Verifieer Security Whitepaper met nul vertrouwen

Inhoud

Inleiding

Dit document beschrijft informatie met betrekking tot Zero Trust en hoe het kan worden gebruikt om de onderneming te beveiligen.

Samenvatting

Nul vertrouwen vertegenwoordigt een model dat veronderstelt geen gebruiker, apparaat, of toepassing, buiten of binnen het netwerk, kan als veilig worden beschouwd, en dat elk moet worden bevestigd alvorens het toegang tot netwerkactiva wordt verleend.

Dit concept is belangrijker geworden in virtualisatie en de snelle beweging van middelen op voorhand naar openbare, privé en hybride clouds.

De term Zero Trust is in 2010 gecreëerd door Forrester met de publicatie van hun Zero Trust Network Architecture Report.

Het is belangrijk om te begrijpen dat Zero Trust moet beginnen als een strategie op bedrijfsniveau om vitale zakelijke belangen en initiatieven te beschermen.

Zero Trust-pijlers

Wat is Zero Trust?

Zero Trust is een strategische benadering die diverse technologieën omvat om te helpen meer praktische beveiliging voor de huidige infrastructuur te bereiken. Het is een veiligheidsarchitectuur en een ondernemingsmethodologie die zijn ontworpen om de huidige combinatie van technologieën, praktijken en beleid effectief te orkestreren.

Het is een evolutie in onze benadering van beveiliging en levert een uitgebreide, interoperabele en holistische oplossingsbenadering die producten en services van meerdere leveranciers omvat.

Zero Trust is gebaseerd op vele gevestigde technologieën zoals netwerksegmentatie, multifactorverificatie en netwerktoegangscontrole.

Waarom is Nul vertrouwen belangrijk

Zero trust helpt de onderneming te beschermen tegen onbevoegde gebruikers, inbreuken en cyberaanvallen. U kunt de identiteit van gebruikers en apparaten voortdurend verifiëren en ze alleen de machtigingen geven die ze nodig hebben om hun werk te doen om het risico van een beveiligingsgebeurtenis te minimaliseren.

Uit marktonderzoek is gebleken dat de omvang van de wereldwijde "Zero trust security"-markt naar verwachting zal groeien van een geschatte waarde van USD 27 miljard in 2022 tot ongeveer USD 60 miljard tegen 2027/2028, bij een samengestelde jaarlijkse groei van ongeveer 17% op dat moment.

Motieven:

- Verhoogde frequentie van doelgebaseerde cyberaanvallen
- Groei in de regelgeving voor gegevensbescherming en informatiebeveiliging
- Meer behoefte om bedrijfs- en organisatierisico's te verminderen
- Naarmate meer services naar de cloud worden gemigreerd, overstijgt gecentraliseerde gegevensimplementatie de grenzen van data en vergroot het de beveiligingsrisico's.
- De noodzaak om de identiteit van de gebruiker tijdens het gehele toegangsproces te

bevestigen en niet alleen in eerste instantie

Eén enkele ransomware aanval kost 5 miljoen dollar. Cybercriminelen discrimineren niet wanneer ze zich op bedrijven richten.

Recente CIO- en Cisco-enquêtes laten zien dat Zero Trust een van de top 5 prioriteiten is. Cisco's zeggen dat een verschuiving naar werk op afstand, een tekort aan arbeidskrachten en een grote piek in cybersecurity aanvallen vereisen dat hun bestaande systemen in de onderneming beveiligd worden.

Traditioneel vs Zero Trust-model

Traditionele omgevingen zijn omgevingen waar beveiliging is toegevoegd nadat de omgeving is gebouwd. Normaal zijn het platte netwerken waar de verdediging rond de rand van het netwerk is gebouwd om aanvallen van het internet te voorkomen.

Zero Trust wordt over het algemeen erkend om zich te richten op de noodzaak om de systemen en gegevens van een organisatie op meerdere niveaus te beschermen met een combinatie van versleuteling, beveiligde computerprotocollen, dynamische werkbelasting en authenticatie en autorisatie op gegevensniveau, en vertrouwt niet alleen op een externe netwerkgrens.

De traditionele perimeter-centrische veiligheidsarchitectuur is minder effectief aangezien de werkbelasting meer en meer uit de cloud wordt geleverd, en mobiele endpoints de norm voor toepassing en gegevenstoegang worden.

Nul Trust Architectural Framework

Een Zero Trust Architectural Framework gaat over de beperking van de toegang tot systemen, toepassingen en gegevensbronnen tot die gebruikers en apparaten die specifiek toegang nodig hebben en gevalideerd zijn. Ze moeten voortdurend worden geauthenticeerd aan hun identiteit en veiligheidshouding om te zorgen voor een juiste autorisatie voor elke bron om toegang te verlenen.

Het kader is om een routekaart te bieden om te migreren en nul vertrouwen security concepten in een ondernemingsomgeving te implementeren en is gebaseerd op NIST Special Publication 800-207.

