NEDERLAND ICT CYBER SECURITY ZOMERONDERZOEK 2014

Om te kunnen profiteren van de impuls die onze internetinfrastructuur en ICT de digitale economie kan geven, is cyber security een essentiële randvoorwaarde. Cybercriminaliteit richt naar schatting jaarlijks voor honderden miljoenen tot enkele miljarden euro's aan schade aan. ICT-bedrijven, gebruikersorganisaties in overheid en de private sector spelen allen een belangrijke rol bij digitale veiligheid. Brancheverenigingen Nederland ICT peilde in augustus 2014 de stemming onder haar leden. Onder andere CEO's, CFO's en security-experts van grote en kleine ICT-bedrijven werkten mee aan het onderzoek.

Belangrijkste bevindingen

- Cyber security is het nummer 1 thema bij ICT-bedrijven
- Klanten zetten beveiliging vaker op de agenda, maar budget blijft achter
- De overheid heeft een belangrijke voorlichtingstaak, beleid ook richten op 'digitale wereld' van morgen
- Cybercriminaliteit is alleen te bestrijden door goede samenwerking tussen overheid en bedrijfsleven
- Kennisniveau gebruikersorganisaties in private en publieke sector stijgt, maar schiet nog steeds tekort
- Focus klanten op certificeringen werkt averechts
- Cybercriminelen moeten steviger worden aangepakt

Cyber security speelt enorm bij ICT-bedrijven. 95 procent van de bedrijven die meededen aan het onderzoek geeft aan dat het een belangrijk thema is binnen de organisatie. Belangrijker dan een thema als kostenefficiëntie of een trend als cloud computing is. De impact die cyber security heeft op het vertrouwen, speelt hier een grote rol. Drie op vier ICT-bedrijven realiseert zich dat een gebrek aan vertrouwen in ICT en internet leidt tot minder investeringen.

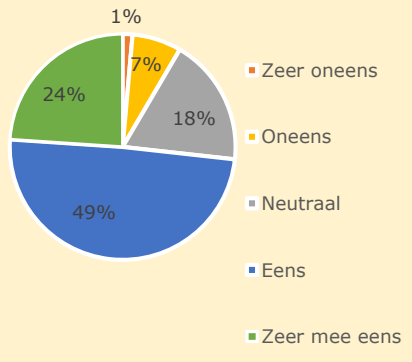
Ook bij gebruikersorganisaties staat cyber security steeds vaker op de agenda. Bijna 90 procent van de ICT-bedrijven merkt dat beveiliging van ICT en informatie de afgelopen drie jaren steeg op de agenda van klanten.

Dat gebruikersorganisaties in zowel het bedrijfsleven als bij de overheid meer belang hechten aan cyber security, is volgens de ICT-bedrijven ook terug te zien in de dagelijkse praktijk. 70 procent van de achterban ziet dat klanten beveiliging vaker in de set van eisen plaatsen. Ongeveer de helft van de ondervraagden merkt dat klanten er duidelijk behoefte aan heeft dat beveiliging aandacht krijgt tijdens klantgesprekken.

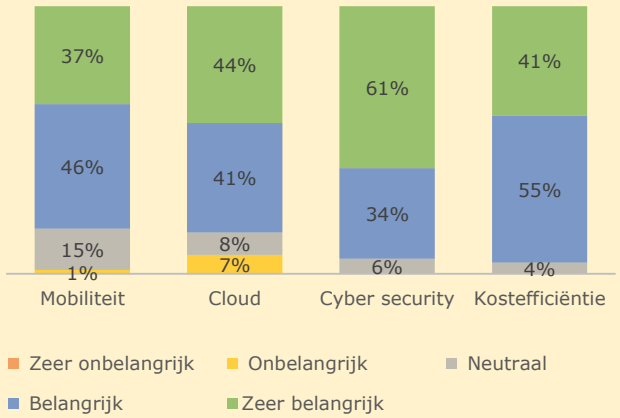
64 procent van de ondervraagden geeft aan dat de vraag vanuit de klant een belangrijke reden is om zich te richten op cyber security. Een andere aanjager is concurrentie: de helft van de ICT-bedrijven wil zich op dit onderwerp onderscheiden van andere bedrijven.

