Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Bereid u voor op Zero Trust

Spring effectief in op Zero Trust bij vervangings- en uitbreidingsinvesteringen

Factsheet FS-2021-02 | versie 1.0 | 17 augustus 2021

Het gebruik van Zero Trust-principes wordt steeds populairder en de noodzaak van het gebruik ervan wordt alsmaar groter. Technologische ontwikkelingen hebben de traditionele kijk op security en het beveiligingsbeleid van veel organisaties ingehaald. Organisaties die Zero Trust omarmen zijn minder vatbaar voor externe aanvallen en dreigingen van binnenuit. Het NCSC adviseert u om een actieplan op te stellen om te zorgen dat u Zero Trust kunt toepassen bij toekomstige investeringen. Dit moet duidelijk maken welke maatregelen moeten worden getroffen om Zero Trust effectief te implementeren.

Achtergrond

Steeds meer organisaties kiezen ervoor om gebruik te maken van Zero Trust-principes bij het beveiligen van hun IT-infrastructuur. Zij zoeken een beveiligingsmodel dat zich effectief weet aan te passen aan de complexe moderne omgeving. In deze omgeving moeten apparaten en gegevens worden beschermd ongeacht de locatie waar zij zich bevinden of het type apparaat dat binnen organisaties wordt gebruikt.

Zero Trust biedt organisaties de mogelijkheid hun risico's te beperken in deze nieuwe situatie. Met behulp van de maatregelen die getroffen worden bij Zero Trust kunt u tekortkomingen in het traditionele beveiligingsmodel verhelpen. Hierdoor wordt bijvoorbeeld horizontale verplaatsing – het tussen systemen verplaatsen op zoek naar data om te exfiltreren – binnen het netwerk bemoeilijkt.

Verschillende organisaties behandelen Zero Trust op dit moment al op leidinggevend niveau. Zo nemen CIO's, CISO's en architecten de ontwerpprincipes vaak al mee in de toekomstige IT-ontwikkelingen van de organisatie.

Naast de organisatorische aandacht die Zero Trust krijgt, neemt ook de noodzaak voor het beveiligingsmodel toe. Dit komt door verschillende technologische veranderingen (plaats-, tijd- en apparaatonafhankelijk werken en adoptie van SaaS en andere cloudtechnologieën) en de grotere en frequentere dreigingen. Het landschap wordt steeds diverser: alles staat niet meer in één datacenter. Het aantal malware-aanvallen neemt toe, waarbij vooral een grote toename van ransomware wordt gesignaleerd. Verdere digitalisering binnen organisaties en nieuwe manieren van werken zorgen ervoor dat het aanvalsoppervlak toeneemt. Dit vereist een nieuwe blik op beveiliging.

De beveiligingsbehoeften en verwachtingen van gebruikers en klanten van organisaties nemen toe. Zij willen dat hun persoonsgegevens en gevoelige informatie nu en in de toekomst effectief worden beveiligd. Dat kunnen organisaties realiseren met Zero Trust.

Doelgroep

CISO's en securitymanagers

Aan deze factsheet hebben bijgedragen:

- DICTU
- KPN
- NBV
- Schuberg Philis

Wat is Zero Trust?[1]

Zero Trust is een beveiligingsmodel met een set ontwerpprincipes dat aanvallen en datalekken helpt te voorkomen. Hierbij wordt het concept van een vertrouwde netwerkpositie uit de architectuur verwijderd. Het is gebaseerd op de erkenning dat traditionele beveiligingsmodellen werken op de verouderde veronderstelling dat alles aan de binnenkant van het netwerk van een organisatie kan worden vertrouwd.

Geworteld in het principe van *never trust, always verify,* is Zero Trust ontworpen om moderne digitale omgevingen te beschermen. Het maakt gebruik van fijnmazige netwerksegmentatie en biedt dreigingspreventie op de randen van segmenten. Daarnaast vereenvoudigt Zero Trust gedetailleerde conditionele gebruikerstoegangscontrole.

