CSO

Microsoft Security

GESPONSORDE CONTENT

Zero Trust Security: **de lessen van early adopters**

CSO Microsoft Security

Inhoud

- Inleiding
- Zero Trust is een realiteit en levert echte meerwaarde
- Factoren die Zero Trust-implementatie bevorderen
- Bedreigingen te over
- Obstakels voor de acceptatie van Zero Trust
- Uitdagingen bij de implementatie
- Best practices voor implementatie van Zero Trust
- Waar bevind jij je op het traject naar Zero Trust?

CSO Microsoft Security

Inleiding

Door de verstoring van de afgelopen twee jaar zijn traditionele IT- en securitymodellen op de schop gegaan. Als gevolg hiervan heeft Zero Trust Security zich razendsnel ontwikkeld van een interessant concept tot de fundamentele basis van moderne security binnen de onderneming.

Uit nieuw onderzoek van Foundry blijkt dat 52% van de organisaties de Zero Trust-architectuur uittesten of deze hebben geïmplementeerd, terwijl nog eens 15% onderzoek doet naar Zero Trust-modellen. Deze pionierende gebruikers melden talloze voordelen van hun implementatie, zoals verbeterde bescherming van klantdata, minder complexiteit en het vermogen om veilige en betrouwbare toegang te leveren tot bedrijfsmiddelen.

In dit eBook verkennen we het resultaat van het onderzoek dat door Foundry is verricht. Dit onderstreept het belang van een Zero Trust-strategie waarmee CISO's hun organisatie kunnen beschermen tegen talloze risico's die afkomstig zijn van een scala aan aanvalsvectoren. We bieden ook advies over de manier waarop je Zero Trust kunt implementeren, voor bedrijven die nog aan het begin van het traject staan.

Over de enquête

Foundry heeft in februari en maart 2022 een enquête uitgevoerd onder Amerikaanse bedrijven om de huidige staat van Zero Trust-implementatie te achterhalen. Respondenten moesten minimaal IT-manager zijn of een hogere functie bekleden in een bedrijf met meer dan 500 medewerkers en een rol vervullen bij de aankoop van cybersecurityproducten en -services.

In totaal waren er 250 respondenten voor deze enquête met 23 vragen.

CSO Microsoft Security

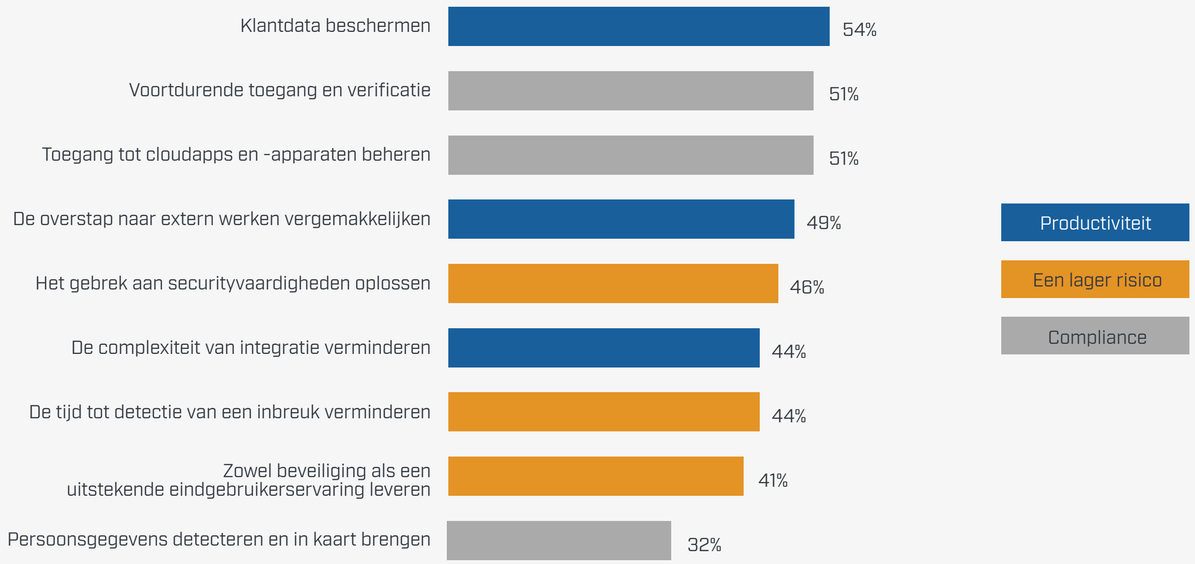
Zero Trust is een realiteit en levert echte meerwaarde

Uit de resultaten van deze enquête en de diepgaande interviews met leidinggevenden op IT- en securitygebied blijkt duidelijk dat Zero Trust voor de meeste organisaties een prioriteit vormt. En de bedrijven die verschillende onderdelen van Zero Trust hebben geïmplementeerd, plukken daarvan al de voordelen.

