E-book

Wat je moet weten om met Zero Trust Security aan de slag te gaan

Cisco Secure. Controle is alles.

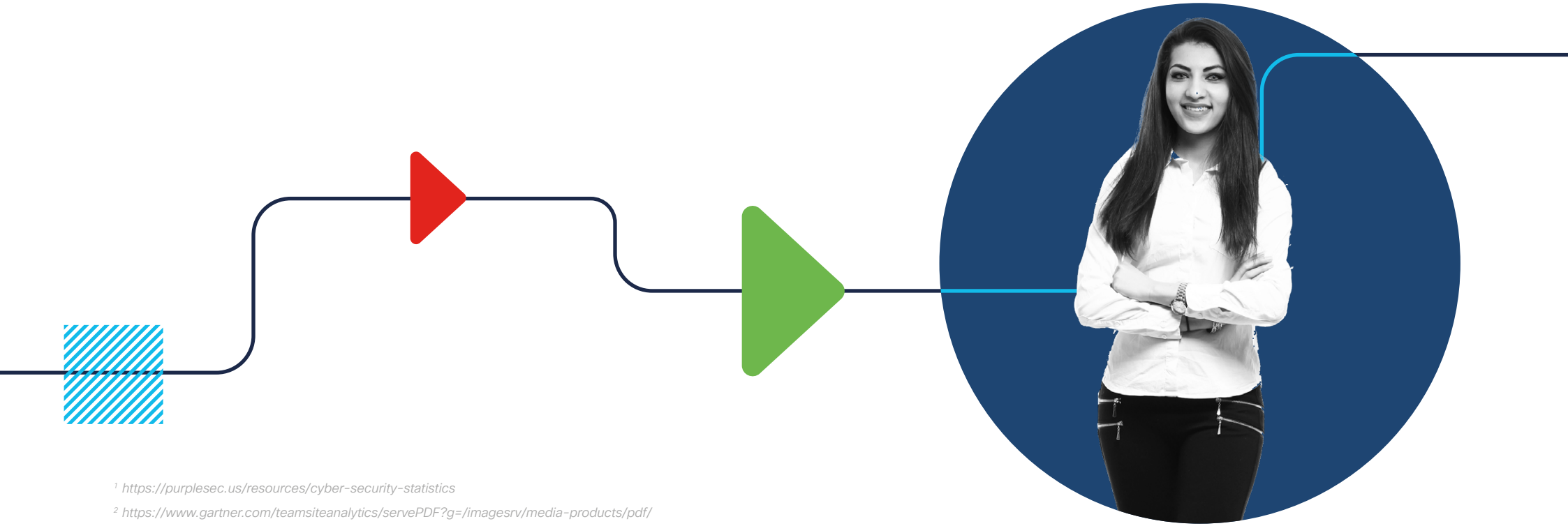
De cloud, IOT (Internet of Things), BYOD (Bring Your Own Device). Allemaal ontwikkelingen die de IT-infrastructuur van organisaties complexer maken en security-risico's vergroten. Cijfers laten zien dat de dreiging reëel is, want elk jaar neemt het aantal cyberaanvallen toe en loopt de schade verder op[1]. Bedrijven geloven al niet meer dat antivirussoftware en wachtwoorden nog volstaan om gevoelige data te beschermen. Volgens Gartner vertoont een traditionele security-architectuur altijd wel ergens een verborgen zwakke plek[2]. In dit e-book lees je hoe je 'Zero Trust Security' tot nieuwe norm verheft, zodat je alle data weer onder controle krijgt.

Zero Trust is een filosofie die ervan uitgaat dat je geen mens, apparaat of applicatie moet vertrouwen. Het maakt daarbij niet uit of ze van buiten of binnen je organisatie toegang willen tot je data. Security moet in deze visie daarom verder gaan dan het bouwen van een schild om je kritische systemen met een firewall en antivirussoftware. De basis is dat je bij veel meer toegangspoorten identiteit en toegangsrechten checkt.

Het fundament van Zero Trust: microsegmentatie

Microsegmentatie is het fundament van Zero Trust. Dit komt in het kort neer op het opdelen van je netwerk in segmenten. Vergelijk het maar met een kantoor dat uit één grote ruimte bestaat. Als iemand daar onder valse voorwendselen binnendringt heeft hij toegang tot alles. Als er meerdere kamers zijn die op slot zitten, wordt het anders. In je netwerk kun je op soortgelijke wijze compartimenteren.