De aandacht voor cyber security richt zich niet alleen naar buiten toe. Ook binnen de eigen organisatie ligt er een stevige nadruk op cyber security. Bijna 85 procent van de bedrijven richt zich bij cyber security in zijn bedrijf op security in de ontwikkeling van producten en diensten, 70 procent van de ICT-bedrijven licht medewerkers voor over beveiliging. Bij twee derde van de bedrijven wordt aandacht besteed aan verdeling van verantwoordelijkheden.

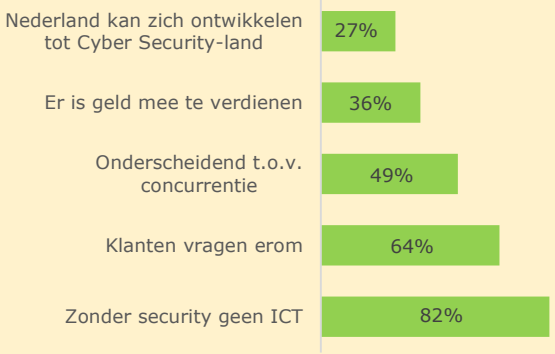
"GEEN VERTROUWEN IN ICT BETEKENT GEEN TOEPASSING EN GEEN INVESTERINGEN"



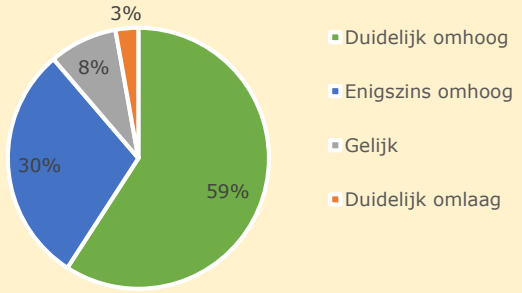
WAT IS HET BELANG VAN DEZE THEMA'S VOOR UW BEDRIJF?



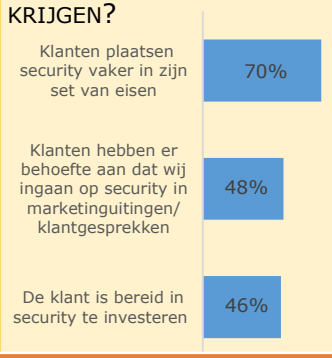
WAT MAAKT CYBER SECURITY VOOR UW ORGANISATIE ZO BELANGRIJK?



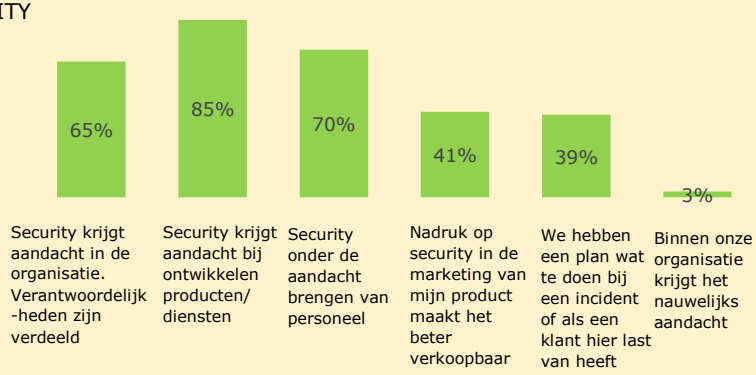
GING BEVEILIGING IN DE AFGELOPEN 3 JAAR BIJ UW KLANTEN OP DE AGENDA OMHOOG OF OMLAAG?



HOE MERKT U DAT UW KLANTEN MEER AANDACHT VOOR SECURITY KRIJGEN?



HOE BESTEEDT U ALS ICT-BEDRIJF AANDACHT AAN SECURITY?



KENNIS IS KEY

De prioriteit die cyber security in het bedrijfsleven en overheid krijgt maakte in de afgelopen jaren een positieve ontwikkeling door. Aandacht moet echter vergezeld gaan van kennis om effectief te zijn. Alleen wanneer organisaties voldoende kennis bezitten over de risico's die zij lopen en deze kunnen omzetten naar acties om zich te beschermen tegen deze risico's, kan er op een veilige manier gewerkt worden. Bijna 80 procent van de ICT-bedrijven geeft aan dat er een verantwoordelijkheid ligt bij gebruikersorganisaties, bijvoorbeeld om te zorgen dat medewerkers de beschikbare ICT-systemen op de juiste manier gebruiken.