Een architectuur is Zero Trust als hij voldoet aan de volgende set van ontwerpprincipes:[2]

- Identificeer de te beschermen onderdelen van de IT-infrastructuur en beveilig alle paden er naartoe.
- Verschaf alleen toegang tot informatie via beveiligde verbindingen, ongeacht de locatie.
- Handhaaf strikte toegangscontrole op een *need-to-know*-basis.
- Bepaal de toegangsrechten op basis van mate van vertrouwen die afgeleid wordt uit verschillende eigenschappen van de toegangsaanvraag: account, apparaat, IP-adres en locatie.
- Zorg voor uitgebreide monitoring en logging.

De traditionele kijk op security zit cloudadoptie in de weg. Cloudomgevingen staan immers per definitie buiten het on-premise netwerk van een organisatie. U kunt daardoor niet zonder meer hetzelfde netwerkbeheer daarop toepassen. Het toepassen van Zero Trust kan daarentegen innovatie stimuleren. Als het makkelijker is om veilig clouddiensten te gebruiken, verlaagt dit immers de drempel voor de adoptie van nieuwe toepassingen. Het toepassen van Zero Trust maakt de reis naar en toegang tot de cloud makkelijker.

Wat is er aan de hand?

Het traditionele beveiligingsmodel, ook wel het kasteel- of kokosnoot-model, heeft structurele zwakheden en is onhoudbaar geworden door moderne malware- en ransomware-aanvallen. Het model schiet tekort wanneer het aankomt op de veranderde technologie en dreigingen van binnenuit. In tegenstelling tot andere aspecten binnen de informatiebeveiliging, waarbij men uitgaat van een *defense-in-depth,* vertrouwen organisaties hier vooral op de perimeter – de grens met de buitenwereld. Een netwerk dat zo is ontworpen, biedt geen beveiligings- en controlemechanisme om horizontale bewegingen te stoppen zodra een aanvaller binnen is gedrongen. Dit komt doordat de binnenkant van het netwerk als een veilige en vertrouwde zone wordt beschouwd in dit model.

Het netwerk blijft kwetsbaar voor dit soort dreigingen totdat organisaties overstappen naar het zogenaamde granaatappel-model. Dit model kenmerkt zich door een grotere toepassing van netwerksegmentatie. Net als bij een granaatappel ontstaan er verschillende kleinere segmenten. De segmenten zijn gecombineerd met een strikt en conditioneel identiteits- en toegangsbeheer. Bij sommige

[1] Zie ook https://www.ncsc.nl/actueel/weblog/weblog/2020/what-about-zero-trust.

[2] Zie https://csrc.nist.gov/publications/detail/sp/800-207/final.

implementaties van Zero Trust brengen organisaties de beveiligingsschil zelfs terug naar het endpoint. Zij beschouwen hun netwerk in zijn geheel als onvertrouwd.

Het traditionele model wordt na verloop van tijd moeilijk te beheren. Dit komt door de grote hoeveelheid clientapparaten die zich buiten de organisatie bevinden en de vele koppelingen met netwerken van ketenpartners. Op deze manier vervaagt het onderscheid tussen binnen en buiten, waardoor het netwerk moelijk te beveiligen is. Het betreft ook vaak het beveiligen van verschillende onderling verbonden netwerken, waarin men niet per se zicht heeft op wat er gebeurt. In zo'n architectuur is er ook altijd meer dan één toegangspoort. Zo is er een in- en uitgang waarlangs de webservers worden bereikt en zijn er vaak meerdere VPN-verbindingen. De uitdaging wordt groter wanneer het over cloud gaat, aangezien er daar meestal meerdere application programming interfaces (API's) zijn. Het gaat hier niet om het aantal clientapparaten, maar om het grote aantal diensten die ervoor zorgen dat er veel toegangsmogelijkheden zijn. Een onveilige externe API biedt namelijk een opening voor ongeautoriseerde toegang door kwaadwillenden.

De behoefte om hardware zelf in beheer te hebben is steeds vaker economisch niet meer rendabel. Hierdoor wordt de on-premise-gedachte langzaam uitgefaseerd. Deze maakt plaats voor de transitie naar de cloud. Dit brengt kansen met zich mee: bij nieuwe investeringen in cloudadoptie kunnen organisaties meteen Zero Trust omarmen. Cloud biedt namelijk de kans om de implementatie van Zero Trust gemakkelijker te realiseren.

