E-book

Maak security eenvoudig met het Cisco SecureX platform

Cisco Secure. Controle is alles.

E-book

Er komen steeds meer aanbieders van security-producten en organisaties hebben steeds meer tools in huis om zich te beschermen tegen cybercrime. Toch verlangt de overheid dat bedrijven hun digitale weerbaarheid nog verder vergroten, omdat het aantal aanvallen explosief stijgt. IT-afdelingen kunnen door deze ontwikkelingen het gevoel krijgen voor een haast onmogelijke opgavete staan. Ze hebben daarom behoefte aan eenvoudige middelen, die security minder complex maken. Lees in dit e-book meer over de oplossingen die Cisco biedt om dreigingen weer onder controle te krijgen, zonder de noodzaak voor een complex systeem.

Wereldwijd zijn duizenden aanbieders actief op het gebied van security. Alleen al in de Verenigde Staten zijn het er meer dan 3.500[1]. Bedrijven hebben ook steeds meer tools voor cybersecurity in huis: kleine bedrijven (tot vijftig werknemers) gebruiken er gemiddeld vijftien tot twintig, middelgrote bedrijven (tot 250 werknemers) zelfs vijftig tot zestig. Grote organisaties of enterprises spannen de kroon met wel meer dan 130 tools.[2] Die getallen maken duidelijk dat het voor IT-medewerkers een pittige uitdaging is om al deze toepassingen te managen en samen te laten werken, om controle te houden.

[1] *https://www.cyberdb.co/database/usa/*

[2] *https://biztechmagazine.com/article/2019/03/rsa-2019-most-organizations-use-too-many-cybersecurity-tools*

Gefragmenteerd landschap van deeloplossingen

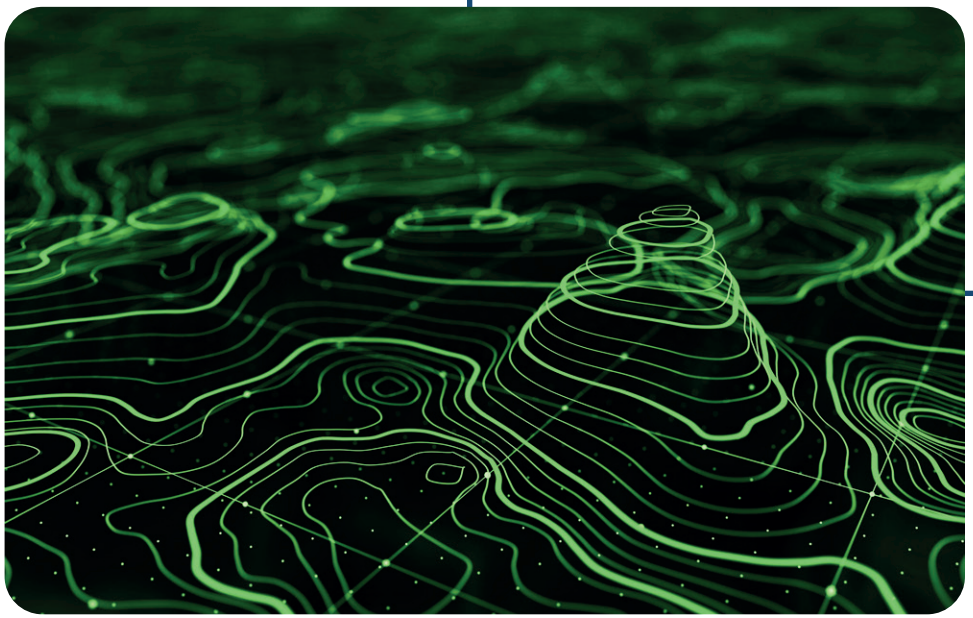
En dan is security nog maar één van de vele taken die IT-afdelingen hebben. IDC zegt dat budgetten voor IT weliswaar ieder jaar met 1 tot 3 procent stijgen, maar de capaciteit neemt niet of nauwelijks toe[3]. Uit onderzoek blijkt dat IT-afdelingen amper op de helft van alle alerts kunnen reageren[4]. Verder geeft 91 procent van executives in grote bedrijven aan integratie van oplossingen als hun grootste uitdaging te beschouwen[5].

Integratie is nodig om bedrijfsprocessen te stroomlijnen, productiviteit te verhogen en complexiteit te verminderen. De praktijk is er dus vaak één van een probleem signaleren en daar een oplossing bij kopen, met een gefragmenteerd landschap van deeloplossingen als gevolg.

