E-book

Volledige controle over alle securitylagen: the next steps

Cisco Secure. Controle is alles.

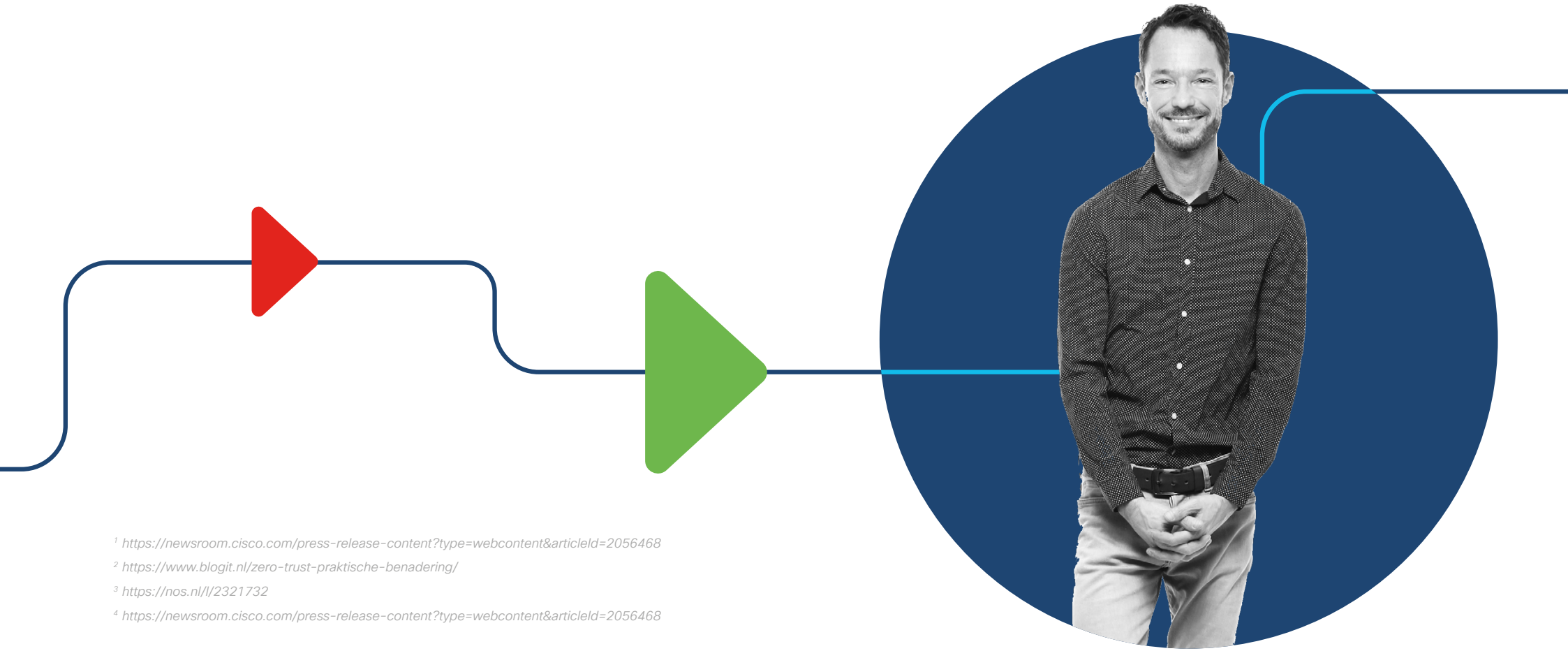
Complexiteit is de grote vijand van cybersecurity. De tijd dat je kon volstaan met een digitaal hek rond de organisatie is allang voorbij. Je hebt nu de cloud, het Internet of Things en mobiele apparaten. Dat biedt businesskansen, maar maakt bedrijven ook kwetsbaarder voor cyberattacks. Een gemiddelde organisatie gebruikt inmiddels meer dan twintig verschillende security-oplossingen om zich hiertegen te beschermen. De situatie wordt daardoor echter zó onoverzichtelijk, dat dreigingen proactief te lijf gaan een illusie is[1]. In dit e-book lees je wat je kunt doen om security alomvattend te laten zijn en volledige controle te bereiken.

Een ontwikkeling in cybersecurity die sterk opkomt, is Zero Trust. Je leest er meer over in ons e-book 'Wat je moet weten om met Zero Trust Security aan de slag te gaan'. Zero Trust is een filosofie die uitgaat van 'minimal access'. Kort gezegd komt het erop neer dat alleen volledig te vertrouwen gebruikers en apparaten toegang krijgen tot data. Er is voortdurend sprake van verificatie of iemand is wie hij lijkt te zijn. Niet alleen vindt controle plaats van dataverkeer dat van binnen naar buiten loopt, ook intern verkeer ligt hierbij onder het vergrootglas[2].

