Cybersecurity trendrapport

Hoe risicobewust zijn Nederlandse organisaties?

digitale versnelling nederland

Hoe houden we Nederland digitaal in de top?

Nederland behoort tot de top-3 landen in Europa als het gaat om de kracht van de digitale economie. Uit de jaarlijkse, toonaangevende Digital Economy and Society Index (DESI) van de Europese Unie blijkt dat Nederland voorop loopt op het gebied van digitale infrastructuur, het gebruik van digitale toepassingen, online vaardigheden van inwoners en de mate en wijze waarop het bedrijfsleven digitaal actief is. De vraag is: hoe houden we Nederland digitaal in de top?

Met de Digitale Agenda stimuleert het kabinet de verdere digitalisering van de Nederlandse economie. Eén van de speerpunten in de agenda is te zorgen dat leerlingen én leraren digitaal vaardiger worden gemaakt, maar het tempo waarin dat gebeurt moet hoger om de veranderingen bij te kunnen houden. Het Internet of Things (IoT), Artificial Intelligence, Machine Learning: digitale veranderingen worden al volop toegepast en zijn voor iedereen relevant. Iedereen moet daarom enig begrip hebben van 'hoe het nou werkt.' Basiskennis over deze technologische ontwikkelingen en zaken als privacy en cybersecurity is op zijn minst nodig. Toch blijkt uit ons onderzoek dat **meer dan één op de drie beslissers van Nederlandse organisaties vindt dat ze over onvoldoende kennis beschikken op het gebied van cybersecurity.**

Met de Networking Academy (NetAcad), een MVO-onderwijsprogramma waarmee Cisco studenten en werknemers verrijkt met digitale vaardigheden, waaronder op het gebied van cybersecurity, draagt Cisco bij aan de Digitale Agenda van de overheid. **De afgelopen twintig jaar heeft NetAcad al miljoenen studenten met IT-vaardigheden verrijkt. De doelstelling is om in 2023 wereldwijd zo'n 3 miljoen studenten per jaar van digitale vaardigheden te voorzien.** Als onderdeel van Cisco's investeringsprogramma 'Digitale Versnelling Nederland' spraken we in 2017 de ambitie uit om binnen vier jaar impact te maken in de levens van 57.000 Nederlanders. Op dit moment staat de teller op meer dan 40.000. Tot 2020 gaan we nog meer dan 17.000 mensen voorzien van de juiste digitale vaardigheden.

Gezien de uitkomsten van dit trendrapport is dat hard nodig; de kennis op het gebied van cybersecurity van beslissers in Nederlandse organisaties laat namelijk te wensen over. **Zo is ruim één op de drie bijvoorbeeld niet bekend met de term 'Two Factor Authentication' en roepen ook termen zoals 'social engineering, 'adware' en 'ransomware' bij meer dan één op de vier beslissers vraagtekens op.** Dit rapport geeft u een beeld van de kennis en het bewustzijn over cybersecurity bij beslissers van Nederlandse organisaties. Naast dat het rapport antwoord geeft op de vraag in hoeverre cybertermen bekend zijn, biedt het rapport ook inzicht in hoe vaak Nederlandse organisaties slachtoffer zijn geworden van cybercrime en welke maatregelen er worden genomen om het te voorkomen. Ook biedt het rapport aan de hand van drie interviews inzicht in hoe cybersecurity-experts aankijken tegen de uitdagingen om cybercrime tegen te gaan en het belang van goede scholing op het gebied van digitale geletterdheid.

Ik wens u veel leesplezier!

Rik Bleeker
CSR Country Engagement Manager voor de Benelux

Risicoperceptie en slachtofferschap van cybercrime

Digitale veiligheid is niet langer een ondergeschoven kindje bij Nederlandse bedrijven. Bij maar liefst 63% van de organisaties staat cybersecurity hoog op de agenda. Toch geeft meer dan 35% van de beslissers van diezelfde organisaties aan dat ze onvoldoende op de hoogte zijn van cybersecurity. Bovendien beoordeelt één op de vier beslissers ook het kennisniveau van hun eigen medewerkers als ‘beperkt’ of zelfs ‘zeer beperkt’.

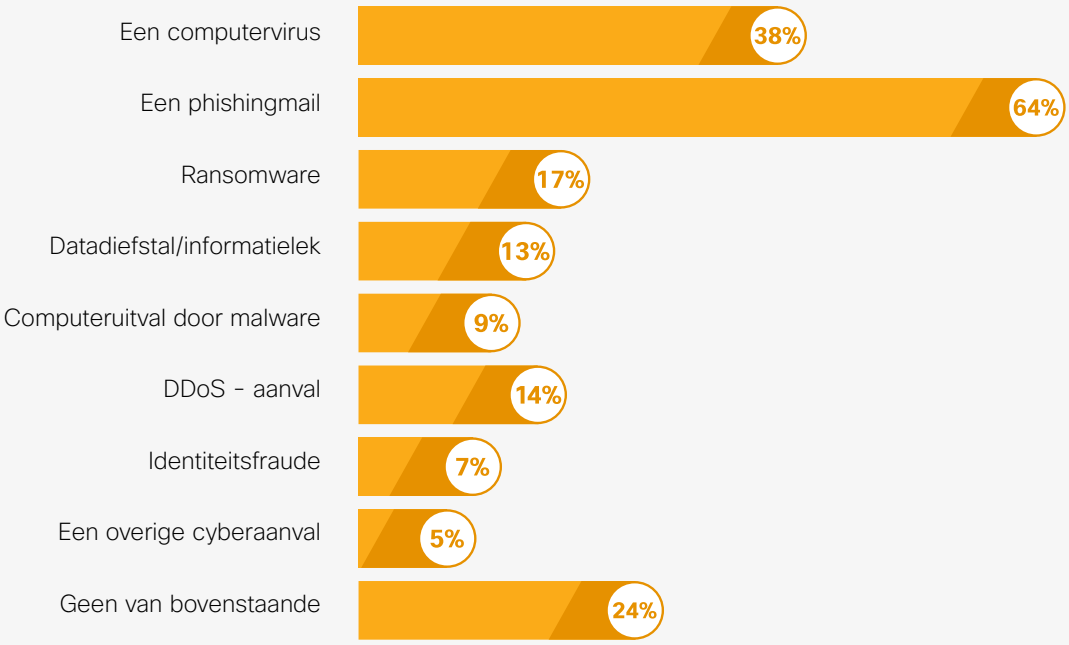
76%

van de beslissers van Nederlandse organisaties geeft aan wel eens slachtoffer te zijn geweest van een cyberaanval tijdens het werk.

