KASPERSKY lab

HET GEBREK AAN CYBERBEVEILIGINGSEXPERTS: EEN TIKKENDE TIJDBOM

FUTUREPROOFING CYBERSECURITY

INVESTING IN TODAY'S TALENT TO SECURE TOMORROW

Een mededeling van Eugene Kaspersky

“We leven in een tijd waarin bedrijven en organisaties uit de publieke sector steeds vaker geconfronteerd worden met alsmaar geavanceerdere dreigingen. Binnen deze grote groep, van ondernemingen tot aan kritieke nationale infrastructuur en financiële instellingen, is algemeen bekend dat dit een verloren strijd is indien een organisatie niet beschikt over werknemers met de vaardigheden die nodig zijn om cybercriminaliteit te bestrijden.

Werkgevers hopen de groeiende vaardigheidskloof te kunnen dichten met de hulp van technologisch goed onderlegde jongeren, om de toenemende dreiging van cybercriminaliteit en grootschalige verstoring van het openbare en privéleven te voorkomen.

Ook Kaspersky Lab maakt zich grote zorgen over het tekort aan cybervaardigheden en heeft daarnaast de verregaande wens om dit probleem aan te pakken. Wij hebben daarom een onderzoek laten uitvoeren om meer inzicht te krijgen in dit probleem. We wilden vooral onderzoeken hoe jongeren aankijken tegen een loopbaan binnen cyberbeveiliging en onderzoek doen naar de mogelijke gevolgen voor het bedrijfsleven en de samenleving als geheel wanneer de vaardigheidskloof blijft groeien.

Uit dit onderzoek komen enkele opmerkelijke resultaten naar voren. De huidige generatie jongeren blijkt zich online zeer goed te kunnen redden. Ook willen jongeren graag meer weten over grootschalige cyberhacks en zijn ze op zoek naar manieren om hun vaardigheden te kunnen inzetten.

Uit het onderzoek blijkt echter ook dat de branche van cyberbeveiliging er onvoldoende in slaagt om de aandacht van deze generatie te trekken en jongeren niet duidelijk laat zien welk pad ze moeten volgen om werk te vinden, vaardigheden aan te scherpen en de samenleving van dienst te zijn. Het is zelfs zo dat vele jongeren juist in de verleiding worden gebracht om van het rechte pad af te dwalen en hun vaardigheden in te zetten om cyberdreigingen te ontwikkelen, in plaats van deze te bestrijden.

Cyberaanvallen worden steeds vaker uitgevoerd door tieners en zijn steeds geavanceerder. Er moet dus meer worden gedaan om jongeren te stimuleren om te kiezen voor een loopbaan binnen de cyberbeveiliging en hun vaardigheden in te zetten voor de goede zaak. We moeten de interesses van de nieuwe generatie in de juiste banen weten te leiden, voordat het te laat is en het tekort aan vaardigheden onoverkomelijk groot is.”

KASPERSKY lab

FUTUREPROOFING CYBERSECURITY

BELANGRIJKE BEVINDINGEN

Eén op de vier (27%) heeft een loopbaan binnen de cyberbeveiliging overwogen en bijna de helft (47%) van de jongeren vindt dat ze hun talent hierin kunnen ontplooien. Anderen geven echter aan dat ze spelen met de gedachte om zich in te laten met dubieuzere activiteiten, en hun vaardigheden bijvoorbeeld willen gebruiken om plezier te maken (17%), voor clandestiene activiteiten (16%) of voor financieel gewin (11%)

27%

Van de 18-jarigen kent 23% iemand die zich bezighoudt met cyberactiviteiten (zoals hacking) die als illegaal gezien kunnen worden

23%

Meer dan de helft (57%) van de jongeren onder de 25 jaar beschouwt hacken als een 'indrukwekkende' vaardigheid