Driekwart van de ICT-bedrijven vindt dat klanten het benodigde kennisniveau nog niet halen. Wel ziet een ruimte meerderheid dat het kennisniveau bij klanten stijgt. In de private sector lijkt dit iets sneller te gaan dan bij de overheid. 75 procent denkt dat opleidingen in de toekomst belangrijker gaan worden voor eindgebruikers én ICT-professionals. Zo vindt bijna 80 procent dat er aandacht moet zijn voor cyber security in het onderwijs.

Hoewel er meer aandacht is voor cyber security binnen organisaties en ook het kennisniveau langzaam stijgt, blijft het budget achter. Zo merkt minder dan de helft van de ICT-bedrijven dat klanten ook echt bereid zijn om te betalen voor veiligheid. Niet alle veiligheidsmaatregelen kosten geld, maar enig budget zal nodig zijn. Nederland ICT heeft als stelregel in de '10 cyber security vuistregels' aangegeven dat ongeveer 10 procent van het ICT-budget aan security besteed moet worden.[1]

In Duitsland is deze stelregel recent ook voor de Duitse federale overheid als uitgangspunt bepaald.[2]

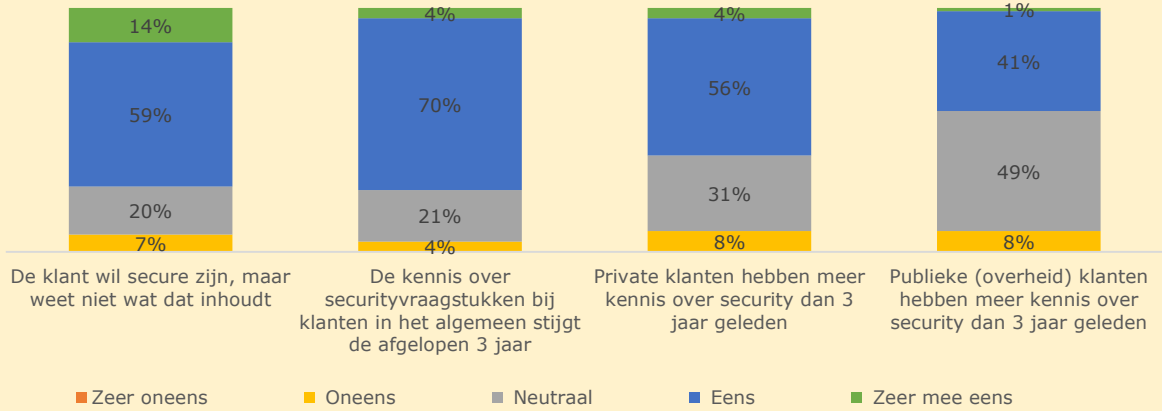
ICT-bedrijven hebben vertrouwen dat de cyber security vragen in de toekomst beantwoord kunnen worden. Daarbij zien ICT-bedrijven dat cyber security prima samengaat met nieuwe ontwikkelingen en innovaties. Slechts 14 procent vreest dat het denken in cyber security belemmerend gaat werken.

Ook bestaat het gevaar dat er enkel kennis wordt opgedaan over het toepassen van regels en standaarden. De helft van de ondervraagde bedrijven geeft aan dat klanten te veel verwachten van certificering. Hoewel certificering nuttig kan zijn, betekent compliance niet per definitie dat er ook veilig wordt gewerkt of dat er veilig wordt aangekocht. Klanten moeten nadenken over de data en systemen die ze gebruiken, welke risico's ze lopen en welke van deze risico's ze (wettelijk) moeten of willen afdekken. Dit is geen eenmalige oefening, maar een proces dat bedrijven keer op keer moeten herhalen. Bedrijven die te veel focussen op afvinklijstjes gaan voorbij aan de kernvragen en zullen niet veiliger worden.