De meeste respondenten die Zero Trust hebben geïmplementeerd (87%) zijn van mening dat de architectuur aan de oorspronkelijke verwachtingen voldoet voor wat betreft implementatie, acceptatie en integratie, of deze overtreft.

'[Zero Trust] is voor ons de standaardprocedure geworden. Ik zie echt niet hoe we ooit terug zouden kunnen gaan naar de oude situatie', aldus een IT-directeur voor een wereldwijde retailer. (Respondenten mochten hun anonimiteit bewaren mits ze vrijuit spraken over hun beveiligingsplannen.)

Ervaren voordelen sinds de implementatie van Zero Trust



12% van de respondenten verklaarde *al* deze voordelen te behalen

Bron: Enquête naar de invoering van Zero Trust, maart 2022, Foundry. Steekproefgrootte: 250

CSO Microsoft Security

Ongeveer 44% van de respondenten meldde tevens dat Zero Trust de complexiteit heeft verminderd van het implementeren van een geïntegreerde beveiligingsarchitectuur. 'Omdat we te maken hebben en werken met een framework, maakt dat de zaken duidelijk eenvoudiger', zegt de CISO voor een callcenterbedrijf met 3500 werknemers.

Een VP en CISO van een bedrijf in de financiële dienstverlening met 17.000 werknemers verklaart dat de meervoudige verificatie die door zijn bedrijf is geïmplementeerd als onderdeel van Zero Trust een groot succes is onder medewerkers. 'Het heeft de tevredenheid onder medewerkers duidelijk verhoogd, en omdat ze nu niet hun door het bedrijf verstrekte machine en een VPN-client hoeven te gebruiken, hebben ze vanaf elke locatie toegang tot resources', zegt hij.

Het concept van toegang met de minst mogelijke bevoegdheden heeft ook zijn vruchten afgeworpen, merkt de CISO op. 'Er zijn minder rampzalige fouten gemaakt door systeembeheerders dankzij de implementatie van het toegangssysteem op basis van bevoegdheden', zegt hij. 'Er worden bevoegdheden verleend voor heel specifieke zaken binnen een specifieke periode, wat betekent dat de kans op een fout kleiner is.'

Gezien de toename in phishing en andere cyberaanvallen, somt de IT-directeur van een retailbedrijf de voordelen van Zero Trust als volgt op: 'Als we niet over dit type tools konden beschikken, zouden we hoogstwaarschijnlijk in de val zijn gelokt en zouden we momenteel waarschijnlijk losgeld in bitcoins betalen.'

CSO Microsoft Security

Factoren die Zero Trust-implementatie bevorderen

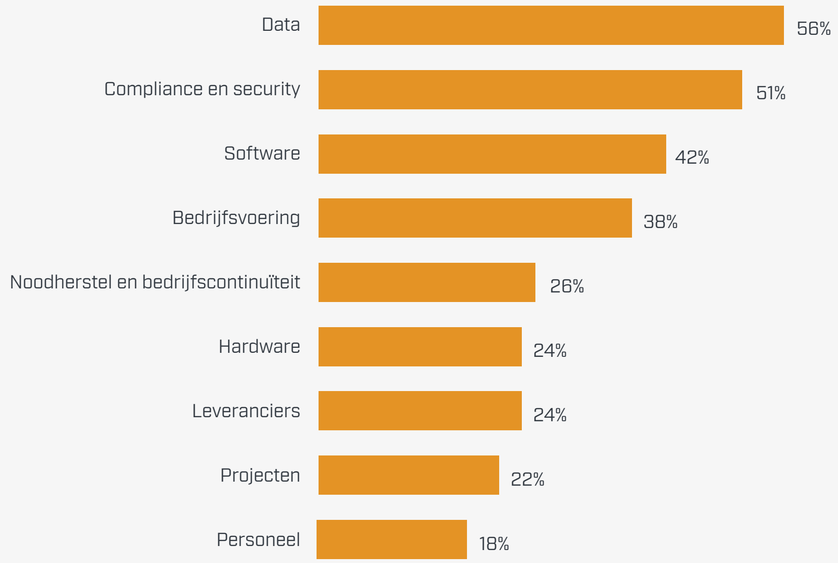
Een samenkomst van omstandigheden leidt ertoe dat bedrijven een Zero Trust-architectuur op zijn minst overwegen. Boven aan de lijst staat de behoefte om de risico's te beheersen voor de vele bestaande resources tegen talloze bedreigingen. Respondenten voor de enquête weten een jaar aan beveiligingsincidenten aan een aantal oorzaken, waarvan zwakke plekken in de beveiliging als gevolg van externe personen of organisaties de belangrijkste was. Overige genoemde oorzaken waren:

- Onverwachte bedrijfsrisico's
- Onjuist geconfigureerde services of systemen
- Kwaadwillende, bewuste aanvallen door insiders
- Fouten van niet-kwaadwillende gebruikers, onder wie slachtoffers van phishing
- Gecompromitteerde identiteiten
- Niet-gepatchte software
- Gestolen referenties

Deze incidenten veroorzaken een aantal risico's, met als voornaamste inbreuk op data.

Voor veel organisaties heeft de plotselinge overstap op extern werken als gevolg van de pandemie geleid tot versnelde invoeringsplannen voor Zero Trust, omdat de traditionele securitymodellen op basis van een netwerkperimeter in één klap verouderd waren. Veel organisaties waren trouwens al die richting ingeslagen met het verplaatsen van meer applicaties en IT-infrastructuur naar de cloud, maar de pandemie zorgde gewoon voor een extra impuls.

De belangrijkste risicocategorieën voor cybersecuritybedreigingen



Bron: Enquête naar de invoering van Zero Trust, maart 2022, Foundry. Steekproefgrootte: 250

CSO Microsoft Security

De CISO voor een bedrijf in medische technologie met 1700 werknemers zegt bijvoorbeeld dat de cloud en de pandemie de invoering van Zero Trust hebben bevorderd, waarmee het bedrijf nu beschikt over een stevig fundament voor welk werkplekmodel het ook kiest.

'De zakelijke factoren die dit bevorderden waren dat we als bedrijf in de cloud werkten en we onze omgeving moesten beveiligen', zegt hij. 'We moesten tevens zorgen dat er tijdens de pandemie bekwaam personeel klaarstond. Dankzij [Zero Trust] konden we onze voetafdruk aan onroerend goed sterk verkleinen, en we zullen voor ten minste 60% een virtueel extern bedrijf blijven.'

CSO Microsoft Security

Bedreigingen te over

De noodzaak van compliance heeft de overstap op een robuuster securitymodel bevorderd. 'Toezichthoudende instanties houden ons in de gaten en verwachten dat we ons securityframework verbeteren', verklaart de SVP van wereldwijde informatiebeveiliging voor een bedrijf in de financiële dienstverlening met 290.000 medewerkers.

Bepaalde organisaties hebben proactieve stappen ondernomen voor de invoering van Zero Trust. Daarmee willen ze met veel publiciteit omgeven inbreuken voorkomen, zodat ze niet om de verkeerde reden in het nieuws komen. 'Het was belangrijk om proactief te handelen en vooral geen nieuwsitem te worden', zegt de CIO bij een hoger onderwijsinstelling met 3500 medewerkers. 'Je leest echt horrorverhalen over andere lokale onderwijsinstellingen die ongeveer even groot zijn als wij en die heel lang uit de lucht waren.'

Andere organisaties hebben al te kampen gehad met een ernstig cybersecurityincident, waardoor ze snel een nieuwe securitystrategie moesten ontwikkelen. Nadat een verzekeringsmaatschappij met 6000 medewerkers een ransomware-aanval kreeg te verduren die het bedrijfsnetwerk twee weken lang platlegde, was het mandaat om Zero Trust in te voeren direct van de CEO afkomstig. 'We hebben de implementatie met turbosnelheid doorgevoerd', zegt de VP IT-ontwikkeling van het bedrijf. 'In het begin ging het alleen om best practices, maar na de ransomware-aanval hebben we de boel echt heel erg versneld.'

