Security Everywhere

De aandacht richten op effectieve beveiliging

cisco

Digitalisering in een complexe wereld

Wij weten dat het binnen uw bedrijf allemaal draait om innovatie die moet leiden tot digitale bedrijfstransformatie.

Aan de netwerk-edge, waar uw apps communiceren met de buitenwereld en waar nieuwe IoT-apparaten fundamentele zakelijke veranderingen stimuleren, zorgen consistente connectiviteit en sterke netwerken ervoor dat gebruikers permanent aan u blijven gebonden. Daarnaast verbeteren ze de prestaties van apparaten en leiden ze tot inzichten die nodig zijn om concurrerend te blijven.

Het streven naar effectieve beveiliging is anders dan het streven naar effectieve IT, waarbij de resultaten kunnen worden uitgedrukt in tastbare waarden zoals hogere uptime en betere connectiviteit, kostenbesparingen of hogere productiviteit en betere prestaties. Beveiliging is effectief wanneer er niets gebeurt: geen gegevensinbreuken, geen DDoS-aanvallen (Distributed Denial of Service) en geen ransomware.

Het bereiken van deze rusttoestand in de complexe en steeds veranderende IT-infrastructuur is vergelijkbaar met ontsnappen uit een eindeloos en steeds complexer labyrint.

Hedendaagse beveiligingsfunctionarissen hebben de taak om een aanvalsgebied te beschermen dat nog nooit zo divers of ingewikkeld is geweest. Laten we eens kijken naar de complexe elementen waar we tegenwoordig mee te kampen hebben.

Frankenstructuren

Het hedendaagse IT-landschap is ingewikkeld – een landschap dat is samengeraapt tot een ‘frankenstructuur’. En ons wordt gevraagd om deze structuur te gebruiken om digitale bedrijfstransformatie te stimuleren. Dat is echter vrijwel onmogelijk met netwerken die overal verspreid zijn, waaraan nieuwe locaties en vestigingen moeten worden toegevoegd en waartoe gebruikers – waar ze ook zijn – toegang hebben via hun slimme apparaten. Wij zien zakelijke apps, servers en gegevens in de cloud van enkele minuten geleden – pal naast oudere servers van jaren geleden. En we hebben apparaten die niet eens lijken op computers, maar wel verbinding maken met onze netwerken.

En om het nog ingewikkelder te maken moeten wij bedenken hoe we beveiliging overal kunnen toepassen om deze complexe infrastructuur te beveiligen.

Geraffineerde aanvallers

Aanvallers zijn zo geraffineerd en professioneel dat het een uitdaging voor de organisatie is om gelijke tred te houden. Ze zijn gemotiveerd door financieel gewin en soms hacktivisme en begrijpen hun doelwitten – van hun voor- en afkeuren tot de manier waarop zij zaken doen. Ze maken genadeloos misbruik van elke zwakke plek die ze vinden. Dit alles betekent dat aanvallers flexibel zijn, terwijl bedrijven dat niet altijd kunnen zeggen.

Onpraktische beveiligingsposturen

Ons beveiligingsantwoord hierop was maar al te vaak een aanpak met een lappendeken van point-producten om een beveiligingspostuur te bouwen. We zien een probleem en kopen een nieuwe beveiligingsproduct om het probleem aan te pakken. Dit betekent dat we uiteindelijk met onpraktische, ineffectieve beveiligingsposturen zitten vanwege de tientallen producten die we bij elkaar vegen, maar die niet ontworpen zijn om samen te werken of bij elkaar te passen. Hierdoor wordt het probleem met onze frankenstructuur alleen maar groter. Dit ondermijnt onze behoefte aan effectievere beveiliging.

Digitalisering: kans, uitdaging of bedreiging?

De digitale economie levert nieuwe zakelijke kansen op omdat transacties sneller, efficiënter en flexibeler kunnen worden afgehandeld. Bedrijven van elke omvang moeten veiliger te werk gaan om in te spelen op de verkoopkansen die door digitalisering mogelijk worden gemaakt. Hiervoor moet beveiliging effectief en eenvoudig zijn, aanwezig zijn van het netwerk tot aan mobiele gebruikers, endpoints en de cloud.

Snelheid is ook cruciaal bij beveiliging. Factoren zoals de tijd die nodig is om een inbreuk te detecteren en erop te reageren en de mogelijkheid om in real-time te handelen, zijn essentieel in een bedrijfsomgeving. Beveiliging moet een doorlopend proces zijn en altijd actief zijn, in tegenstelling tot verouderde modellen waarbij geplande point-in-time detectie plaatsvond.