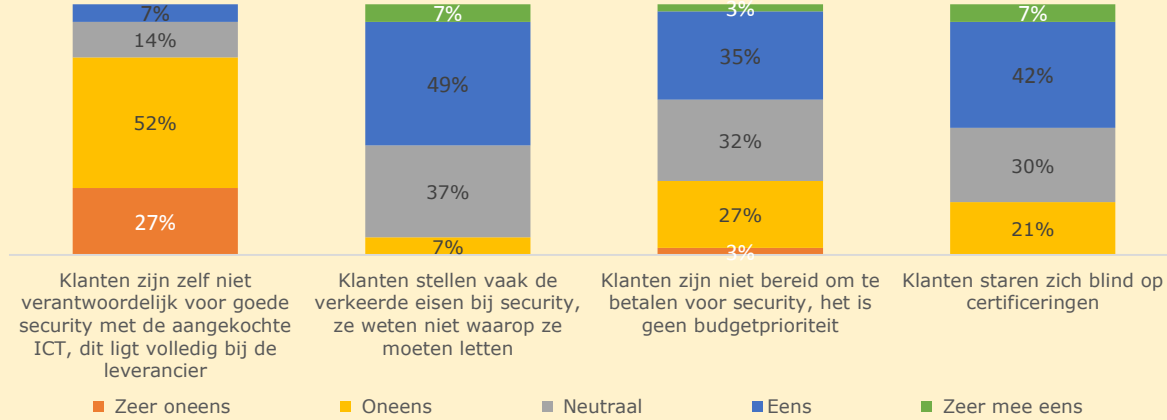
[1] http://www.nederlandict.nl/Files/TER/Tien_cyber_security_vuistregels_voor_bestuurders_en_ondernemers.pdf

[2] http://www.bundesregierung.de/Content/DE/_Anlagen/2013/2013-12-17-koalitionsvertrag.pdf?__blob=publicationFile

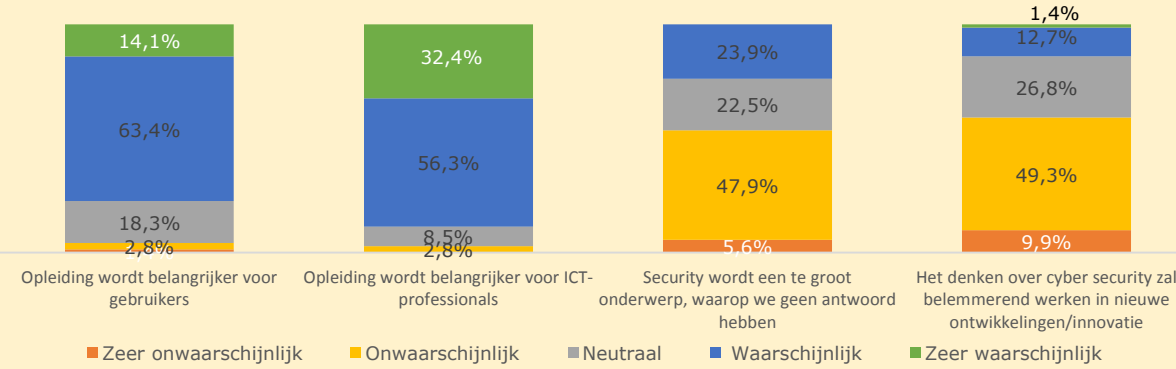
WEET DE KLANT WAT HIJ WIL ALS HET OM SECURITY GAAT?



WAAR LIGT DE VERANTWOORDELIJKHEID EN LETTEN KLANTEN OP DE JUISTE ZAKEN?