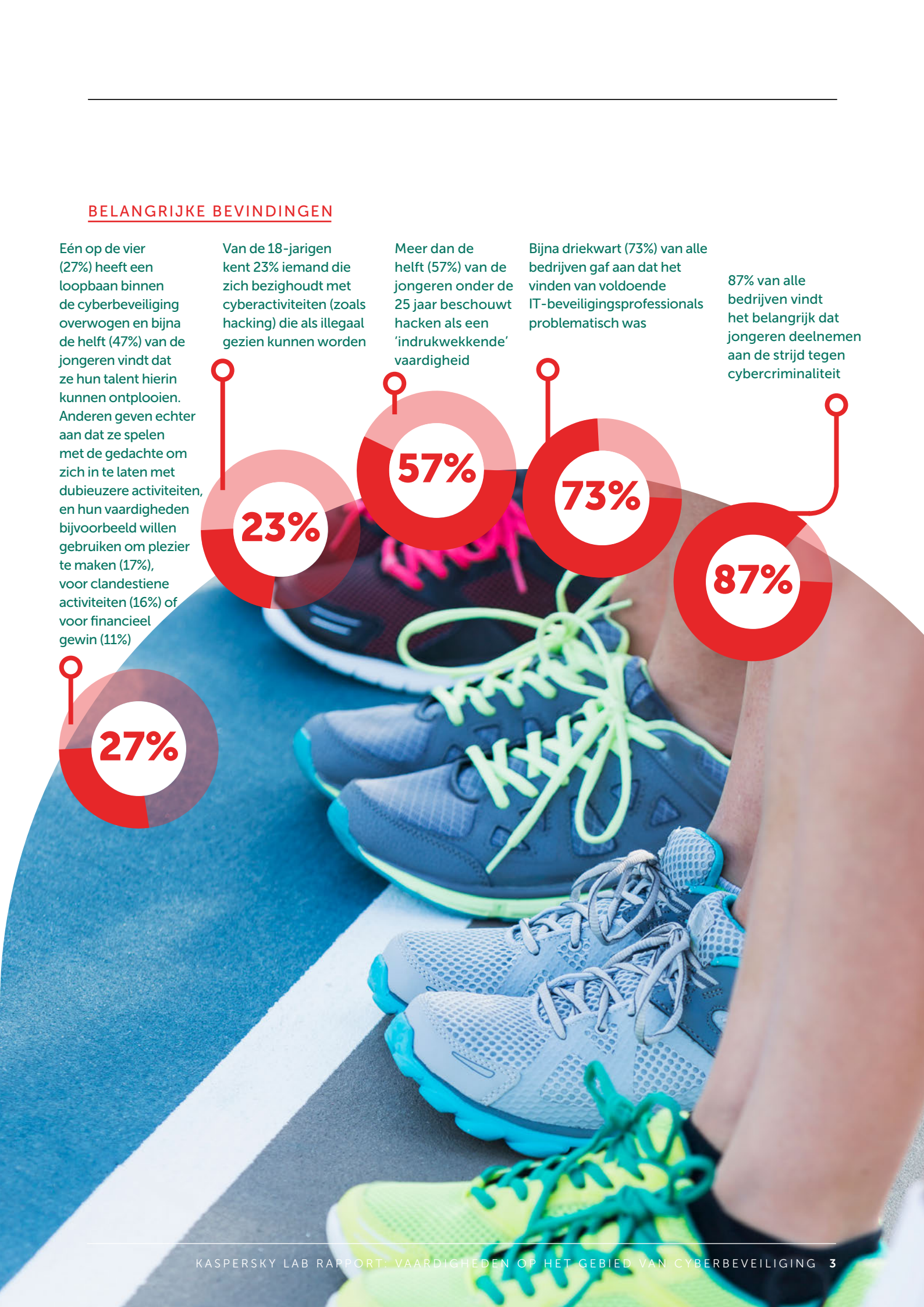
57%

Bijna driekwart (73%) van alle bedrijven gaf aan dat het vinden van voldoende IT-beveiligingsprofessionals problematisch was

73%

87% van alle bedrijven vindt het belangrijk dat jongeren deelnemen aan de strijd tegen cybercriminaliteit

87%



Inleiding

Organisaties beseffen dat het geen kwestie meer is **of** een cyberaanval gaat plaatsvinden, maar **wanneer**. Als gevolg daarvan willen veel leidinggevenden binnen de zakenwereld meer en meer inzicht in wat er wordt gedaan om de organisatie te beschermen en dat leidt ertoe dat er steeds meer steun is ontstaan voor uitbreiding van cyberbeveiliging. Een probleem daarbij is echter dat het aantal talenten dat is opgeleid op het gebied van cyberbeveiliging niet evenredig toeneemt.

Wereldwijd groeit de vraag naar cyberbeveiligingsexperts en men verwacht dat deze vraag het aanbod met een derde zal overtreffen voor het einde van het decennium. Uit de meest recente Global Workforce Survey van Frost and Sullivan komt zelfs naar voren dat er in 2020 een tekort van 1,5 miljoen beveiligingsprofessionals zal zijn, gebaseerd op de huidige trends. Het is dus zaak dat het aanvullen van dit tekort snel prioriteit krijgt, voor het te laat is.