Drie op de vier ondervraagden heeft weleens te maken gehad met een cyberaanval op de werkvloer. Zo werd 64% tijdens het werk benaderd met een phishingmail, heeft 37% wel eens een computervirus gehad en werd 17% getroffen door ransomware, de malware die uit is op losgeld. Andere genoemde cyberaanvallen zijn DDoS-aanvallen (14%), datadiefstal (13%) en identiteitsfraude (7%). Bijna een kwart van de beslissers heeft nog nooit een cyberaanval meegemaakt op de werkvloer.

Cyberaanvallen op de werkvloer

Heeft u tijdens uw werk weleens te maken gehad met een van de volgende zaken?

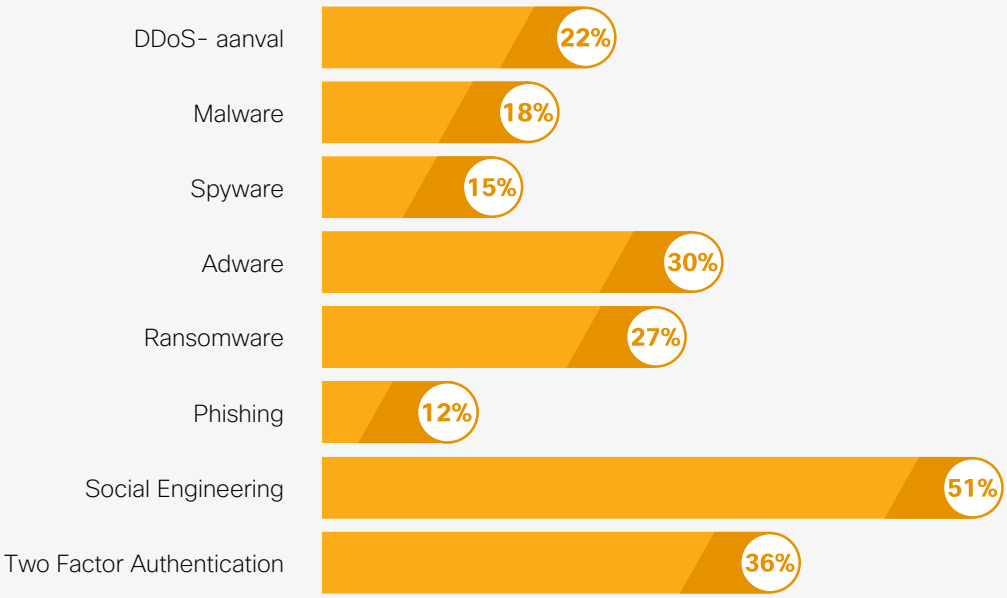


Cyberterminologie onvoldoende op de radar

Hoewel Nederlandse bedrijven veelvuldig worden getroffen door cyberaanvallen, zijn de termen om deze gevaren aan te duiden nog nauwelijks bekend. Zo heeft meer dan de helft nog nooit van social engineering gehoord; de hacking techniek waarbij de aanvaller probeert om individuelen zodanig te manipuleren dat ze acties ondernemen of vertrouwelijke informatie openbaar maken. En dat terwijl beslissers volgens het ‘Verizon 2019 Data Breach Investigations Report’ juist steeds vaker het specifieke doelwit zijn bij hackpogingen. Vooral bij leidinggevenden die toegang hebben tot allerlei gevoelige bedrijfsgegevens, is de kans dat ze worden getroffen door een aanval via social engineering de afgelopen jaren flink toegenomen. Daarnaast is 36% van de Nederlandse beslissers niet bekend met Two Factor Authentication, de authenticatiemethode waarbij je twee stappen succesvol moet doorlopen om ergens toegang tot te krijgen, zoals het invullen van een gebruikersnaam en wachtwoord, in combinatie met een sms-code. Two Factor Authentication is echter een beproefde manier om accounts te behoeden voor een cyberinbraak door derden.

Mate van onbekendheid van cybersecurity-gerelateerde termen

In hoeverre zijn onderstaande zaken bij u onbekend?



Social engineering

Social engineers zijn vaak afhankelijk van de gewilligheid van een persoon, maar jagen ook op de zwakheden van mensen. Een aanvaller kan bijvoorbeeld een bevoegde werknemer bellen met een dringend probleem die onmiddellijke toegang tot het netwerk vereist. Enkele voorbeelden van social-engineeringaanvallen zijn pretexting (wanneer een aanvaller een individu belt en leugens verspreidt om toegang te krijgen tot bepaalde gegevens), tailgating (wanneer een aanvaller een bevoegd persoon naar een beveiligde locatie volgt) en quid pro quo (wanneer een aanvaller persoonlijke informatie vraagt aan een partij in ruil voor iets, zoals een gratis geschenk). Wilt u helemaal op de hoogte zijn alle cyberaanval-methodes? Volg dan **de gratis NetAcad-cursus Introduction to Cybersecurity.**

Binnen het thema van cybersecurity krijgt ‘social engineering’ terecht veel aandacht. Want hoewel je bij beveiliging vooral aan technologie denkt, is de ‘menselijke firewall’ van wezenlijk belang. Toch blijkt dat veel beslissers nog nauwelijks op de hoogte zijn van deze vorm van cybercrime.

Joris den Bruinen

Algemeen directeur van
The Hague Security Delta

The Hague Security Delta (HSD) het nationale veiligheidscluster, waarin bedrijven, overheden en kennisinstellingen samenwerken aan innovatieve veiligheidsoplossingen. Vraagstukken op het gebied van cybersecurity worden steeds complexer. Volgens Joris den Bruinen, algemeen directeur van HSD, is kennisdeling over cybersecurity daarom essentieel: “We beschikken in Nederland over voldoende kennis over cybersecurity, maar het komt nog niet altijd bij de juiste organisaties, teams of personen terecht.”

Kennis op verschillende niveaus

Over het algemeen zou de kennis op drie verschillende bedrijfsniveaus moeten worden geborgd. Te beginnen op beslisniveau: “Beslissers moeten precies weten waar de kansen en bedreigingen liggen van cybersecurity in relatie tot de kernactiviteiten van hun organisatie. Je moet voorkomen dat ze besluiten moeten nemen over iets wat ze niet goed begrijpen en doorgronden. Als de cybersecuritykennis in de top van een organisatie daarom niet geborgd is, dan heb je een probleem,” aldus Den Bruinen. Op het tweede niveau – het niveau van de CISO en de IT-afdeling – moet er volgens Den Bruinen niet alleen voldoende kennis geborgd zijn, belangrijker nog is dat zij de kennis op heldere wijze kunnen doorvertalen naar het beslisniveau. “IT’ers en beslissers moeten dezelfde taal spreken. Alleen dan weten beslissers welke gevolgen cybersecuritykansen en -bedreigingen kunnen hebben op de kernactiviteiten van hun organisatie.” Tevens moet er op het derde niveau – bij alle medewerkers binnen de organisatie – een bepaalde basiskennis worden gecreëerd op het gebied van cybersecurity. Den Bruinen neemt phishing als voorbeeld: “Er zijn in Nederland voldoende initiatieven om de kennis en awareness rondom phishingmails te stimuleren, je moet er alleen voor zorgen dat deze kennis op ieder niveau van je organisatie terechtkomt.”

