Advies aan de staatssecretarissen van Veiligheid en Justitie en Onderwijs, Cultuur en Wetenschap inzake cybersecurity in het onderwijs en het bedrijfsleven.

CSR
Cyber Security Council
Cyber Security Raad

Excellenties,

De wereld digitaliseert in hoog tempo. Nederland heeft daarin een vooraanstaande positie op het terrein van digitalisering en behoort tot de top 10 van meest concurrerende kenniseconomieën in de wereld[1]. Wil ons land deze positie blijven behouden, dan moeten we zorgen voor een open, veilige en economisch kansrijke digitale samenleving. Een samenleving die innovatief en ondernemend is, maar die ook weerbaar is tegen de risico's die de grote afhankelijkheid van ICT met zich meebrengt. Een samenleving waarin zorgvuldig omgegaan wordt met digitale gegevens en waar cybersecurity voldoende aandacht krijgt. Als Nederland niet genoeg investeert in cybersecurity, kunnen bedrijfsleven, overheid en burgers kwetsbaar worden voor onder andere bedrijfsspionage, het stelen van privacygevoelige gegevens, identiteitsfraude, productieverstoring of imagoschade. Dat komt onze welvaart en maatschappij niet ten goede. De digitale toekomst van Nederland moet veilig worden gesteld. Dat kan door te zorgen voor voldoende cybersecurity professionals en door de Nederlandse jeugd voor te bereiden op de digitale toekomst. De Cyber Security Raad acht het van belang deze zaken voortvarend aan te pakken.

Tekort aan cybersecurity professionals

Een van de doelstellingen uit de Nationale Cybersecurity Strategie 2[2] is dat Nederland beschikt over voldoende kennis en kunde op het gebied van cybersecurity en investeert in ICT-innovatie. Om dat te bereiken heeft Nederland goed gekwalificeerde ICT- en cybersecurity-professionals nodig die over de juiste kennis en vaardigheden beschikken. Zij zijn nu, en in de toekomst, nodig om Nederland digitaal veilig en onze economie welvarend te houden. Uit het onlangs verschenen onderzoek 'Arbeidsmarkt voor Cyber Security Professionals'[3] blijkt dat er op dit moment vooral een kwalitatief tekort is aan cybersecurity professionals en dat op iets langere termijn een kwantitatief tekort is te verwachten. De geschatte omvang van het te verwachten tekort aan digitale professionals is uiteenlopend[4]. Zeker is dat de vraag naar cybersecurity specialisten zowel in de publieke als private sector de komende jaren zal toenemen. Het onderzoeksrapport signaleert ook het risico van een disbalans tussen vraag en aanbod. De arbeidsmarkt (vraag) en de opleidingswereld (aanbod) sluiten nog onvoldoende op elkaar aan[5]. Dat maakt de digitale samenleving extra kwetsbaar en vraagt om anticipatie op korte termijn.

Cybersecurity in het onderwijscurriculum

De doelstellingen uit de Nationale Cybersecurity Strategie 2 bereiken we niet alléén door voldoende en kwalitatieve cybersecurity professionals op te leiden, maar ook door jongeren binnen het onderwijs voldoende algemene cybersecuritykennis en -kunde bij te brengen. In dat kader is het van groot belang om in het onderwijs aandacht te besteden aan digitale geletterdheid[6] van leerlingen. Jong geleerd is immers oud gedaan. Digitale geletterdheid is de combinatie van ICT-basisvaardigheden, computational thinking, informatievaardigheden en mediawijsheid[7]. Deze competenties stellen hen in staat actief en bewust veilig deel te nemen aan de digitale samenleving. De afgelopen jaren zijn er diverse initiatieven ontplooid op het terrein van digitale geletterdheid in onderwijs en bedrijfsleven.

1 Global Competitiveness Report 20142015
2 Nationale Cybersecurity Strategie 2, *'Van bewust naar bekwaam'*, ministerie van Veiligheid en Justitie, 20142016.
3 *Arbeidsmarkt voor Cyber Security Professionals*, december 2014, PLATO, in opdracht van het Wetenschappelijk Onderzoek en Documentatie Centrum van het Ministerie van Veiligheid en Justitie.
4 Dialogic rapport: '*De ICT-er bestaat niet*', mei 2014.
5 Het *Human Capital Report van het World Economic Forum* (mei 2015) geeft aan dat werkgevers moeite hebben om bepaalde digitale functies in te vullen vanwege het relatief eenzijdige aanbod van beroeps vaardigheden. Het UWV noemt in een rapport van februari 2015 ook expliciet een dreigend tekort aan security specialisten.
6 De term 'Digitale geletterdheid' komt uit het rapport *'21e eeuwse vaardigheden in het curriculum van het funderend onderwijs'*, SLO 2014.