Gestimuleerd door de cloud

De VP en CISO van een grote financiële dienstverlener zegt dat zijn team de behoefte aan een nieuwe securityarchitectuur een paar jaar geleden onderkende, vanwege de invoering van een groter aantal cloudresources en gebruikers die steeds mobieler waren.

'We beseften dat de traditionele securityarchitectuur van een kasteel met een slotgracht waarop we in het verleden vertrouwden, ons niet langer kon beschermen tegen aanvallers', zegt hij.

Die realiteit werd overduidelijk aan het begin van 2020, toen het bedrijf ontdekte dat er ergens in het jaar daarvoor inbreuk was gemaakt op het perimeternetwerk en een aanvaller lateraal binnen de omgeving kon bewegen zonder te worden opgemerkt. 'We hadden een nieuwe architectuur nodig waarbij we het gebruik van de resources moesten beschermen en verifiëren, waar die zich ook bevonden, en Zero Trust is een architectuur die daarvoor is ontworpen.'

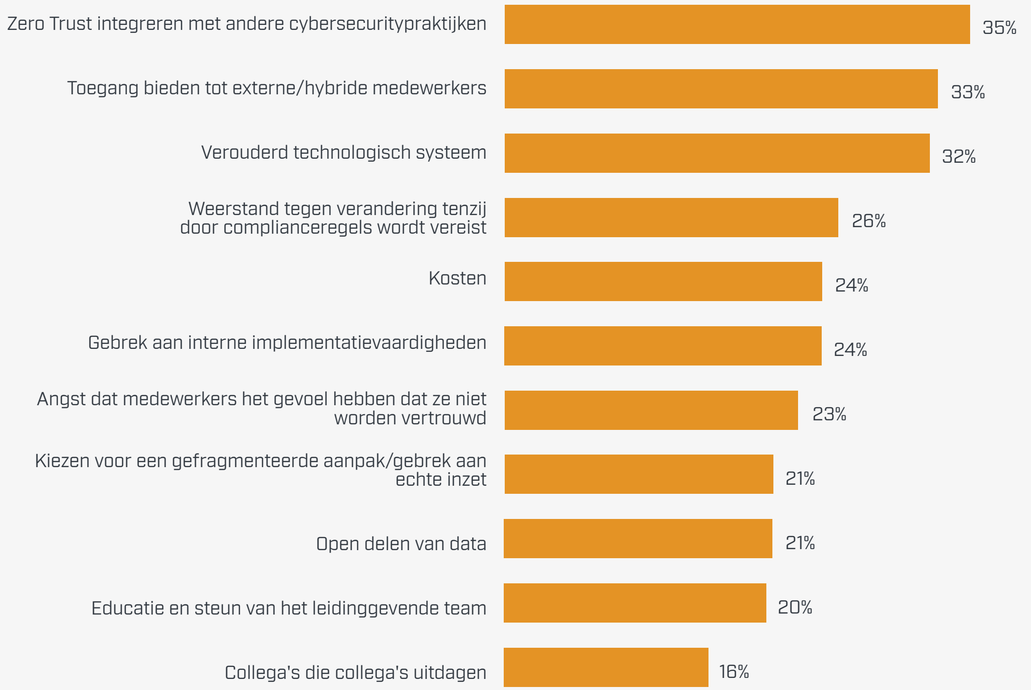
CSO Microsoft Security

Obstakels voor de acceptatie van Zero Trust

Voor veel organisaties betekent Zero Trust een radicale verschuiving van de structuur, de processen en houding in verband met security, en dat verklaart dat er heel wat horden moeten worden genomen voordat het kan worden ingevoerd.

'Er waren zoveel silo's die we binnen de organisatie tegenkwamen', merkt de CISO van een callcenter op, die uitlegt dat de teams voor servers, het netwerk en de databases elk hun eigen reeks webservers en -tools hadden. 'Dat hield ons sterk tegen, omdat iedereen anders dacht over de doelstellingen en aanpak.'

Wat houdt de invoering van Zero Trust tegen?