[3] *https://www.lto.org/wp-content/uploads/2019/06/Tape-and-Cloud-Solving-Storage-Problems-in-the-Zettabyte-Era.pdf*

[4] *https://www.cisco.com/c/en/us/products/security/ciso-benchmark-report-2020.html*

[5] *https://enterprise-cio.com/news/2019/jun/25/more-tales-woe-enterprise-network-security-report-warns/*



Digitale dreiging neemt toe, de weerbaarheid moet omhoog

Dat hackers steeds geavanceerdere methodes gebruiken om in systemen binnen te dringen, maakt het security-vraagstuk zo mogelijk nog lastiger. Interpol waarschuwt dat het aantal cyberattacks duizelingwekkend snel stijgt en alarmerende vormen aanneemt[6]. Steeds vaker verschuift de aandacht van individuen en kleine bedrijven naar 'grote bedrijven, overheden en kritieke infrastructuur.'

Dat er zelfs 'statelijke actoren' zijn die zich met cybercrime bezighouden was voor minister van justitie Ferd Grapperhaus een van de redenen om de ontwikkeling van digitale dreiging in Nederland 'zorgwekkend' te noemen[7]. De digitale weerbaarheid moet omhoog, vindt de rijksoverheid. Het voorkomen van 'ontwrichting door incidenten binnen vitale processen' heeft dan ook de hoogste prioriteit binnen de Nederlandse Cybersecurity Agenda.

[6] *https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19*

[7] *https://www.rijksoverheid.nl/actueel/nieuws/2020/06/29/grapperhaus-ontwikkeling-digitale-dreiging-nederland-is-zorgwekkend*

Cisco als securityleider

Cisco staat van oudsher vooral bekend als netwerkspecialist, maar heeft zeker de laatste jaren enorm geïnvesteerd in security. Er is veel geld gestoken in research en development op het gebied van databescherming. Daarnaast kocht Cisco verschillende bedrijven aan, waardoor het nu over een portfolio beschikt dat een breed scala aan security-uitdagingen afdekt. Inmiddels wordt Cisco dan ook erkend als een van de koplopers op security-gebied[8].

Een platform zorgt voor overzicht en controle

De visie van Cisco is dat IT in staat moet worden gesteld weer grip op security te krijgen door de complexiteit te laten verdwijnen. Op de RSA Cybersecurity Conference werd 'cloud native' platform SecureX gepresenteerd als de belangrijkste oplossing hiervoor[9]. Dit is niet de zoveelste extra tool of een tool die alle andere vervangt. Het is meer een laag over bestaande tools (ook van andere vendoren naast Cisco) die daardoor werken als één geheel. Een dashboard dat op een overzichtelijke manier laat zien wat al die tools doen om dreigingen buiten de deur te houden.

Vaak wordt geroepen dat vereenvoudiging begint bij het verminderen van het aantal tools. Inmiddels worden al zeventig categorieën cybersecurity-producten onderscheiden[10]. Er gaan echter ook stemmen op die beweren dat al die tools blijkbaar noodzakelijk zijn om alle dreigingen het hoofd te bieden. Firewalls en virusscanners zijn belangrijk maar volstaan op zichzelf niet.

In de presentatie tijdens de RSA Conference, werd als voorbeeld genoemd dat door SecureX plots opvalt dat een tool veel dataverkeer richting China detecteert. Als de gebruiker daar normaal geen contact mee heeft, kan dat een verdachte stroom zijn. Zonder het platform was deze wellicht over het hoofd gezien. Nu kan direct worden ingegrepen waardoor de kans op uitval van kritische systemen drastisch afneemt.

[8] https://www.csoonline.com/article/3205926/ciscolive-and-cybersecurity.html

[9] https://duo.com/blog/cisco-named-a-leader-in-2019-forrester-zero-trust-wave

[10] https://blogs.cisco.com/security/the-firewall-the-foundation-for-a-robust-security-platform

Umbrella beschermt tegen geïnfecteerde sites

Als een opvallende datastroom naar een verdachte site gaat, is het mogelijk om deze site te blokkeren voor een complete organisatie. Het product dat Cisco hiervoor aanbiedt heet Umbrella. Deze toepassing is in feite een database met daarin ongekend grote aantallen adressen van malafide websites. De toepassing werkt als paraplu of schild tegen deze sites. Umbrella is te integreren in SecureX en werkt zo als één geheel.

Naast geïnfecteerde datastromen vormt identiteitsfraude een van de grootste cyberdreigingen[11]. Gebruikers doen die zich dan voor als iemand anders en verschaffen zich zo toegang tot gevoelige data. Met name de trend dat steeds meer mensen overal en altijd willen kunnen werken zoals zij dat het liefste willen, maakt organisaties kwetsbaarder. Er wordt immers steeds vaker op afstand met verschillende (mobiele) apparaten contact gemaakt met het bedrijfsnetwerk.

