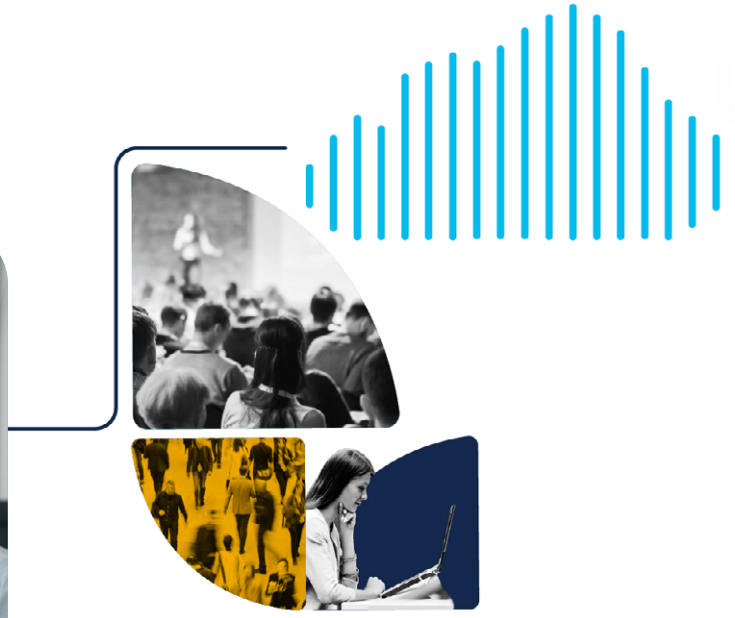
Whitepaper

Hoe je de strijd aan gaat tegen alle cyberrisico's: controle is alles

Cisco Secure. Controle is alles.



Hoe je er zeker van kunt zijn dat je netwerk altijd werkt: Controle is alles.

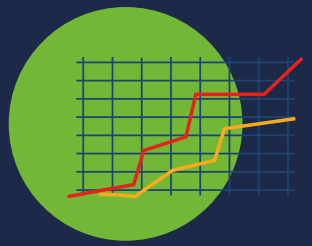
Digitale transformatie biedt businesskansen maar maakt ook kwetsbaar. De risico's van een cyberaanval worden volgens de Nederlandse overheid sterk onderschat. De digitale dreiging is inmiddels permanent en het gevaar is door covid-19 alleen maar toe genomen omdat het nu veel drukker is in 'de digitale ruimte', wat betekent dat de impact van uitval van ICT-systemen groter is dan ooit tevoren. Controle is daarom belangrijker dan ooit. Security is geen bijzaak, maar heeft invloed op je core business. In dit whitepaper leesje meer over hoe je door meer controle je digitale weerbaarheid kunt vergroten, zodat je netwerk áltijd veilig is.

Je denkt vaak 'dat overkomt mij niet' maar twee recente praktijkvoorbeelden maken duidelijk dat de kans om slachtoffer te worden van cybercriminaliteit zeker niet denkbeeldig is. De universiteit Maastricht betaalde in december 2019 twee ton aan losgeld, nadat hackers ransomware uitrolden. Zij hadden toen al maanden in het netwerk gezeten. De gemeente Lochem kroop datzelfde jaar door het oog van de naald, toen bleek dat na een hack maandenlang gegevens van medewerkers en raadsleden waren bekeken. Persoonsgegevens van inwoners vielen niet ten prooi aan cybercriminelen, maar Lochem was wel twee ton kwijt aan herstel.

Kosten van schade door cybercriminaliteit lopen elk jaar op en komen in 2021 naar verwachting uit op 6 biljoen dollar. In 2015 was dit nog 3 biljoen dollar.

De schade door ransomware zal in 2021 20 miljard dollar zijn, dit was 325 miljoen in 2015.

Cybersecurity uitgaven gaan naar meer dan 1 biljoen dollar gerekend over de periode 2017 -2021. In 2004 was de wereldwijde markt nog 3,5 miljard dollar waard, in 2017 120 miljard.



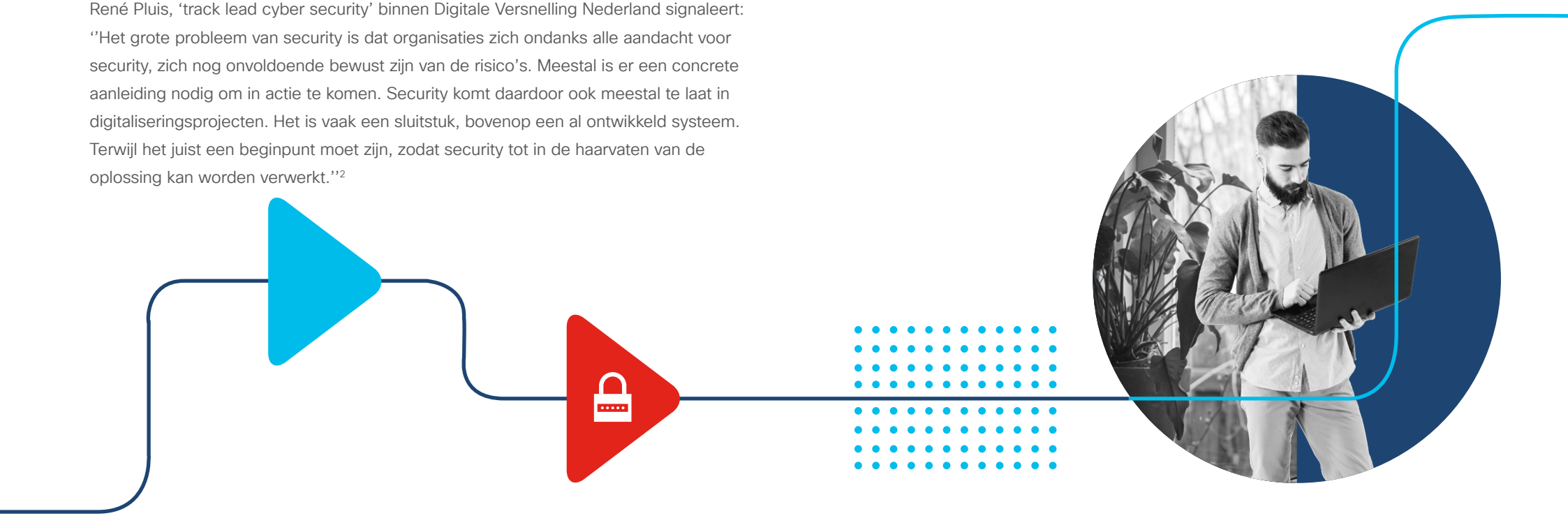
Bron: https://www.cybercrimeinfo.nl/cybercrime/395174_cybercrime-feiten-cijfers-en-voorspellingen-2019-tot-2021

Meer mensen werken op afstand, dus neemt de dreiging toe

Uit deze spraakmakende gevallen blijkt hoe groot de risico's zijn en met de uitbraak van de covid-19 pandemie zijn die alleen maar toegenomen. We werken meer op afstand en zijn dus afhankelijker van ICT-systemen. Volgens een rapport van de rijksoverheid laat de digitale weerbaarheid in ons land te wensen over en worden risico's onderschat.[1]

René Pluis, 'track lead cyber security' binnen Digitale Versnelling Nederland signaleert: ''Het grote probleem van security is dat organisaties zich ondanks alle aandacht voor security, zich nog onvoldoende bewust zijn van de risico's. Meestal is er een concrete aanleiding nodig om in actie te komen. Security komt daardoor ook meestal te laat in digitaliseringsprojecten. Het is vaak een sluitstuk, bovenop een al ontwikkeld systeem. Terwijl het juist een beginpunt moet zijn, zodat security tot in de haarvaten van de oplossing kan worden verwerkt.''[2]

De overheid noemt daarom ook de noodzaak om met name kritieke infrastructuren, informatiesystemen en belangrijke online diensten goed te beveiligen tegen cyberdreigingen. Hacks worden tegenwoordig gepleegd door goed georganiseerde bendes, die innovatie technieken inzetten zoals deep fake. Daardoor kun je ten onrechte denken een bekende aan de telefoon te hebben. Soms zitten er staten achter een aanval die aan politieke spionage of bedrijfsspionage doen. Kapitaalkrachtige organisaties zijn hoe dan ook een geliefd doelwit.



[1] *https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2020/juni/29/csbn-2020/CSBN+2020.pdf*
[2] *https://www.cisco.com/c/nl_nl/solutions/digitale-versnelling-nederland/Security-rode-draad-DVN/index.html*

Bewustwording gevaren groeit niet mee met de afhankelijkheid van ICT

Het eerder genoemde rapport stelt dat het niet alleen overheidsinstanties zijn die hun digitale veiligheid niet op orde hebben. Dit geldt net zo goed voor bedrijven en instellingen. De Onderzoeksraad Voor Veiligheid (OVV) constateert bijvoorbeeld ‘dat de bewustwording van het risico op ICT-uitval in ziekenhuizen niet in gelijke mate is meegegroeid met de toegenomen afhankelijkheid van ICT.’[3]

[3] *https://www.onderzoeksraad.nl/nl/media/attachment/2020/2/13/patientveiligheid_bij_ict_uitval_in_ziekenhuizen.pdf*

Mens vaak de zwakste schakel

Wat verder naar voren komt in het rapport, is dat organisaties mensen er ondanks trainingen niet van kunnen weerhouden op verkeerde linkjes te klikken. Ook valt te lezen dat beveiligingsupdates vaak niet worden geïnstalleerd, ook niet als ze al jaren beschikbaar zijn. Dat hackers maandenlang hun gang kunnen gaan blijkt overigens geen uitzondering, gemiddeld duurt het 56 dagen voor een inbreuk wordt gemerkt. Dat is trouwens al een verbetering ten opzichte van de 78 dagen het jaar ervoor.[4]

[4] *https://content.fireeye.com/m-trends/rpt-m-trends-2020*

Risico's nemen toe

Er zijn nog meer trends aan te wijzen die veiligheidsrisico's vergroten:[5]

- Globalisatie.
- Digitale transformatie.
- Uitdijend applicatielandschap.
- Meer (mobiele) apparaten.
- Meer vermenging van thuis en op kantoor werken

Als gezegd zijn we sinds covid-19 meer thuis gaan werken. Productiviteit heeft vaak voorrang boven veiligheid. Werk- en privégebruik van apparaten loopt vaak door elkaar zonder dat er goed zicht op is. Los hiervan zijn organisaties vaak wereldwijd actief, sluiten ze meer locaties aan en dus ook meer gebruikers en apparaten. Het Internet of Things explodeert inmiddels, er is een gigantische toename van verbonden apparaten die ons werk uit handen nemen. Maar een hacker ziet elk apparaat als een toegangspoort tot je netwerk. Agentschap Telecom hield 22 veelgebruikte apparaten tegen het licht en ontdekte dat 17 niet digitaal veilig waren. Het ging hierbij om consumentenapparaten, maar daarbij zaten er ook die door bedrijven worden gebruikt, zoals routers, slimme camera's, slimme sloten en thermostaten.[6]

Door digitale transformatie gaan organisaties aan de slag met vernieuwende technologieën voor bijvoorbeeld analytics. Ook gebruiken ze steeds meer apps die taken automatiseren. Vaak bouwen ze zelf voortdurend apps om aan de vraag van de business te voldoen, al dan niet door gebruik van containertechniek. Het gevolg is dat steeds meer workloads richting de cloud verschuiven.

Er ontstaan verbindingen tussen organisaties en clouds, tussen clouds onderling. Het wordt ingewikkeld om in de gaten te houden hoe datastromen precies lopen. Door gebrek aan IT-capaciteit verliezen organisaties grip op hun eigen digitale ecosysteem. Ook is lang niet altijd zicht op het gebruik van mobiele devices. Mensen willen overal en altijd kunnen werken met het apparaat van hun keus, maar zakelijk en privégebruik gaat hierdoor wel door elkaar lopen. Ook dat maakt organisaties extra kwetsbaar.

[5] *https://www.cisco.com/c/m/en_us/solutions/enterprise-networks/networking-report.html?ccid=cc001244&oid=rpten018612#*
[6] *https://www.rijksoverheid.nl/actueel/nieuws/2019/09/25/digitale-veiligheid-slimme-consumentenapparaten-niet-op-orde*

Naar een oplossing: hoe krijg je alles onder controle?

Kernvragen die je moet stellen om je weerbaarheid te vergroten zijn:

- Heb ik een goed beeld van alle hard- en software die deel uitmaakt van mijn netwerk?
- Beschik ik over actuele informatie over kwetsbaarheden in mijn IT-infrastructuur?
- Heb ik inzicht in hoe het staat met security updates?
- Beschik ik over een goede back-up strategie?
- Is mijn netwerk gesegmenteerd?
- Heb ik inzicht in wat er op mijn netwerk gebeurt, kan ik snel genoeg detecteren dat er iets mis en kan ik dan op tijd ingrijpen?
- Zijn bedrijfskritische toepassingen (mijn 'kroonjuwelen') extra beschermd?
- Zijn mijn medewerkers goed genoeg getraind om de juiste actie te ondernemen tegen dreigingen?

Recente statistieken wijzen uit dat het antwoord (te) vaak 'nee' is.[7] Zo ontbreekt het in veel gevallen aan genoeg IT-capaciteit, waardoor slechts op een beperkt aantal alerts wordt gereageerd.

[7] *https://www.thesslstore.com/blog/cyber-security-statistics/#cyber-security-statistics-what-organizations-are-investing-in-cyber-security*

Segmenteren en voortdurend inzicht in je netwerk is belangrijk

Een gesegmenteerd netwerk heeft ook lang niet iedereen, omdat het tamelijk complex is om dit voor elkaar te krijgen.[8] In een niet-gesegmenteerd netwerk kunnen alle computers met elkaar 'praten'. Hierdoor is het voor virussen mogelijk om van één computer automatisch naar de volgende te springen en zo in korte tijd je hele netwerk te besmetten. Door virtuele groepen te maken in je netwerk, kun je met een firewall het verkeer tussen deze netwerken controleren of blokkeren. Zo sluit je een incident als het ware op in een deel van je netwerk, je legt digitale branddeuren aan.

Segmenteren is ook een goede manier om dreigingen van binnenuit tegen te gaan, want vaak is een beveiligingsstrategie er vooral gericht op dreigingen van buiten. Als iemand eenmaal binnen is, wordt die aanwezigheid als 'vertrouwd' beschouwd, waardoor hackers dus lang onopgemerkt blijven.

Volgens René Pluis (Digitale Versnelling Nederland) is het voor een goede aanpak van security essentieel om voortdurend inzicht te hebben in wat er precies op het netwerk gebeurt. ''Tegen wat je niet ziet kan je je niet beveiligen'', zegt hij. ''Bovendien moet een aanval direct worden gedetecteerd om de bewegingsruimte van aanvallers zoveel mogelijk te beperken en de schade te minimaliseren."

[8] *https://www.blogit.nl/netwerksegmentatie-7-stappen/*

Het netwerk als brandmelder

In de visie van Cisco moet het netwerk een centrale rol spelen in het verkrijgen van inzicht: ‘the network as a sensor’. Het netwerk is als het ware een ‘brandmelder’, want elke aanval loopt via het netwerk. Op die manier ben je dus niet steeds brandjes aan het blussen, maar doe je aan brandpreventie.

Dit netwerk is gebouwd op een ‘zero trust’ strategie.[9] Dit houdt in dat je er vanuit gaat dat je niets of niemand volledig kunt vertrouwen en je security op elk niveau van je infrastructuur inbouwt, tot diep in de haarvaten. Cisco maakt onderscheid tussen:

1. Workforce

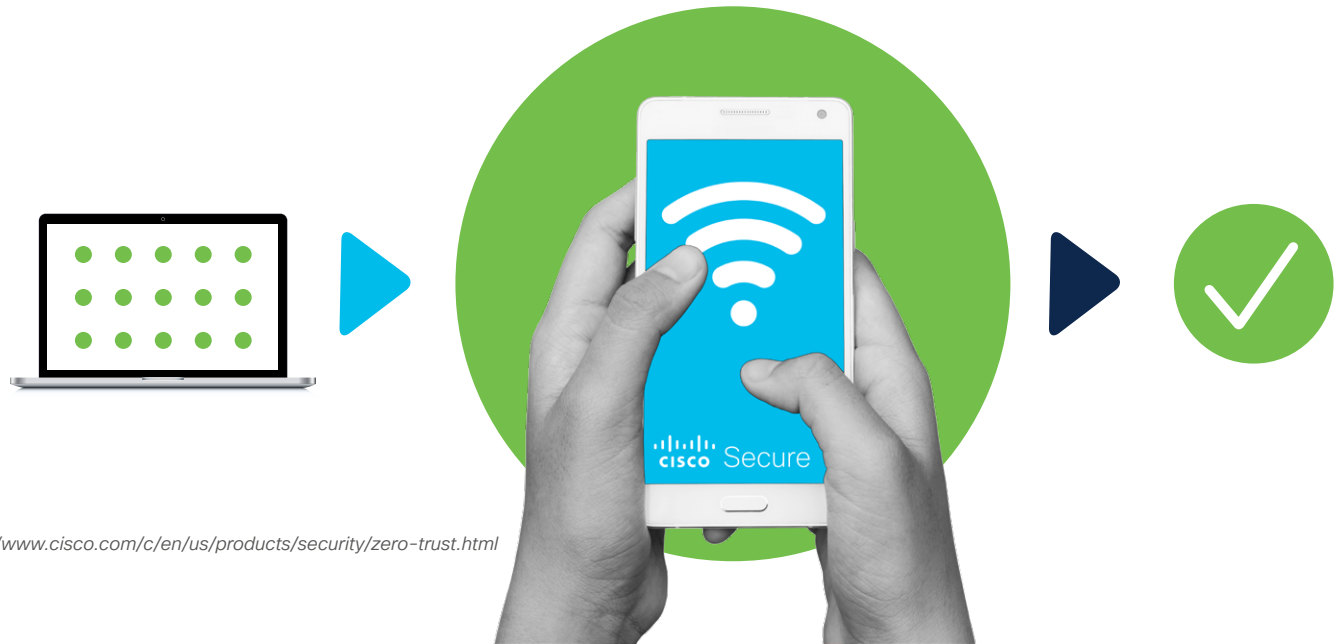
Security op het niveau van je werknemers houdt bijvoorbeeld in dat je altijd om tweevoudige identificatie vraagt, bijvoorbeeld een wachtwoord en een vingerafdruk. Zo weet je zeker dat degene die om toegang tot je netwerk vraagt niet stiekem iemand anders is. Hierbij hoort ook, dat je alleen goedgekeurde apparaten en apps toelaat.

2. Workloads

Als het gaat om workloads, moet je dus zicht krijgen op hoe data stroomt. Je moet ook apps kunnen segmenteren, zodat verkeer tussen apps niet tot besmetting leidt. Als er toch iets mis gaat, moet je systeem je vroegtijdig waarschuwen, zodat je verdachte stromen kunt blokkeren.

3. Workplace

Bij workplace gaat het om het uitrollen van beleid, denk aan het aanmaken van profielen. Je kunt dan aan verschillende gebruikers verschillende rechten toekennen, zodat niet iedereen bij gevoelige data kan. Ook het segmenteren van je netwerk valt hieronder, evenals het continue monitoren van je netwerk, snelle detectie van inbreuken en snelle respons.



[9] *https://www.cisco.com/c/en/us/products/security/zero-trust.html*

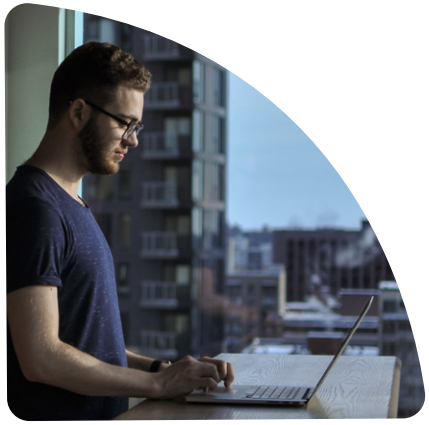
De bouwstenen van de Cisco-strategie

De security van Cisco is dus gebouwd op drie pijlers:

1. Continue zichtbaarheid
2. Zero Trust Access
3. Constante bescherming

Cisco noemt dit Security by design.[10] Daarmee wordt bedoeld dat security ingebakken moet zijn, in elke laag van je IT-infrastructuur, in elk apparaat. Cisco is wereldwijd bekend als leverancier van routers en switches maar het security portfolio is veel uitgebreider dan dat. Belangrijk in de Cisco-strategie is de platform benadering, onder de noemer DNA Center.[11] Daarbij krijg je via een dashboard helder inzicht in je IT-ecosysteem. Netwerkmanagement wordt eenvoudiger en kost minder tijd. Je veiligheid is geregeld vanuit één punt; door integratie heb je geen last meer van al die door verschillende fabrikanten geleverde apps met elk hun eigen beveiligingsmethode.

Je ziet op deze manier in één oogopslag hoe het met de veiligheid van apparaten en apps is gesteld. De oplossing neemt taken over, zoals het uitrollen van profielen en het doorvoeren van beveiligingsupdates. Door gebruik van artificial intelligence is een platform in staat om te leren en nieuwe dreigingen te herkennen. Op die manier ontvang je een signaal dat je actie moet ondernemen, nog voor er daadwerkelijk schade is toegebracht. Het netwerk wordt voortdurend gemonitord. Niet alleen dreigingen worden in de gaten gehouden, het systeem controleert ook of alle onderdelen nog optimaal functioneren.



[10] *https://discover.cisco.com/en/us/enterprise-networks/network-security-guide/security-by-design#*
[11] *https://www.cisco.com/c/en/us/products/cloud-systems-management/dna-center/index.html*

Weer ‘in control’

Door deze benadering, uitgaande van Zero Trust en continue zichtbaarheid, krijg je dus weer grip op je netwerk. Je weerbaarheid tegen dreigingen neemt toe, je kunt ze elimineren al voor ze schade toebrengen. Je beperkt de kans op downtime tot het minimum. Dat zorgt niet alleen voor een betere gebruikerservaring maar maakt je ook wendbaarder. Je kunt sneller inspelen op vragen van de business en kunt innovatiever zijn. Ook bespaar je kosten door vereenvoudiging van processen en door automatisering. Tot slot kun je doordat je data goed beschermd is er zeker van zijn dat je aan privacywetgeving voldoet. Kortom: Met een netwerk als brandmelder heb je alles onder controle. Blussen is verleden tijd.

Meer weten over security?
Bezoek controleisalles.nl

76 procent van de inspanningen van security professionals is gericht op ontdekking en bestrijding in plaats van preventie.	Elke dag is er om de 3 tot 4 secondes een DDos aanval.	64 procent van alle professionals weet niet precies hoeveel apparaten en web apps hun organisatie in gebruik heeft.
60 procent van de IT-professionals vindt dat budgetten voor cybersecurity tekort schieten.	Drie keer per minuut gaat er een phishing site live.	60 procent heeft geen goed inzicht in wie allemaal toegang heeft tot gevoelige informatie.
62 procent van de cybersecurityteams in organisaties zijn onderbezet, 57 procent van de teams heeft vacatures openstaan.	Oplichting door deepfake is dit jaar naar schatting goed voor 250 miljoen dollar schade.	Ongeveer de helft van de schade door cyber incidenten wordt door ‘eigen’ personeel veroorzaakt.

Bron: https://www.thesslstore.com/blog/cyber-security-statistics/#cyber-security-statistics-what-organizations-are-investing-in-cyber-security

Cisco Secure.

Controle is alles.