Een effectief nul Trust Architectural framework coördineert en integreert over deze zeven hoofdcomponenten.

- Nulvertrouwensnetwerken zijn een belangrijk kenmerk van een Nulvertrouwensstrategie die betrekking heeft op de mogelijkheid om netwerken te segmenteren of netwerkactiva te isoleren en de controle over de communicatie tussen netwerken te behouden. Ook, het beveiligt vertrouwde verbindingen om de werkplaats voor ver gebruik uit te breiden.
- Zero Trust Workforce omvat methoden om gebruikerstoegang te beperken en af te dwingen, wat technologieën omvat om gebruikers te verifiëren en hun toegangsrechten voortdurend te bewaken en te beheren. Deze toegang wordt beveiligd door technologieën zoals DNS, multifactor-verificatie en netwerkcodering.
- Nul Trust Devices richt zich op de noodzaak om alle netwerkverbonden apparaten te isoleren, beveiligen en beheren, die zijn gegroeid met de toevoeging van mobiliteit en het internet van

dingen, om een immense kwetsbaarheid te creëren voor aanvallers om te exploiteren.
- Zero Trust Worloads beveiligen de front-to-back toepassingsstacks die kritieke bedrijfsprocessen uitvoeren. Zorgt voor de beveiliging van het oost/west-verkeer tussen toepassingen, gegevens en services in een datacenter om kritieke toepassingen beter te beschermen.
- Nul Trust Data verwijst naar methodologieën voor het classificeren en categoriseren van gegevens, in combinatie met technologische oplossingen voor het beveiligen en beheren van gegevens, waaronder het versleutelen van gegevens.
- De zichtbaarheid en de analyse verwijzen naar technologieën die het bewustzijn voor automatisering en orkestratie verstrekken en beheerders toelaten om niet alleen de activiteit in hun milieu's te zien maar ook te begrijpen, die de aanwezigheid van bedreigingen in real time omvatten.
- Automatisering en orkestratie omvat tools en technologieën zoals algoritmen voor machinaal leren en kunstmatige intelligentie om automatisch netwerk- en datacenteractiva te classificeren, en om segmentatie en beveiligingsmaatregelen, -beleid en -regels voor te stellen en toe te passen die automatisch moeten worden geïmplementeerd; daarom moet de last voor beveiligingsteams worden verminderd en de mitigatie van aanvallen worden versneld.

Nul vertrouwen en segmentering

Elk op netwerken gebaseerd middel moet worden beveiligd en gesegmenteerd met het principe van de minste voorrechten. Dit kan het best worden bereikt via een asset management systeem dat inloggegevens en toegang voor elk doel controleert.

De behoefte aan Zero Trust segmentatie omvat merkbescherming, beperkte aanvalsoppervlakte, verbeterde netwerkstabiliteit, en het in staat stellen van snelle service-implementatie.

Om de bescherming van individuele hulpbronnen verder te verbeteren, kan micro-segmentering worden gebruikt. Scalable Group Tags (SGTs) kunnen worden gebruikt waar een tagwaarde in het Ethernet frame wordt ingevoegd om een resource uniek te identificeren. Bovendien omvatten infrastructuur-apparaten intelligente switches, routers of next-generation firewalls die kunnen worden gebruikt als gatewayapparaten om elke resource te beschermen.

Zichtbaarheid, analyses en automatisering

Het is van belang dat alle middelen van de organisatie en alle activiteiten die met deze middelen verband houden, volledig zichtbaar zijn. Dit is de basis van Zero Trust.

Om dynamische beleids- en vertrouwensbeslissingen te kunnen nemen, is een continue verzameling van analyses nodig. Onze Zero Trust architecturale benadering richt zich op de kern logische componenten van een SDN-strategie met een Policy Engine en Policy Administrator om een Control Plane te vormen om de toegang tot resources te beperken via Policy Enforcement Point(s) in een Data Plane.

De functies die nodig zijn voor Zero Trust Architecture om een grotere netwerkcontext, leerprocessen en betrouwbaarheid te bieden om zijn missie veilig uit te voeren:

- Granulaire microsegmentatie van toegang tot gebruikers, apparaten, toepassingen,

werkbelastingen en gegevens.
- Handhaving van beveiligingsbeleid overal waar dit werk wordt uitgevoerd, waaronder LAN's, WAN's, datacenters, clouds en de rand.
- Uitgebreid identiteitsbeheer - uitbreiding van het identiteits- en toegangsbeheer tot de identiteit van gebruikers, apparaten, toepassingen, werkbelastingen en gegevens die via softwaregedefinieerde toegang nieuwe microperimeters worden.
- Geïntegreerde verdediging tegen bedreigingen die gebruik maakt van wereldwijde inlichtingen over bedreigingen en feeds.
- Volledig geautomatiseerde, soepele controle van het netwerk van uw organisatie om veilig te functioneren op de gewenste schaal, prestaties en betrouwbaarheid die nodig zijn om de doelstelling te bereiken.