Veel organisaties weten niet waar ze moeten beginnen met het implementeren van Zero Trust. Zo gaan ze er vaak vanuit dat de toepassing ervan veel geld en tijd gaat kosten. Ze gaan er daarom niet mee aan de slag. Wanneer de mogelijkheid zich voordoet om op een voordelige manier Zero Trust toe te passen in de IT-infrastructuur van de organisatie, is het handig om een plan klaar te hebben liggen om er ook daadwerkelijk mee aan de slag te gaan. Een transitie naar de cloud is bijvoorbeeld een uitgelezen moment om te beginnen met de implementatie van Zero Trust. Op dit moment rekenen organisaties vooral nog op hun IT-leveranciers om hen te wijzen op goedkope en efficiënte manieren om Zero Trust te implementeren.

Wat kan er gebeuren?

Indien u er voor kiest Zero Trust te implementeren, dan vergroot u de weerbaarheid van uw organisatie tegen aanvallen en dreigingen van binnenuit en is de beveiliging van uw IT-infrastructuur meer toekomstvast. Op het moment dat een aanvaller toegang heeft gekregen tot uw netwerk, dan kan hij zich normaal gesproken makkelijk verplaatsen tussen uw systemen. In de praktijk betekent dit dat hij toegang heeft tot een groot deel van uw netwerk en informatie. Daarnaast heeft u ook mogelijk te maken met het insider-risico. Hierbij veroorzaakt een van uw eigen medewerkers onbewust of kwaadwillend een datalek of aanvallers geeft toegang tot uw netwerk.

Wanneer aanvallers toegang hebben tot uw netwerk kunnen zij malware installeren. Deze kunnen zij gebruiken als een achterdeur in uw netwerk om gevoelige informatie te exfiltreren. Ook kunnen aanvallers hun privileges gebruiken om toegang te krijgen tot verschillende informatiesystemen binnnen uw netwerk.

Als uw organisatie een plan heeft om aan de slag te gaan met Zero Trust, kunt u effectief inspringen wanneer kansen zich voordoen. Het hebben van een plan geeft ook meer zekerheid rond een brede implementatie en zorgt ervoor dat u Zero Trust op een professionele manier kunt toepassen. U kunt Zero Trust namelijk efficiënter implementeren door dit te doen tijdens een vervangings- of uitbreidingsinvestering. Wanneer u op een

ander moment besluit om Zero Trust alsnog te implementeren, dan leidt dit tot hogere kosten. Daarnaast kan het lang duren voordat zich een volgende kans voordoet. Tot die tijd is de beveiliging van uw netwerk minder effectief en is de potentiële impact van een incident groter.

Wanneer u een nieuw beveiligingsmodel omarmt, bent u in staat om de IT-infrastructuur van uw organisatie efficiënt te beveiligen terwijl andere organisaties dit voordeel mogelijk nog niet hebben hebben. Hierdoor ontstaat de kans dat zij eerder slachtoffer kunnen worden van een aanval, aangezien zij achterlopen op de trend.

Wat adviseert het NCSC?

Het NCSC adviseert u om een actieplan op te stellen om te zorgen dat u Zero Trust kunt toepassen bij toekomstige vervangings- of uitbreidingsinvesteringen. Het actieplan maakt duidelijk in welke tijdspanne veranderingen mogelijk zijn en hoeveel werk ervoor nodig is.

Als u Zero Trust goed implementeert, dan leidt dit tot een minimale blootstelling aan aanvallen, een hogere continuïteit van kritieke processen, een verhoogde en kosteneffectievere compliance en een toekomstvaste architectuur.

Wanneer u een transitie naar een cloudomgeving op de planning heeft staan, is het verstandig om Zero Trust daar meteen in mee te nemen. Het kost namelijk extra tijd en geld om Zero Trust daar achteraf in te bouwen, omdat uw organisatie de infrastructuur die net is gebouwd dan moet aanpassen.