Bron: Enquête naar de invoering van Zero Trust, maart 2022, Foundry. Steekproefgrootte: 250

CSO Microsoft Security

Dat soort problemen aan het licht brengen kan eigenlijk een heel positieve bijwerking van Zero Trust zijn, aldus Anthony Mocny, Senior Product Marketing Manager voor Zero Trust bij Microsoft. 'Als architectuur is Zero Trust bedoeld om silo's met securityteams die binnen technologische zuilen bestaan, af te breken, zodat de teams als één geheel kunnen samenwerken', zegt hij. 'Dat kan betekenen dat ook de cultuur moet veranderen, voor wat betreft de manier waarop teams samenwerken.'

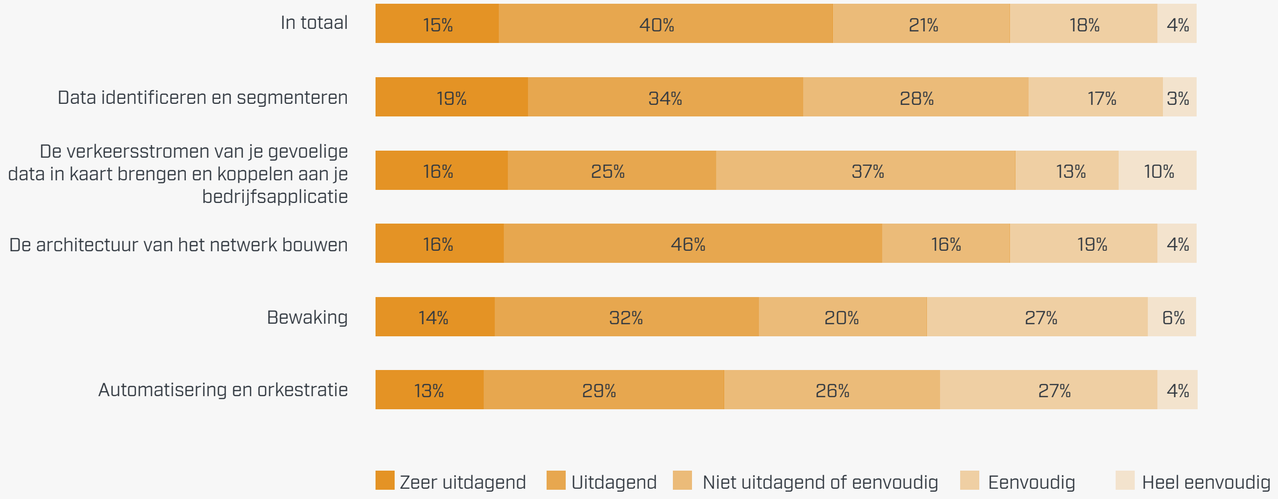
Voor de VP/CISO in de financiële dienstverlening vormden verouderde applicaties een obstakel in het traject naar Zero Trust. 'Ze moeten worden bijgewerkt met moderne verificatietechnologie', legt hij uit. 'Dat is, afhankelijk van hun leeftijd, niet altijd even gemakkelijk.'

CSO Microsoft Security

Uitdagingen bij de implementatie

Als bedrijven het traject naar Zero Trust eenmaal beginnen, kan een scala aan implementatieproblemen de kop opsteken. Meer dan de helft van de respondenten voor deze enquête (56%) gaf toe dat implementatie van Zero Trust een uitdaging of een zeer grote uitdaging vormde. Met name:

Hoe lastig is een Zero Trust-implementatie?



Bron: Enquête naar de invoering van Zero Trust, maart 2022, Foundry. Steekproefgrootte: 168

CSO Microsoft Security

Uitdagingen in verband met segmentatie en microsegmentatie werden vaak genoemd in de diepgaande interviews.

'Je segmenteert je netwerk tot aan de afzonderlijke hosts aan toe, aldus de VP/CISO in de financiële dienstverlening. 'Het is alsof je een kleine firewall tussen elke host op het interne netwerk plaatst, zodat je al het verkeer kunt zien en tot op individuele machines kunt beheren. Dat heeft enorme securityvoordelen, maar is heel erg moeilijk te implementeren omdat je feitelijk tienduizenden firewalls moet beheren.'

Het in kaart brengen van verkeersstromen is ook een proces dat maanden in beslag kan nemen. De CTO van een uitgevers- en mediabedrijf met 5000 medewerkers zegt dat, na het definiëren van kritieke data-, applicatie- en netwerkservices die ze moesten beschermen, 'we transactiestromen op het netwerk in kaart brachten in een poging om er inzicht in te krijgen als groepen informatie.'

'[Vervolgens] segmenteerden we delen van die informatie en hoe die het netwerk doorkruist, tot op afzonderlijke informatiepackages aan toe.' Op dat punt paste het bedrijf Zero Trust-beleid toe op elke type verkeersstroom. 'We hebben ook nieuwe mogelijkheden geïmplementeerd voor het bewaken en onderhouden van ons netwerk.'

Ondanks deze uitdagingen zijn veel respondenten ervan overtuigd dat Zero Trust de dagelijkse activiteiten uiteindelijk eenvoudiger maakt. Met traditionele technologie 'duurt het dagen om wijzigingen aan te brengen; je moet ze namelijk op alle hardware- en softwareonderdelen implementeren en daarvoor gebruiken we heel veel resources', zegt de SVP voor wereldwijde informatiebeveiliging in de financiële dienstverlening. 'Als we naar Zero Trust kijken, zie je dat de complexiteit van de architectuur uiteindelijk minimaal is, en we veel minder medewerkers nodig hebben om hetzelfde type werk uit te voeren.'

CSO Microsoft Security

Best practices voor implementatie van Zero Trust

Naarmate steeds meer bedrijven een Zero Trust-architectuur implementeren, ontwikkelen ze tevens roadmaps en best practices die anderen kunnen volgen. We bieden je vijf overwegingen voor het plannen van een implementatie.

Begin niet te ambitieus

Een Zero Trust-strategie opstellen kan een grote opgave lijken als je deze alleen bekijkt binnen de bredere context van het aanpassen van je beleid en de beschermingsmaatregelen op je netwerk, voor je data, applicaties, identiteiten, endpoints en infrastructuur. 'In het begin leek de taak gewoon te overweldigend en we vroegen ons echt af of we dit wel konden doen', aldus de CIO in het hoger onderwijs. 'Maar je moet het met één stap tegelijk doen.'

De CIO en het team kozen uiteindelijk voor een aanpak waarbij ze het 'geldspoor volgden'. Ze verleenden prioriteit aan segmentatie van de applicaties voor financiën en de loonadministratie op een afzonderlijk netwerk.

De meest kritieke assets die je moet beschermen aanduiden, is een goede aanpak volgens Mocny. 'Houd altijd de reden waarom je Zero Trust überhaupt implementeert in de gaten', zegt hij.

Begin bij twijfel met meervoudige verificatie

Bij het verlenen van een prioriteit aan de securitystack raden veel CISO's en securityleveranciers een eerste focus op verificatie en andere op identiteiten gebaseerde beveiligingsmaatregelen aan. 'Als je nog geen uitgangspunt hebt gekozen, is meervoudige verificatie een heel goede keuze', zegt Mocny. Microsoft schat dat meervoudige verificatie meer dan 90% van op identiteit gebaseerde aanvallen kan voorkomen.

De VP in de financiële dienstverlening is het daarmee eens. 'Verificatie is een fundamenteel onderdeel van de implementatie van een Zero Trust-architectuur. De andere onderdelen werken gewoonweg niet als we de identiteit van de eindgebruiker niet kunnen verifiëren, en dus zijn we daar begonnen.'

Als volgende ging de VP/CISO in de financiële dienstverlening het netwerkonderdeel te lijf. Dat leverde direct voordeel op bij het ondersteunen van externe werknemers. Het team stelde microsegmentatie uit tot later tijdens het traject, omdat dit niet direct zo zichtbaar is voor het bedrijf als geheel. 'Wanneer je daarmee klaar bent, ben je echt heel wat veiliger, maar niemand weet wat precies het verschil is', zegt hij.

CSO Microsoft Security

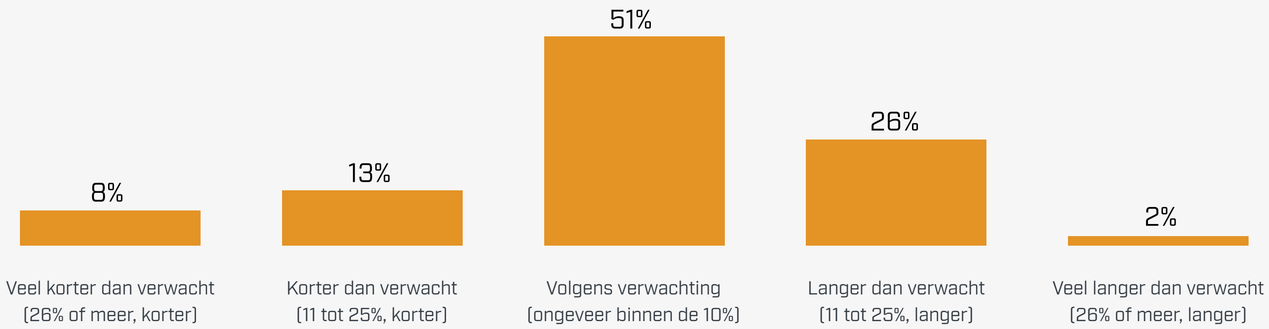
Wees realistisch over je tijdlijnen

Het is belangrijk dat CISO's realistische verwachtingen wekken over de implementatie van Zero Trust. 'Implementatie van een Zero Trust-architectuur is een programma en geen project', zegt de VP/CISO in de financiële dienstverlening. 'Dit vormde een enorme verandering. Als je het op de juiste manier wilt aanpakken, moet je dat via talloze projecten doen. Die waarschijnlijk jaren in beslag zullen nemen. Een snelle en eenvoudige implementatie van een Zero Trust-architectuur bestaat gewoonweg niet.'

Zijn collega-SVP is het hiermee eens. 'Ik betwijfel of we het proces ooit volledig zullen afronden, omdat er altijd weer nieuwe technologie wordt uitgebracht, nieuwe malware wordt gelanceerd en altijd nieuwe bedreigingen de kop opsteken', zegt hij.

De meerderheid van de respondenten voor deze enquête (72%) verklaart dat ze hun tijdlijn voor implementatie konden halen of hierop zelfs wat voor lagen, terwijl de rest verklaarde dat de implementatie langer duurde dan ze hadden verwacht.

Voldoet Zero Trust aan je doestellingen voor je tijdlijn?



Bron: Enquête naar de invoering van Zero Trust, maart 2022, Foundry. Steekproefgrootte: 168

