal is hierbij de spin in het web die alle informatie samenbrengt. De portal biedt de mogelijkheid om de CMDB (Zero Trust Risk Map) op te bouwen, maar ook te tonen wat de huidige status van de omgeving of een specifiek segment is. Dit zijn segmentstatussen, zoals: "Hoeveel incidenten/ tickets zijn er en hoe worden deze afgehandeld?" en "Wat is de status van mijn beveiligingsmaatregelen?"

Daarnaast rapporteert ON2IT actief welke maatregelen je kunt nemen om de beveiliging te verbeteren, oftewel de SIAs (security improvement advisories). Het portal toont de informatie die voor jou relevant is, ongeacht of je een beheerder bent die tickets wil oplossen of een CEO[4] die wil weten wat de algehele (security) status van de omgeving is.

[1] DAAS - Data, Assets, Applications en Services

[2] Het ON2IT Framework biedt hier richtlijnen voor over 8 'control' categorieën, ieder uitgediept met specifieke security maatregelen.

[3] Wie is er verantwoordelijk voor de asset, het risico en de controls ?

[4] After a data breach, can you empower your CEO in thirty minutes?