Neem bij het opstellen van het actieplan de volgende gedachten mee:

- Baseer het actieplan op de strategische doelen van uw organisatie en de uitkomsten van een risicoanalyse.
- Definieer een visie en missie waarin de doelen, resultaten en architectuur duidelijk zijn vormgegeven.
- Gebruik het actieplan om de leiding van uw organisatie mee te krijgen door u te richten op de doelen en resultaten die uw organisatie voor ogen heeft. Op deze manier krijgt u ondersteuning voor uw eigen doelen, budgettoewijzingen en interne afstemming.
- Stel eindgebruikers in staat om mee te denken over de implementatie van Zero Trust. Zo kunt u uw beveiliging inrichten op een manier die niet nadelig is voor hun gebruikerservaring en productiviteit. Als de maatregelen die Zero Trust toevoegt eindgebruikers hinderen, dan zoeken zij er een weg omheen en kunt u de voordelen van Zero Trust niet realiseren.
- Zoek indien nodig de samenwerking op met ICT- en securityleveranciers die bewezen expertise hebben in cloudgebaseerde beveiliging.

Wanneer u Zero Trust wilt implementeren, begin dan klein en richt u op haalbare doelen. Begin niet meteen met uw belangrijkste assets (‘kroonjuwelen’). Hierdoor wordt de impact van de transitie op uw organisatie duidelijk. Zo kunt u nagaan of Zero Trust geschikt is om verder uit te rollen.

Houd in uw ontwerp en investeringen rekening met het concept van *people-centred security.*[3] Hiermee voorkomt u dat gebruikers op zoek gaan naar een manier om de beveiliging te omzeilen en het daarmee nutteloos te maken. Een Zero Trust-omgeving kan onnodige

[3] Zie ook https://www.ncsc.gov.uk/collection/10-steps/engagement-and-training.

hindernissen en ongemak voor gebruikers met zich meebrengen. Het is belangrijk u een balans vindt tussen continue bescherming tegen dreigingen en het gemak en de productiviteit van de gebruikers.

Om Zero Trust effectief te implementeren zijn investeringen nodig:

Netwerksegmentatie

Bouw niet alles in één netwerk, maar investeer in een uitgebreide en losstaande omgevingen met ieder een eigen perimeter. Houd uw netwerksegmenten zo klein mogelijk. In grotere segmenten is er minder controle mogelijk. Vind een balans tussen zo klein mogelijke functionele segmenten en een werkbare controle op de toegang van die segmenten.

Authenticatie en autorisatie

Zorg voor een sterke controle van identiteit[4] door multifactorauthenticatie, voorwaardelijke toegang en detectie van sessierisico's op te nemen als de ruggengraat van uw toegangsstrategie. Autorisatie dient plaatst te vinden op de verschillende applicaties binnen uw netwerk en op basis van het *principle of least privilege*. Dit betekent dat de gebruiker alleen toegang krijgt tot tools, data en segmenten die daadwerkelijk nodig zijn voor het werk dat diegene doet. Gebruikers koppelen aan vooropgestelde rollen en groepen, helpt om dit inzichtelijk te maken. Met behulp van een centrale identiteitsprovider die open standaarden (bijvoorbeeld SAML) ondersteunt, kunt u het risico op identiteitsfraude beperken.

Toegangs- en beveiligingsbeleid

Definieer acceptabel toegangsbeleid voor uw segmenten en informatie. Handhaaf dit met een beveiligingsbeleid dat zowel inzicht als handelingsperspectief biedt in afwijkingen.

Monitoring en automatisering

Zorg dat uw SOC/SIEM-medewerkers op de hoogte zijn van de netwerksegmentering die is toegepast vanuit Zero Trust. Op deze manier maken zij gebruik van alle informatie die uw Zero Trust-omgeving oplevert. Het beoordelingsproces van mogelijke incidenten is afhankelijk van verschillende gegevensbronnen die weer betrekking hebben op verschillende segmenten in het netwerk. Bij Zero Trust ligt de nadruk op het monitoren van de segmenten en de individuele apparaten binnen uw netwerk. Automatiseer de monitoring van deze informatiestromen om de belangrijkste hits als eerst naar boven te krijgen. Hierdoor blijven de SOC-medewerkers op de hoogte van wat er speelt en kunt zij misbruik sneller detecteren en duiden om zo dreigingen het hoofd bieden.