Doet de branche genoeg om een loopbaan binnen de cyberbeveiliging aantrekkelijk te maken voor jongeren? Moeten werkgevers meer doen om de interesses en het talent van jongeren te benutten in de praktijk? Of zouden onderwijsinstellingen moeten zorgen dat hun studenten beter voorbereid zijn en beschikken over meer cybervaardigheden?

Om hier achter te komen, heeft Kaspersky Lab een onderzoek uitgevoerd onder bijna 12.000 consumenten en IT-professionals uit de VS en Europa (VK, Duitsland, Frankrijk, Italië, Spanje en Nederland). We wilden op deze manier te weten komen hoe we de groeiende vaardigheidskloof kunnen dichten en wie daarvoor verantwoordelijk zou moeten zijn.

De wereldwijde vraag naar cybersecurityexperts zal naar verwachting voor het einde van dit decennium een derde hoger zijn dan het aantal beschikbare experts

Uit de resultaten blijkt dat een gezamenlijke inspanning van de branche en het onderwijs nodig is om deze kloof te dichten en dat we de handen ineen moeten slaan als we jongeren enthousiast willen maken voor een carrière in de cyberbeveiliging. Deze generatie is meer verweven met technologie dan eerdere generaties, maar als dit niet in goede banen wordt geleid, dreigt het gevaar dat jongeren met technologisch talent snel in de verleiding komen om hun vaardigheden te gebruiken voor criminele activiteiten. Jongeren moeten worden gewezen op de carrièremogelijkheden binnen de cyberbeveiliging en moeten worden aangemoedigd om hun vaardigheden te ontwikkelen ten behoeve van de samenleving. Met behulp van een combinatie van onderwijs en leren in de praktijk moeten we jongeren vormen en ze stimuleren om te kiezen voor een carrière in de cyberbeveiliging, voordat de kloof nog groter wordt.

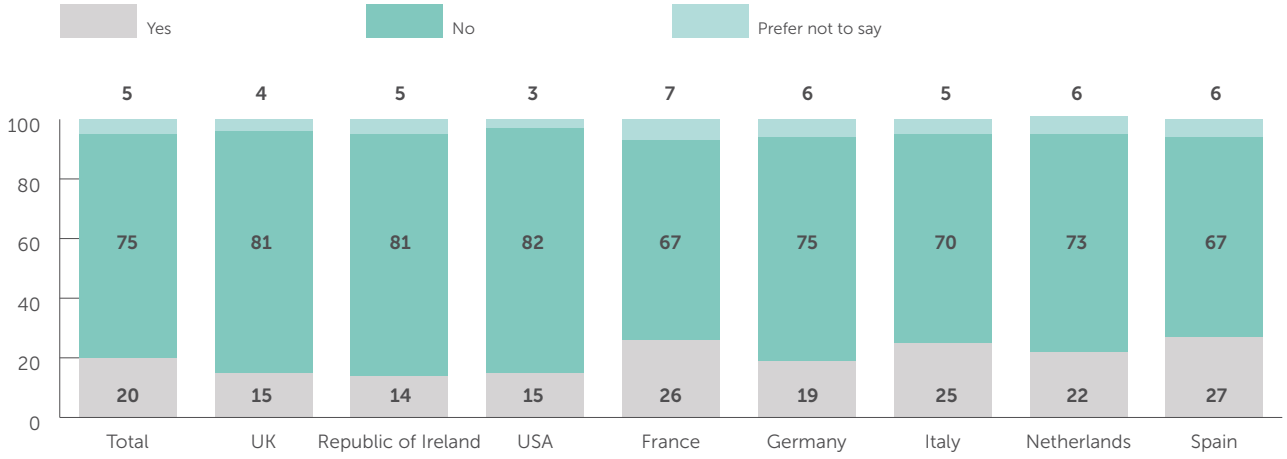
De uitkomsten van het onderzoek

Jongeren komen veelvuldig in de verleiding om zich in te laten met cybercriminaliteit, in plaats van deze te voorkomen

De huidige generatie jongvolwassenen is zeer goed opgeleid, maar vaak ook zeer beïnvloedbaar als ze beginnen aan het volgende hoofdstuk in hun leven: wanneer ze beginnen in het voortgezet onderwijs, zelfstandig gaan wonen of beginnen in een nieuwe baan. Omdat ze zijn opgegroeid in de digitale wereld, is technologie verweven met hun leven, maar dat zorgt er ook voor dat ze niet meer opkijken van grootschalige cyberaanvallen.