Zero Trust: ook binnen je muren

De hack bij Universiteit Maastricht in 2019 maakt duidelijk hoe belangrijk interne toegangscontrole is: indringers konden maanden ongestoord hun gang gaan in het netwerk[3]. Als je meer inzicht hebt ontdek je eerder dat er iets aan de hand is. Inzicht in alle stromen is de sleutel tot het krijgen van volledige controle.

In Maastricht bleken sommige servers onvoldoende geüpdatet, wat het de hackers makkelijker maakte om toe te slaan. Achterstand in patching vormt een groot risico blijkt uit onderzoek van Cisco[4].



[1] https://newsroom.cisco.com/press-release-content?type=webcontent&articleId=2056468

[2] https://www.blogit.nl/zero-trust-praktische-benadering/

[3] https://nos.nl/l/2321732

[4] https://newsroom.cisco.com/press-release-content?type=webcontent&articleId=2056468

Complexiteit stelt organisaties voor extreme uitdagingen

Volgens datzelfde onderzoek is op meer punten verbetering mogelijk, zoals:

- Bescherming van workloads. Voor veel organisaties is dit ‘extreem uitdagend’. 42 procent van de ondervraagden vindt het met name lastig om datacenters te beveiligen. Dit percentage ligt bij public en private cloud nog hoger.
- Het beveiligen van gebruikers die op afstand werken met telefoons, laptops en tablets vindt meer dan de helft behoorlijk lastig, omdat het aantal blijft groeien.

Volgens de onderzoekers zetten IT-professionals wel stappen in de goede richting om security te verbeteren. Zo werken netwerk- en securityteams doorgaans al nauw samen. Ook proberen ze door automatisering het aantal handelingen dat IT-mensen moeten verrichten terug te dringen, zodat ondanks schaarse capaciteit sneller kan worden gereageerd op incidenten.

De implementatiegraad van op Zero Trust gebaseerde technologie is echter nog laag. Zo gebruikt slechts 27 procent Multifactor Authenticatie (MFA) voor gebruikersverificatie. Ook microsegmentatie (een techniek voor toegangsbeperking op het netwerk) past maar 17 procent van de ondervraagden toe. Tijd voor verandering dus.

Een platformbenadering geeft meer inzicht

Zero Trust is als gezegd een filosofie, geen technologie. Er is wel een samenspel van technologieën nodig om identiteit, toegang en gedrag van gebruikers, apparaten en applicaties adequaat te beveiligen. Cisco biedt tal van oplossingen voor een gelaagde beveiligingsstructuur; van MFA tot netwerksegmentatie en beveiliging van apps en apparaten. Door een platformbenadering ontstaat meer inzicht, neemt de complexiteit af en fungeert het netwerk als sensor die vroegtijdig waarschuwt voor dreigingen.

Voordelen in de praktijk: MFA

Hoe werkt dit in de praktijk? Cisco gaat uit van optimale bescherming van workforce, workload en workspace.

Voor de protectie van mensen is er MFA door Duo. Een authenticatiemethode die ‘iets wat mensen kennen’ (gebruikersnaam en wachtwoord) combineert met ‘iets wat ze hebben’ (bevestiging via bijvoorbeeld hun telefoon).

Facebook gebruikt Duo, maar Cisco zelf ook . De oplossing beschermt wereldwijd drieduizend apps, vierhonderdduizend apparaten en honderdtwintigduizend gebruikers. Duo is snel uit te rollen: 70 procent van de gebruikers werkt er al mee binnen 48 uur na ontvangst van de uitnodiging. Gebruikers en apparaten hebben zo altijd veilig toegang tot elke omgeving, waar ze ook contact maken.

Voordelen in de praktijk: zichtbaarheid

Voor bescherming van workloads is er het Tetration-platform, ondersteund door de network detection and response- oplossing: Cisco Stealthwatch. IDC onderzocht de praktische voordelen[7]. Een dienstverlener in de zorgsector kan door Tetration bijvoorbeeld beter zien of latency in de app zelf zit, of in het netwerk. Problemen worden zo sneller opgelost. De beschikbaarheid en performance van apps neemt sterk toe. Het allergrootste voordeel voor organisaties is ook de automatische segmentatie in het netwerk. “Wanneer je iets koppelt aan het netwerk, dan moet je weten waar het mee moet communiceren en hoe.’ Een dreiging kun je door segmentatie snel isoleren en buiten werking stellen.