“Als de kennis van cybersecurity in de top van je organisatie niet geborgd is, dan heb je een probleem.”

Specialisten van de toekomst

Ook het opleiden van de cybersecurity-specialisten van de toekomst vereist volgens Den Bruinen voldoende kenniscirculatie. “De overheid is hard op weg om digitale geletterdheid versneld op te nemen in het curriculum, maar heeft daarbij de hulp van het bedrijfsleven hard nodig. Dat kan alleen wanneer er voldoende kennis wordt gedeeld. Initiatieven waarbij het onderwijs, overheid en het bedrijfsleven nauw samenwerken, zoals P@CT en NetAcad, zijn daarvan het levende bewijs.”

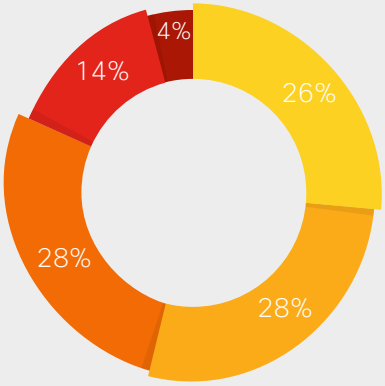
Weinig zorgen over online veiligheid op de werkvloer

Hoewel drie op de vier beslissers wel eens te maken heeft gehad met een vorm van cybercrime, maken ze zich over het algemeen nauwelijks zorgen over hun online veiligheid op de werkvloer. Meer dan de helft maakt zich geen zorgen over de veiligheid van bedrijfsdata (54%), de veiligheid van klantdata (53%), de veiligheid van personeelsgegevens (54%) of dat iemand zich online voordoet als zijn of haar bedrijf (55%).

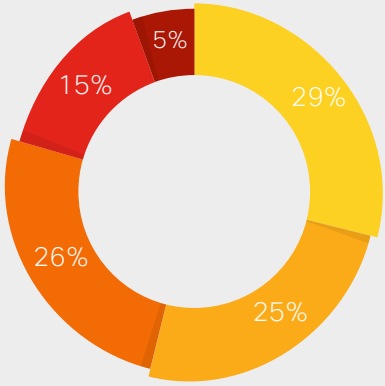
Deze cijfers komen overeen met de uitkomsten uit het Nationaal Cybersecurity Bewustzijnsonderzoek 2018, uitgevoerd door NCTV en Alert Online. Ook uit dit onderzoek blijkt dat Nederlanders zich niet heel druk maken over cybercrime en ons veiliger wanen dan dat we daadwerkelijk zijn.

Zorgen om online veiligheid op de werkvloer

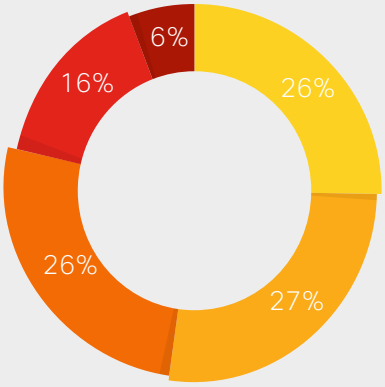
In hoeverre maakt u zich zorgen over de volgende zaken?



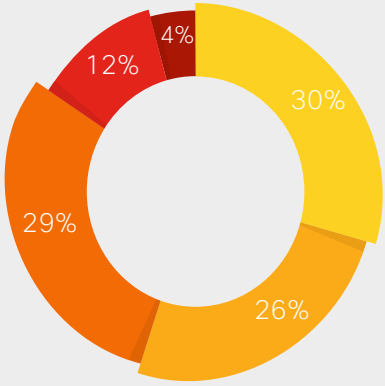
De veiligheid van de bedrijfsdata



De veiligheid van de personeelsgegevens



De veiligheid van de klantdata



Dat iemand zich online voordoet als mijn bedrijf

Zeer klein | Klein | Niet klein niet groot | Groot | Zeer groot

26%

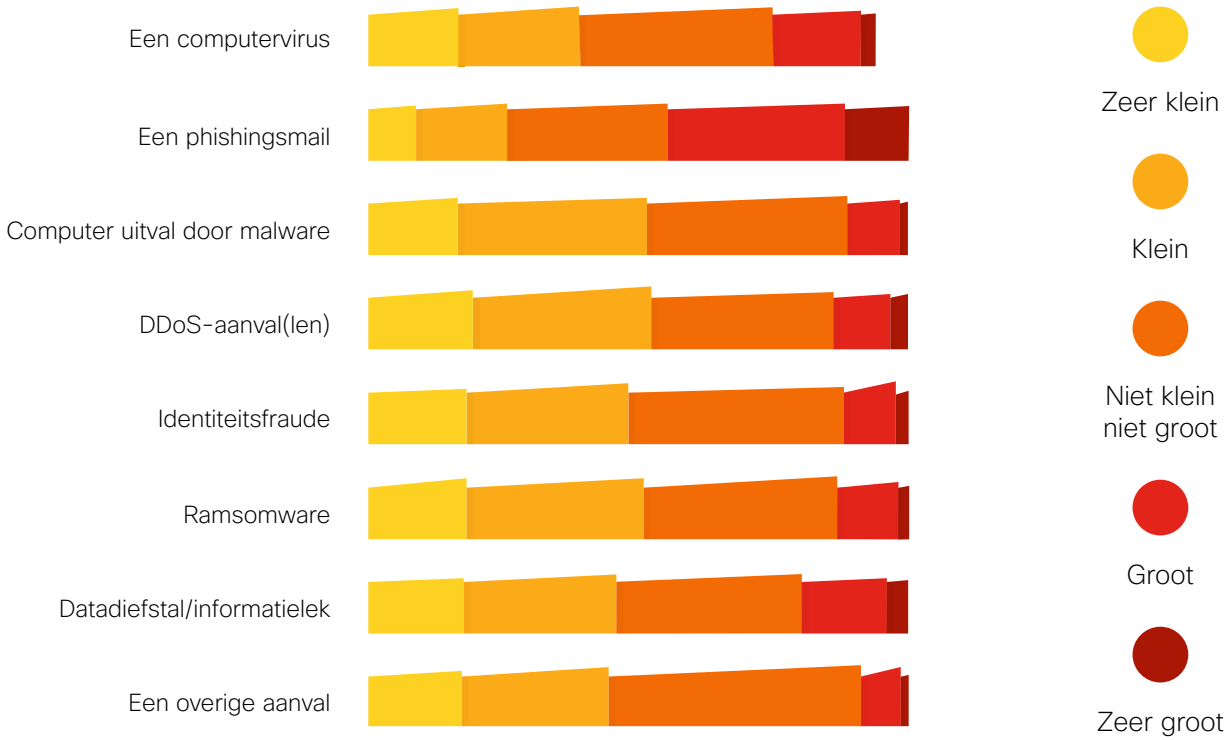
van de beslissers acht de kans klein dat ze tijdens hun werk een phishingmail ontvangen, terwijl 64% daadwerkelijk met phishing werd geconfronteerd.