Kent u iemand in uw omgeving die zich bezighoudt met mogelijk illegale cyberactiviteiten (bijvoorbeeld hacken)?

We hebben ondervonden dat 23% van de 18-jarigen iemand kent die zich bezighoudt met cyberactiviteiten (zoals hacken) die als illegaal gezien kunnen worden. Dergelijke activiteiten komen vaker voor onder jongeren die een opleiding volgen aan een universiteit (24%) en onder jongeren die pas afgestudeerd zijn en een baan hebben (23%). Ter vergelijking: van de ondervraagde werkeloze schoolverlaters kent slechts 15% iemand die zich bezighoudt met mogelijk illegale cyberactiviteiten.



Hun bezorgdheid is slechts marginaal groter dan hun nieuwsgierigheid, en sommigen hebben zelfs bewondering voor dit soort misdaden. Bijna de helft (47%) van de jongeren onder de 25 jaar zegt 'onder de indruk' te zijn als ze horen dat een bedrijf is gehackt en een derde (33%) van alle jongeren is zelfs geïnteresseerd in hoe de hack is uitgevoerd. Uit ons onderzoek blijkt wel dat de bezorgdheid groter wordt naarmate de leeftijd hoger is. Van de jongeren tussen 21 en 25 jaar geeft 40% aan dat ze zich zorgen maken over de schade die is veroorzaakt en hoe een bedrijf daarmee omgaat, tegenover slechts 36% van de ondervraagde 16-jarigen.

Alarmerender is dat hacken door meer dan de helft (57%) van de jongeren onder de 25 jaar wordt beschouwd als een 'indrukwekkende' vaardigheid. Een groot aantal jongeren geeft bovendien aan dat ze hun vaardigheden graag inzetten om lol te maken (17%), voor clandestiene activiteiten (16%) of voor financieel gewin (11%).

Velen onder hen zijn al in staat om deze grenzen te laten vervagen. Zo weet bijna een derde (31%) van de jongeren onder de 25 jaar hoe ze hun IP-adres kunnen verbergen. Het feit dat slechts 50% van de ondervraagde jongeren zegt daadwerkelijk te willen meewerken aan het bestrijden van cybercriminaliteit toont aan dat er een duidelijk tekort aan betrokkenheid is onder jongeren als het gaat om het inzetten van hun cybervaardigheden ter voorkoming van criminaliteit.

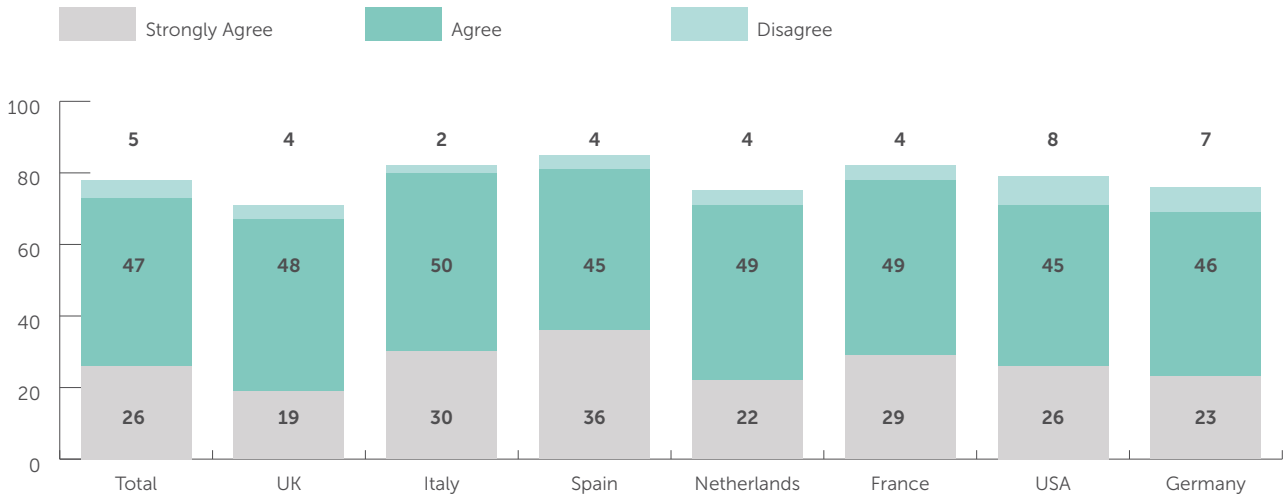
Bedrijven hebben jonge mensen nodig in de strijd tegen cybercriminaliteit

Nu de kloof op het gebied van cybervaardigheden steeds wijder wordt, is er een grote rol weggelegd voor jonge IT-fanaten om de frontlinie van de cyberbeveiliging van nieuw bloed te voorzien. Bovengenoemde groep beschikt al over de basiskennis en de wil om te leren, maar helaas kunnen werkgevers de interesses en het talent van deze jongeren nog niet benutten in de praktijk.