[11] *https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime*

Duo is de oplossing tegen identiteitsfraude

Multifactor authenticatie of MFA is hier de remedie tegen. Onder de naam Duo heeft Cisco een oplossing, die zodra iemand toegang tot het netwerkt vraag in actie komt. Na het invoeren van gebruikersnaam en wachtwoord volgt een extra check. Duo vraagt om bevestiging via de mobiele telefoon. De juiste identiteit wordt vastgesteld door gebruik van biometrische gegevens zoals een vingerafdruk of gezichtsherkenning.

Digitale dreiging neemt toe, de weerbaarheid moet omhoog

De visie van Cisco draait behalve om vereenvoudiging ook om het principe van Zero Trust. De opmars van die filosofie houdt gelijke tred met die van het aantal mobiele apparaten[13]. Uitgangspunt is dat je niets of niemand moet vertrouwen. Bedreigingen moeten op alle mogelijke niveaus te lijf worden gaan. Het portfolio van Cisco is daarom gericht op de bescherming van:

- Workloads
- Workforce
- Workspace

SecureX, Umbrella en Duo zijn belangrijke producten om deze uitgangspunten waar te maken. Het portfolio van Cisco bevat vanzelfsprekend meer softwarematige oplossingen, zoals Any Connect (veilig werken met bedrijfs- of privélaptop) en Avanced Malware protection, maar ook producten om het netwerk te segmenteren. Door compartimenten aan te leggen heeft een indringer niet meer via één deur toegang tot alles. In plaats daarvan wordt hij geconfronteerd met een stelsel aan ‘branddeuren’ en wordt het mogelijk om een geïnfecteerd compartiment te isoleren. De impact op bedrijfskritische systemen wordt op die manier tot het minimum beperkt.

Daarnaast biedt Cisco ook hardware die het veiligheidsniveau verhoogt. Switches en routers bijvoorbeeld, waarin security is ingebakken doordat ze netwerkverkeer regelen en bepalen welke gebruikers internettoegang krijgen.

[12] https://www.darkreading.com/perimeter/zero-trust-efforts-rise-with-the-tide-of-remote-working/d/d-id/1338343 https://www.darkreading.com/perimeter/zero-trust-efforts-rise-with-the-tide-of-remote-working/d/d-id/1338343

Krijg controle en bespaar tijd

De oplossingen van Cisco brengen dus het zicht terug op wat er allemaal op security-gebied op het netwerk gebeurt. Daardoor wordt bij verstoringen de responstijd flink verkort. Door gebruik van analysetools en Artificial Intelligence wordt het mogelijk dreigingen te voorspellen en vroegtijdig onschadelijk te maken. Zo krijgt IT weer controle en neemt de kans dat er daadwerkelijk iets mis gaat sterk af.

Doordat veel oplossingen bovendien gericht zijn op het automatiseren van beheers- en onderhoudstaken rond security, bespaart IT kostbare tijd die kan worden gebruikt om aan andere taken te besteden. Ook de aandacht voor gebruiksgemak ontlast IT-mensen flink. Zo kan Umbrella al binnen een paar minuten werken en kunnen gebruikers Duo zelf installeren.

Vraag om advies

Cisco heeft dus voor elke security-uitdaging een oplossing in huis. Als je wilt weten wat in jouw specifieke situatie het beste werkt om weer in control te zijn, kun je het beste advies inwinnen bij een van onze partners. Zij hebben veel kennis van onze producten en kunnen je helpen met advies. Ook zijn ze ervaren in het opstellen van stappenplannen en de implementatie van producten. Verder kunnen ze je ontzorgen met beheer en onderhoud of met trainingen.

Neem ook preventieve maatregelen los van techniek

Behalve voor techniek is het ook belangrijk om oog te hebben voor de mens. Individuen zijn immers ook vaak doelwit van cybercriminelen. Het is daarom belangrijk medewerkers ervan te doordringen van de sluipende gevaren. Veel bedrijven zetten al in op preventie met praktische maatregelen, zoals het aansporen van mensen om verschillende sterke wachtwoorden te gebruiken, software-updates direct uit te voeren en regelmatig back-ups te maken.[13]

Daarnaast is het belangrijk om een draaiboek klaar te hebben liggen voor als het toch mis gaat. Daarin kun je beschrijven hoe je in geval van nood systemen kunt (laten) herstellen.

Meer weten?

www.controleisalles.nl

[13] https://hetccv.nl/nieuws/overheid-en-bedrijfsleven-bundelen-krachten-tegen-cybercrime

Bedrijfsschade, informatiediefstal en imagoschade. De drie grootste cyberrisico's voor uw bedrijf en voor uw klanten. De afgelopen twee jaar liep 32% van de bedrijven wereldwijd dit soort schade op.

bron: interpolis.nl

Cisco Secure.
Controle is alles.