Stappen naar Nul vertrouwen

De sleutel tot uitgebreide Zero Trust-beveiliging is om de beveiliging uit te breiden in de gehele netwerkomgeving, of het nu LAN, datacenter, Cloud edge of Cloud is. Naleving is natuurlijk verplicht.

Deze beveiliging moet het totale zicht op de netwerkomgeving van uw organisatie omvatten. Belangrijkste stappen naar het uitgebreide Zero Trust center rond:

- Identificeer apparaten en gevoelige gegevens. Identificatie en classificatie van apparaten, gevoelige gegevens en werkbelasting uitvoeren.
- Begrijp de stromen van uw gevoelige gegevens.
- Architect Uw Zero Trust segmentatiebeleid. Elk op een netwerk gebaseerd actief moet worden beveiligd en gesegmenteerd met het principe van de minste privileges en strikt afgedwongen, granulaire controles, zodat gebruikers alleen toegang hebben tot de resources die nodig zijn om hun werk te kunnen uitvoeren.
- Voer beleid en houding uit. Dit kan worden uitgevoerd met platforms zoals Cisco NAC of ISE.
- Bewaak de Zero trust omgeving continu. Voer security analytics uit om security incidenten in real time te monitoren en analyseren en snel kwaadaardige activiteit te identificeren. Inspecteer en registreer continu al het verkeer, zowel intern als extern.

Bereik betrouwbare toegang

Om de uitgebreide Zero Trust-beveiliging te kunnen realiseren, moeten organisaties hun Zero Trust-aanpak uitbreiden naar al hun werknemers, werkplekken en werkbelastingen.

- Nul Trust Workforce - Gebruikers en apparaten moeten worden geauthenticeerd en geautoriseerd en toegang en privileges moeten voortdurend worden bewaakt en geregeerd om resources te beschermen.
- Zero Trust Workplace - Toegang moet worden gecontroleerd over de gehele werkplek, inclusief de cloud en edge.
- Nul Trust Workloads - Granulaire toegangscontrole moet worden afgedwongen op hele toepassingsstacks, die bestaan uit tussen containers, hypervisors en microservices in de cloud en traditionele agency datacenters.

Cisco, een door Forrester herkende Zero Trust Leader, is een sterk pleitbezorger van Zero Trust

enablement op uw hele netwerk - zowel op kantoor als in de cloud. U kunt uw Cisco-netwerkinfrastructuur niet alleen gebruiken als een cruciale basis voor uw Zero Trust Architecture, maar u kunt ook meer leren over andere belangrijke Cisco Zero Trust-beveiligingsfuncties die uw organisatie kunnen helpen bij uw Zero Trust-traject.

Cisco Secure-portfolio

Deze kunnen worden gebruikt om een succesvol Zero Trust framework op te bouwen:

- Draadloze, beveiligde toegang voor gebruikers, apparaten en toepassingen via **Cisco Duo**
- Flexibele cloudbeveiliging via **Cisco Umbrella**
- Intelligente pakketinspectie via **Cisco Secure-firewall**
- Advanced Malware Protection via **Secure Endpoint** (voorheen AMP)
- Beveiligde VPN en externe toegang via **Cisco AnyConnect**
- Holistische werklastbescherming via **Cisco-verificatie**
- Beschermde netwerksegmentatie met de **Cisco Identity Services Engine** (ISE)
- Toepassingszichtbaarheid en microsegmentering via **Cisco Secure Workload**
- Geïntegreerd security platform via **Cisco SecureX**
- Unified SASE-oplossing met as-a-service abonnement via **Cisco+ Secure Connect**
- Deskundigenadvies van de **Cisco Zero Trust Strategy Service**
- Ondersteuning en end-to-end services via **consultancy-, advies- en oplossingsservices**

Samenvatting

Een van de eenvoudigste manieren om aan Zero Trust te denken is om "Nooit vertrouwen en altijd verifiëren." Dit is van toepassing op elke netwerkverbinding, elke sessie en elk verzoek om toegang tot kritieke toepassingen, werkbelastingen en gegevens.

Zero trust security frameworks creëren gelokaliseerde micro-perimeter verdediging rond elke bron in het netwerk van de organisatie. Als correct ontworpen, kunnen de kaders activa ongeacht beschermen waar zij worden gevestigd.

Een efficiënte manier om risico's te verminderen is de toegang tot geprivilegieerde en gedeelde gegevens te controleren en het beginsel van de minste voorrechten toe te passen. Dit beveiligingsmodel maakt orkestratie via API's mogelijk, evenals integratie met workflowautomatiseringsplatforms die zichtbaarheid in gebruikers en toepassingen bieden.

Met succes geïmplementeerd kan Zero Trust helpen veilige en naadloze bedrijfsvoering te garanderen in de gehele IT-omgeving van een organisatie en resulteren in continue betrouwbare toegang tot de kritieke werkbelastingen, toepassingen en gegevens van een organisatie, om de taken van uw organisatie te verbeteren.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.