Een overweldigend aantal professionals uit de branche (93%) is zich ervan bewust dat het vak zal moeten meegroeien met het huidige en het toekomstige landschap. Daarnaast vindt 87% vindt het belangrijk dat jongeren deelnemen aan de strijd tegen cybercriminaliteit.

Het probleem is echter dat in vele bedrijven er geen of onvoldoende functies beschikbaar zijn op instapniveau. De meeste werkgevers (72%) werven intern en bieden waar nodig mogelijkheden voor interne trainingen. Als ze al extern werven, zoekt het overgrote deel (53%) alleen doorgewinterde beveiligingsprofessionals.

In hoeverre bent u het eens met de stelling: "Het is moeilijk om voldoende IT securityprofessionals te vinden om te rekruteren"?

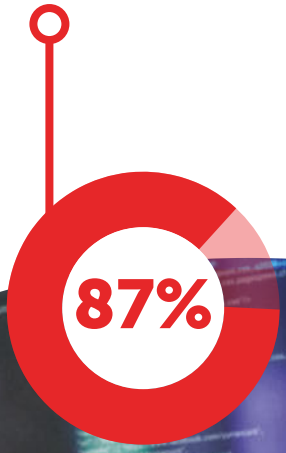


Het is belangrijk om te realiseren dat het tijd kost om vaardigheden op het gebied van beveiliging te ontwikkelen en ervaring op te doen, net als bij andere vakgebieden binnen de IT en andere beroepen. Medewerkers krijgen een functie toebedeeld die aansluit bij hun vaardigheidsniveau, ze leren door in de praktijk en krijgen passende trainingen. Maar aangezien bijna drie kwart (73%) van de bedrijven te kennen geeft dat het lastig is om juist opgeleide IT-professionals te vinden, is het misschien tijd om de traditionele wegen naar een baan binnen de cyberbeveiliging opnieuw vorm te geven.

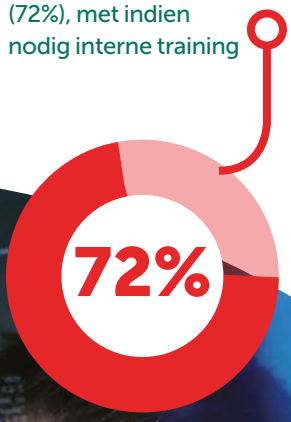
BELANGRIJKE BEVINDINGEN

Een overweldigende meerderheid van de professionals in de industrie (93%) zegt dat het beroep zich moet blijven ontwikkelen om bij te blijven met het huidige én toekomstige dreigingslandschap

87% vindt het belangrijk dat jongeren deelnemen aan de strijd tegen cybercriminaliteit



Het probleem is dat veel werkgevers geen cybersecurityfuncties op instapniveau bieden; de meesten promoveren mensen binnen de organisatie (72%), met indien nodig interne training