Een financiële instelling heeft door de security oplossingen van Cisco minder tools nodig voor inzicht in datastromen, monitoring en toegangscontrole. Segmentatie maakt het ook mogelijk om te testen zonder impact op het hele netwerk.

IDC concludeert onder meer dat het Tetration-platform gebruikers helpt operationele processen effectiever in te richten, wat ook scheelt in de kosten.

Voordelen in de praktijk: SD-Access

IDC bekeek ook het effect van workspace-beveiling door Software-Defined Access, een andere pijler onder Cisco's Zero Trust-architectuur. Hiervoor werden elf organisaties geïnterviewd, waaronder onderwijs-, overheids- en zorginstellingen. Elk tellen ze gemiddeld 42.000 werknemers en 239 businessapps.

Als grootste voordeel noemen ondervraagden dat het geautomatiseerd onboarden van gebruikers en apparaten. Het systeem kent de bijbehorende rechten toe, zodat niet iedereen bij gevoelige data kan. Toegangsbeperking maakt het managen van het netwerk eenvoudiger. De performance van apps verbetert. Doordat SD-Access IT werk uit handen neemt 'gaan we van een reactief naar een proactieve werkwijze,' vertelt een respondent. 'We hebben nu ook meer tijd om achterstand op security-gebied in te lopen.'

Volgens IDC zijn IT-afdelingen mede door SD-Access minder bezig met 'keeping the lights on'. Ze gaan zich meer op strategisch niveau bewegen.

[5] *https://www.linkedin.com/pulse/zero-trust-security-hocus-pocus-voor-belgie-om-weg-te-bonne/*
[6] *https://duo.com/use-cases/case-studies/cisco*
[7] *https://www.cisco.com/c/dam/en/us/products/collateral/data-center-analytics/tetration-analytics/idc-growing-holistic.pdf*
[8] *https://www.cisco.com/c/dam/m/digital/elq-cmcglobal/OCA/Assets/NB/NB06/nb-06-IDC-assurance-sd-access-analyst-rpt-cte-en.pdf*

Zero Trust: the next steps

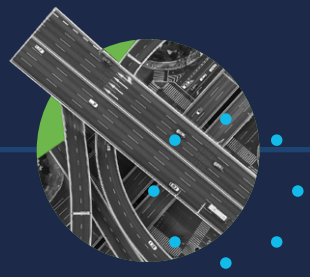
Welke stappen kun je nu zetten om op Zero Trust gebaseerde security effectief in te zetten?

Onderzoek de staat van de cybersecurity in je organisatie

De eerste stap op weg naar gerichte beveiliging, is onderzoek naar gevoelige gegevens. Analyseer waar die zich bevinden. Stel vast wie toegang heeft tot deze data[5]. Bekijk daarna welke middelen en technologieën je al hebt om indringers te voorkomen. Als security op vaste apparaten is afgedekt, hoef je daar niet meer in te investeren. Maar hoe zit het met de eigen devices waarmee mensen het netwerk opgaan?

Ontdek en toets risico's

Er zijn slimme tools die kwetsbaarheden in netwerken blootleggen. Je kunt vervolgens onderzoeken hoe groot de potentiële impact hiervan is op kritische processen. Een slecht beveiligd IoT-apparaat kan een toegangspoort zijn voor een hacker. Als je zeker wilt zijn dat nergens gevoelige data lekt, kun je een tool inzetten om in- en uitgaand verkeer te scannen. Ook interne stromen kun je automatisch laten onderzoeken. Is het echt nodig dat apps met elkaar praten? Slimme tools herkennen risico's en slaan alarm.



Maak een roadmap

Als je alle risico's in beeld hebt, stel je een roadmap op. Misschien is voor sommige oplossingen eerst nog intern zendingswerk nodig en moet budget worden gereserveerd. Een prioriteitenlijst is een vast onderdeel van zo'n plan; de ene dreiging is nu eenmaal groter dan de andere.

E-book

Zero Trust brengt de controle terug

Een op Zero Trust gebaseerde security-strategie maakt je IT-afdeling dus productiever, laat IT proactiever zijn, maakt het managen van het netwerk eenvoudiger en helpt kosten te besparen. Maar het belangrijkste is dat je weer controle krijgt; de kans dat een cyberaanval je treft neemt sterk af. Je kunt 'vertrouwen' op Zero Trust en kunt streven naar volledige controle.

Meer weten?

Ontdek meer over de
Controle is alles-aanpak op:

www.controleisalles.nl

Cisco Secure.
Controle is alles.