Maar Zero Trust omvat meer. In een complexe omgeving waar steeds meer mensen op afstand werken bijvoorbeeld, moet je ook de toegang tot de cloud bewaken. Je kunt nog een stap verder gaan door te controleren wie contact wil maken met je datacenter en je microservices, de onderdelen waaruit veel apps tegenwoordig zijn opgebouwd. Security moet in feite overal zijn waar gebruikers en apparaten ook zijn.



[1] *https://purplesec.us/resources/cyber-security-statistics*

[2] *https://www.gartner.com/teamsiteanalytics/servePDF?g=/imagesrv/media-products/pdf/Qi-An-Xin/Qi-An-Xin-1-1OKONUN2.pdf*

Zero Trust-toegang in plaats van een open VPN

Gartner verwacht dat in 2022 80 procent van de nieuwe zakelijke applicaties die openstaan voor partners in het ecosysteem, worden benaderd via 'Zero Trust netwerktoegang.' En tegen 2023 heeft naar verwachting 60 procent van alle organisatie VPN ingeruild voor Zero Trust-toegang. VPN is van oudsher de manier om een beveiligde verbinding te maken tussen jou en het internet; al je internetverkeer gaat door een versleutelde virtuele tunnel. Maar deze benadering gaat er vooral van uit dat de kwaadwillende buiten zijn en de betrouwbare personen binnen. Die visie is te beperkt in een tijd dat data niet alleen binnen de muren van een bedrijfsdatacenter is te vinden maar ook daarbuiten, in multicloud-omgevingen. Het gevaar is ook dat een aanvaller die binnenkomt door iemands identiteit te stelen, zonder meer als betrouwbaar wordt gezien en overal bij kan.

Aan de slag in vijf stappen

Welke concrete stappen kun je nu zetten om Zero Trust in de praktijk tot een succes te maken?

John Kindervag, lang actief voor Forrester, geldt als de ‘Godfather’ van de Zero Trust-filosofie. Hij ziet de benadering als ‘een databeveiligingssysteem of firewall op steroïden.’ Hij trekt die vergelijking omdat allerlei technieken worden ingezet, op meerdere niveaus. ’Zero Trust gebruikt firewalls, systemen die kwetsbaarheden signaleren, verdachte stromen blokkeren, data-encryptie en noem maar op.’[3]

Bepaal welke data het gevoeligst is.

Met andere woorden: wat zijn de kroonjuwelen van je organisatie, die extra bescherming nodig hebben?

Breng datastromen in beeld.

Als je weet hoe data beweegt binnen je netwerk, tussen gebruikers, apps en resources, dan kun je daar waar nodig (virtuele) schotten tussen zetten.

Ontwerp je nieuwe Zero Trust-architectuur.

Breng in beeld hoe je fysieke en virtuele oplossingen met elkaar verbindt.

Regel organisatorisch en technisch wie toegang heeft tot welke data.

Stel need-to-know basisregels op. Kijk naar elk niveau, dus ook naar apps: moeten die echt met elkaar kunnen praten? Of kunnen we ook zonder deze koppelingen?

Houd je ecosysteem continu in de gaten.

Controleer en verifieer al het dataverkeer doorlopend, zodat je elke afwijking direct opmerkt en kunt ingrijpen.

Dreigingen met minstens 37 procent verminderen

Volgens Forrester kan Zero Trust het risico dat je daadwerkelijk door een dreiging getroffen wordt met minstens 37 procent verminderen. Securitykosten dalen daardoor ook, met ongeveer 30 procent.

Kindervag ziet Zero Trust als nieuwe norm. Een benadering die ook je interne netwerkverkeer niet zomaar vertrouwt en die alle datastromen in de gaten houdt. Het is de manier om je data slimmer te beveiligen, waarbij je goed vertrouwen vervangt voor volledige controle. Want controle is alles.

Meer weten?

www.controleisalles.nl

[3] *https://www.darkreading.com/attacks-breaches/forrester-pushes-zero-trust-model-for-security/d/d-id/1134373*

[4] *https://duo.com/resources/ebooks/cisco-named-a-leader-in-the-2019-forrester-zero-trust-wave-report?utm_source=cisco&utm_medium=website&utm_campaign=zt-wave*

[5] *https://www.darkreading.com/cloud/debunking-5-myths-about-zero-trust-security/a/d-id/1334064*

Cisco Secure.
Controle is alles.