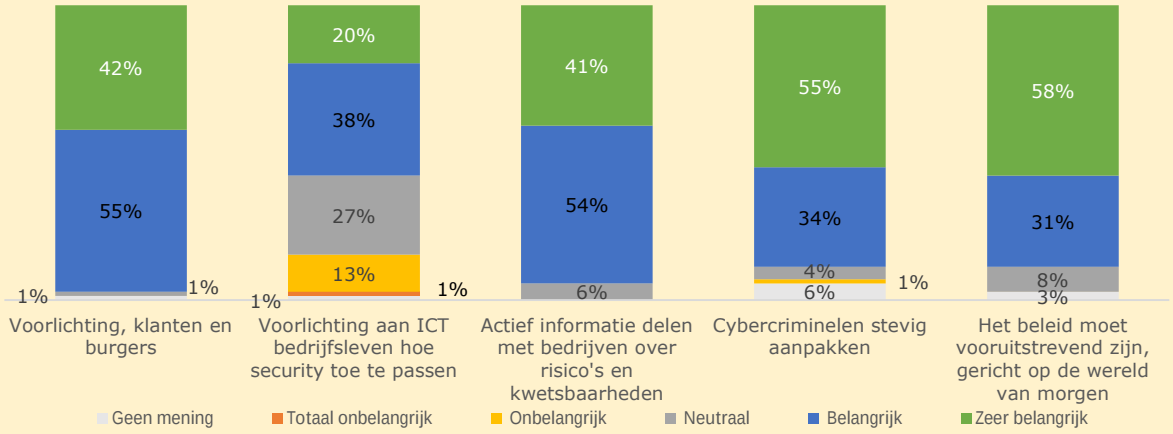


TOEKOMSTVERWACHTINGEN



NEDERLAND ICT CYBER SECURITY ZOMERONDERZOEK 2014

ROL OVERHEID IN CYBER SECURITY



BEWUSTWORDING

Uit het onderzoek blijkt dat op het gebied van voorlichting om bewustwording te krijgen een nadrukkelijke inzet van de overheid wordt verwacht. 98 procent stelt dat de overheid een rol heeft in de voorlichting aan overheidsorganisaties, bedrijven en burgers.

Nederland ICT draagt bij aan bewustwording over cyber security, zowel bij haar eigen achterban als bij organisaties die de producten en diensten van ICT-bedrijven afnemen. Zo bracht Nederland ICT de ¶ vuistregels voor cyber sec X U L W LW,¶ waaraan bestuurders en ondernemers kunnen toetsen of er voldoende kennis over cyber security aanwezig is in hun organisatie.

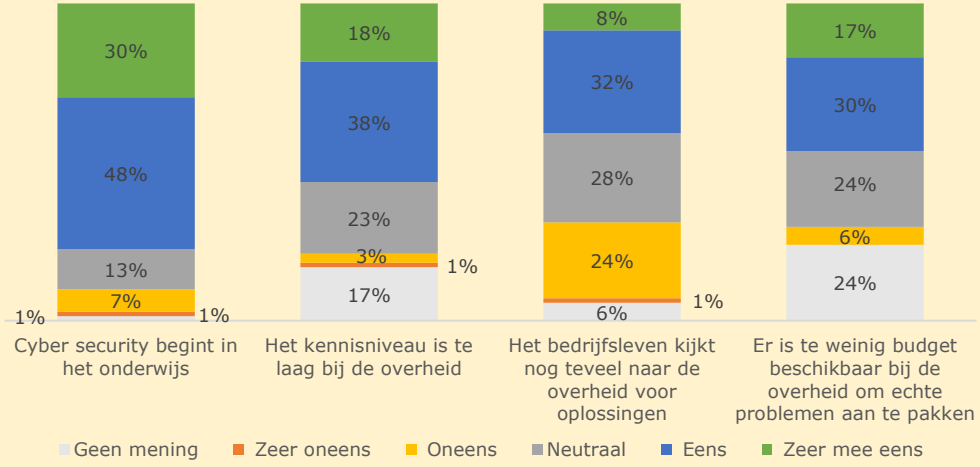
Op www.beschermjebedrijf.nl kunnen MKB-bedrijven een quick scan doen, Z D D U P H H] L M L Q] L F K W N U L M voor hun bedrijfsvoering. Voor ICT-bedrijven biedt de brancheverenigingeen checklist aan over incidentrespons & communicatie. Daarnaast is cyber security een terugkerend onderwerp bij veel van de bijeenkomsten van Nederland ICT, zoals bij masterclasses cyber security die vorig jaar werden gegeven.

BELANGRIJKE ROL OVERH EID

De overheid heeft volgens het ICT-bedrijfsleven naast voorlichting nog een aantal duidelijke rollen. Zo zou cybercriminaliteit volgens ICT-bedrijven steviger aangepakt moeten worden, zodat de pakkans omhoog gaat. Een meerderheid ziet echter niets in het overheidsplan om µ W H U X J W H K D F N H Q ¶ 6 O H F K V dat de overheid zelf mag inbreken op systemen om cybercriminelen tegen te houden. Verder vinden ICT-bedrijven het belangrijk dat beleid meer in de pas loopt met de voortdurende innovatie die op het gebied van ICT en cyber security plaatsvindt.