Echter, de aanpak van deze verschillende initiatieven is onvoldoende op elkaar afgestemd. Vaak worden cybersecurity-aspecten onderbelicht. Deze nalatigheid kan Nederland zich niet veroorloven.

Advies

Om Nederland een concurrerende kenniseconomie te laten blijven, die wordt gekenmerkt door een open, veilige en economisch kansrijke digitale samenleving, moet er meer samenhang komen in de initiatieven op het gebied van cybersecurity in het onderwijs en het bedrijfsleven. Tevens is er meer aandacht nodig voor de digitale opvoeding van jongeren, zodat zij zich van jongs af aan veilig in het cyberdomein kunnen begeven. De doelstelling van dit CSR-advies is dan ook tweeledig:

1. Nederland beschikt over voldoende en juist gekwalificeerde cybersecurity professionals die zich kunnen begeven op een transparante arbeidsmarkt, zodat organisaties in de juiste mate voorzien kunnen worden van werknemers in het groeiende aantal digitale functies.
2. Nederlandse jongeren zijn goed voorbereid op de digitale toekomst door middel van een geïntegreerde aanpak in het onderwijs die ervoor zorgt dat digitale geletterdheid en cybersecurity onderdeel worden van het curriculum.

Ad. 1 Nederland beschikt over voldoende en juist gekwalificeerde cybersecurity professionals die zich kunnen begeven op een transparante arbeidsmarkt, zodat organisaties in de juiste mate voorzien kunnen worden van werknemers in het groeiende aantal digitale functies.

Om ervoor te zorgen dat er voldoende professionals zijn met de juiste competenties, moet nu al begonnen worden met het interesseren van potentiële professionals en het ontwikkelen van de juiste vaardigheden. Bedrijven moeten zich bekwamen in het stellen van de juiste eisen aan de professionals. Er moeten heldere omschrijvingen komen van digitale functies en bijbehorende functie-eisen. Om de disbalans tussen vraag en aanbod weg te nemen is er transparantie nodig in de opleidingsroutes en loopbaanmogelijkheden. Er is veel aanbod van opleidingen, maar studenten weten vaak niet welke studie hen specifiek voorbereid op de functies die aangeboden worden. En soms is die opleiding er (nog) niet. Meer contact tussen werkveld, bedrijven en beroepsopleidingen is nodig, zodat beter kan worden afgestemd waaraan behoefte is bij bedrijven. Hiervoor dient de cyber-bewustwording bij bedrijven en instellingen te worden verhoogd[8]. Tevens is er behoefte aan meer gekwalificeerde opleiders, learning on the job en/of duale trajecten, waarbij studenten en eventuele zijinstromers leren en werken in het vakgebied. Kennis wordt direct overgebracht met behulp van de nieuwste vormen van kennisoverdracht.
Meer aandacht voor het onderwerp cybersecurity en de loopbaanmogelijkheden in dit domein zou tevens kunnen leiden tot meer jongeren die op dit terrein werkzaam willen zijn. Ook dat is namelijk een onderliggend probleem; nog te weinig jongeren kiezen voor een opleiding of een baan in het cybersecurity domein. De Human Capital Agenda ICTinnovatie[9], de pilots ‘flexibilisering en

7 Mediawijsheid (ook wel: digital awareness) : het geheel van kennis, vaardigheden en mentaliteit waar mee burgers zich bewust, kritisch en actief kunnen bewegen in een complexe, veranderlijke en digitale wereld (Raad voor Cultuur, 2005)

8 QIS (Qualification of Information Security Professionals) stelt een kwalificatiestelsel voor cybersecurity functies op, op basis van Europese normen. QIS stimuleert de ontwikkeling van opleidingen voor jong talent en voor huidige professionals in aansluiting op de Europese arbeidsmarkt.

experimenten vraagfinanciering'[10], en het Techniekpact[11] richten zich op de oplossing van deze vraagstukken. Het Cyber Security Research and Education Platform (CSRE) is een stap in de goede richting, waar het gaat om het verbinden van onderwijs en onderzoek. De Raad onderschrijft het belang van deze initiatieven.

Ad. 2 Nederlandse jongeren zijn goed voorbereid op de digitale toekomst door middel van een geïntegreerde aanpak in het onderwijs die ervoor zorgt dat digitale geletterdheid en cybersecurity onderdeel worden van het curriculum.