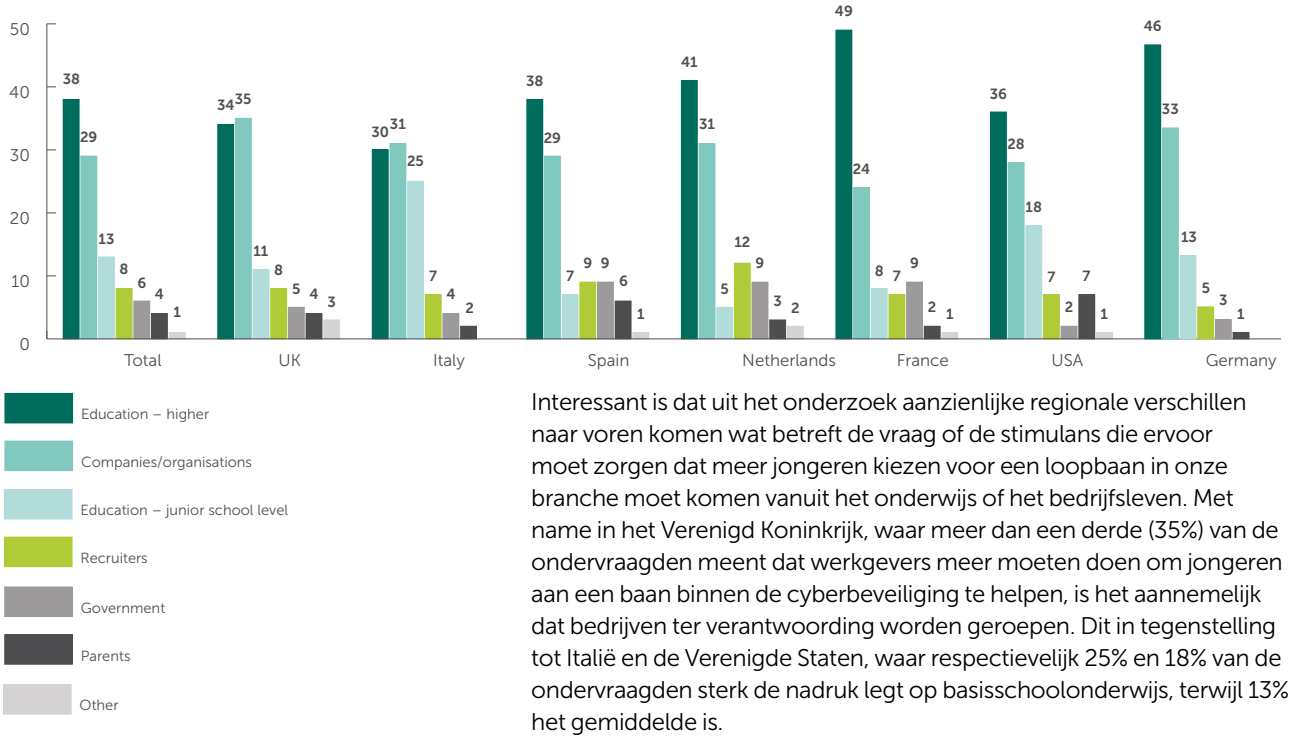


Ligt de verantwoordelijkheid bij de werkgevers of bij het onderwijs?

De vraag wie verantwoordelijk is om de volgende generatie van cyberbeveiligers enthousiast te maken, is een belangrijke omdat ons een omvangrijke uitdaging wacht. We hebben een plan nodig waarmee we de duidelijk aanwezige interesse van jongeren kunnen trekken voor cyberbeveiliging, voordat ze besluiten om hun vaardigheden te gebruiken voor crimineel gewin.

De IT-branche is van mening dat het onderwijssysteem daarin een grote rol dient te spelen door jong talent al tijdens de opleiding aan te moedigen om een carrière in ons beroep na te streven en zo het vaardigheidsniveau op peil te brengen. Uit het door ons uitgevoerde onderzoek blijkt dat bijna twee derde (62%) van de IT-professionals vindt dat het de verantwoordelijkheid van onderwijsinstellingen is om de toekomstige generatie cyberbeveiligingsprofessionals op te leiden. Maar het gegeven dat 27% de primaire verantwoordelijkheid bij het bedrijfsleven legt, geeft aan dat de branche zelf ook een duidelijke rol heeft bij het beschermen van haar eigen toekomst.

Wie zou de hoofdverantwoordelijkheid moeten dragen om jong talent te stimuleren om voor dit beroep te kiezen?



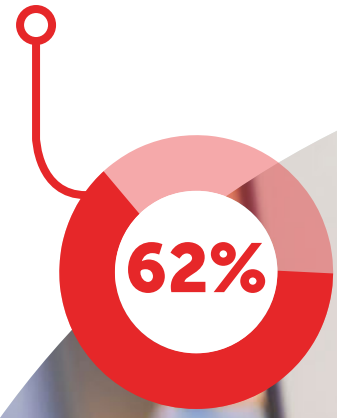
Interessant is dat uit het onderzoek aanzienlijke regionale verschillen naar voren komen wat betreft de vraag of de stimulans die ervoor moet zorgen dat meer jongeren kiezen voor een loopbaan in onze branche moet komen vanuit het onderwijs of het bedrijfsleven. Met name in het Verenigd Koninkrijk, waar meer dan een derde (35%) van de ondervraagden meent dat werkgevers meer moeten doen om jongeren aan een baan binnen de cyberbeveiliging te helpen, is het aannemelijk dat bedrijven ter verantwoording worden geroepen. Dit in tegenstelling tot Italië en de Verenigde Staten, waar respectievelijk 25% en 18% van de ondervraagden sterk de nadruk legt op basisschoolonderwijs, terwijl 13% het gemiddelde is.