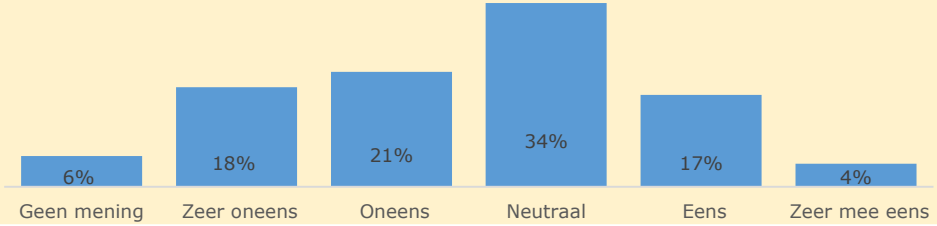
Uit het onderzoek blijkt dat ICT-bedrijven zowel de politiek als de overheid zichtbaar vinden op dit gebied. Eén derde van de ICT-bedrijven is echter wel van mening dat waar wet- en regelgeving omtrent cyber security nodig is, deze beter moet worden vormgegeven. Groot risico bij wetgeving op cyber security is dat deze vooral symbolische waarde krijgt en in realiteit maar beperkt bijdraagt veiligheid.

CYBER EN OVERHEID



HOE ZICHTBAAR VINDT U DE OVERHEID OP CYBER SECURITY?

³ 'E OVERHEID MOET ZELF OP SYSTEMEN KUNNEN INBREKEN OM CYBERCRIMINELEN TEGEN TE HOUDEN ´

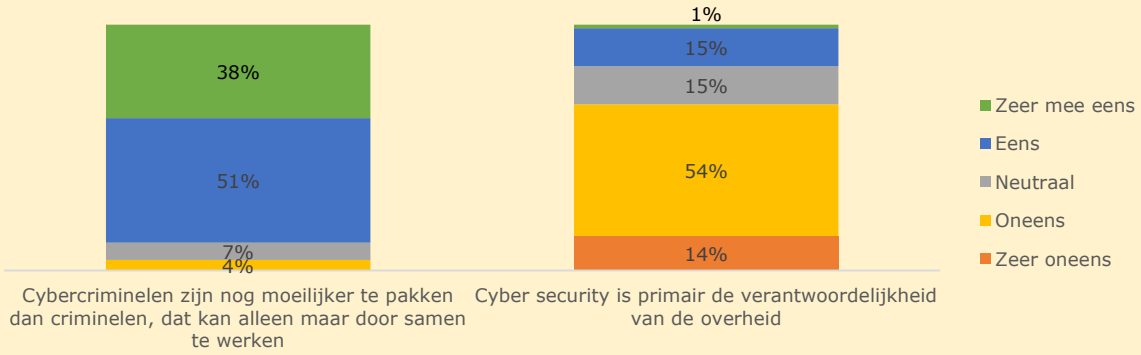


SAMENWERKING TUSSEN OVERHEID EN BEDRIJFSLEVEN

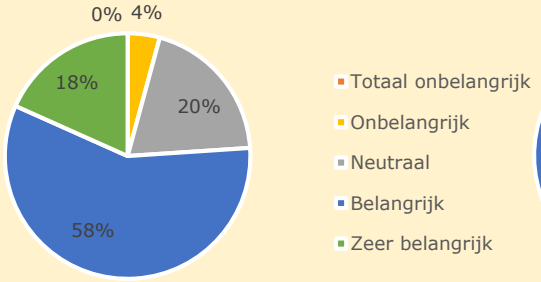
Cyber security vraagt een samenspel van bedrijfsleven en overheid: cybercriminaliteit is van een andere orde dan andere vormen van criminaliteit, waardoor samenwerking volgens 89 procent nodig is. 60 procent van de ICT-bedrijven vindt dat cyber security niet primair bij de overheid kan worden neergelegd. Dat is goed te verklaren, want uiteindelijk zijn de private sector en overheid samen verantwoordelijk om te investeren in cyber security.