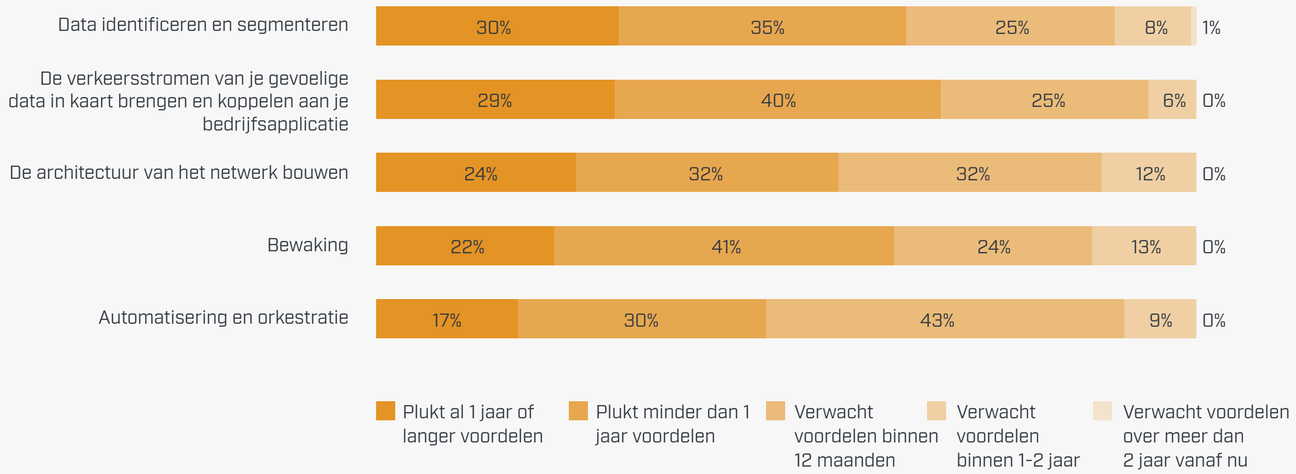
CSO Microsoft Security

Meet je resultaten regelmatig

Terwijl CISO's een Zero Trust-implementatie uitvoeren, moeten ze mijlpalen opstellen die moeten worden gehaald, om de voortgang te kunnen meten. Het is een goed teken dat ongeveer twee derde van de respondenten voor de enquête verklaarde binnen een jaar voordeel te hebben behaald uit de meeste aspecten van hun project, terwijl ongeveer een kwart of meer verwacht dat binnen 12 maanden te kunnen doen. Daarbij gaat het om belangrijke activiteiten zoals het aanduiden en segmenteren van data, het in kaart brengen van verkeersstromen en het architectuurontwerp van het netwerk.

'Zero Trust is een traject vanwege de voortdurende evaluatie die je moet uitvoeren om je te beschermen tegen de steeds veranderende aard van aanvallen', zegt Mocny. 'Je moet altijd alert blijven op verbeteringen.'

Tijdlijn voor het behalen van de voordelen van Zero Trust



Bron: Enquête naar de invoering van Zero Trust, maart 2022, Foundry. Steekproefgrootte: 103

CSO Microsoft Security

Focus op mensen en niet alleen op technologie

Het brede bereik van een Zero Trust Security-model is van invloed op elke medewerker, waaronder ook de IT- en securityteams die dit moeten implementeren. Daarom is het, net als voor elk ander groot technologisch project, zo belangrijk om te zorgen dat implementaties synchroon verlopen met nieuwe processen en verandermanagementpraktijken, zodat implementatie soepel en succesvol is.

'Naast de veranderingen op technologisch gebied, vindt er een verandering in de cultuur plaats', aldus Mocny. 'Als je meerdere teams hebt die aan security werken, waaronder netwerkarchitecten of identiteitsexperts, moet je ook de manier veranderen waarop die teams samenwerken. Je moet silo's afbreken en zorgen dat alle technologie als één geheel samenwerkt.'

Voor het afbreken van silo's moeten de teams voor al deze functies nauw worden betrokken bij pilot- en proof of concept-projecten (POC). Een directeur voor IT-systemen bij een telecommunicatiebedrijf met ongeveer 2000 werknemers heeft deze les geleerd nadat verschillende afzonderlijke foutpunten ontstonden tijdens de implementatie, waaronder voor services die niet konden worden geverifieerd en opeens 'niet-vertrouwd' waren. Hierdoor waren deze services, en bepaalde systemen, niet langer beschikbaar.

'Het implementeren van die ene service kan een domino-effect veroorzaken en ertoe leiden dat andere services niet langer beschikbaar zijn. In de toekomst 'zullen we veel voorzichtiger te werk gaan: meer tijd voor de POC's, meer beoordelingen en meer evaluaties van de architectuur met deskundigen voordat we implementeren.'

ROI van Zero Trust

Een in 2021 in opdracht uitgevoerd **Forrester Consulting Total Economic Impact™-onderzoek** kwantificeert de kostenbesparingen en zakelijke voordelen van Microsoft Zero Trust-oplossingen. Op basis van de vijf ondernemingen waar Forrester navraag deed, behaalde een samengestelde organisatie in drie jaar een rendement op de investering van 92% dankzij de implementatie van een Zero Trust-architectuur met Microsoft.

Deze samengestelde organisatie bespaarde tevens gemiddeld 20 USD per medewerker per maand doordat bepaalde securitytools overbodig waren geworden dankzij Zero Trust, waaronder endpoint management, antivirus en antimalware-oplossingen.

CSO Microsoft Security

Waar bevind jij je op het traject naar Zero Trust?

Zoals door de enquête wordt aangetoond, wegen de voordelen van een Zero Trust Security-model duidelijk zwaarder dan bepaalde implementatieproblemen waarmee CISO's en hun securityteams kampen. Door deze uitdagingen aan te gaan met een goed uitgedacht plan kunnen organisaties hun beveiliging snel verbeteren, risico's verminderen en het bedrijf als geheel meerwaarde bieden.

Voer de **evaluatie van de volwassenheid van het Zero Trust-model** van Microsoft uit om te beoordelen wat de volwassenheid van Zero Trust van je organisatie is en om meer praktische implementatieresources te ontdekken.