Wanneer het echter gaat over wie ervoor moet zorgen dat jongeren de juiste vaardigheden ontwikkelen, wijst het overgrote deel naar het hoger onderwijs (49%) en een iets minder groot deel naar bedrijven en organisaties (27%). Maar, zoals gezegd, lopen de meningen per regio uiteen en zo wordt in een regio als Nederland bijvoorbeeld weer meer verwacht van werkgevers (40%).

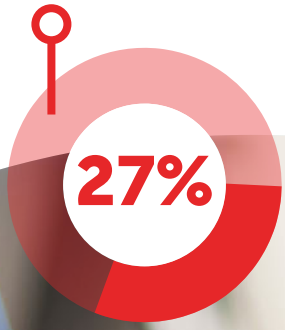
Het is duidelijk dat er verschillen zijn als gevolg van verschillende onderwijssystemen en prioriteiten van de overheid. Toch zal er een gezamenlijke benadering gehanteerd moeten worden waarbij zowel werkgevers als onderwijs betrokken zijn zodat de vaardigheden van deze generatie met veel interesse in technologie tot wasdom kunnen komen.

BELANGRIJKE BEVINDINGEN

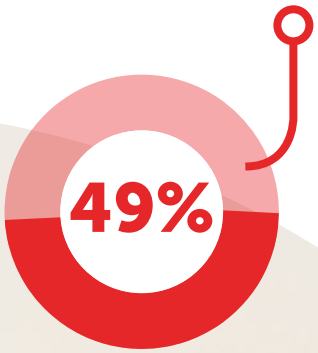
Ons onderzoek wijst uit dat bijna twee derde van de IT-professionals (62%) van mening is dat in de eerste plaats educatieve instellingen verantwoordelijk zouden moeten zijn voor het voorbereiden van toekomstige generaties van cybersecurityprofessionals



Er ligt ook een duidelijke rol voor de sector om zijn eigen toekomst veilig te stellen: 27% legt de primaire verantwoordelijkheid bij de business



Voor wat betreft het garanderen dat jongeren beschikken over de juiste vaardigheden, wordt de grootste nadruk gelegd op hogere educatie (49%)



De toekomst van de beveiligingsbranche veiligstellen

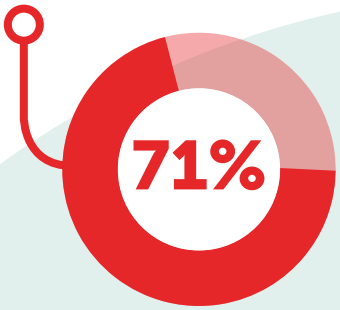
Er zal meer gedaan moeten worden om jong talent te ontwikkelen en richting onze branche te trekken omdat de huidige, groeiende vaardigheidskloof gelijk staat aan een tikkende tijdbom.

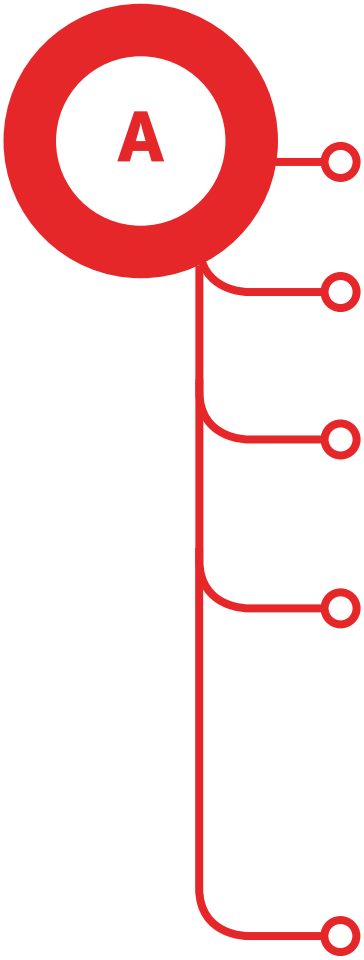
We moeten zorgen dat cyberbeveiliging gemakkelijker toegankelijk is en aantrekkelijk wordt gemaakt voor deze goed opgeleide jongeren. Een van de uitkomsten van ons onderzoek is dat bijna drie kwart (71%) van de ondervraagde jongeren onvoldoende of niet op de hoogte is van alle afstudeer- en stagemogelijkheden op het gebied van IT-beveiliging.