Handelingsperspectief

1. Voer een risicoanalyse uit en stel op basis van de uitkomsten van uw analyse en de strategische doelen van uw organisatie een business case voor Zero Trust op.[5]
2. Ga met de betrokken partijen om de tafel zitten. Stel samen vast waar in uw netwerk u wilt beginnen met het implementeren van Zero Trust en aan welke eisen het moet voldoen. Zorg hierbij voor steun vanuit de leiding van uw organisatie. Informeer de leiding van de gevolgen als ze Zero Trust niet implementeren. Mogelijke partijen die u kunnen helpen bij het afstemmen van uw actieplan zijn IT-staf, de Chief Information Officer (CIO), de Functionaris gegevensbescherming (FG) en eindgebruikers. Betrek indien van toepassing ook uw ICT- en securityleveranciers. Welke partijen er aan

[4] Zie ook https://www.ncsc.nl/onderwerpen/authenticatie.

[5] Zie https://www.ncsc.nl/documenten/publicaties/2020/juli/21/factsheet-risicobeheersing.

tafel moeten zitten, verschilt per organisatie.
3. Stel, per te vervangen of uit te breiden onderdeel van uw netwerk, een plan van aanpak op met bijbehorende tijdlijn. Achterhaal wanneer het volgende moment is dat een investering gaat plaatsvinden. Stel vast wat nodig is om de veranderingen die in het vorige hoofdstuk beschreven zijn te realiseren. Stel vast hoe lang de leverancier nodig heeft om de nieuwe voorzieningen aan te leveren en te implementeren.
4. Begin met implementatie op kleine schaal. Gebruik hiervoor het stappenplan voor de implementatie van Zero Trust hieronder.
5. Monitor en evalueer de implementatie en gebruik de uitkomsten hiervan om verbeteringen te realiseren. Stel op basis van de uitkomsten vast of Zero Trust geschikt is om stapsgewijs in de hele organisatie uit te rollen. Stel vast of er verbeteringen te maken zijn bij het implementeren van Zero Trust op het volgende onderdeel van uw netwerk.

Hoe begin ik met de technische implementatie van Zero Trust?[6]

1. Bepaal met welk onderdeel van uw infrastructuur u wilt beginnen en definieer daarvoor het te beschermen segment. Identificeer daarbij welke kritieke Data, Assests, Applicaties en/of Services (DAAS) u in het te beschermen compartiment wil plaatsen.
2. Breng de transactiestromen in kaart op basis van de interacties van de in stap 1 geïdentificeerde DAAS-elementen. Op deze manier kunt u de onderlinge afhankelijkheden tussen gevoelige gegevens, applicaties (bijvoorbeeld web-, applicatie-, en databaseservers), netwerkservices en gebruikers achterhalen en leren begrijpen.
3. Ontwerp eerst op papier een Zero Trust-omgeving waarin u netwerksegmentatie toepast, specifieke toegang tot gevoelige gegevens mogelijk maakt en beleidshandhaving voor de verschillende segmenten biedt om dreigingen te voorkomen. Bouw daarna een proof-of-concept.
4. Ontwikkel het toegangsbeleid voor uw Zero Trust-omgeving vanuit de "Kipling-vragen": wie, wat, wanneer, waar, waarom en hoe moet er al dan niet toegang verleend worden?
5. Bewaak en onderhoud het geheel door het analyseren van de informatiestromen van uw netwerk, systemen, applicaties en de cloud. Zorg dat verzamelde loggegevens en informatiestromen samen komen in uw SIEM. Dit betreft gebruikersgedrag, Identity and Access Management (IAM) logs, netwerkgedrag en informatie over externe dreigingen. Op deze manier stelt u uw beveiligingsteam/SOC in staat om onderscheid te maken tussen normaal en abnormaal gedrag. Op basis van de uitkomst kunt u de classificatie van uw informatie aanpassen.

[6] Zie https://www.paloaltonetworks.com/resources/guides/zero-trust-maturity-model.

Uitgave
Nationaal Cyber Security Centrum (NCSC)
Postbus 117, 2501 CC Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5555

Meer informatie
https://www.ncsc.nl
info@ncsc.nl
@ncsc_nl

augustus 2021