Moderne netwerken zijn voortdurend in ontwikkeling waardoor nieuwe aanvalsvectoren ontstaan, waaronder: mobiele apparaten, web- en mobiele toepassingen, hypervisors, sociale media, webbrowsers, thuiscomputers en zelfs voertuigen. Daarnaast hebben mobiliteit en de cloud geleid tot een constant veranderende verzameling gebruikers, locaties, toepassingen, toegangsmethoden en apparaten. Al deze factoren bieden meer kansen voor aanvallers, die steeds geraffineerder en professioneler te werk gaan.

Gebruikelijke beveiligingsuitdagingen:

- **Te veel point-oplossingen:** sommige organisaties hebben 40 tot 60 verschillende beveiligingsoplossingen die niet samenwerken. Investeren in een architectuur met elementen die zijn ontworpen voor integratie kan de beveiliging verbeteren.

- **Lange detectietijd (TTD):** de gemiddelde tijd binnen de branche om een aanwezige bedreiging te detecteren is 100 tot 200 dagen. Met Cisco's geavanceerde beveiligingsoplossingen kunt u de gemiddelde TTD verkorten tot 13 uur.

Digitalisering biedt vele mogelijkheden voor bedrijven en, nog belangrijker, verhoogde efficiëntie voor de eindgebruikers. Bedrijven moeten zich echter niet alleen bewust zijn van de beveiligingsuitdagingen die in dit nieuwe landschap optreden, maar ook vastbesloten zijn deze aan te gaan.

Veilig profiteren van nieuwe zakelijke kansen

Het hedendaagse bedreigingslandschap lijkt in niets op dat van 10 jaar geleden. Eenvoudige aanvallen waarbij de schade te overzien was, zijn vervangen door moderne, geraffineerde cybercriminaliteit die grote verliezen en disruptie bij organisaties kan veroorzaken.

Dergelijke geavanceerde aanvallen kunnen moeilijk worden gedetecteerd, blijven lange tijd achter in netwerken en verzamelen netwerkresources om elders aanvallen uit te voeren. In andere gevallen, zoals ransomwareaanvallen, vindt de inbreuk plaats in een veel kortere periode, maar kan deze zo desastreus zijn dat de activiteiten van de getroffen organisatie volledig stil komen te liggen. Recente ransomwarevarianten waren in staat om volledige systemen te versleutelen en gegevens werden niet aan de slachtoffers teruggegeven, zelfs niet nadat het losgeld was betaald.

Leveranciers moedigen beveiligingsorganisaties aan point-oplossingen op te stapelen om een heel scala aan behoeften aan te pakken. De producten in deze complexe lappendeken passen gewoonlijk niet bij elkaar en dit leidt tot gaten in de beveiliging, beheerproblemen en inefficiëntie. Hier kunnen aanvallers misbruik van maken. Bovendien bevatten point-oplossingen vaak overlappende functies. Dit betekent dat bedrijven al snel betalen voor overbodige, onnodige beveiligingsfunctionaliteit. Dit alles leidt tot uiterst onpraktische, niet-sluitende beveiligingsposturen.

Traditionele antivirus- en firewallmethoden die voor bescherming uitsluitend op detectie en blokkering vertrouwen, zijn niet meer toereikend. Wij zijn van mening dat effectieve beveiliging wordt bereikt met oplossingen die eenvoudig, open en geautomatiseerd zijn. Daar komen we hierna nog op terug.

Cyberbeveiliging: een groeimotor voor de digitale economie

Verbonden wereld, digitaal bedrijf, IoE – al deze factoren verstoren de traditionele manier van zakendoen. Wanneer we de implementatie van nieuwe technologieën evalueren (ongeacht of dit een nieuw bedrijfsmodel of aanvullende services betreft), moeten organisaties vanaf het begin in alle bedrijfskritische gebieden beveiliging inbouwen. Het is belangrijk om te overwegen hoe effectief de verouderde beveiligingsoplossingen zijn in het beveiligen van deze nieuwe omgevingen.

Alleen Cisco heeft de benodigde uitgebreide technologie en het talent in huis om een geïntegreerde bescherming tegen bedreigingen te bouwen, waarmee een bedreiging zodra deze wordt gedetecteerd overal kan worden geblokkeerd. Met de steun van deze mogelijkheid kunnen organisaties hun bedrijf sneller laten groeien en kansen grijpen in de wetenschap dat ze beveiligd zijn.

Het is duidelijk dat een geïntegreerde bescherming tegen bedreigingen de effectiviteit tegen geavanceerde aanvallen vergroot. Maar het stelt bedrijven ook in staat volledig te profiteren van de kansen die worden geboden door digitalisering.

Om effectief te zijn, moet beveiliging eenvoudig, open en geautomatiseerd zijn

Cisco levert effectieve beveiliging met een superieure portfolio, de allerbeste bedreigingsinformatie, een toonaangevende serviceorganisatie en een op architectuur gebaseerde benadering met producten die bij elkaar passen voor effectievere en eenvoudigere beveiliging met een aanzienlijk hogere effectiviteit.