Kans op slachtofferschap van cybercrime wordt laag ingeschat

Dat Nederlandse organisaties zich relatief weinig zorgen maken over hun digitale veiligheid op de werkvloer, is waarschijnlijk omdat ze niet verwachten te worden getroffen door cybercrime. Met name de kans op het ontvangen van phishingmails wordt laag ingeschat; ruim één op de vier beslissers acht de kans klein dat ze tijdens hun werk een phishingmail ontvangen, terwijl 64% heeft aangegeven dat ze tijdens hun werk daadwerkelijk met een phishingmail werden geconfronteerd.

De kans op (computer)schade door alle andere vormen van cybercrime, zoals een virus, een DDoS-aanval of identiteitsfraude, wordt niet hoger dan 20% ingeschat, en dat terwijl 76% van de beslissers heeft aangegeven dat ze op de werkvloer weleens te maken hebben gehad met één van diezelfde vormen van cybercrime.

Hoe groot schat u de kans in dat u tijdens uw werk te maken krijgt met de volgende zaken?



Bart van Rijn

CISO en Functionaris gegevensbescherming bij UMC Utrecht

Digitale bedreigingen zijn aan de orde van de dag. In de zorgsector is dat niet anders, zo weet Bart van Rijn, CISO (Chief Information Security Officer) en Functionaris gegevensbescherming bij UMC Utrecht.

Duidelijke regels en voorwaarden

Van Rijn houdt zich dagelijks bezig met de informatiebeveiliging binnen het UMC en stelt dat de digitalisering van de samenleving zowel kansen als uitdagingen met zich mee brengt voor de zorgsector: “Digitalisering binnen ziekenhuizen neemt een enorme vlucht, denk aan zorg op afstand, Internet of Things-oplossingen of zelfdiagnose via apps. Om al deze ontwikkelingen in goede banen te leiden, moeten er binnen zorgorganisaties duidelijke regels en voorwaarden worden gecreëerd op het gebied van cybersecurity. Binnen het UMC worden daarom uitgebreide campagnes gehouden om de awareness rondom privacy en security te vergroten. Bovendien krijgt iedere nieuwe medewerker van het UMC een cursus Digitaal Werken, zodat medewerkers bewust worden van cybergevaren en kennis en vaardigheden ontwikkelen om veilig digitaal te werken.”

“Het aanpakken van phishing blijft een enorme uitdaging.”

Phishing

Een andere uitdaging die bij ziekenhuizen speelt is het beveiligen van patiëntgegevens. Ziekenhuizen zijn een aantrekkelijk doelwit voor hackers, mede doordat ziekenhuizen vaak gebruik maken van oude software en beveiligingssystemen. Zo stelt Van Rijn dat het bestrijden van phishing tot een van de grootste uitdagingen behoort op het gebied van cybersecurity voor zorgorganisaties. “Bij het UMC bestrijden we dit enerzijds aan de hand van techniek. Onze spamfilter houdt ongeveer 7 keer zoveel mails tegen, dan dat het er doorlaat.”

Anderzijds speelt ook kennisontwikkeling en bewustwording op dit gebied een enorm grote rol. “We kunnen cybersecurity voor zo’n 10 procent op orde brengen via techniek, voor 20 procent door goede regels en voorwaarden op te stellen, maar 70 procent van het toepassen van cybersecurity is afhankelijk van voldoende educatie en alertheid.”

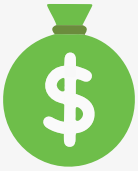
Internationaal slachtofferschap van cybercrime

Waar 76% van de beslissers van Nederlandse organisaties aangeven al een keer te zijn getroffen door een cyberaanval, lijkt het slachtofferpercentage internationaal nóg hoger te liggen. Uit het jaarlijkse, internationale Cisco Cybersecurity Report, uitgevoerd onder meer dan 3.000 security-experts verdeeld over 18 Europese landen – waaronder ook Nederland – blijkt namelijk dat 93% van de ondervraagde bedrijven het afgelopen jaar werd getroffen door een cyberaanval, waarbij het in 57% van de gevallen resulteerde in een schade van meer dan 400.000 euro. Daarnaast kreeg 68% van de ondervraagde Europese bedrijven het afgelopen jaar te maken met een storing van langer dan vijf uur vanwege een cyberaanval.

Uitkomsten Cisco Cybersecurity Report 2018

93%

van de ondervraagde Europese bedrijven werden het afgelopen jaar getroffen door een cyberaanval.



57%

van de aanvallen op Europese bedrijven resulteerden in een schade van meer dan € 400.000.

68%

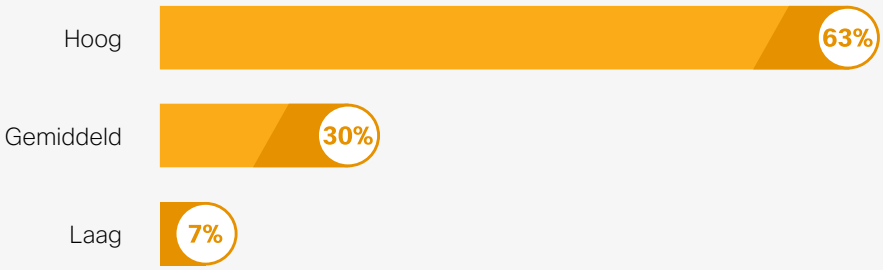
van de ondervraagde Europese bedrijven werden getroffen door een storing van langer dan vijf uur, als gevolg van een cyberaanval.

Lage prioriteit en tijdgebrek voornaamste redenen voor onvoorbereidheid

Gevraagd naar in hoeverre organisaties voorbereid zijn op cybercrime, schat 59% in goed of zeer goed voorbereid te zijn. Ongeveer één op de drie geeft aan 'enigszins voorbereid' te zijn, terwijl 9% aangeeft onvoldoende of zelfs zeer slecht voorbereid te zijn. Hierin zijn er gelijkenissen waar te nemen met het aantal organisaties waarbij cybersecurity hoog dan wel laag op de agenda staat.