Het basis- en voortgezet onderwijs spelen een structurele rol in het voorbereiden van de jeugd op de digitale samenleving. Om actief en op verantwoorde wijze deel te kunnen nemen aan de digitale samenleving, de groeiende kennismaatschappij en technologische ontwikkelingen, zouden jongeren zo vroeg mogelijk moeten leren omgaan met ICT, digitale media en (persoonlijke) digitale informatie. Het begrijpen van de belangrijkste sociale aspecten, wettelijke en morele grenzen en cybersecurity vraagstukken zou moeten uitmonden in een digitaal vaardigheidsbewijs voor jongeren. In het primair en voortgezet onderwijs zou digitale geletterdheid en cybersecurity daarom onderdeel van het curriculum moeten zijn. De CSR hecht in dit kader belang aan de voorstellen van het Platform 2032 (OCW/SER).

Leraren zullen moeten worden bijgeschoold om leerlingen meer richting, stimulans en inhoudelijke bagage te geven op het gebied van ICT en cybersecurity. Het is belangrijk dat leerkrachten in staat worden gesteld zelf te begrijpen waar het om gaat, wat hun leerlingen moeten weten en hoe ze deze kennis het beste kunnen overbrengen. ICT'ers zouden daarbij kunnen helpen door docenten te 'coachen'. De Raad adviseert dat alle opleidingen (basis-, voortgezet en beroepsonderwijs) in Nederland standaard aandacht besteden aan digitale geletterdheid en in het bijzonder aan cybersecurity. In vrijwel alle beroepen is immers een digitale component te vinden.

9 Om specifieke tekorten op het gebied van ICT op de arbeidsmarkt te verkleinen, werkt het Team ICT innovatie, aan een Human Capital Agenda. Deze Human Capital Agenda ICTinnovatie bevat voorstellen om onderwijs en arbeidsmarkt beter op elkaar te laten aansluiten én om Leven Lang Leren te stimuleren.

10 http://www.rijksoverheid.nl/documentenenpublicaties/brieven/2015/06/26/briefoverkadersexperimentenvraagfinancieringenpilotsflexibilisering.html

11 Techniekpact moet de aansluiting van onderwijs op de arbeidsmarkt in de techniekssector verbeteren en daarmee het tekort aan technisch personeel terugdringen.

AANBEVELINGEN

1. Bestaande en nieuwe initiatieven worden met elkaar verbonden vanuit een gedeelde visie. De Human Capital Agenda, het Platform 2032 en het Cyber Security Research and Education Platform (CSRE) bundelen de krachten op het gebied van cybersecurity in het onderwijs en de aansluiting van het onderwijs op de arbeidsmarkt.

2. Er komt meer transparantie in het aanbod van opleidingen, vacatures en loopbaanmogelijkheden voor cybersecurity specialisten. Er komt meer inzicht in de benodigde kennis en vaardigheden voor banen in het cybersecurity domein.

3. De samenwerking tussen bedrijfsleven en opleidingen wordt geïntensiveerd, zodat vraag en aanbod beter op elkaar worden afgestemd. Er worden duale trajecten ingevoerd bij bedrijven. Deze aanpak voorziet in 'learning on the job', waarbij specialisten de kans krijgen op een moderne manier hun kennis snel over te dragen aan (zij)instromers op de arbeidsmarkt. De overheid en het bedrijfsleven stellen structureel stageplaatsen/traineeships beschikbaar op het gebied van cybersecurity.

4. Er komt een geïntegreerde aanpak in het onderwijs die ervoor zorgt dat digitale geletterdheid en cybersecurity onderdeel worden van het curriculum om jongeren de vaardigheden van de toekomst aan te leren.

5. Leerlingen in het primair onderwijs halen een digitaal vaardigheidsbewijs.
   Dit vaardigheidsbewijs stelt kinderen in staat zich veilig in het digitale domein te begeven.[12] Ook is er aandacht voor wettelijke en morele grenzen op het internet, zodat kinderen leren hoe ver ze mogen gaan en wat de risico's zijn van het overtreden van deze regels.

6. Leraren in primair en hoger onderwijs worden geprofessionaliseerd op het gebied van digitale geletterdheid en cybersecurity. ICT'ers krijgen een rol in het geven van onderwijs en het coachen van leraren op ICT-gebied.

's-Gravenhage, 2 november 2015

Namens de Cyber Security Raad

Eelco Blok

Dick Schoof

12 *Academie voor Media en maatschappij*. Dit is in september 2015 gelanceerd. Scholen kunnen er zelf toe overgaan dat aan te schaffen.