94 procent van de deelnemende ICT-bedrijven geeft wel aan dat de overheid actiever informatie moet delen met bedrijven over risico's en kwetsbaarheden. Dit is immers ook een voorwaarde om samen te werken aan cybercrimebestrijding. 96 procent vindt dan ook dat Nederland ICT als vertegenwoordiger van de branche moet meedenken met de overheid om goed cyber security-beleid te ontwikkelen. Dat is de reden dat Nederland ICT met de overheid samenwerkt aan de Nationale Cyber Security Strategie. Ook zit Nederland ICT-voorzitter Bart Hogendoorn in de Cyber Security Raad, dat het kabinet adviseert op cyber security. Binnen Nederland ICT is de adviesgroep cyber security een gesprekspartner voor overheid, gebruikersorganisaties en vitale sectoren. Door actief samen te werken, samen problemen te analyseren en oplossingen te bedenken, krijgt de overheid ook meer inzicht in wat de markt aan kennis al aanbiedt. Bedrijven zien hierbij een duidelijk belang om Nederland digitaal veilig te maken en te houden.

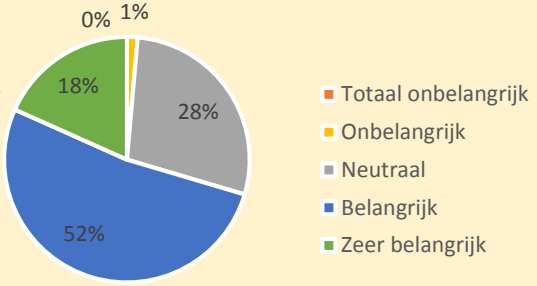
CYBERCRIMINALITEIT EN OVERHEID



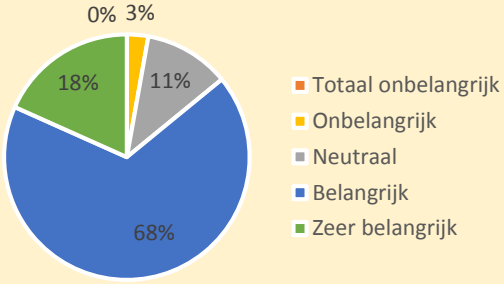
GEWENSTE ROL NEDERLAND ICT: "WORKSHOPS ORGANISEREN OVER ONTWIKKELINGEN IN CYBER SECURITY"



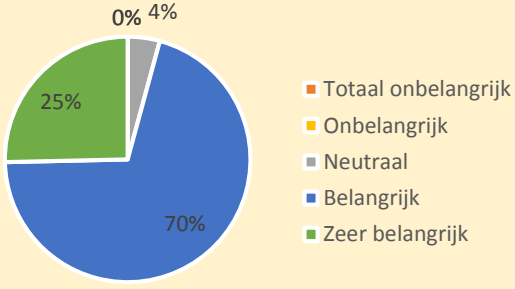
GEWENSTE ROL NEDERLAND ICT: "VOORLICHTING OVER WAT ER SPEELT IN DEN HAAG"



GEWENSTE ROL NEDERLAND ICT: "NETWERKFUNCTIE; VERBINDEN VAN BEDRIJVEN MET KENNIS VAN CYBER SECURITY"



GEWENSTE ROL NEDERLAND ICT: "MET DE OVERHEID MEEDENKEN VOOR GOED CYBER SECURITY-BELEID"



OVER HET ONDERZOEK

Een aantal keer per jaar onderzoekt Nederland ICT de kijk van haar leden op markt- en andere ontwikkelingen. Het cyber security-onderzoek werd in juli en augustus 2014 uitgevoerd door Keala Consultancy.

Aan het onderzoek deden medewerkers van lidbedrijven van Nederland ICT mee. Onder de respondenten zaten onder andere CEO's, CFO's en specialisten op het gebied van cyber security.

Voor dit onderzoek is de volgende definitie van cyber security gebruikt:

Cyber security is het streven (als samenleving of als individueel bedrijf) naar het voorkomen van schade door verstoring, uitval of misbruik van ICT en, indien er toch schade is ontstaan, het herstellen hiervan.

OVER NEDERLAND ICT

Nederland ICT is de brancheverenging van ruim 550 ICT-bedrijven in Nederland, waarvan 80% tot het Midden- en Kleinbedrijf behoort. Ook de grootste ICT-bedrijven in Nederland zijn lid.

Nederland ICT vertegenwoordigt een sector met een omzet van ruim €30 miljard, die werk biedt aan een kwart miljoen mensen en bijdraagt aan 70% van alle innovaties.

NEDERLAND ICT

Postbus 401 | 3440 AK Woerden | Pompmolenlaan 7 | 3447 GK Woerden

0348 49 36 36 | info@nederlandict.nl| www.nederlandict.nl| @Nederland_ICT