Prioriteit cybersecurity

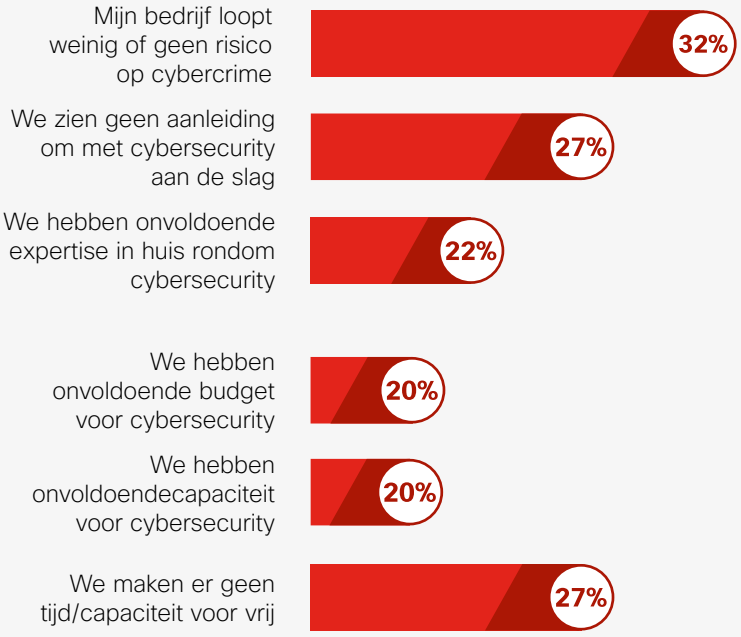
In hoeverre bent u het eens met de volgende stelling:
Binnen mijn bedrijf staat Cybersecurity hoog op de agenda



Van de organisaties waarbij cybersecurity laag op de agenda staat, denkt 32% dat hun organisatie weinig of geen risico loopt op cybercrime. Daarnaast beschikt 27% over onvoldoende tijd en ziet hetzelfde percentage simpelweg geen aanleiding om ermee aan de slag te gaan. Opvallend, gezien de vele voorbeelden van getroffen organisaties die de media hebben gehaald en de hoeveelheid organisaties die volgens zowel dit rapport als het Cisco Cybersecurity Report de afgelopen periode te maken kregen met cybercrime. Kennelijk zijn deze organisaties nog steeds niet voldoende op de hoogte van de gevolgen van cybercrime en onderschatten ze de gevolgen van cybercriminaliteit.

Voornaamste redenen om niet aan de slag te gaan met cybersecurity

Wat zijn de voornaamste redenen dat cybersecurity binnen uw bedrijf niet hoog op de agenda staat?



Maatregelen ter preventie

Dat beslissers zich weinig zorgen maken over cybercrime, blijkt ook uit het gebrek aan maatregelen die worden genomen om het te voorkomen. Bij 69% van de ondervraagde organisaties wordt er namelijk geen gebruik gemaakt van een beveiligingsdraaiboek of beveiligingsbeleid. Slechts 59% maakt gebruik van Two Factor Authentication om in te loggen in werkaccounts- en -applicaties, terwijl er bij 39% van de organisaties geen regels zijn voor het opstellen van sterke wachtwoorden. Bovendien geeft 24% aan geen beveiligingsapparatuur op werkcomputers te hebben geïnstalleerd, zoals routers, firewalls en antivirussoftware. Daarnaast geeft 41% aan dat er binnen hun organisatie geen duidelijke afspraken zijn gemaakt over de omgang van klantgegevens.

Tips voor het beschermen van uw (bedrijfs)gegevens

Uw computerapparatuur beschermen

TIP	TOELICHTING
Laat uw firewall aan staan	Of het nu gaat om een software- of een hardwarefirewall van een router, de firewall moet steeds aan staan en geüpdatet zijn om te voorkomen dat hackers toegang krijgen tot uw persoonlijke gegevens of die van uw bedrijf.
Gebruik antivirussoftware en antispyware	Download alleen software van vertrouwde websites om te voorkomen dat spyware uw computer infecteert. Antivirussoftware is ontworpen om uw computer en binnenkomende e-mails te scannen op virussen en deze te verwijderen. Houd uw software up-to-date om uw computer te beschermen tegen de nieuwste schadelijke software.
Beheer uw besturingssysteem en browser	Om uw computer en gegevens te beschermen, stelt u de beveiligingsinstellingen op uw computer en browser in op medium of hoger. Werk het besturingssysteem van uw computer, inclusief uw webbrowser, bij en download en installeer regelmatig de nieuwste softwarepatches en beveiligingsupdates van de leveranciers.
Bescherm al uw apparaten	Uw computerapparatuur moet met een wachtwoord worden beveiligd om ongeoorloofde toegang te voorkomen. De opgeslagen informatie moet gecodeerd zijn, vooral wanneer het gaat om gevoelige of vertrouwelijke gegevens.

UW APPARATEN EN NETWERK BESCHERMEN	
Gebruik unieke wachtwoorden voor elke online account	· Gebruik geen woorden die in het woordenboek voorkomen of wachtwoorden die overeenkomen met de loginnaam · Gebruik geen veelvoorkomende verkeerd gespelde woorden uit het woordenboek · Gebruik geen computernamen of accountnamen · Gebruik indien mogelijk speciale tekens zoals ! @ # $ % ^ & * ( ) · Gebruik een wachtwoord met tien of meer tekens
Gebruik een wachtwoordzin in plaats van een wachtwoord	· Kies een uitspraak die zinvol is voor jou · Gebruik speciale tekens zoals ! @ # $ % ^ & * ( ) · Hoe langer, hoe beter · Vermijd bekende of beroemde uitspraken, bijvoorbeeld teksten van een populair liedje

BEVEILIGINGSDRAAIBOEK	
Stel een beveiligingsdraaiboek op	Een van de beste manieren om u voor te bereiden op een beveiligingslek is er een te voorkomen. Er zou begeleiding moeten zijn bij het opsporen van cybersecurity-risico's voor systemen, assets, gegevens en vermogens, bij het beschermen van de systemen door safeguards en opleidingen te implementeren en bij het zo snel mogelijk detecteren van cybersecurity-events. Als er een beveiligingslek wordt opgemerkt, moeten gepaste stappen ondernomen worden om de impact en schade te minimaliseren.

Meer tips over het beschermen van uw (bedrijfs)gegevens? Doe de gratis NetAcad-cursus Introduction to Cybersecurity.

Risicovolle handelingen

Op de werkvloer zijn er verschillende situaties denkbaar waarin je extra risico loopt om getroffen te worden door een cyberaanval. Denk bijvoorbeeld aan het klikken op linkjes in e-mails van onbekenden of het surfen op het web via een openbaar Wi-Fi-netwerk op plekken zoals een hotel, restaurant of in de trein. Kennelijk zijn beslissers niet altijd op de hoogte van deze risico's. Maar liefst één op de drie beslissers geeft namelijk aan wel eens mails te openen van onbekenden en 28% bekijkt wel eens bedrijfsinformatie via een openbaar Wi-Fi-netwerk.

Veilig gebruikmaken van openbare WiFi-netwerken

Het gebruik van een openbaar Wi-Fi-netwerk neemt risico's met zich mee. Wil je toch gebruik maken van een openbaar WiFi-netwerk? Hier volgen enkele stappen die u kunt nemen om de risico's te verkleinen:

- Controleer – met name bij internetbankieren – of het webadres klopt en of het gaat om een beveiligde website die start met 'https'. Dit betekent dat de verbinding tussen de browser en de webserver versleuteld is, zodat gegevens die naar de website worden verbonden, zijn beschermd tegen spionage en manipulatie.
- Pas de instellingen van je smartphone aan zodat deze niet automatisch verbinding maakt met het nabijgelegen WiFi-netwerken. Op die manier heb je meer controle over waar en wanneer je verbinding maakt met een openbaar Wi-Fi-netwerk.
- Ben je van plan om betrouwbare informatie te bekijken via je smartphone? Gebruik dan bij voorkeur de databundel van je telefoon in plaats van een openbaar WiFi-netwerk.
- Als je regelmatig gebruik maakt van openbare Wi-Fi-netwerken of hotspots, gebruik dan bij voorkeur een Virtueel Privaat Netwerk (VPN). Hiermee worden alle transmissies tussen je apparaat en het internet versleuteld en beveiligd. Veel bedrijven bieden tegenwoordig VPN's aan hun werknemers voor werkdoeleinden.

Meer tips over het beschermen van uw (bedrijfs)gegevens?
Doe de gratis NetAcad-cursus Introduction to Cybersecurity.

Preventieve handelingen

Ook de mate van bereidheid om preventieve handelingen te treffen tegen cybercrime laat nog te wensen over. Zo blijkt 36% nooit of zelden gevoelige bedrijfsgegevens te versleutelen en geeft 32% aan (vrijwel) nooit hun instellingen van hun webbrowser aanpassen. Dit terwijl door het aanpassen en updaten van de beveiligingsinstellingen van je browser de kans kleiner wordt dat hackers kunnen profiteren van zwakke plekken in je besturingssysteem. Daarnaast geeft 22% aan dat ze nooit of zelden de website-URL's controleren van webpagina's die ze tijdens hun werk bezoeken.

Gerben Klein Baltink

Voorzitter van Platform Internetstandaarden

E-mails en websites moeten veiliger, en veiligheidsstandaarden kunnen daarbij helpen. Gerben Klein Baltink, voorzitter van het Platform Internetstandaarden, is van mening dat cybersecurity binnen iedere organisatie bespreekbaar moet worden gemaakt: “Praat er over, al is het maar tijdens de lunch of in een werkoverleg. We moeten toe naar een bedrijfscultuur waarin cybersecurity continu onder de aandacht wordt gebracht. Het helpt daarom om de gevolgen van cyberaanvallen zoals spear phishing, CEO-fraude en factuurfraude regelmatig met elkaar te bespreken.”

Internetstandaarden

Het Platform Internetstandaarden is een samenwerking tussen partners uit de internetgemeenschap en de Nederlandse overheid. Het platform maakt zich sterk voor de adoptie van internetstandaarden, die zijn vastgelegd in de ‘pas-toe-of-leg-uit-lijst’ van het Forum Standaardisatie. Klein Baltink: “Een voorbeeld hiervan is DNSSEC. Hiermee kan de internetgebruiker de echtheid van de domeinnaaminformatie controleren, zoals bijvoorbeeld het IP-adres. Dit voorkomt dat internetcriminelen het IP-adres onopgemerkt kunnen manipuleren, om zo gebruikers bijvoorbeeld te misleiden naar een frauduleuze website.” Om fraude met e-mail en websites tegen te gaan, heeft het Platform Internetstandaarden de website Internet.nl opgericht. “Op deze site kan iedere burger of organisatie testen of zijn website, e-mail of internetverbinding veilig en betrouwbaar is,” aldus Klein Baltink.

“Het opleiden van het personeel voor de digitale toekomst is belangrijker dan ooit.”

Awareness campagnes

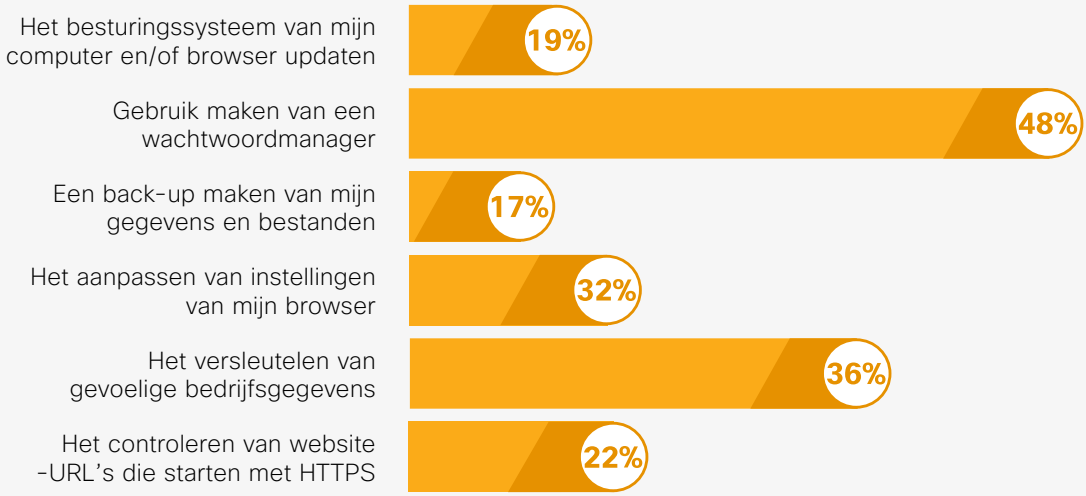
Naast het adopteren van standaarden en het bespreekbaar maken van de gevolgen van cybercriminaliteit pleit Klein Baltink ook voor awareness campagnes waarin medewerkers onaangekondigd bijvoorbeeld een phishing mail ontvangen, om zo de alertheid van de medewerkers te testen. “Zo kun je inzichtelijk maken hoeveel medewerkers de phishing mail voor echt aanzien en kun je meteen de mensen aanspreken die op linkjes hebben geklikt. Hen kun je bijvoorbeeld een training laten volgen over het herkennen van een phishing mail.”

Digitale toekomst

Volgens Klein Baltink moet er voldoende aandacht worden besteed aan technologische vaardigheden in het onderwijs: “De digitale toekomst is nu al begonnen. We zitten er middenin. Het is daarom belangrijker dan ooit dat studenten een aantal basisvaardigheden over ICT en het internet meekrijgen. Alleen dan kunnen ze de complexiteit achter digitale toepassingen begrijpen en de technologische ontwikkelingen bijbenen.”

Handelingen ter voorkoming van cybercrime

In hoeverre onderneemt u de volgende handelingen op uw werk (op uw zakelijke device)?



35%

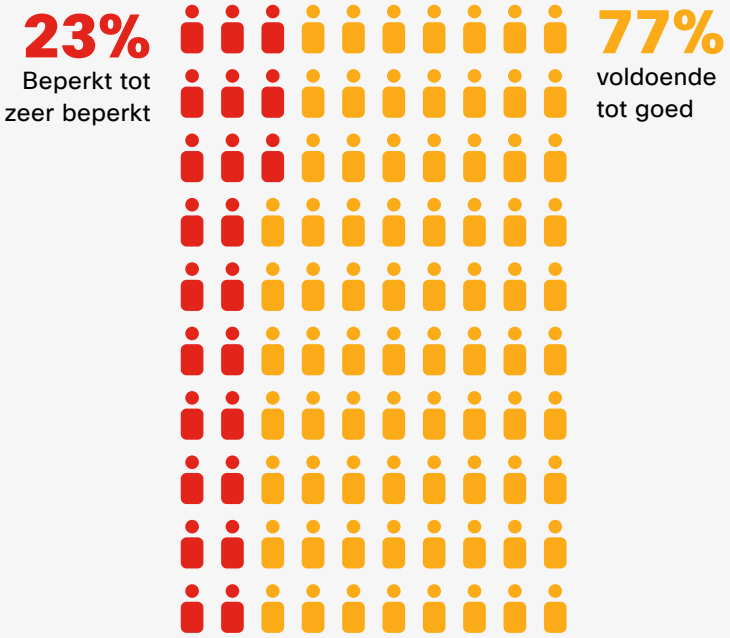
van de beslissers van Nederlandse beoordeelt het eigen kennisniveau over cybersecurity als beperkt tot zeer beperkt

Geen grote verschillen tussen kennisniveau beslissers en medewerkers

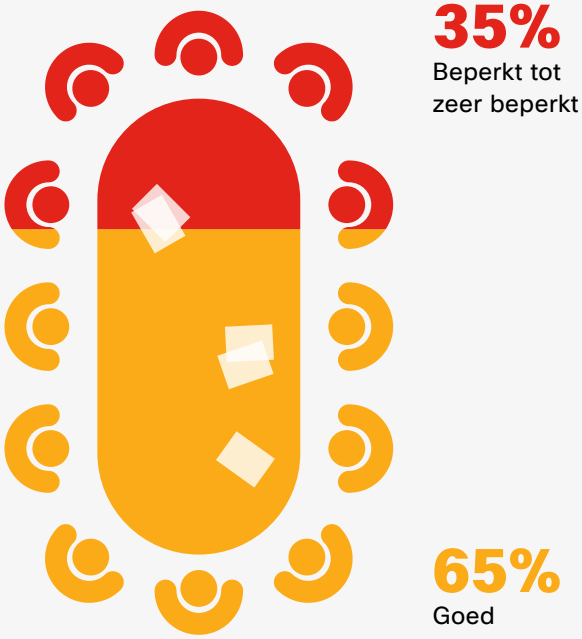
Ondanks het gebrek aan preventiemaatregelen, schat meer dan één op de vier beslissers het eigen kennisniveau over cybersecurity in als goed of zelfs uitstekend. Een groter deel (35%) geeft aan dat hun kennis beperkt tot zeer beperkt is. Het kennisniveau binnen de eigen organisatie wordt over het algemeen iets hoger ingeschat dan het kennisniveau van de beslissers van de betreffende organisaties, al zijn hierin geen grote verschillen waar te nemen.

Kennisniveau van cybersecurity

Percentage van medewerkers met beperkt kennisniveau van cybersecurity volgens beslissers



Beoordeling van eigen kennisniveau over cybersecurity volgens beslissers



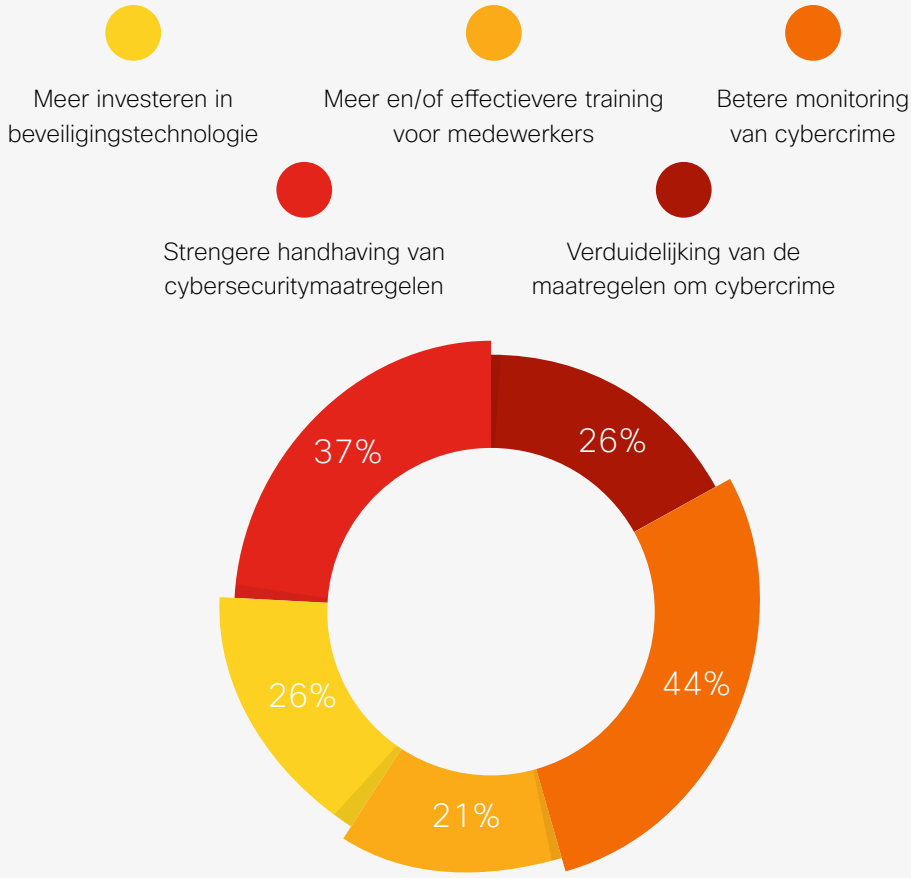
Beslissers kritisch over cybersecuritybeleid van eigen organisatie

Slechts een handvol beslissers is helemaal tevreden over het cybersecuritybeleid binnen hun organisatie. De meest genoemde punten van kritiek gaan over het aantal werknemers die zich kunnen toewijden aan cybersecurity, de hoeveelheid aandacht die wordt besteed aan het trainen en opleiden van personeel en de beschikbare budgetten voor cybersecurity.

Gevraagd naar de belangrijkste maatregelen om het beleid rondom cybersecurity in de organisaties van de ondervraagde beleidsmakers en beslissers te verbeteren, worden verschillende maatregelen genoemd. De meest genoemde maatregel is meer of effectievere training voor medewerkers rondom cybersecurity; 44% van de beslissers denkt op die manier het kennisniveau rondom cybersecurity binnen hun organisatie omhoog te krikken. Een andere veelgenoemde maatregel is het verduidelijken van de regels om cybercrime te voorkomen (37%). Andere maatregelen die worden genoemd om het cybersecurity-beleid binnen de organisatie te verbeteren zijn meer investeringen in beveiligingstechnologie (26%).

Rol van de overheid rondom cybersecurity

Wat zijn volgens u de belangrijkste maatregelen om het beleid rondom cybersecurity in uw bedrijf te verbeteren?



>60%

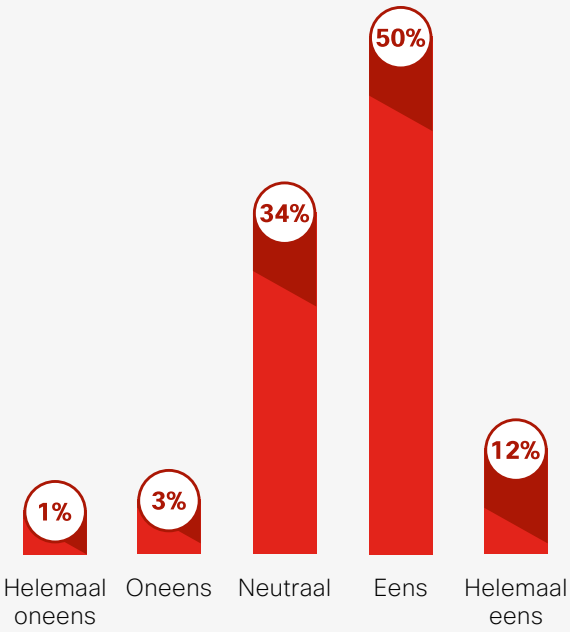
is van mening dat de overheid meer moet investeren in onderwijs en bewustwording rondom cybersecurity.

Tot slot legden we beslissers van Nederlandse organisaties drie stellingen voor over de rol van de overheid als het gaat om bewustwording, onderwijs en onderzoek naar cybersecurity. Hieruit blijkt dat het merendeel het erover eens is dat de overheid op alle drie de gebieden meer moet investeren.

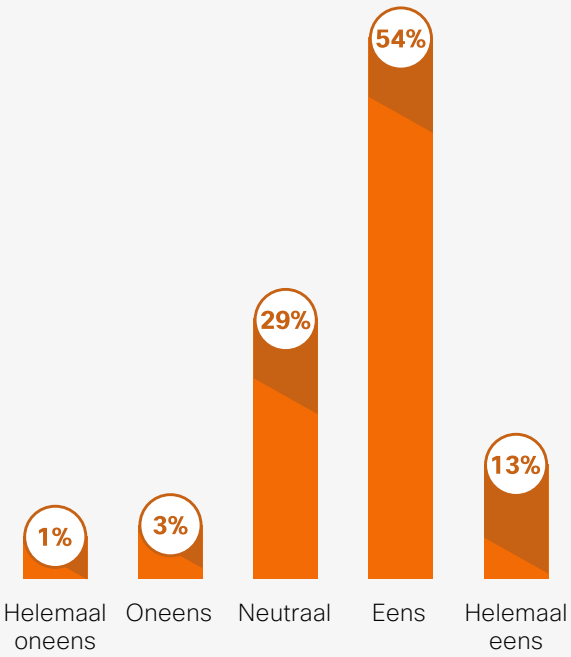
Rol van de overheid rondom cybersecurity

In hoeverre bent u het eens met de volgende stellingen over de rol van de overheid rondom cybersecurity?

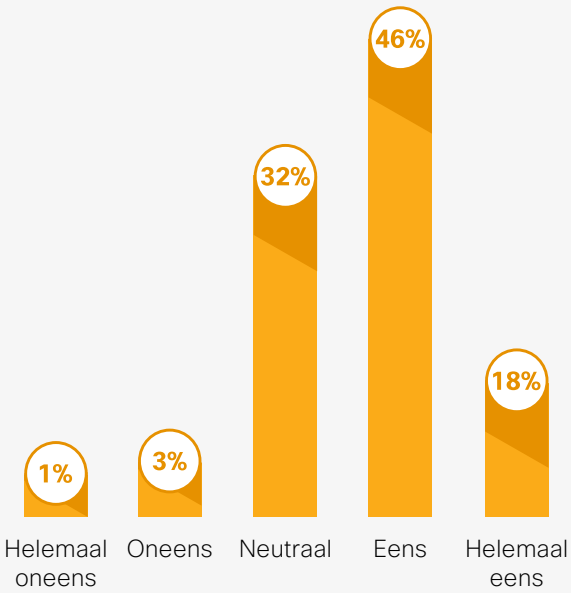
De Nederlandse overheid moet meer investeren in onderwijs



De Nederlandse overheid moet meer investeren in bewustwording



De Nederlandse overheid moet meer investeren in onderzoek



Cisco Cybersecurity Trendrapport

Dit onderzoek is uitgevoerd in opdracht van de Cisco Networking Academy (NetAcad), onderdeel van het programma **Digitale Versnelling Nederland (DVN)**. Om erachter te komen hoe risicobewust beslissers bij Nederlandse organisaties zijn op het gebied van cybersecurity, ondervroeg Cisco in samenwerking met onafhankelijk onderzoeksbureau Multiscope 556 Nederlandse mede- en eindbeslissers, waaronder I(C)T-managers, Marketing Directors en Chief Financial Officers.

De respondenten werken vooral in loondienst (76%), bijna een kwart van de respondenten (24%) is zelfstandig ondernemer. De respondenten zijn vooral actief in de volgende sectoren: zakelijke dienstverlening (23%), gezondheids- en welzijnszorg (14%), openbaar bestuur, overheidsdiensten en sociale verzekeringen (8%), onderwijs (8%), detailhandel, groothandel en reparatie (8%) en de industriesector (6%).

Cisco ondervroeg met name respondenten die werkzaam zijn bij bedrijven met meer dan 250 werknemers (39%), maar ook middenbedrijven (17%), kleinbedrijven (21%) en SoHo's (23%) zijn meegenomen in het onderzoek.

Over Netacad

Cisco's Networking Academy (NetAcad) brengt studenten en medewerkers digitale vaardigheden bij die nodig zijn in de steeds meer digitaliserende economie. Jaarlijks nemen bijna 2 miljoen studenten deel aan het MVO-programma in de 180 landen waar het programma actief is. Netacad werd opgericht in 1997. In Nederland bestaat het programma dit jaar 20 jaar en heeft ca. 140.000 IT-studenten opgeleid. Meer informatie of meedoen aan een cursus? Ga naar: **www.netacad.com**.