Bedrijven stellen dat nieuwkomers niet beschikken over de benodigde vaardigheden of ervaring in cyberbeveiliging, maar daar staat tegenover dat maar weinig bedrijven functies openstellen voor beginners of stages aanbieden die kunnen bijdragen aan de ontwikkeling van talent. Het is zelfs zo dat slechts in 45% van de bedrijven dergelijke functies of mogelijkheden bestaan.

Drie op de tien bedrijven (30%) geven toe dat ze niet beschikken over de interne middelen om afgestudeerden te laten groeien naar een functie binnen de cyberbeveiliging. Zorgwekkender nog is dat slechts één op de vijf (20%) van de ondervraagden vond dat IT-beveiliging binnen vijf jaar zou moeten vallen onder de verantwoordelijkheid van een speciaal cyberbeveiligingsteam, waarbij bijna de helft (50%) zelfs van mening was dat het aanpakken van cybercriminaliteit een taak zou moeten zijn voor het algemene IT-team.

We ontdekten dat bijna driekwart van de jongeren (71%) niet bewust is van afstudeermogelijkheden of stageplaatsen op het gebied van IT security





De oplossing

Vanuit Kaspersky Lab beschouwen we dit rapport als het begin van een lange weg om de kloof op het gebied van cybervaardigheden te dichten. Wij denken dat een probleem van deze omvang alleen opgelost kan worden via gecoördineerde inspanningen van het bedrijfsleven, het onderwijs en de overheid.

Wij zijn ook van mening dat werkgevers meer moeten doen om een loopbaan binnen de cyberbeveiliging aantrekkelijker te maken voor jongeren. Binnen de groep IT-beveiligingsprofessionals geeft 27% toe dat organisaties zich meer moeten inspannen om trainingen en mogelijkheden voor afgestudeerden te creëren.

Initiatieven vanuit de branche kunnen bijdragen aan de promotie van een loopbaan binnen de cyberbeveiliging. Tijdens internationale wedstrijden voor universitaire studenten en jonge professionals wordt jong talent bijvoorbeeld gestimuleerd om hun vaardigheden te gebruiken door diverse uitdagingen op het gebied van cyberbeveiliging op te lossen. Hierdoor merken ze hoe waardevol ze kunnen zijn voor de branche en de maatschappij.

In nauwe samenwerking met universiteiten kan onze branche een cruciale rol vervullen bij de ontwikkeling van talent en zorgen dat zowel de theorie- als de praktijklessen aansluiten bij verwachtingen en toekomstige behoeften. Door te overleggen over cursusmateriaal, gastcolleges te geven, presentaties te houden over technologie en samen te werken aan onderzoeken, kan de branche bijdragen aan het stimuleren, betrekken en, belangrijker nog, informeren en opleiden van een volgende generatie cyberbeveiligers. Als we stages, traineeships en functies voor afgestudeerden kunnen aanbieden, kunnen we de relatie tussen het bedrijfsleven en het onderwijs verstevigen en waarborgen dat we waardevolle vaardigheden kunnen inzetten wanneer ze het hardst nodig zijn.

Uit de bevindingen in dit rapport blijkt hoe groot de uitdaging is waar de branche voor staat en op welke gebieden nog vooruitgang kan worden geboekt. We zullen deze stappen moeten zetten om de tikkende tijdbom die de cyberbeveiliging bedreigt op tijd te ontmantelen.

1 Over het onderzoek: dit onderzoek is in opdracht van Kaspersky Lab uitgevoerd door Arlington Research onder in totaal 2.120 IT-professionals in Nederland, het Verenigd Koninkrijk, Ierland, Italië, Spanje, Frankrijk, Duitsland en de VS. Arlington Research heeft in opdracht van Kaspersky Lab tevens 11.531 jonge consumenten tussen 16 en 25 jaar ondervraagd in Nederland, het Verenigd Koninkrijk, Ierland, Italië, Spanje, Frankrijk en Duitsland. Beide onderzoeken zijn afgerond in juli 2016.

KASPERSKY LAB

Kaspersky Lab, 1st Floor
2 Kingdom Street
London, W2 6BD, UK

www.kaspersky.co.uk

KASPERSKY lab

FUTUREPROOFING CYBERSECURITY

INVESTING IN TODAY'S TALENT TO SECURE TOMORROW