Eenvoudig

Wij zetten ons in om de complexiteit eruit te halen zodat de meest effectieve technologieën eenvoudig worden. Dit betekent niet dat we niet ook ongekend innovatief en technisch zijn. Het betekent alleen dat onze innovatie een eenvoudigere beveiligingservaring voor onze klanten biedt: ongeacht of dit eenvoud bij het implementeren, schalen of beheren betreft.

Open

Cisco bouwt producten die zijn ontwikkeld om op elk niveau van de beveiligingsstack samen te werken, niet alleen binnen onze gehele portfolio, maar ook met producten van andere leveranciers. Het aanbod van open oplossingen vormt de basis voor een ecosysteem dat integratie toepast om aanzienlijk krachtiger te worden wanneer producten samen worden gebruikt.

Geautomatiseerd

Cisco-oplossingen zijn geautomatiseerd om de effectiviteit te optimaliseren, de belasting van teams te verminderen en organisaties meer slagkracht te bieden met kortere detectie- en responstijden.

Statuscontrole: heeft uw organisatie gaten in de beveiliging?

- **Fragmentatie:** organisaties hebben gemiddeld 45 verschillende beveiligingsleveranciers in hun IT-omgevingen
- **Trage respons:** 60% van de gegevens wordt bij een inbreuk binnen enkele uren gestolen en bij 75% van de aanvallen begint het doorsluizen van gegevens binnen enkele minuten, maar duurt het detecteren ervan veel langer
- **Trage detectie:** 54% van de inbreuken blijft maandenlang of zelfs jaren onontdekt
- **Beperkte zichtbaarheid:** 90% van de organisaties is zich niet volledig bewust van al hun netwerkapparaten
- **Kwetsbare mobiele apps:** 92% van de 500 populairste Android-apps bevatten beveiligings- en/of privacyrisico's
- **Silo's:** er worden 5 tot 10 keer meer cloudservices gebruikt dan het IT-personeel denkt

Enkele belangrijke vragen wanneer u digitaal gaat werken:

- Voldoet onze beveiliging aan de eisen van een digitaal, verbonden bedrijf?
- Weten we wat onze bedrijfskritische services en systemen zijn en begrijpen we de impact die een inbreuk op de beveiliging daarop kan hebben?
- Kunnen we snel genoeg reageren wanneer we worden aangevallen?
- Zijn we voorbereid om onze beveiligingsstrategie aan te passen aan nieuwe bedrijfsmodellen en aanvalsvectoren, naarmate ons IT-landschap blijft veranderen?
- Hoe verbeteren we in een veranderend bedreigingslandschap onze mogelijkheden om doorlopend te beschermen tegen aanvallen en steeds geraffineerdere bedreigingen?
- Hoe gaan we de complexiteit en fragmentatie van onze beveiligingsoplossingen verminderen?

Beveiliging in de DNA van het netwerk

Netwerk als sensor en netwerk als handhaver: laat uw bedrijf veilig groeien

Hoe zou het zijn als u uw netwerk en alle informatie over verkeer die u al hebt, kunt gebruiken om een sterkere beveiligingsarchitectuur te bouwen? Dit is nu al mogelijk.

Het netwerk kan bijvoorbeeld als sensor worden gebruikt om de zichtbaarheid van bedreigingen te vergroten. In dit geval worden verdachte verkeersstromen aangemerkt en geanalyseerd om kwaadaardig gedrag en potentiële bedreigingen nauwkeuriger te identificeren. Het netwerk kan ook een handhaver zijn door dynamisch op deze abnormaliteiten te reageren. Het kan helpen het beveiligingsbeleid te handhaven om het gehele aanvalsgebied te verkleinen, malware tegen te houden en besmette apparaten in quarantaine te plaatsen. Het netwerk als handhaver biedt ook een hoge mate van automatisering – waardoor het sneller enorme hoeveelheden gegevens over netwerkgedrag kan analyseren – om bedreigingen sneller in te perken en inzicht te bieden in de ontwikkeling van bedreigingen.

Het netwerk zelf kan helpen om geavanceerde bescherming tegen bedreigingen te implementeren en de detectietijd en responstijd te verminderen.

Over Cisco

Cisco bouwt effectieve beveiligingsoplossingen die eenvoudig, open en geautomatiseerd zijn. Door optimaal gebruik te maken van onze ongeëvenaarde aanwezigheid in netwerken en dankzij de meest uitgebreide technologie, services en talentvolle medewerkers binnen de branche, levert Cisco ultieme zichtbaarheid en responsiviteit om meer bedreigingen te detecteren en deze sneller te herstellen. Met Cisco Security staan bedrijven klaar om beveiligd te profiteren van een nieuwe wereld vol digitale zakelijke kansen.

Neem voor meer informatie contact op met uw plaatselijke Cisco Security-team.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices