CSR MAGAZINE

Cyber Security Raad

De economische en maatschappelijke noodzaak van meer cybersecurity • Nederland digitaal droge voeten • Top van Nederland aan het woord over de digitale veiligheid van Nederland

SPECIALE UITGAVE

Jaargang 3, nummer 1, maart 2017

Foto: Niels Vos - Nationale Beeldbank

CYBERSECURITY: HET BELANG VAN DIGITAAL DROGE VOETEN

Hans Brinker. Een jongen die een heel dorp redt door zijn vinger in een dijk te steken. Een oer-Hollands verhaal, in 1865 bedacht door een Amerikaanse schrijfster. De Nederlandse strijd tegen het water is wereldwijd bekend. Iedereen is overtuigd van het belang ervan. Het kabinet investeert in onze veiligheid met een Deltaplan. Visie, ambitie, actieprogramma en budget zijn vastgesteld.

Hans Brinker. Een hacker die Nederland redt door een digitaal lek te dichten. Dat zou zomaar een oer-Hollands verhaal kunnen zijn, want onze digitale 'waterkeringen' zijn nog niet op orde. Het niveau van cybersecurity in Nederland moet beslist beter, omdat we één van de meest ICT-intensieve economieën hebben van Europa en dus kwetsbaar zijn voor de sterk toenemende cyberdreigingen.

De Nederlandse overheid moet, in samenwerking met het bedrijfsleven, ook als het om cybersecurity gaat vooruitkijken en zorgen voor visie, ambitie, actieprogramma's en financiën. In publiek-private samenwerking moet een ecosysteem gebouwd worden dat ons land veilig houdt en economische kansen benut. Het onafhankelijke rapport van Herna Verhagen – 'De economische en maatschappelijke noodzaak van meer cybersecurity' – onderschrijft dit en geeft hier richting aan. Landen als Duitsland en het Verenigd Koninkrijk investeren flink in cybersecurity. En zij zijn niet de enige. Nederland *kan* en *mag* niet achterblijven. Dankzij onze digitale economie en samenleving kan Nederland als gidsland een toppositie bekleden als het gaat om cybersecurity. Maar dan moet er wel worden geïnvesteerd. Dan moeten de handen wel ineengeslagen worden. Politiek, overheid, bedrijfsleven en wetenschap zijn gezamenlijk aanzet.

Eigenlijk zou een hoog cybersecurityniveau net zo vanzelfsprekend moeten zijn als hoge waterkeringen. In dit magazine geven topfunctionarissen uit overheid en bedrijfsleven hun visie op wat er nodig is om het digitale veiligheidsniveau in Nederland te verhogen.

Namens de Cyber Security Raad,
Eelco Blok, Dick Schoof

INHOUDSOPGAVE

Wat is de economische en maatschappelijke noodzaak van meer cybersecurity? Hiernaar heeft Herna Verhagen, CEO van PostNL, een onafhankelijk onderzoek gedaan op verzoek van de Cyber Security Raad. Ze sprak onder meer met diverse cyberexperts. “Het leverde interessante inzichten op en goede adviezen, óók over de kansen.”

Herna Verhagen
CEO PostNL

NEDERLAND DIGITAAL DROGE VOETEN

DIGITALISERING BIEDT ENORME KANSEN

In oktober 2016 overhandigde Verhagen het onderzoeksrapport en bijbehorende adviezen onder grote belangstelling in Nieuwspoort aan premier Mark Rutte en VNO-NCW voorzitter Hans de Boer. Dat droeg bij aan een belangrijk doel van de Cyber Security Raad (CSR): cybersecurity hoog op de politieke agenda krijgen.

Wat was voor u de reden om in te gaan op het verzoek van de CSR?

“Cybersecurity raakt iedereen. De overheid en veel grotere bedrijven zijn er al langer mee bezig. Ook voor kleine bedrijven en mensen thuis is het een steeds urgenter onderwerp. Tegelijkertijd is cybersecurity nogal abstract en voor velen *ver-van-mijn-bed*. De meeste mensen kunnen zich weinig voorstellen bij cyberrisico’s. Iedereen kent de *phishing*-mails en velen beseffen dat niet iedere website betrouwbaar is. Dat consumenten de risico’s niet zo helder hebben, is misschien te verwachten. Toch geldt dat ook nog voor veel overheden en bedrijven. Meer bekendheid geven aan cyberrisico’s en een advies geven over mogelijke oplossingen is in het belang van de Nederlandse economie en Nederlandse bedrijven en overheden. Graag draag ik er – vanuit mijn positie als CEO van PostNL – aan bij dat het onderwerp steviger op de kaart komt.
Persoonlijk zou ik niet alleen de risico’s willen benadrukken, maar óók de kansen. Nederland loopt voorop in de digitalisering. We hebben het grootste internetknooppunt ter wereld, de *Amsterdam Internet Exchange* (AMS-IX), en diverse razendsnelle, breedbandige telecom-netwerken. Hierdoor zijn we een van de meest ICT-intensieve economieën van Europa.
Ruim 5 procent van ons Nationaal Inkomen werd in 2015 verdiend met ICT. Onze digitale infrastructuur vormt, naast Schiphol en de Rotterdamse haven, de derde mainport van ons land. Dat brengt ons veel groei en werk-gelegenheid. Hoe beter we de cybersecurity op orde hebben, hoe meer we daarvan kunnen profiteren.”

Voor het advies sprak u experts op het gebied van cybersecurity. Wat viel u op in de gesprekken?

"Wat de cyberexperts vertellen, stelt helaas niet gerust: het dreigingsbeeld is echt zorgelijk. Veel ICT-systemen zijn kwetsbaar, bijvoorbeeld door lekken, programmeerfouten en tekortschietende beveiliging. Daarnaast is er een beperkte coördinatie en sturing vanuit de overheid. Samenwerking tussen overheidspartijen onderling en tussen private partijen en overheden is niet voldoende geborgd. Er zijn veel partijen betrokken bij cybersecurity, maar het is onduidelijk welke partij waarvoor verantwoordelijk is als het gaat om cybersecurity. Criminelen maken dankbaar gebruik van de beperkte controle en de zwakke beveiliging van onze digitale wereld. Cyberspionage en cybercriminaliteit zijn aan de orde van de dag. Ook diverse wetenschappelijke rapporten en publicaties die we hebben geraadpleegd over dit onderwerp bevestigen dat beeld. Alleen al in Nederland is de becijferde schadepost als gevolg van cybercrime en spionage jaarlijks 10 miljard euro, circa 1,5 procent van ons bnp. Daarnaast blijkt uit onderzoek dat een significant deel van de schade niet eens opgemerkt wordt. Kortom, we moeten ons echt zorgen maken en in actie komen. Het rapport bevat heldere adviezen en concrete acties voor het versterken van cybersecurity. Het begint met meer aandacht: in de Tweede Kamer, de bestuurskamer en de huiskamer."

Wat zijn de belangrijkste punten uit het adviesrapport?

"De adviezen gaan over de rol van de overheid, de rol van de private sector, de samenwerking tussen beide en digitale vaardigheden. Een belangrijk advies aan het nieuwe kabinet is wat mij betreft: zorg voor een eenduidige politieke aansturing van de digitale mainport via een onderraad van de Ministerraad én benoem een hoge functionaris voor cybersecurity. De taak van deze functionaris is een meerjarig actieprogramma met investeringsagenda opstellen en uitvoeren. Verder is het zaak dat de

Eelco Blok, covoorzitter Cyber Security Raad:

"De concurrentiepositie van Nederland staat onder druk. En daarmee ook onze economie en welvaart."

Minister-president Mark Rutte:

"Het is goed dat dit rapport digitale vaardigheden als standaardonderdeel in het onderwijs aanbeveelt. Als we mensen al op jonge leeftijd cyberwijs maken heeft dat een gunstige doorwerking op de lange termijn."

Hans de Boer, voorzitter Vereniging VNO-NCW:

"Cybersecurity is een essentiële randvoorwaarde voor economische groei en welvaart. Het thema verdient aandacht, op álle niveaus, bij de overheid, het bedrijfsleven en bij de consument."

private sector de basis op orde heeft en voldoet aan alle randvoorwaarden voor cybersecurity. En dat de sector ketens veiliger maakt door het invoeren van een ketenverantwoordelijkheid. Voor private dienstverleners is het mogelijk een accreditatie- of certificeringssystematiek te ontwikkelen. Een ander actiepunt is om digitale geletterdheid, inclusief cybersecurity, versneld op te nemen in het kerncurriculum voor het basis- en voortgezet onderwijs. Ook is het van belang kennisontwikkeling op het gebied van cybersecurity te stimuleren. Tot slot geldt dat we allemaal bereid moeten zijn te investeren in cybersecurity. Zowel de overheid als het bedrijfsleven doen er goed aan om jaarlijks 10 procent van het IT-budget te reserveren voor specifieke cybersecurity-maatregelen. Deze maatstaf is gebaseerd op onderzoek naar dit soort investeringen in vergelijkbare landen als Nederland. Ook voor consumenten is het een goed uitgangspunt om bijvoorbeeld bij de aanschaf van een laptop 10 procent van dat bedrag te besteden aan de beveiliging."

Er is duidelijk nog veel werk aan de winkel. Wat heeft naar uw idee de hoogste prioriteit?

"Wat belangrijk is, is dat er nu aandacht is voor cybersecurity. In de periode dat het advies uitkwam, verschenen er steeds meer berichten in de media over de noodzaak van cybersecurity. De urgentie is helder, en ik hoop en verwacht dat het volgende kabinet ermee verder gaat. En dat zowel overheid en multinationals als mkb-bedrijven en burgers zich verantwoordelijk voelen voor cybersecurity. Iedereen kan iets doen. Naast groeiend bewustzijn gaat het om actie, aan de slag."

Hoe kijkt u naar de toekomst?

"Maatregelen en investeringen in digitale veiligheid zijn noodzakelijk, zoveel is duidelijk. Als we ook daarin voorop lopen, levert dat economische mogelijkheden op. Vergelijkbaar met onze kennis en ervaring op het gebied van bijvoorbeeld watermanagement. We hebben onszelf bewezen met onze deltatechnologie. We beschermen onszelf tegen het water en zorgen ervoor dat we droge voeten houden. Zoiets is ook mogelijk op digitaal gebied. Daarom hebben we het adviesrapport 'Nederland digitaal droge voeten' genoemd. Wanneer burgers en bedrijven vertrouwen op een veilig internet, kunnen we de economische kansen van digitalisering volop benutten."

"10% van het IT-budget investeren in cybersecurity"

"Om grip te krijgen op cybersecurity moet niet alleen de overheid zich verantwoordelijk voelen, maar alle partijen in de samenleving." Dat zegt Melanie Peters, directeur van het Rathenau Instituut. "De discussie moet niet alleen gaan over onze veiligheid, maar ook over andere waarden zoals gezondheid, gelijke behandeling, toegang tot noodzakelijke diensten en goederen, eerlijke informatie, een eerlijke prijs en uiteindelijk onze menselijke waardigheid."

Dr. ir. Melanie Peters
directeur Rathenau Instituut

DEBAT NODIG OVER DE BALANS TUSSEN WAARDEN

CYBERSECURITY? HET GAAT NIET ALLEEN OM VEILIGHEID

In 1993 kreeg ik mijn eerste e-mailaccount. Ik werkte toen aan de universiteit van Texas. Wij waren in Texas een van de eersten met een account. Dat kwam dankzij een van de docenten: dr. Combs. Hij had een bijzondere belangstelling voor digitale zaken. Combs had een handleiding ontwikkeld met de titel "Veilig surfen op het web". Het omslag toonde een plaatje van een man in een gebloemde surfbroek die voor hoge golven stond. De boodschap was: surfen is fun, maar ook gevaarlijk.
Combs vertelde ons dat het web was ontwikkeld door het leger en dat je nooit wist welke route je berichten namen. Dit om ervoor te zorgen dat niet de hele communicatie via het web onmogelijk zou worden als er een route zou uitvallen. "Alles wat je schrijft, wordt gescreend en je weet dus niet waar en door wie", zei hij. "Als je een mail naar een collega stuurt met een doodswens aan de president zul je bezoek krijgen van de autoriteiten."
Nu, 24 jaar later, ben ik me bij elke mail die ik stuur nog steeds ervan bewust dat er iemand meekijkt. Als ik denk aan mijn dochters en hun klasgenoten, dan besef ik dat zij dit idee absoluut niet hebben. Ze zijn opgegroeid met internet en zien het alleen maar als leuk en handig.

Mails naar de halve wereld

Sinds 2015 ben ik directeur van het Rathenau Instituut. Mijn instituut gaat over onderzoek en dialoog over nieuwe ontwikkelingen in wetenschap, technologie en innovatie. Het instituut heeft een speciale taak om de politiek en het publiek te informeren en in staat te stellen zelf betere beslissingen te nemen. Vanaf mijn werk bij het Rathenau Instituut mail ik de spreekwoordelijke halve wereld. Wie staan er niet allemaal in de cc? En hoe makkelijk wordt een mailtje doorgestuurd? Ik krijg ook 's avonds en in het weekend mail. Een oponthoud van een of twee dagen? Het zou onwerkbaar zijn. Ik merk dat het contact tussen collega's onderling en tussen organisaties veel minder formeel is geworden. Er worden maar weinig brieven nog officieel ingeboekt.
De wereld is duidelijk veranderd sinds het internet 25 jaar geleden het domein van de liefhebbers verliet en iets werd voor ons allemaal. Kleuters halen spelletjes van het web. Een iPad is speelgoed geworden. Mijn

“Surfen is fun, maar ook gevaarlijk”

tienerdochter en haar klasgenoten appen het liefst tot midden in de nacht en bestellen kleding online (als ze het ID van hun ouders kunnen gebruiken).
Internet en alle applicaties die daar bij horen zijn zo gemakkelijk te gebruiken, dat je niet hoeft na te denken over de wereld die daar achter zit. Dat maakt het juist zo aantrekkelijk. Maar hoe moet dat dan met veiligheid op internet als we er zo onbewust mee om gaan? Of hoeven we ons daar als gebruiker eigenlijk niet mee bezig te houden?

Internet als kritische infrastructuur
Lange tijd was de veiligheid van consumentenproducten misschien niet zo’n probleem. Tenminste, het werd in ieder geval niet in verband gebracht met cybersecurity. Tot zo'n vijf jaar gelden. Toen publiceerde het Rathenau Instituut bijvoorbeeld de uitgave ‘You have been hacked!’, een magazine met als ondertitel ‘cybersecurity can no longer be an afterthought’. Het magazine kwam voort uit een internationaal project en inventariseerde studies van collega-instituten wereldwijd. Het concentreerde zich op risico’s voor kritische infrastructuren. Dat zijn infrastructuren die essentieel zijn voor het functioneren van onze samenleving. Denk daarbij aan het elektriciteitsnet, aan olie en gasbedrijven, aan de waterleiding of het aan verkeerssysteem. Maar denk ook aan ziekenhuizen en alle andere infrastructuur die nodig is voor gezondheid, veiligheid, de openbare orde en economisch welzijn. Bij al deze voorbeelden gold toen al dat ze vaak digitaal aangestuurd werden. Vaak gebeurde dat via netwerken die geleased werden van private partijen en die niet in het zicht waren van overheidsbescherming en controle. Wij waarschuwden toen dat dit de achilleshiel zou worden van deze systemen.

Oorlogen in cyberspace
Een van de voorbeelden uit het Rathenaurapport kan ik me nog goed herinneren. Het ging over een Iraanse kerncentrale. In 2010 werd Stuxnet gevonden in een uraniumfabriek in Iran. Stuxnet is software die spioneert of sabotage pleegt op het type computers dat gebruikt wordt in industriële processen. Stuxnet werd ontwikkeld om software van Siemens-systemen aan te vallen en kon onopgemerkt pompen, centrifuges en andere onderdelen ontregelen. De capaciteit van de uraniumfabriek daalde tot 30%. Aangenomen werd dat alleen een andere staat een dergelijk complexe en gerichte software kon schrijven en dus achter de aanval zou zitten.
Het is niet verwonderlijk dat alle rapporten in die tijd wezen op nationale actie en internationale afspraken tegen wat toen al ‘oorlogen in cyberspace’ heette. Als je een opwerkingsfabriek kon stilleggen, dan kon ook de olietoevoer of de samenstelling van drinkwater veranderd worden en dan kon je ook een heel land schaden.

Kleine speler, grote schade
Het World Economic Forum zette het onderwerp op de agenda, de NAVO werd wakker en nationale overheden lieten onderzoek doen. Ook de Verenigde Naties werden opgeroepen om met acties te komen. Er moest nieuwe internationale wetgeving komen en afspraken in WTO-achtige setting. Het gaat namelijk om vergrijpen die over de grenzen heen gaan en die opsporing en handhaving bemoeilijken. Toch werd toen al duidelijk dat deze kritische infrastructuur niet alleen door staten kon worden aangevallen, maar ook door individuen of in groepen opererende hackers. De groep Anonymus sprak tot de verbeelding. Kleine spelers zijn ook al snel in staat om grote schade aan te richten. Om dit aan te tonen hackten tv-journalisten bijvoorbeeld een pompstation dat ervoor zorgt dat Nederland niet onder water loopt.

Internet of everything
Wat als deze kritische infrastructuur ook nog eens verweven wordt met consumentensoftware? Dat is op dit moment gaande. Alles wordt met alles verbonden.
Neem het voorbeeld van een decentrale elektriciteitsvoorziening. Energie van zonnepanelen wordt teruggeleverd aan het net op het moment dat een huishouden te veel energie heeft opgewekt. Bewoners kunnen dit volgen via een slimme meter, die zo gebruiksvriendelijk mogelijk is vormgegeven. Hoe beveilig je alle schakels in dat netwerk? Is het dan nog voldoende om het internet en apps alleen te zien als behulpzaam en als gadget? Nog een voorbeeld van kritische infrastructuur is wat mij betreft valse Facebookberichten. De berichten zijn heel makkelijk in omloop te brengen en beïnvloeden de publieke opinie en de democratie. Vroeger kon je de gedrukte krant niet zomaar veranderen.
En het gaat verder. Wij gebruiken niet alleen het internet, het internet gebruikt ons ook. Wij lezen niet alleen Facebook, Facebook leest ons ook. De elektronische infrastructuur verzamelt data over ons en combineert die zonder dat wij als gebruikers daar zicht op hebben.

Balans tussen waarden
Al met al kunnen we concluderen dat niet alleen het internet kwetsbaar is en daarmee onze kritische infrastructuur en collectieve voorzieningen. Ook wij als personen zijn kwetsbaar. Ook onze waardigheid is kwetsbaar. Want cybersecurity gaat inmiddels ook over het hacken of misbruiken van persoonsdata. Nou staan privacy en veiligheid wel aardig hoog op de agenda, maar andere waarden zoals onze gezondheid, onze autonomie, gelijke behandeling en eerlijke informatie nog niet. Wat mij betreft zou het debat moeten gaan over de balans tussen deze waarden.
Als het gaat om de ontwikkelingen rondom nieuwe technologieën en de impact daarvan op de Nederlandse samenleving, dan hebben weinig partijen het totaalbeeld op het netvlies. Daarmee is er ook te weinig zicht op de negatieve en positieve mogelijkheden voor de samenleving.
Ik vind het overigens niet vreemd dat we geen goed overzicht hebben over alle ontwikkelingen. Aan de ene kant diende internet het gemak en de mens en hoefden we ons er ook niet mee bezig te houden. Aan de andere kant hebben we de grote discussies over ‘cyber’, waar internationale afspraken voor nodig zijn. Nu komen die twee werelden bij elkaar. Het cybersecurityprobleem is in elk geval niet opgelost als burgers hun privacy opgeven en denken dat alleen de overheid ons zal beschermen.

Vormgeven van samenleving
Nederland bevindt zich op een mooie positie. We lopen op veel terreinen voor in de ICT-ontwikkeling. Maar dat kan alleen zo blijven als gebruikers alerter worden en als maatschappelijke spelers een grotere rol gaan spelen. Dan denk ik aan het onderwijs, aan de werkgevers, aan softwareontwerpers en aan de bedrijven die apps in de markt zetten en die slimme apparaten ontwikkelen. Cybersecurity gaat niet alleen over veiligheid. Het gaat om de samenleving die we met hulp van digitale technologie met elkaar willen vormgeven.

Meer informatie
- You have been hacked! Magazine van het Rathenau Instituut (2012) https://www.rathenau.nl/en/publication/volta02
- Big data en slimme algoritmen - projecten van het Rathenau Instituut die gaan over cybersecurity https://www.rathenau.nl/nl/page/big-data-en-slimme-algoritmen

In de afgelopen jaren heeft de AIVD met toenemende nadruk de gevaren van het gebruik van de digitale ruimte onder de aandacht gebracht. Natuurlijk vallen het World Wide Web, de smartphones en de tablets niet meer uit ons dagelijks leven weg te denken. En we vinden het al lang niet vreemd meer dat alles in ons huis en in ons vervoer steeds 'smarter' wordt. Maar ik vraag me af of we zelf wel voldoende nadenken over de risico's.

Dhr. R.A.C. (Rob) Bertholee
Directeur-generaal AIVD

DENKEN WE GENOEG NA OVER DE RISICO'S?

De toename van digitalisering leidt niet alleen tot een toename van cybercriminaliteit. Ik zie in mijn dagelijks werk ook een behoorlijke toename wereldwijd van digitale spionage en van zogenoemde heimelijke beïnvloeding. Op bijna industriële schaal. Dat is natuurlijk niet zo vreemd. Met relatief weinig inspanning, tegen geringe kosten en met een laag afbreukrisico kunnen statelijke actoren naar hartenlust via de digitale infrastructuur rondneuzen in de economische, industriële, wetenschappelijke en politieke dossiers van andere staten. Als je meer dan een miljard monden moet voeden, loont het de moeite doorontwikkelde en beproefde landbouwtechnieken digitaal te stelen in plaats van te kopen of zelf te ontwikkelen. Als je van mening bent dat jouw land eigenlijk een supermacht status moet hebben, dan loont het de moeite de invloed van anderen te verminderen door publiek en politiek heimelijk te beïnvloeden met gebruik van internet en sociale media.

Doelwit digitale spionage

Nederland heeft een geweldige digitale infrastructuur en zowel de publieke als de private sector zijn rijkelijk voorzien van allerlei digitaal gestuurde elektronica. We hebben bovendien nogal wat waardevolle bezittingen: lucht- en ruimtevaarttechnologie, innovatieve kracht in de agrarische sector en een breed palet aan wetenschappelijke kennis, om er maar eens een paar te noemen. De betrokkenheid en de rol van Nederland in Europa kun je ook niet uitvlakken. Nederland is echt luilekkerland voor kwaadwillende statelijke actoren. Ik zie dat het Nederlandse overheidsinstellingen en in Nederland gevestigde bedrijven structureel doelwit zijn van digitale spionage. We lopen voorop in digitalisering, maar onze bescherming houdt geen gelijke tred.

Structurele aandacht

Ik ben dan ook verheugd over het rapport van Herna Verhagen. Het rapport bevestigt ons beeld en onderstreept de urgentie en de noodzaak forse maatregelen te nemen op het gebied van cybersecurity. Doen we dat niet, dan zijn de gevolgen en kosten voor ons enorm als onze veiligheid en economisch verdienvermogen worden aangetast.

Die maatregelen kunnen alleen maar effectief zijn in een gezamenlijke publiek-private aanpak. Het vereist structurele aandacht van regering, parlement, beleidsmakers, bestuurders, toezichthouders, bedrijven en burgers. Iedereen heeft een verantwoordelijkheid in het gezamenlijk beschermen van onze nationale digitale veiligheid, en daarmee van onze economie, welvaart en maatschappij. Als overheid met een grote digitale ambitie moeten wij in elk geval cybersecurity standaard in ons beleid en onze activiteiten meenemen.

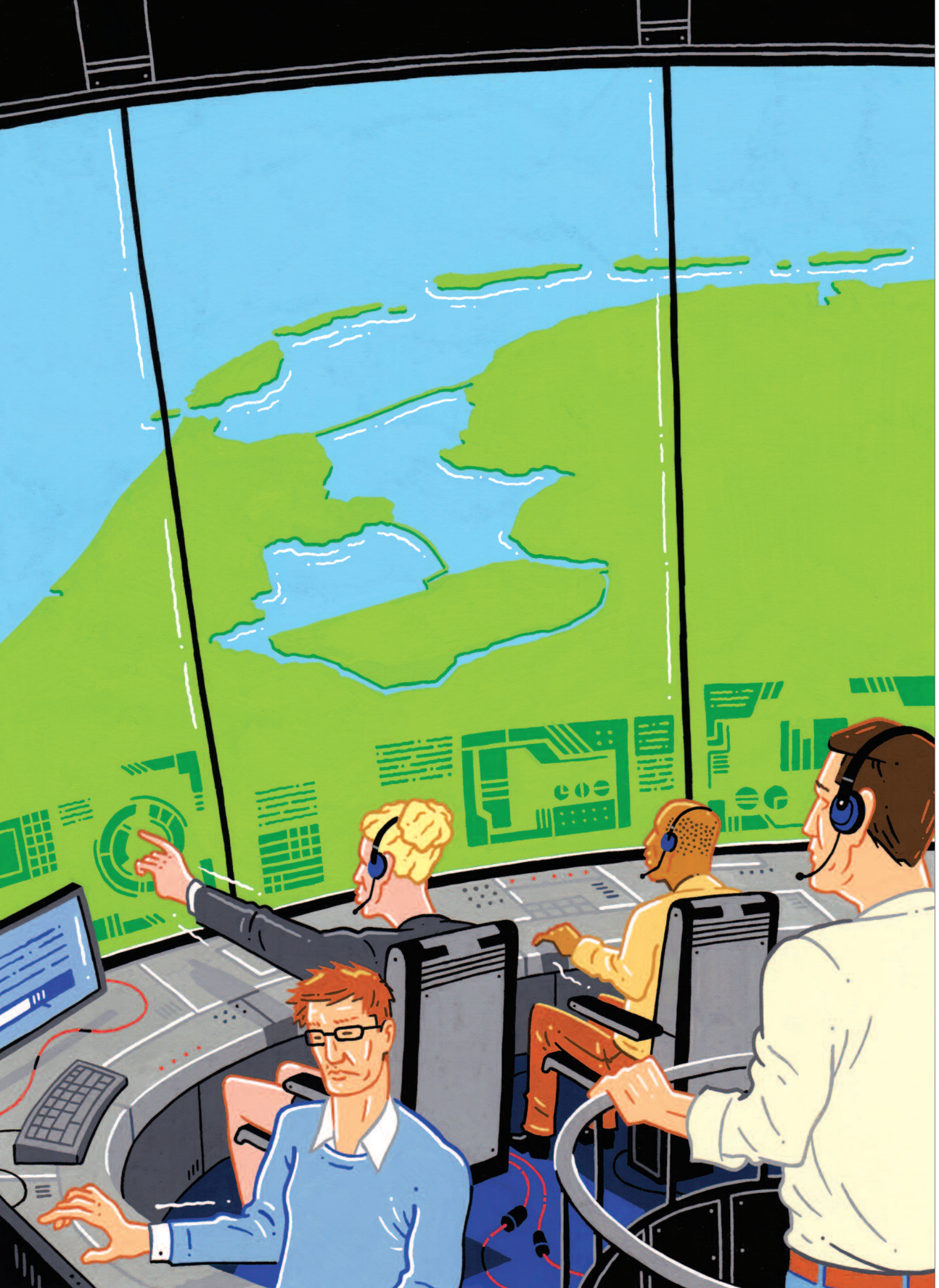
Checks and balances

De unieke taken van de AIVD en de bijzondere bevoegdheden die daarbij horen, stellen ons in staat een wezenlijke bijdrage te leveren aan cybersecurity. Wij zijn in staat complexe digitale aanvallen te detecteren en te analyseren. Op basis daarvan kunnen we hoogwaardige beveiligingsadviezen geven aan publieke en private instanties. We kunnen in geval van succesvolle spionage of sabotage hoogwaardige bijstand leveren om de schade te beperken. We doen dat nu al en we zullen dat in de toekomst blijven doen. Ik vind daarom een versterking van het Nationaal Detectie Netwerk (NDN) een goed begin. Daarnaast ben ik net als Herna Verhagen overtuigd van de noodzaak de bevoegdheden van de AIVD en van de MIVD te moderniseren in de nieuwe Wet op de inlichtingen- en veiligheidsdiensten (Wiv). De huidige Wiv dateert immers nog van vóór de tijd dat de iPhone in Europa werd geïntroduceerd. Op punten achterhaald dus. Ik ben er ook van overtuigd dat de checks and balances daarop moeten worden aangepast in een vorm die werkbaar blijft. We zijn er voor de Nederlandse burger en niet om een of ander schimmig regime in het zadel te houden. We zijn immers een geheime dienst in een democratie.

Reduceren van risico's

De met grote snelheid voortschrijdende digitalisering biedt geweldige kansen. Om die goed te benutten moeten we ons bewust blijven van de digitale risico's. We mogen ons op dat gebied niet van de domme houden. De AIVD draagt graag bij aan die bewustwording en aan het reduceren van de risico's.

"Ik zie behoorlijke toename van digitale spionage en heimelijke beïnvloeding"



Digitale veiligheid en veiligheid door digitale oplossingen. Dat is volgens mij de kern van het toekomstig veiligheidsbeleid. Er zal geïnvesteerd moeten worden om gewenste maatschappelijke ontwikkelingen te bevorderen, maar ook om dreigende maatschappelijke ontwrichting te voorkomen. Dat gebeurt nog veel te weinig, zoals ook in het rapport 'De economische en maatschappelijke noodzaak van meer cyber security' van Herna Verhagen beschreven wordt. De ontwikkelingen gaan razend snel. Daarom is urgent politieke aandacht nodig.

Wim Kuijken
Voorzitter bestuur
'The Hague Security Delta'

NIEUW KABINET ZAL FORS MOETEN INVESTEREN IN CYBERSECURITY

"Naast territoriale veiligheid (Defensie), sociale veiligheid (Politie, Brandweer) en fysieke veiligheid (deltaplannen) is digitale veiligheid het onderwerp van de toekomst."

Naast territoriale veiligheid (Defensie), sociale veiligheid (Politie, Brandweer) en fysieke veiligheid (deltaplannen) is digitale veiligheid het onderwerp van de toekomst. Laten we niet, net als in de fysieke wereld, wachten op een overstroming voordat we in actie komen. Digitale criminaliteit is potentieel maatschappelijk zeer ontwrichtend. Onze vitale infrastructuur, zoals het mobiele netwerk of energienet, kan in gevaar komen door aanvallen van criminelen of zelfs landen. Dit betekent dat we deze vitale infrastructuur beter moeten beveiligen en daar staat de overheid uiteindelijk toch voor aan de lat. Het zou mooi zijn als we bij wijze van spreken ook de digitale ophaalbrug in Nederland kunnen ophalen bij een incident. Dit vereist meer inzicht en bevoegdheden. Hoe eerder wij deze maatregelen nemen des te aantrekkelijker is Nederland voor vestiging van bedrijven en instellingen. Ook zorgen we er zo voor dat mensen vertrouwen houden in de overheid op het gebied van veiligheid.

Investeer aan de voorkant

De aanpak van digitale veiligheid moet publiek-privaat, kan het beste in een netwerkstructuur en zal innovatief moeten zijn. De overheid is daarbij een belangrijke aanjager. Zij zal, zeker op het terrein van (digitale) veiligheid, in innovaties moeten investeren en gaan optreden als eerste afnemer. Deze publiek-private aanpak zal wel onder regie moeten worden uitgevoerd (Nationaal Coördinator Terrorismebestrijding en Veiligheid) en met de benodigde middelen voor ontwikkeling en toepassing (Nationaal Cyberfonds). Investeren aan de voorkant is mijn advies en het mes snijdt aan meerdere kanten: digitale toepassingen veilig maken en houden, digitale netwerken en vitale infrastructuur duurzaam beter beveiligen, economische groei bevorderen en vertrouwen opbouwen.

Afhankelijkheid ICT

De Nederlandse maatschappij en economie krijgt steeds meer een digitaal karakter en is daardoor

steeds afhankelijker van ICT. ‘The Internet of Things’ ontwikkeling is niet meer te stoppen. We gebruiken internet niet alleen meer om online nieuws te bekijken en te shoppen, ook onze bankzaken regelen we online en de verwarming thuis staat steeds vaker via onze mobiel in verbinding met het internet. Daarbij rijden we mogelijk over niet al te lange tijd ook in zelfrijdende auto’s en ontvangen we pakketjes via onbemande drones.
Niet alleen onze huizen en apparaten zijn via allerlei sensoren aan internet verbonden. Dit geldt bijvoorbeeld ook voor onze leefomgeving, waar stoplichten met elkaar verbonden zijn in zogenaamde slimme steden. Maar ook hele industriële automatiseringssystemen van onze vitale infrastructuur op het gebied van onder andere water, energie, telecom en gezondheidszorg zijn gedigitaliseerd. Deze ontwikkeling biedt veel nieuwe mogelijkheden en economische kansen, maar brengt ook risico’s met zich mee. Zeker omdat het gaat om de meest cruciale delen van onze maatschappij. Er rest ons daarom geen enkele keuze: de digitale veiligheid van onze vitale infrastructuren moet worden opgevoerd. En daar zal dus meer geld in gestoken moeten worden.

Unieke digitale infrastructuur

Nederland heeft een perfecte uitgangspositie om mee te kunnen gaan met de trends van digitalisering, Internet of Things en 3D printing als onderdeel van de zogenaamde vierde industriële revolutie. We beschikken namelijk over een unieke digitale infrastructuur die hiervoor de basis legt. Daarbij zijn we ook nog eens een ‘global centre’ voor dataverkeer, omdat we hier de twee grootste internet hubs van Europa hebben. Dit maakt ons land aantrekkelijk voor internationale bedrijven en organisaties en zijn er volop economische kansen voor de IT- en veiligheidssector.

“Er rest ons geen enkele keuze: de digitale veiligheid van onze vitale infrastructuren moet worden opgevoerd.”

“De Nederlandse maatschappij en economie krijgt steeds meer een digitaal karakter en is daardoor steeds afhankelijker van ICT.”

Nationaal Cyber Plan

Om de vlieger vanuit maatschappelijk en economische perspectief op te laten gaan, moeten we borgen dat onze digitale vitale infrastructuur neutraal en veilig is. Het is daarom belangrijk een nationale digitale veiligheidsaanpak te ontwikkelen, net zoals het Deltaplan dat de fysieke vitale infrastructuur borgt. En omdat er niet één organisatie in z’n eentje verantwoordelijk is voor de digitale beveiliging van Nederland, dient dit zowel dwars door ‘het huis van Thorbecke’ als publiek-privaat georganiseerd te worden. Het zal integraal door zowel de politiek als het bedrijfsleven opgepakt moeten worden. Een aanpak die alleen werkt als er ook een meerjarig nationaal investeringsprogramma aan ten grondslag ligt. Bij elkaar gebracht in een ‘Nationaal Cyber Plan’.

Nationaal Cyber Testbed

Binnen het nationale veiligheidscluster The Hague Security Delta zijn we hier al op aan het voorsorteren. Bedrijven, kennisinstellingen en overheden werken er samen aan innovatieve oplossingen op gebied van onder andere IT-security. Zo zijn we bijvoorbeeld samen met onze partners bezig om te kijken hoe we een Nationaal Cyber Testbed voor vitale infrastructuren op kunnen zetten. Dit zou het eerste cyber test- en ontwikkelingscentrum in Europa kunnen worden, waar bijvoorbeeld datacenters, telecompartijen en energieleveranciers in een beschermde omgeving de digitale veiligheid van hun systemen kunnen testen, innovatieve veiligheidsoplossingen kunnen toetsen en trainingen kunnen geven.

Daarnaast zie ik een rol voor het testbed rondom de ontwikkeling van ‘The Internet of Things’ en ‘Smart Cities’. We moeten naar een situatie toe dat producten, zoals slimme thermostaten, verkeerslichten en sluizen pas op de markt komen nadat ze op hun digitale veiligheid getest zijn en een keurmerk hebben meegekregen. Net zoals we dat met het KEMA-keur hebben gedaan na de introductie van elektriciteit. Alleen door op een vergelijkbare manier met digitale veiligheid om gaan, kunnen we ernstige cyberstoringen voorkomen.

Het opzetten van een dergelijk testbed vereist een nauwe samenwerking tussen de vitale infrastructuur sectoren én een investering van miljoenen, maar is een conditio sine qua non om onze maatschappelijke veiligheid te borgen, de economische potentie van onze IT en cyber-security-sector uit te kunnen nutten en onze kennis internationaal te vermarkten.

Tenslotte

Kortom, naarmate de digitalisering van onze samenleving steeds verder gaat, is digitale beveiliging het enige antwoord om met deze nieuwe wereld om te gaan. Daarom moeten we inzetten op een combinatie van het economisch benutten van de mogelijkheden en anderzijds het afdekken van de risico’s. Een ‘Nationaal Cyber Plan’, inclusief investeringsprogramma is hiervoor een vereiste. Zo leggen we een essentiële basis onder het Nederlandse vestigingsklimaat en positioneert Nederland zich met recht als ‘secure digital gateway to Europe’.

Nederland is géén klein land. We behoren tot de top in de wereld als het gaat om onze economie en IT. Onze IT-kennis en -infrastructuur is van topklasse. Ook op andere lijstjes staan we steevast bovenaan. We moeten onszelf niet klein maken. We staan er goed voor en we kunnen de koppositie in de wereld pakken in het bestrijden van cybercrime en het ontwikkelen van systemen die het cybersecurityniveau verhogen. Meer zelfvertrouwen is nodig om enorme economische kansen te verzilveren.

Paul de Krom
Voorzitter Raad van Bestuur
Chief Executive Officer
TNO

LAAT ONS LAND NIET LEEGJATTEN!

VERZILVER ECONOMISCHE KANSEN

Onze huidige toppositie is te danken aan investeringen in het verleden. Maar inmiddels dreigen we de boot te missen. Nederland zit volgens Harvard Business Review in de categorie “rapidly receding” (snel aan het afzakken). Investeringen in andere landen zijn massaler en gaan sneller. Als er in Nederland geen actie wordt ondernomen, glijden we af en houdt veiligheid geen gelijke tred met digitale dreigingen. Een achterhoedepositie in de wereld dreigt, terwijl dit niet nodig is.

Advies 1: ontwikkel visie

Om de koppositie te kunnen pakken, adviseer ik als eerste dat Nederland een departement-overstijgende visie en stevige ambitie op cyber-security moet ontwikkelen. Alleen dan kunnen we economische kansen verzilveren. Er wordt nu te versnipperd gewerkt. Zo is voor mij niet duidelijk welke rol de drie hoofdspelers Defensie, Veiligheid en Justitie, en Economische Zaken op dit thema hebben. In ieder geval is het belang van cybersecurity voor Nederland te groot, en is Nederland te klein om ons bezig te houden met allerlei ‘koninkrijkjes gedoe’. Ook is er gebrek aan investeringen, massa en focus. De rol van de overheid, als behartiger van het algemeen belang, het verzekeren van maximale veiligheid, als investeerder en launching customer, is cruciaal. Het is noodzakelijk de krachten te bundelen en Nederland te versterken, om zo de cybersecurity-problemen het hoofd te bieden, Nederland te beschermen en de economische kansen die cybersecurity ons biedt te verzilveren.

Advies 2: maak weerbaar

De nationale cybersecurityvisie en -ambitie moet ook ingaan op het weerbaar maken van ons land. Dat krijgt nog te weinig aandacht. Op het verwachte kun je je voorbereiden, maar het zit ‘m juist in het onverwachte. Daar moet je mee om kunnen gaan. Mijn tweede advies is daarom: ontwikkel scenario’s. Wat moet je doen bij onverwachte cyber(security) ontwikkelingen? Hoe bescherm je je tegen digitale aanvallen? 100% veiligheid bestaat niet; maximaal beperken van de risico’s wel. Ook zijn scenario’s nodig die helpen bij het pakken van de wereldwijde koppositie en het ondernemen van actie als we daarbij tegenslag ondervinden. Zo wordt Nederland op twee fronten weerbaar.

“Een achterhoedepositie in de wereld dreigt, terwijl dit niet nodig is”

Advies 3: neem de regie

De cybersecuritystructuur in Nederland is in de basis goed. We hebben het Nationaal Cyber Security Centrum als operationele dienst, de directie Cyber Security als beleidsafdeling (beiden ondergebracht bij het ministerie van Veiligheid en Justitie) en de Cyber Security Raad als onafhankelijk adviesorgaan. Een prima gelaagde aanpak, waarbij publiek-privaat wordt samengewerkt. En daar zijn we goed in. Veel beter dan het buitenland. Landen proberen ons model wel eens te kopiëren, maar het lukt ze niet. Het is gewoon in het DNA van Nederland. Alleen zo organiseren we massa en focus om snel en effectief bedreigingen het hoofd te bieden en economische kansen te pakken. De structuur die we hebben, moeten we gebruiken om nu snel door te pakken. Er is een gezamenlijke, meerjarige kennis- en investeringsagenda nodig, waarbij departementen, bedrijfsleven, kennisinstituten en wetenschap nauw samenwerken. Mijn derde advies is één hoge functionaris of minister aan te stellen die dit gaat organiseren, de regie heeft, coördinatie aanbrengt en rapporteert aan een stuurgroep in het Kabinet, geadviseerd door de Cyber Security Raad. Deze raad zou de nationale visie en ambitie moeten bewaken en adviezen moeten geven aan alle spelers die hieraan meewerken.

Advies 4: deel kennis

We zouden in Nederland veel meer aan technologie- en productontwikkeling moeten doen. Nu komen veel producten uit Amerika en Israël, maar ze zouden ook uit Nederland kunnen komen. Er is ontzettend veel kennis beschikbaar, maar het ligt op de plank en is nauwelijks toegankelijk. We hoppen van kennisopbouw naar kennisopbouw, zonder dat overheid, bedrijven en wetenschappelijke instituten op een goede manier kennisdelen en dit vertalen naar veiligheidsproducten die op de markt gebracht kunnen worden. Dat moet anders. Mijn vierde advies is daarom kennisdeling tussen overheid, bedrijfsleven en wetenschap makkelijker te maken. Ook moet duidelijker zijn wie over welke kennis beschikt, zodat het wiel niet twee keer uitgevonden hoeft te worden. Het delen van informatie moet anoniem kunnen – bijvoorbeeld als het gaat om cyberaanvallen en -inbraken. Door kennis te delen wordt Nederland veiliger én kunnen we uitstekende veiligheidsproducten ontwikkelen die gewild zijn in de wereld vanwege hun effectiviteit en betrouwbaarheid.

Advies 5: investeer

Het is doodzonde als goede ontwikkeltrajecten om te komen tot cybersecurityproducten een vroege dood sterven omdat ze niet van proof-of-concept tot een daadwerkelijk product komen. Dit is een bekend fenomeen en wordt de ‘valley of death’ genoemd. Het ontbreekt dan aan de wil om risicovol te investeren. Dit doet zich bijvoorbeeld voor als het rendement op investeringen te onzeker wordt voor bedrijven. Zij kunnen die last niet alleen dragen. Daarom adviseer ik voldoende risicokapitaal ter beschikking te stellen, zodat die ‘valley of death’ overbrugd wordt. In deze fase is echt de ‘overheidseuro’ nodig. Deze zal als een multiplier werken, omdat bedrijven dan wel zullen investeren. Dit levert veilige Nederlandse producten op waar we op kunnen vertrouwen, en waar de Nederlandse overheid als eerste gebruik van kan maken.

“Nederland moet een departement-overstijgende visie en stevige ambitie ontwikkelen”

Foto: Aerovista Luchtfotografie - Nationale Beeldbank

100% veiligheid bestaat niet; maximaal beperken van de risico's wel. Maak Nederland digitaal weerbaar.

Advies 6: creëer een ecosysteem

Naar mijn mening moeten we in Nederland toe naar een 'cyber ecosysteem'. Universiteiten, kennisinstituten, overheid en bedrijfsleven zouden hieraan deel moeten nemen. In zo'n ecosysteem ontstaat zicht op elkaars kennis en deze kan vertrouwelijk en makkelijk worden gedeeld met als doel producten te ontwikkelen die op de markt worden gebracht. Continu wordt kennis gedeeld en samengewerkt aan cyber-securityproducten, inspelend op actuele ontwikkelingen. In een ecosysteem is sprake van co-creatie, van lef om dingen uit te proberen, van het nemen van risico's omdat innovaties ook kunnen mislukken en van de wil om samen te werken, Nederland veiliger te maken en economische kansen te verzilveren. Er moet een programma komen om dit ecosysteem te faciliteren.

En tot slot...

Cyberspionage is een grote uitdaging. We moeten voorkomen dat ideeën, innovaties en blauwdrukken voor producten verdwijnen naar het buitenland. En omgekeerd weet je met producten uit het buitenland niet precies wat en wie je binnenhaalt. Nederlandse producten helpen om onze eigen veiligheid op orde te brengen. We moeten ons land niet leeg laten jatten. Daar is het landsbelang te groot voor.

"Start een programma om het 'cyber ecosysteem' te faciliteren"

Hans de Boer

Voorzitter VNO-NCW

Cybersecurity is voor mij een cruciale randvoorwaarde om de kansen die digitalisering biedt te pakken en om het vertrouwen hierin vast te houden. Cyberoorlog is goedkoop en doeltreffend hebben we de afgelopen maanden gezien. Dat vraagt om 'top of the bill' beveiliging. Anders liggen straks misschien wel delen van de samenleving stil op een manier die we niet meer kennen.

CYBEROORLOG IS GOEDKOOP EN DOELTREFFEND

NIETS DOEN IS GEEN OPTIE

Vitale infrastructuren, als energie, water en telecom, komen bij mij als eerste naar boven als ik denk aan kwetsbare sectoren waar cyberaanvallen grote impact kunnen hebben. Zie hoeveel schade een kapotte sluisdeur onlangs aanrichtte voor bedrijven en burgers. Dat was nog een fysiek ongeval. Een ouderwets ongeluk, maar het had net zo goed een digitale aanval kunnen zijn.

Vertrouwen vasthouden

Tegelijkertijd is cybersecurity voor de hele samenleving van groot belang. Onze afhankelijkheid van IT wordt met de dag groter. We kunnen niet meer zonder. We winkelen, we bestellen, we betalen, we chatten en we daten online. Binnen bedrijven zijn steeds meer processen geheel of gedeeltelijk geauto-matiseerd. Van betalingsverkeer, tot logistiek, van productieprocessen tot klantenbestanden. Informatietechnologie leidt tot ongekende nieuwe mogelijkheden en kansen, maar de afhankelijkheid van ICT heeft ook een keerzijde. Het maakt ons kwetsbaar voor misbruik en uitval. Nu al vormt cybercrime een flinke schadepost van vele miljarden voor de

economie. Cybersecurity is voor mij een cruciale randvoorwaarde om de kansen die digitalisering biedt te pakken en om het vertrouwen hierin vast te houden. Het is dan ook een centraal onderdeel van ons Next level programma dat is gericht op het volgende Kabinet.

Oplossingsrichtingen

Hoewel de hele zaak in de VS met de democratische partij natuurlijk bizar is laat het hopelijk wel de bewustwording flink stijgen. Of het nou is bij bedrijven, politieke partijen of burgers en NGO's. De belangrijkste oplossingen liggen voor mij in drie dingen:

- Meer awareness.
  Dat begint al thuis. Maar ik zie die grotere awareness vervolgens ook graag gekoppeld aan actie!
- Meer samenwerking.
  Tussen bedrijven en de overheid, maar bijvoorbeeld ook grensoverschrijdend. Veel van de cyberdreigingen zijn immers internationaal en die vragen om internationale oplossingen. Ik denk dan onder andere aan de uitwisseling van informatie over cyberdreigingen, aan de ontwikkeling van standaarden, maar ook aan de opsporing en vervolging van cybercriminelen.
- Meer middelen.

Aan de bak

Het rapport van mevrouw Verhagen is een puik staaltje werk en benoemt exact de onderwerpen waar actie nodig is. Zowel de overheid als het bedrijfsleven van groot tot klein moeten 'aan de bak'. Niets doen is geen optie. Wij zullen ons daarnaast blijven inzetten om cybersecurity hoog op de agenda te houden bij onze achterban. Juist in het MKB is er bijvoorbeeld relatief vaak nog onbekendheid met de dreigingen die er digitaal zijn. Vandaar dat we daar ook extra aandacht aan besteden.

Internationale aanpak

Een ontwikkeling die zich steeds meer en sneller manifesteert is het zgn. *Internet of Things*. Allerlei apparaten worden aan internet gekoppeld. Of het nou gaat over de thermostaat, de slimme koelkast, de auto of medische apparatuur. Miljarden apparaten zijn inmiddels verbonden en dit worden er dagelijks meer. Deze apparaten moeten natuurlijk veilig zijn. Ik moet er niet aan denken dat een rijdende auto of medische apparatuur worden gehackt. Laat duidelijk zijn: Internet of Things biedt grote kansen, maar we moeten de veiligheidsrisico's serieus nemen, ook om het vertrouwen in de veiligheid ervan te behouden. Een internationale aanpak ligt hier voor de hand.

Top of the bill beveiliging

De ontwikkelingen gaan zo snel en we zijn relatief kwetsbaar door onze sterke groei in de digitale dienstverlening de afgelopen vijftien jaar. Ik was laatst in België en daar is de overheid nog beperkt gedigitaliseerd. Bij ons is dat anders. Neem dat voorbeeld van die sluisdeur dat ik net noemde. Geen digitaal incident, maar die digitale risico's zijn er wel. In Oekraïne zijn al elektriciteitscentrales stilgelegd. Daar moeten we ons tegen wapenen.
Cyberoorlog is goedkoop en doeltreffend hebben we de afgelopen maanden gezien. Dat vraagt om *top of the bill* beveiliging. Anders liggen straks misschien wel delen van de samenleving stil op een manier die we niet meer kennen. En dan heb ik het nog niet over andere effecten als nepnieuws, beïnvloeding van de politiek en ga zo maar door.

Nieuw Kabinet

Van een nieuw kabinet verwacht ik om te beginnen drie dingen: middelen, maatregelen en maatwerk. Op alle drie die fronten is actie nodig en zonder extra middelen kan het niet.
Maatwerk en gerichte acties zijn nodig voor de bescherming van de vitale infrastructuur, maar óók voor andere delen van onze economie. Bedrijven in de topsectoren, cruciaal voor het verdienvermogen van onze economie, blijken bijvoorbeeld zeer kwetsbaar te zijn voor digitale spionage.
Een goede aanpak vraagt ook om gerichte investeringen van de overheid. Een paar maanden geleden presenteerden wij onze toekomstvisie en bijbehorende investerings-agenda ' De digitale kwantumsprong'. Terecht neemt cybersecurity hierin een prominente plek in en wij roepen de overheid op om 100 miljoen te investeren in cyberweerbaarheid.

Digital trust center

Wij pleiten onder andere voor de oprichting van een *digital trust center*, een kenniscentrum waar ondernemers terecht kunnen met meldingen van dreigingen, vragen en advies. Intensieve publiek private samenwerking is wat mij betreft de basis van een goede aanpak van de cyber-problematiek. Overheid en bedrijfsleven zijn afhankelijk van elkaar voor het verhogen van de weerbaarheid tegen cyberdreigingen en het bedenken van oplossingen. Overigens zie ik cybersecurity nadrukkelijk ook als een kans voor de Nederlandse cyberveiligheidsindustrie. Wij zouden graag zien dat de overheid de nationale markt voor cyberoplossingen stimuleert.

Duidelijke regie

Ik heb vertrouwen in de toekomst. Er gebeurt al veel. Ik ga ervan uit dat we dit probleem als Nederland door onze kleine schaal, onze sterke overheid en onze sterke bedrijven met succes weten aan te pakken. Die kennis exporteren we al en wie weet nog meer in de toekomst. Als we maar samenwerken met elkaar, dus overheid en bedrijfsleven en maatschappelijke partijen.
Belangrijk is daarbij wel dat er op het cybervlak een duidelijke regie komt over de verschillende departementen heen. Een goed gecoördineerde, gezamenlijke aanpak is van belang. Ook het opnemen van digitale geletterdheid in het onderwijs is voor ons een belangrijk punt. Van jongs af aan moeten kinderen leren omgaan met de digitale werkelijkheid en weerbaar worden tegen de schaduwzijden.

"Nu al vormt cybercrime een flinke schadepost van vele miljarden voor de economie"

Foto: Frank Noordenbos - Nationale Beeldbank

Maatwerk en gerichte acties zijn nodig voor de bescherming van de vitale infrastructuur, maar óók voor andere delen van onze economie. Bedrijven in de topsectoren, cruciaal voor het verdienvermogen van onze economie, blijken bijvoorbeeld zeer kwetsbaar te zijn voor digitale spionage.

Bas Eenhoorn
Digicommissaris

URGENTIE BIJ BESTUURDERS EN KABINET MOET OMHOOG

Robespierre, vrijheidsstrijder én tiran ten tijde van de Franse revolutie, schetste treffend de delicate spagaat tussen transparantie en onwetendheid: “Het geheim van vrijheid ligt in het opleiden van mensen, het geheim achter tirannie is daarentegen om ze onwetend te houden”. Bijna 250 jaar later, in het tijdperk van de vierde - digitale - revolutie, is zijn uitspraak nog altijd treffend.

In een tijd waarin technologische ontwikkelingen exponentieel toenemen en het soms lastig is alle ontwikkelingen tot je te nemen, is het desondanks van belang bij te blijven en kritisch te blijven over wat er op je af komt. De uitspraak van Robespierre over opleiden en onwetendheid fascineert mij in de huidige tijd. Aan de ene kant wil ik weten wat kunstmatige intelligentie en big data mij brengen en wat ik er mee kan. Aan de andere kant heb ik het idee dat ik onwetend wordt gehouden door de bedrijven die hier een voortrekkersrol in spelen.

Vertrouwen neemt af

Grote tech-bedrijven uit Silicon Valley lopen voorop in het ontwikkelen van kunstmatige intelligentie en het gebruik van big data. Zij passen de mogelijkheden die deze ontwikkelingen bieden toe in hun dienst-verlening. Hierdoor raken mensen ‘afhankelijk’ van hun gratis diensten. Gratis; na het aanvinken van de gebruiksvoorwaarden die ik, waarschijnlijk als elke andere consument, niet uitpluis voordat ik ze aanvink. Onwetend waarvoor ik toestemming heb gegeven, ga ik aan de slag en heb ik een groot deel van mijn privacy afgestaan aan de tech-giganten. Het vertrouwen dat ik in deze bedrijven had om mijn data goed beschermen en kundig te gebruiken, neemt snel af door berichten over veiligheidslekken, hacks, spyware en malware. Maar vooral ook door een groeiend besef dat de code achter hun diensten - de algoritmes - voor een mens niet meer te begrijpen of te controleren zijn. Waardoor niemand nog weet of hij wel alle relevante informatie krijgt en of het gebrachte nieuws wel echts is. De complexiteit en de snelheid waarin ontwikkelingen gaan, bevestigen mijn mening dat samenspel tussen overheden en burgers nodig is om een gezonde balans te herstellen.

Nederland gidsland

Op het gebied van het duiden en toepassen van nieuwe ontwikkelingen is nauwere samenwerking tussen politiek, bestuurders en overheid, bedrijfsleven en wetenschap nodig. Hierdoor kunnen we de kansen grijpen die deze nieuwe technieken ons bieden en Nederland als gidsland in die vierde revolutie laten acteren. Het is belangrijk dat mensen digitaal zelfredzaam zijn, en daarin - waar nodig - worden ondersteund. Opvoeders en het onderwijs spelen een belangrijke rol in het digivaardiger en digiwijzer maken van kinderen.

Hoge urgentie

Of Robespierre nu een tiran of vrijheidstrijder was, laat ik aan u over. Wat ik wel weet is dat exponentiële technologische ontwikkelingen weinig tijd laten voor eindeloze reflectie en dat er hoge urgentie is om over te gaan tot actie. Ik omarm dan ook de conclusies van het rapport Verhagen en zie investeren in cybersecurity als randvoorwaarde voor veilige digitale dienstverlening. Vanuit mijn rol zie ik een uitdaging om de sense of *urgency* bij bestuurders en bij het nieuwe kabinet aan te jagen. Ik wil me daarnaast inzetten voor een betere samenwerking tussen bedrijfsleven, wetenschap en overheid. Alleen in een ecosysteem waarin een gezamenlijk belang en gezamenlijke doelen vooropstaan, kunnen we de in toenemende mate schaarse middelen effectief inzetten en optimaal gebruikmaken van de kansen die de nieuwe technologie ons biedt.

> “Algoritmes zijn voor een mens niet meer te begrijpen of te controleren”

Medewerkers van Shell die enkele jaren geleden ‘s morgens op hun werk verschenen konden tot hun verbazing geen gebruik maken van diverse ICT-diensten. Applicaties waren niet meer benaderbaar of genereerden vreemde foutmeldingen, bestanden konden niet worden benaderd en gekoppelde systemen wachtten eindeloos op responses.

Marjan van Loon
President-Directeur
Shell Nederland

VERDERE DIGITALISERING MAAKT HET BELANG VAN CYBER SECURITY ALLEEN MAAR GROTER

EEN SCRIPT SABOTEERDE ALLE SERVERS IN MALEISIË

De oorzaak lag in een datacentrum in Maleisië. Daar waren honderden servers ongepland en onverwachts gedeactiveerd en hierdoor werden vele duizenden Shell-medewerkers over de gehele wereld belemmerd om hun werkzaamheden uit te voeren.

Sabotage met enorme impact

De eigen IT-organisatie van Shell en onze IT-suppliers waren destijds al snel op de hoogte van deze enorme storing. Met man en macht werd getracht om de applicatieservers weer online te krijgen. Dit herstelproces heeft uiteindelijk vele weken gekost, geleid tot duizenden uren productieverlies en had uiteindelijk een enorme financiële impact. Al snel bleek de storing geen technisch mankement te zijn. Er werd een script ontdekt dat systematisch alle servers in het datacentrum in Maleisië probeerde te saboteren.

Industrial Control Systems

Ik zou hier graag willen zeggen dat dit incident het laatste binnen Shell is geweest. Helaas is de werkelijkheid anders. Cyber-incidenten vinden regelmatig plaats, al zijn ze gelukkig niet allemaal van dezelfde omvang als destijds in Maleisië. Deze incidenten maken pijnlijk duidelijk hoe afhankelijk grote organisaties als Shell zijn geworden van hun ICT-diensten. Niet alleen ondersteunende diensten binnen Shell zijn afhankelijk van IT, ook Industrial Control Systems bij olie- en gaswinning, raffineren en distributie van half- en eindproducten spelen een cruciale rol in onze processen. Die moeten adequaat worden beveiligd tegen cyberdreigingen.

Cybersecurity is een prioriteit

Bij Shell zijn we dagelijks bezig met het vereenvoudigen, efficiënter maken en digitaliseren van onze bedrijfsprocessen. Shell heeft hiertoe een IT-strategie opgesteld waarbij voor het merendeel van de bestaande en nieuwe ICT-diensten zogenoemde Market Standard services worden gebruikt. Deze strategie (‘Market Standard, unless’) houdt kort gezegd in dat het merendeel van onze data niet meer in door Shell beheerde datacentra wordt vastgelegd, maar verspreid wordt in verschillende Software-as-a-Service (SaaS)-oplossingen. Daarnaast worden Shell-medewerkers in toenemende mate in staat gesteld om bedrijfsprocessen met behulp van digitalisering efficiënter te kunnen uitvoeren.

Als gevolg hiervan zal de IT-voetafdruk van Shell komende jaren sterk veranderen. Het beschermen van onze data – onze *Intellectual*

“Bestuurders worden regelmatig geïnformeerd over nieuwe cybersecuritydreigingen”

Property en *Competitive Sensitive Information* – mag natuurlijk geen gevaar lopen bij het realiseren van deze strategie. Dit vraagt om een vernieuwde cybersecurity-aanpak en om daarop toegesneden vaardigheden. Dit moet ervoor zorgen dat alleen de juiste gebruikers toegang krijgen tot onze data en dat wanneer security-incidenten in onze IT-systemen worden gesignaleerd, wij als organisatie toegerust zijn om hierop adequaat te reageren. Cybersecurity is en blijft derhalve een prioriteit voor Shell.

Op de agenda in de board

Cybersecurity is dus een essentiële voorwaarde om goed en veilig te kunnen werken. Shell heeft een Information Risk Management (IRM) afdeling die zich richt op risicomanagement, kritische IT-systemen bewaakt en cyber security processen coördineert. Ook is het de taak van IRM om collega’s binnen Shell op de hoogte brengen van ICT-risico’s binnen hun bedrijfs-processen. Daarnaast wordt het cybersecurity-bewustzijn van eindgebruikers met hulp van campagnes verhoogd. Ook binnen de Shell Board staat cybersecurity hoog op de agenda; zo worden de bestuurders regelmatig geïnformeerd over nieuwe cybersecuritydreigingen, security-incidenten die hebben plaatsgevonden, of omvangrijke IT- of informatierisico’s die onze bedrijfsprocessen zouden kunnen verstoren.

Meer geïntegreerde cyberwetgeving

Ik heb het Cyber Security advies van Herna Verhagen met meer dan gemiddelde belangstelling gelezen en het is voor mij een bevestiging dat Shell het onderwerp informatiebeveiliging terecht serieus neemt. Binnen Shell zijn we met een belangrijk deel van haar adviezen al geruime tijd aan de slag. Daarnaast biedt het rapport ons ook concrete nieuwe adviezen die wij verder intern zullen evalueren. Er zijn specifieke aspecten in het rapport die mij aanspreken, zoals meer cybersecuritywetgeving op Europees niveau. Voor een multinational als Shell, opererend in meer dan 70 landen, is het voldoen aan nationale IT-wetgevingen een complex en tijdrovend proces. Wanneer wij bijvoorbeeld een mobiele App uitbrengen, dienen we voor ieder land opnieuw te toetsen of de applicatie en de vergaring van persoonsgegevens voldoet aan de regelgeving van dat land. Meer geïntegreerde cyberwetgeving op Europees of bij voorkeur zelfs op mondiaal niveau, kunnen internationaal opererende organisaties kansen bieden om slagvaardiger te opereren.

Platform voor informatiedeling

Ook het delen van informatie tussen publiek-private organisaties over actuele cyber-dreigingen tegen bijvoorbeeld vitale infra-structuur is een advies dat wij ondersteunen. Cybercriminelen zijn doorgaans goed georganiseerd en opereren als professionele groepen om overheden, bedrijven of kritische infrastructuur als elektriciteitscentrales, drinkwatervoorziening, gasdistributie-netwerken aan te vallen. Het al dan niet onder embargo delen van gedetecteerde aanvallen kan zowel overheid als bedrijven helpen om zich voor te bereiden. De overheid zou hier, zoals aangeven in het rapport, nog meer een regisserende rol in kunnen spelen door een afgeschermd platform te creëren waarop relevante informatie per sector kan worden gedeeld.

Investeer in onderwijs

Tenslotte, het maakt niet uit of het gaat om Amerikaanse presidentsverkiezingen, het elektriciteitsnetwerk in Oekraïne, de exacte omvang van de hoeveelheid verloren accounts bij Yahoo! of om de gecompromitteerde IT van overheidsdiensten: cyberdreigingen krijgen in ons leven een steeds prominentere rol waartegen we ons adequaat moeten wapenen. Hiervoor is investeren in specialistische kennis op het gebied van cyberveiligheid in het middelbaar en hoger onderwijs van groot belang. Dit aspect komt terug in het rapport, maar mag wat mij betreft hoger op de agenda van de overheid staan.

Soms denken mensen dat cyberaanvallen een ver-van-mijn-bedshow is. Maar niets is minder waar. Nog niet al te lang geleden toonde RTL nieuws aan hoe makkelijk het is een twitter-account van Tweede Kamerleden over te nemen. Dit lijkt misschien iets kleins, maar dezelfde ‘aanvalsmethode’ wordt ook gebruikt door hackers om binnen te dringen. Vervolgens stelen ze belangrijke informatie, verspreiden ze desinformatie of zetten ze de harddrive op slot met ransomware. Of saboteren systemen in vitale sectoren waar we als samenleving van afhankelijk zijn, zoals onze energie- of water-voorziening. Laat dergelijke voorbeelden en alle nieuwsartikelen over cybercrime en cyber-aanvallen een wake-up call zijn. We kunnen onze ogen niet sluiten en doen alsof we geen gevaar lopen. We zien een toenemende en reële dreiging vanuit beroepscriminelen en buiten-landse inlichtingendiensten en het is belangrijk dat onze inzet hiermee in de pas blijft lopen.

Cybergeweten

Wat mij betreft zijn er parallellen te trekken tussen de fysieke wereld en de digitale wereld. De overheid komt geen slot op je voordeur zetten; laat staan dat een ambtenaar het iedere avond voor je op slot draait. Dan moet je ook niet verwachten dat de overheid dit digitaal wel doet. Zo ben je bijvoorbeeld zelf verant-woordelijk voor het veilig gebruik van wacht-woorden. Dat is de basis die iedereen zelf voor elkaar moet hebben. Een andere parallel zie ik met samenwerkingsverbanden tussen overheid, bedrijfsleven en wetenschap om Nederland veilig te houden. De overheid kan het niet alleen. Dat is ook digitaal het geval. Het overgrote deel van de digitale infrastructuur in ons land is in handen van de private sector. We moeten dus wel met elkaar samenwerken om wat te bereiken. In dat kader vind ik het hartstikke mooi dat er een Cyber Security Raad (CSR) bestaat, waarin deze sectoren zijn vertegenwoordigd. De raad kijkt vanuit een strategisch perspectief vanuit diverse invalshoeken naar de kansen en dreigingen van nieuwe technologische ontwikkelingen en die rol wordt steeds belangrijker. Wat mij betreft mag de CSR nog veel meer als ‘cybergeweten’ gaan fungeren voor overheid, bedrijfsleven en wetenschap.

Digitale ‘safe place’

Die publiek-privaat-wetenschappelijke samenwerking is uniek en past bij Nederland. Zelfs de hacking community doet mee. Wij zijn gewend om te polderen, elkaar op te zoeken om gezamenlijk resultaat te boeken. Je ziet dat ook terug in het Nationaal Cyber Security Centrum (NCSC), onderdeel van het NCTV. Daarin werken publieke en private partijen zij aan zij om Nederland digitaal veilig te houden. Dat doet een ander land ons niet zo snel na. Daarom durf ik te stellen dat we nog altijd in de voorhoede lopen. Regelmatig worden we vanwege die positie door andere landen om advies gevraagd. Via het actieprogramma van de tweede Nationale Cyber Security Strategie zijn grote stappen gezet. Zo wordt de aanschaf van veilige software gestimuleerd. Publiekscampagnes zoals Alert Online vergroten het bewustzijn. Ook wordt geïnvesteerd in innovatie en onderwijs, zo is bijvoorbeeld het kennisplatform Dcypher opgezet. Bovendien heeft Nederland het voortouw genomen tijdens het EU-voorzitter-schap om cybersecurity internationaal goed op de agenda te zetten. Het kabinet heeft verder extra investeringen gedaan in de aanpak van

Nederland acteert internationaal op topniveau in het digitale domein en heeft de afgelopen jaren een goede basis voor cybersecurity opgebouwd. Tegelijkertijd blijkt uit het Cybersecuritybeeld Nederland 2016 dat er sprake is van toenemende dreigingen in het cyberdomein. Cybercrime, -spionage en -sabotage vormen een groot risico voor onze economie en samenleving. Het is noodzakelijk dat we hier een krachtig antwoord op hebben, zodat we een ‘safe place to do business’ blijven. Nederland moet de volgende stap zetten om in het digitale tijdperk mee te blijven komen en dat kan alleen als overheid en het bedrijfsleven samen optrekken.

Patricia Zorko
Plv. NCTV en directeur Cybersecurity, ministerie van Veiligheid en Justitie

NEDERLAND ALS ‘SAFE PLACE TO DO BUSINESS’

WE MOETEN SAMEN DE VOLGENDE STAP ZETTEN

cybercrime en het Nationaal Detectie Netwerk, waarbij overheid en bedrijven elkaar informeren over actuele dreigingen. En recent heeft de Tweede Kamer het wetsvoorstel cybersecurity aangenomen. Hieronder valt een meldplicht voor rijksoverheid en vitale sectoren als het gaat om ernstige veiligheidsincidenten, zodat het NCSC zicht heeft op risico’s voor de samenleving en advies en hulp kan bieden. Maar dat is geen reden om achterover te leunen. Andere landen maken ook een cyberstrategie en investeren flink. Het lijkt erop dat we last hebben van de wet van de remmende voorsprong. Daar moeten we niet in blijven hangen. Als Nederland echt een digitale ‘safe place to do business’ wil blijven, dan moeten zowel overheid als bedrijfsleven de komende jaren hier extra in investeren.

Helpende hand

Cybersecurity staat gelukkig bij steeds meer organisaties op de agenda. Ook hier is samen-werking van belang. Zo kunnen grotere bedrijven voor hun digitale veiligheid afhankelijk zijn van kleinere bedrijven. Tegelijk is het MKB een van de sectoren die meer ondersteuning nodig heeft. Gelukkig zijn er grote bedrijven als de Rotterdamse haven en luchthaven Schiphol die kleinere bedrijven in hun keten helpen om de cybersecurity op orde te brengen. Dat zijn mooie initiatieven. Waar nodig kan ook de overheid hier een helpende hand toesteken, in gezamenlijke coalitie met het bedrijfsleven. Verder moet de overheid het voortouw nemen als het gaat om de bestrijding en preventie van bijvoorbeeld zware cybercriminaliteit en economische spionage. Deze onderwerpen zijn grensoverschrijdend en maken we bespreekbaar binnen de Europese Unie. En als het om regelgeving gaat, is het onze taak om deze zoveel mogelijk te harmoniseren.

Serieus investeren

Het rapport van Herna Verhagen geeft goed aan wat er moet gebeuren om Nederland veiliger te maken. Ik onderschrijf dat er in de Tweede Kamer, in de bestuurskamer en in de huiskamer wat moet gebeuren. We moeten ons allemaal veel meer in het onderwerp cybersecurity verdiepen, kijken hoe we digitaal veilig blijven, zeker nu steeds meer apparaten aan het internet gekoppeld worden. We kunnen het ons niet meer veroorloven om naïef te zijn. Verder vind ik de norm om tien procent van het ICT-budget te reserveren voor cybersecurity, een goede stelregel voor iedereen en een start om serieus te investeren in de eigen digitale veiligheid en die van Nederland. Ook moeten we meer investeren in onderwijs: in de basiskennis over cybersecurity en in het opleiden van cybersecurityspecialisten om aan de groeiende vraag te kunnen blijven voldoen.

Kom in beweging!

Er is veel werk te doen en het is van belang dat iedereen in Nederland in beweging komt. Een overkoepelende visie, ambitie en strategie is nodig, waar iedereen zich aan kan verbinden en actie op kan ondernemen. Het gaat vooral om die actie. We moeten kijken waar vernieuwing nodig is en waar de innovaties zitten om ons land vooruit te helpen. En dus zowel de kansen die digitalisering ons biedt blijven benutten als de dreigingen aanpakken. Overheid en bedrijfsleven moeten samen de handen ineen slaan om ook voor de toekomst de digitale dijkbewaking van Nederland op orde te houden!

Jos de Groot
Directeur Telecommarkt, directoraat-generaal Energie, Telecom en Mededinging
Ministerie van Economische Zaken

NEDERLAND VOOROP IN CYBERSECURITY!

De laatste tijd is er binnen het ministerie van Economische Zaken (EZ) steeds meer aandacht voor de toenemende cyberspionage gericht op innovatieve Nederlandse bedrijven. Zo ook voor de dreiging van digitale aanvallen op vitale infrastructuren. Ik moet er niet aan denken dat infrastructuren als energie en telecommunicatie uitvallen. Dat zou ons maatschappelijk en economisch leven flink ontwrichten.

Het mooie is dat ik nu, als beleidsverantwoordelijke directeur voor telecommunicatie, mijn beleidservaring met de energiesector kan benutten om de kans op dit soort scenario's in die sectoren te verkleinen. En dat kan niet zonder een goede samenwerking met het bedrijfsleven. Ik ben dan ook zeer content met het recente rapport van Herna Verhagen, CEO van PostNL. Zij onderstreept dat cybersecurity een basisvoorwaarde is voor economische groei en maatschappelijke ontwikkeling. En ze doet een aantal aanbevelingen. Welke aanbevelingen spreken mij aan? Er zijn er veel, maar ik licht er hier een paar uit. Vanuit de optiek dat Nederland zijn concurrentievermogen en zijn vestigingsklimaat op peil wil houden én het economisch potentieel van cybersecurity wil benutten. Er is werk aan de winkel.

Kennisontwikkeling

De eerste aanbeveling die mij aanspreekt, betreft het stimuleren van kennisontwikkeling op het gebied van cybersecurity. Het bieden van innovatieve diensten en producten is een 'race-to-the-top'. Om deze race te kunnen winnen, is naast het ontwikkelen van kennis een snelle valorisatie naar bedrijven van essentieel belang. Pas dan kunnen bedrijven meer *state-of-the-art* producten en diensten leveren die schade voorkomen en economische kansen bieden. En die kansen zijn er. De afgelopen jaren groeide de omzet en de toegevoegde waarde van cybersecurity binnen de ICT-sector jaarlijks met 14,5%.

Veilige hard- en software

Onveilige hard- en software wordt vaak genoemd als achilleshiel van cybersecurity. Zeker met de opkomst van het Internet of Things worden de effecten van kwetsbaarheden steeds zichtbaarder. Daarom is dit mijn tweede punt. EZ zet zich samen met het bedrijfsleven reeds in voor veiliger hard- en software. Zoals het opstellen van een normenkader voor het ontwikkelen van veilige software, maar ook door het stimuleren van innovatieve, veilige producten. Maar er is meer nodig. In samenwerking met het ministerie van Veiligheid en Justitie en het bedrijfsleven willen we komen tot een 'roadmap veilige hard- en software'. Deze roadmap moet in kaart brengen welk instrumentarium het beste kan bijdragen aan een betere veiligheid van onder meer het Internet of Things; opdat we goed doordacht de volgende stappen kunnen zetten, nationaal en internationaal.

Digitaal vaardig

Het digitaal vaardig maken van Nederland is het laatste punt dat ik hier belicht. Digitaal vaardig betekent voor mij bewustzijn én het in staat zijn om bekwaam te handelen. Voorlichtingscampagnes gericht op MKB en het brede publiek zijn hierin een belangrijk element. Samen met partners ondersteunt EZ diverse initiatieven op dit vlak, zoals veiliginternetten.nl. Een belangrijk aandachtspunt voor EZ is hoe het bredere MKB meer cybersecure kan worden. Mooi om te zien is hoe diverse grote bedrijven al kleinere bedrijven in hun productieketen bij de hand nemen. Zelf kijken we onder andere naar een verdere uitbreiding van de Information Sharing and Analysis Centres, zodat naast vitale sectoren ook niet-vitale kennisintensieve sectoren betrokken kunnen worden.

Veel goede acties lopen, maar er is meer nodig om dreigingen het hoofd te bieden en economische kansen te pakken. Op watergebied hebben we als Nederland laten zien dat we dat kunnen. Laat het een stimulans zijn om dat ook op cybergebied met elkaar te doen!

"Het bieden van innovatieve diensten en producten is een 'race-to-the-top'. Om deze race te kunnen winnen, is naast het ontwikkelen van kennis een snelle valorisatie naar bedrijven van essentieel belang."

Ronald Prins
Chief Technology Officer &
Founder Fox-IT

De verkiezingen staan voor de deur. Niet alleen in Nederland, maar ook in Frankrijk en Duitsland. Volgens Ronald Prins moeten deze landen ervan uitgaan dat er digitaal ingebroken wordt bij de pers en in politieke omgevingen. “De voortekenen zijn er al.” Hij pleit voor een hoge Cybercommissaris die net als de Deltacommissaris dijken opwerpt in het kader van de nationale veiligheid en vanuit een regierol economische kansen pakt. “Als we niet oppassen, missen we de boot.”

INVESTEER IN EEN DIGITAAL VESTIGINGSKLIMAAT

“De Russen zien het als een spelletje om andere landen via cyberaanvallen te beïnvloeden. Hun succes motiveert hen om hier nog zwaarder op in te zetten. Dit hoeft niet per se in Nederland te gebeuren of op dezelfde schaal als in Amerika; maar houd er maar rekening mee dat het gaat gebeuren.” Prins is ervan overtuigd dat als Fox-IT gaat zoeken, zijn mensen iets zullen vinden bij politieke partijen; in het heden of verleden. Maar het zijn niet alleen de Russen die invloed willen uitoefenen. “Ook de Turken zijn op dit vlak bezig. Zij willen graag weten welke kant het opgaat in Nederland. Daar hebben we al incidenten van gezien.” Momenteel vinden er gesprekken plaats tussen inlichtingendiensten en bedrijfsleven om Nederland tegen digitale beïnvloeding te wapenen. Maar Prins ziet liever dat er geen elektronische verkiezingen worden gehouden. “Ik ben een paar jaar bezig geweest om de risico’s hiervan uit te leggen. Steevast kreeg ik als reactie: ‘Laten we realistisch zijn, wie wil Nederland nou hacken?’ Ik denk dat die discussie wel voorbij is en dat iedereen inmiddels ziet dat we als digitale samenleving enorm kwetsbaar zijn.”

Cybercommissaris

Juist omdat Nederland als digitale samenleving en als digitale economie ontzettend kwetsbaar is, moet het nieuwe Kabinet volgens Prins een Cybercommissaris benoemen. “Er moet een hoge functionaris komen met mandaat, budget en een staf die serieuze plannen maakt. We hebben momenteel in Nederland een cybersecurity-strategie die actieplannen bundelt van dingen die al lopen. Maar het moet compleet anders! Daarom is het belangrijk dat de Cyber-commissaris doorzettingsmacht heeft over alle departementen heen. De urgentie van het onderwerp cybersecurity is zo hoog, dat alleen maar ‘polderen’ geen oplossingen biedt. Wim Kuijken neemt als Deltacommissaris ook besluiten waar niet iedereen het altijd mee eens is. Die bevoegdheid heeft hij. En de Cybercommissaris moet dat net zo hebben.” De doorzettingsmacht van deze nieuwe Cybercommissaris moet ook gelden voor het bedrijfsleven, vindt Prins. “Het bedrijfsleven moet maar wennen aan het feit dat een dergelijke hoge functionaris cyberzaken reguleert. De vitale infrastructuur is toch al een gereguleerde sector, waar voorschriften van de overheid gelden. Waarom dan niet voor cybersecurity? Misschien voelt dit bij bedrijven als het afdwingen van iets, maar ik zou vooral willen zien dat de Cybercommissaris verantwoordelijkheid neemt voor wat er in het bedrijfsleven gebeurt en leiderschap toont vanuit een overkoepelende visie en ambitie. Dan wordt er niet zomaar iets verplicht; dan streven we gezamenlijk een bepaald doel na. Kortom, de Cybercommissaris neemt de totale cyber-verantwoordelijkheid van Nederland op zich.”

Digitaal vestigingsklimaat

Een Cybercommissaris zou als geen ander de koppeling moeten leggen tussen cybersecurity enerzijds en economische kansen anderzijds. Prins: “Nederland is een handelsland en we zijn ontzettend afhankelijk van onze gedigitaliseerde economie. Zelfs het hele Westland hangt aan het internet; er komt geen komkommer meer uit de grond als het internet platligt. Dat biedt voordelen. In potentie kunnen we binnen Europa een leidende rol spelen op het gebied van cybersecurity, mogelijk zelf in de wereld. Bedrijven zullen steeds meer gaan zoeken naar een veilig land waar ze hun datacenter en IT willen onderbrengen. Ze kijken naar landen waar ze de minste kans hebben op problemen en waar de overheid helpt; een overheid als vangnet bij calamiteiten en als eerste filter om bij het voorkomen van incidenten.” De nieuwe Wet Computer-criminaliteit III en de Wet Inlichtingen- en Veiligheidsdiensten zijn volgens de oprichter van Fox-IT belangrijke instrumenten om dat aantrekkelijke digitale vestigingsklimaat voor bedrijven vorm te geven. “Internet Service Providers vinden het misschien vervelend dat hun signaal dankzij deze wetten kan worden afgeluisterd of gehackt, maar onze nationale banken zijn er juist blij mee. Normale bedrijven zien graag dat de overheid buitenlandse hackers en buitenlandse mogendheden tegenhoudt. Zij zijn niet zo bang dat onze overheid enge dingen doet in hun netwerk. Als we niet de handen ineenslaan en gezamenlijk investeren in het realiseren van een digitaal veilig vestigings-klimaat, dan ben ik echt bang dat we de boot missen. Als Duitsland bijvoorbeeld tegen ons bedrijfsleven zegt: ‘Kom maar hier, wij houden de Chinezen wel voor je tegen’, dan zijn ze zo de grens over. In mijn optiek is het vanuit economische veiligheid gedacht niet zo gek om het ministerie van Economische Zaken hierin het voortouw te laten nemen. Dit ministerie zou de economische kansen moeten zien en kunnen pakken.”

Besluitvorming
Probleempje is nog wel dat Nederland een dreigend tekort aan cybersecurityspecialisten heeft. Prins herkent dit, maar ziet het als een gevolg van te weinig aandacht voor cybersecurity in ons land. “Als we maar een keer de ambitie uitspreken dat we dit land digitaal veilig gaan maken, dan komen ze vanzelf. Jongeren gaan een studie doen, als ze weten dat er een goed en uitdagend werkveld op hen wacht. Het grootste probleem van dit moment, is dat beslissers besluiten moeten nemen over iets wat ze niet goed begrijpen en doorgronden. Een rechter zegt gerust tegen een hacker dat hij als straf twee jaar niet op internet mag. Hij begrijpt niet dat dit in ons digitale tijdperk een zeer zware straf is en dat deze jongen er misschien de rest van zijn leven digitaal door achterloopt. Hoe moet zo’n rechter straks de proportionaliteit en subsidiariteit afwegen van een te zetten tap? Opleiden kan, maar ik denk dat dit probleem zich pas bij volgende generaties oplost. Die groeien op in een digitaal leven en worden in zo’n context volwassen. Het is dan wel zaak dat ze op school goed worden begeleid, en digitale normen en waarden krijgen aangeleerd.”

Waarschuwing
Tot slot waarschuwt Prins voor zelfgenoegzaamheid in Nederland. “Doen we het echt allemaal zo goed als we denken? Kijk naar het internet of things (IoT). Door alles op een onveilige manier met internet te verknopen, wordt onze samenleving alleen maar kwetsbaarder. Het blijft akelig stil in ons land, maar daar moeten we ons echt zorgen over maken. Steeds meer landen gaan zien hoe krachtig en goedkoop het cyberwapen is. Dat geldt ook voor vreemde regimes en terroristen. Daarom wordt het tijd dat we ons goed gaan organiseren.”

Een hoge Cybercommissaris zou net als de Deltacommissaris dijken moeten opwerpen in het kader van de nationale veiligheid en vanuit een regierol economische kansen moeten pakken.

Foto: TasFoto - Nationale Beeldbank

Hans de Jong
Voorzitter directie en CEO
Philips Benelux

BOUWEN AAN NEDERLAND MET DIGITALE TECHNOLOGIE

We moeten met elkaar expliciet uitspreken dat cybersecurity een belangrijke kwestie is, hierop nauwer gaan samenwerken en onze inspanningen structureren. Dan kunnen we samen een digitale kwantumsprong maken.

Je kunt over cybersecurity nooit zeggen: nu hebben we het geregeld. Wat vandaag goed genoeg is, zal morgen achterhaald zijn. Daarom moeten overheid, bedrijfsleven en consument er samen voor zorgen dat we onze digitale bescherming zo goed mogelijk organiseren. De hele wereld staat voor die uitdaging. Dat biedt enorme kansen voor een digitaal hoogontwikkeld land als Nederland.

Samenwerken in een netwerk
Philips vind het belangrijk om de cybersecurity te kunnen waarborgen voor onze professionele en consumentenproducten en oplossingen. Des te meer omdat dit meestal om medische hulpmiddelen en oplossingen voor de persoonlijke gezondheid gaat. Om dit te kunnen realiseren is het ook van belang dat we cybersecurity binnen de onderneming zelf kunnen waarborgen. Wij werken samen in een keten die zich uitstrekt van onze toeleveranciers tot en met onze afnemers. Maar ketens zijn altijd zo sterk als de zwakste schakel. Daarom is voor ons de cybersecurity van de gehele keten cruciaal. Dat betekent dat wij hoge eisen stellen aan onze partners om de veiligheid van hun systemen in orde te hebben en te houden. En we bieden de helpende hand door informatie met ze te delen, te verwijzen naar de juiste tools en partijen. Het is niet voor

“Veilige digitale technologie biedt enorme economische kansen voor Nederland ”

elk bedrijf, zoals in het MKB, even makkelijk om de ontwikkelingen op dit vlak bij te houden. Daarom wisselen wij op vrijwillige basis onze kennis uit met collega-bedrijven. Hiervoor hebben we samen met chipfabrikant ASML in de regio Brainport het initiatief genomen tot een samenwerking met inmiddels meer dan 25 bedrijven. Zo houden we elkaar op de hoogte van de nieuwste mogelijkheden op het gebied van bescherming en we informeren elkaar over aanvallen. Het moet voor overheden ook vanzelfsprekend worden om deel te nemen aan dit soort netwerken. Ook is Philips actief binnen Nationale, Europese en Internationale werkgroepen op het gebied van security.

Security-by-design

Steeds meer producten zijn verbonden met het internet. Bij producten die te maken hebben met onze gezondheid vervaagt steeds meer het verschil tussen het gebruik om gezond te leven, of om na een aandoening (bijvoorbeeld aan ons hart) gezond te blijven. Een voorbeeld is het gebruik van *health watches*. De toegang en het gebruik tot gegevens ligt gevoelig. Daarom is het noodzakelijk dat cybersecurity direct wordt meegenomen in alles wat ontwikkeld wordt – *security-by-design* – waarbij niet alleen het goed ontwerpen en testen van belang is, maar zeker ook het snel en adequaat kunnen reageren als er toch nog iets fout gaat. Kwaliteit betekent voor bedrijven als de onze inmiddels meer dan alleen het goed functioneren van producten en diensten. Het gaat ook om veilig gebruik. Vertrouwen in veilige uitwisseling, zowel van professionele als individuele gebruikers, is cruciaal. Dit goed borgen bepaalt mede je bestaansrecht.

eHealth

Overigens hebben consumenten zelf ook een grote rol als het gaat om hun digitale veiligheid. Als wij bijvoorbeeld apparatuur leveren aan ziekenhuizen of zorginstellingen, dan zorgen wij dat deze optimaal beschermd is tegen hacks en aanvallen. Maar een systeem kan nog zo goed ingericht zijn; wanneer buitenstaanders bijvoorbeeld gemakkelijk fysieke toegang kunnen krijgen tot de apparatuur, medewerkers wachtwoorden op het scherm plakken of zich onvoldoende bewust zijn van de risico’s, dan is het systeem kwetsbaar voor mensen die kwaad in de zin hebben. Ik constateer dat de meeste entiteiten – ziekenhuizen, onderwijsinstellingen, etc. – maatregelen nemen. Maar met de opkomst van eHealth, het Internet of Things en allerlei nieuwe toepassingen op het niveau van de individuele consument, moet de strijd tegen cybercriminaliteit op steeds meer niveaus gevoerd worden. Daarom moet er echt werk gemaakt worden van het creëren van bewustwording bij de gebruiker. Daar ligt in mijn ogen een belangrijke opdracht voor de overheid, maar ook voor bedrijven in hun interne communicatie.

Normenstelsel

Om als land optimaal in te kunnen spelen op digitalisering, moeten we ten eerste beginnen met kinderen van jongs af aan bekend te maken en te leren omgaan met de kansen én de uitdagingen van onlineontwikkelingen. Omdat die ontwikkelingen zo snel gaan, geldt hetzelfde eigenlijk voor de generaties die de schoolbanken reeds ontgroeid zijn. Ten tweede zou de overheid, behalve inzetten op bewustwording, ook moeten werken aan een integrale aanpak op het gebied van cybersecurity. Daarbij houdt elk departement natuurlijk haar eigen verantwoordelijkheden, maar wordt er meer samengewerkt. Hier horen in mijn ogen niet in eerste instantie wetten bij, maar wel een normenstelsel, gekoppeld aan bijvoorbeeld een keurmerk. Dat kan dan bijvoorbeeld doordat er veel sterker ingezet wordt op publiek-private samenwerkingen. Grote bedrijven zoals wij wisselen al decennialang informatie en ervaringen uit met overheden. Maar op het operationele vlak moet dat echt intensiever. De recente oefening van Defensie met een fictieve cyberattack, waaraan verschillende bedrijven met expertise op dit vlak deelnamen, is hier een goed voorbeeld van. Daarvoor hoeft niet wederzijds de deur naar alle kritieke processen en bedrijfsinformatie wagenwijd open, maar kun je toch enorm veel van elkaar leren.

Digitale kwantumsprong

Bij Philips zijn we ons er terdege van bewust dat niemand cybercriminaliteit alleen de baas kan. Overheid, bedrijven, instituties, kennisinstellingen en burgers hebben elk hun eigen verantwoordelijkheid. Ons succes wordt bepaald door de mate waarin we tot samenwerking weten te komen. Ik ben ervan overtuigd dat wanneer we al die losse onderdelen van kennis en ervaring op het gebied van cybersecurity die we in Nederland hebben opgedaan bundelen en structureren, we een digitale kwantumsprong kunnen maken. Die ambitie moeten we ook uitstralen. Veilige digitale technologie biedt enorme kansen om bij te dragen aan het oplossen van maatschappelijke uitdagingen in de zorg, mobiliteit, etc. Daar moeten wij als land leidend in willen zijn. En dat kan. Dat biedt enorme economische kansen. Kansen waarmee we voor de komende generaties verder bouwen aan dit fantastische land.

“De overheid moet inzetten op een integrale aanpak”

Foto: Kees Looijesteijn - Nationale Beeldbank

Een systeem kan nog zo goed ingericht zijn; wanneer buitenstaanders gemakkelijk fysieke toegang krijgen tot de apparatuur, medewerkers wachtwoorden op het scherm plakken of zich onvoldoende bewust zijn van de risico’s, dan is het systeem kwetsbaar voor mensen die kwaad in de zin hebben.

Wie aan de beveiliging van Schiphol denkt, denkt al gauw aan securitypersoneel in de vertrekhal en medewerkers van de Koninklijke Marechaussee die al die miljoenen passagiers dag in dag uit veilig via Schiphol laten reizen. Digitale veiligheid is echter net zo belangrijk. Als we niet meer kunnen steunen op internet omdat het niet meer betrouwbaar is of omdat digitale diensten uitvallen, zijn we uiterst kwetsbaar. Dat moeten we voorkomen, door nu volop te investeren in digitale veiligheidsmaatregelen.

Jos Nijhuis
President en CEO
Schiphol Groep

ZETTEN WE ONZE DIGITALE FIETS WEL OP SLOT?

Alle partijen die opereren met behulp van internet moeten zich beseffen dat online veiligheid niet anders is dan fysieke veiligheid. Als mijn drie kinderen met hun fiets op pad gingen, drukte ik ze op het hart om hun fiets op slot te zetten. En afhankelijk van waar ze heen gingen, gaf ik ook het advies om een ketting mee te nemen om de fiets aan een rek vast te kunnen maken.

Scherp op veiligheid

Ik vraag mij af of wij als ouders en op school wel voldoende veiligheid schenken aan de 'digitale fiets'. Weten leraren wel hoe je die 'op slot' zet? Spreken ze daar genoeg over met hun leerlingen? Het besef dat je scherp moet zijn op veiligheid, ook online, begint namelijk al bij de jeugd. Daarnaast baart het mij zorgen dat er in het hoger onderwijs, aan onze universiteiten, te weinig cybersecurity-experts worden opgeleid. Het is allicht niet haalbaar om cybercriminelen in alle ontwikkelingen voor te blijven, maar waarom streven we er niet naar om op zijn minst gelijke pas te houden? Ik ben ervan overtuigd dat dat kan als we investeren in onderwijs op dit vlak en als we het meer sexy maken voor jongeren om cybersecurityprofessional te worden. Hier ligt een schone taak voor de overheid en het lijkt mij een uitstekend speerpunt voor de Cybercommissaris, waarvoor in het rapport van Herna Verhagen wordt gepleit.

Stelregel voor ICT-budget

Overigens mag de private sector de cybersecurity problematiek zeker niet in zijn geheel afschuiven op de overheid. Wij hebben onze eigen verantwoordelijkheid. Ik ben het dan ook grondig eens met de aanbeveling uit het rapport om als regel 10% van je ICT-budget te reserveren voor cybersecurity. Als je lager zit, moet je je echt op je achterhoofd krabben of je wel genoeg doet. Niet dat we ons blind moeten staren op dat precieze cijfer, maar de stelregel alleen al dwingt je om er serieus mee bezig te zijn. Zo kunnen we voorkomen dat cybersecurity een sluitpost wordt en kunnen we ervoor zorgen dat aandacht voor cybersecurity integreert in alles wat je als bedrijf op het vlak van digitalisering doet. Hierbij kan het geen kwaad als de grotere bedrijven, die zich vaak al heel goed het belang van cybersecurity realiseren, het MKB enigszins bij de hand nemen.

Derde mainport

Het is niet voldoende om alleen te kijken naar onderwijs en de toekomst, we moeten ook nadenken over het heden. Schiphol geldt net als de Haven van Rotterdam als mainport, oftewel vitale infrastructuur voor Nederland. Ik vind het geen gek idee om de digitale economie – die harder groeit dan welke sector ook – te benoemen als derde mainport met een Cybercommissaris als aanjager. Ik zou het dapper vinden als het nieuw te vormen kabinet die verantwoordelijkheid oppakt. Daar hoort wat mij betreft ook bij dat de overheid een klimaat schept waarin er een toegevoegde waarde is voor bedrijven en organisaties om melding te maken van problemen op het vlak van cybersecurity.
We hebben elkaar immers nodig om een inhaalslag op het gebied van cybersecurity te maken. Het is cruciaal dat het nieuwe kabinet dit inziet en daarnaar handelt. Zolang onze politici in de fout gaan met hun eigen e-mailgebruik – ze in feite dus niet hun eigen 'digitale fiets' goed op slot zetten - kunnen we concluderen dat er in alle lagen van onze maatschappij werk aan de winkel is op het gebied van cybersecurity.

"Cybercommissaris als aanjager van digitale economie is geen gek idee"

Nederland is een handelsland en wij adopteren snel nieuwe technologieën. Daar zetten wij met Schiphol ook vol op in. Dat geeft ons een voorsprong. Maar daardoor hebben we ook als eerste en misschien wel het meeste te maken met de uitdagingen van digitale onveiligheid. Verstevig daarom de samenwerking tussen de private en publieke sector, intensiveer onderzoek naar cyberaanvallen voor snellere respons en betere preventie. Maak Nederland digitaal veilig en vaardig.

Ketenveiligheid

Het is niet alleen de overheid die verantwoordelijkheid draagt om Nederland digitaal vaardig te maken, die verantwoordelijkheid dragen wij allemaal. Schiphol heeft de ambitie geformuleerd om wereldwijd de 'best digital airport' te worden. Dat betekent fors investeren in onze ICT en dus ook in onze cybersecurity. Dat is net zo'n wezenlijk onderdeel van onze processen als fysiek controleren of passagiers geen bommen meenemen. We werken intensief samen met een hele reeks aan ketenpartners – douane, afhandelingsbedrijven, luchtvaartmaatschappijen, de NS, etc. – met wie wij veilig informatie en data moeten kunnen uitwisselen. Dat kan alleen in een digital safe environment. Daarom gaan we ook verder dan de eenvoudige vraag aan onze onderaannemers: "heb je het geregeld?" We kijken met hen hoe het beter kan, wat optimaal is, en hoe we daar samen kunnen komen.

"Ik zou het dapper vinden als het nieuw te vormen kabinet die verantwoordelijkheid oppakt"

Ecosysteem

Om hier concrete invulling aan te geven hebben we het Cyber Synergie Schiphol Ecosysteem (Cyssec) opgericht, een platform dat organisaties op Schiphol handvatten biedt voor het bevorderen van cybersecurity. Het doel van dit platform is om de gezamenlijke weerbaarheid in cybersecurity te verhogen, door met vierhonderd partners kennis en informatie te delen en best practices uit te wisselen. Ook zijn we van plan om dit jaar een gezamenlijke cyberoefening te houden. De ketens waarin wij opereren zijn immers zo sterk als de zwakste schakel.

De digitalisering van Nederland brengt enorme economische en maatschappelijke kansen met zich mee, zo stelde Herna Verhagen in haar onlangs verschenen Cybersecurity Advies. Vertrouwen in de digitale wereld is hiervoor een absolute voorwaarde. Ze roept dan ook terecht zowel de overheid alsook de private sector op om versneld in actie te komen om cybersecurity in Nederland te versterken.

Johan Arts
Vice President
IBM Security Europe

ZOEKEN WE CYBERSECURITYSPECIALISTEN OF RAKETGELEERDEN?

TECHNOLOGIE HELPT OM CYBEREXPERTS SNEL EN EFFECTIEF IN TE ZETTEN

Een enorme potentiële belemmering vormt het grote tekort aan cybersecurity specialisten. (ISC)², de vooraanstaande security associatie, prognosticeert voor 2020 een wereldwijde schaarste van 1,5 miljoen vakkrachten, waarbij securityanalisten het meest gevraagd zijn. 46% van alle ondervraagde organisaties geeft aan hier nu al een tekort aan te hebben[1]. Concrete cijfers voor Nederland ontbreken, maar ingeschat op basis van ons BNP zou dit een tekort van circa 20.000 experts betreffen.

Tekort aan opleidingen

Hoe komt dit? Aan deze schaarste liggen verschillende factoren ten grondslag. Niet alleen is er een tekort aan opleidingen, maar ook aan opgeleide specialisten uit het verleden wat zich nu wreekt. Daarnaast vergt het een hoge opleiding, voortdurende bijscholing en een behoorlijke dosis ervaring om effectief te zijn in het securityvak. Het lijkt erop dat je bijna een raketgeleerde moet zijn geweest. Naast een tekort blijkt er dus ook een hoge toetredings-drempel te zijn.

Technologische innovatie

Herna Verhagen breekt in haar rapport al een lans voor meer investeringen in cybersecurity opleidingen, en dit ondersteun ik ten volle. Meer en beter opleiden zal niet voldoende zijn en levert ook pas na vijf tot tien jaar resultaat op. Wat doen we in de tussentijd? Kunnen we technologie inzetten om de toetredingsdrempel in het vak structureel te verlagen? Is dit een realistische verwachting? Persoonlijk denk ik het wel, er zijn genoeg voorbeelden in andere beroepsgroepen en industrieën waar technologische innovatie heeft geleid tot drempelverlaging.
Een eenvoudig voorbeeld: Vroeger ging je voor het maken van een foto naar een fotograaf, een specialist met ervaring, opleiding en apparatuur. Nu maakt iedereen zijn eigen foto's met een smartphone. De fotograaf is echter niet verdwenen, maar legt zich toe op projecten met hogere eisen, zoals modereportages of portretten. De vakexpert schuift op naar een meer specialistische inzet, omdat een deel van het werk door mensen met minder vooropleiding

"Door de inzet van kunstmatige intelligentie zullen meer mensen sneller aan de slag kunnen in de cybersecuritysector"

en ervaring kan worden uitgevoerd. Wanneer je dit eenvoudige voorbeeld vertaalt naar de huidige werkomgeving, is de implicatie dat technologie zal helpen om meer experts sneller en effectiever in te zetten.

Menselijke experts

Ook cybersecurity kan profiteren van technologie om de barrieres van vooropleiding en ervaring te verlagen. Om een beeld te schetsen kun je denken aan de inrichting van het Security Operating Center (SOC), een belangrijke schakel in de security-organisatie: Een level SOC 3 analist heeft normaal gesproken een zeer diepe technische achtergrond en meer dan tien jaar cybersecurity-ervaring. Een level 1 SOC analist kan niet zomaar het werk van een level 3 SOC expert overnemen. Maar kan dit wellicht in de toekomst wel?
Om deze vraag te kunnen beantwoorden is het van belang te begrijpen hoe en waarom de hoge toegangsdrempel in het vakgebied is onstaan. Ondanks het feit dat het een op technologie georiënteerd vakgebied is, blijkt het in hoge mate afhankelijk te zijn van menselijke experts. De hoge toegangseisen zijn ontstaan, omdat informatie over cybersecurity gefragmenteerd en ongestructureerd wordt aangeboden.
Specialisten bouwen hun kennis op door zich jarenlang binnen de securitycommunity te engageren, bijvoorbeeld door blogs te lezen, experts te volgen en conferenties te bezoeken. Maar zelfs voor specialisten is dit steeds vaker onbegonnen werk: jaarlijks worden er alleen al meer dan 700.000 securityblogs en 10.000 onderzoeksdocumenten gepubliceerd.

Cognitieve technologie

Cognitieve technologie kan helpen om grote hoeveelheden ongestructureerde data, zoals blogs, razendsnel te ontsluiten, en hieruit kennis te destilleren die bijvoorbeeld door middel van een digitale adviseur beschikbaar wordt gemaakt aan cybersecurityspecialisten. Hiermee krijgen junior specialisten, zoals de level 1 SOC analist, onmiddellijk toegang tot actuele kennis die ze anders pas door jarenlange ervaring zouden kunnen vergaren.
Recente testen in Europese landen, waaronder door IBM met Watson for Cybersecurity, tonen aan dat dergelijke toepassingen daadwerkelijk helpen om incidenten sneller te ontdekken. Ik wil benadrukken dat dit zeker geen toekomstmuziek is, maar technologie van nu betreft.
Dit alles helpt specialisten van alle geledingen om cyberincidenten sneller op te sporen en vooral sneller op te lossen. Iets wat naast de schaarste aan cyberspecialisten een ander aandachtsgebied van Chief Information Security Officers (CISO's) blijkt te zijn, volgens het recent verschenen rapport *Cybersecurity In The Cognitive Era* van het IBM Institute Of Business Value. Uit deze studie, gebaseerd op interviews met zevenhonderd CISO's uit 35 landen en 18 industrieën, blijkt dat het verminderen van de gemiddelde incidentresponse- en oplostijd zelfs de belangrijkste uitdaging van de komende drie jaar is[2].

Kunstmatige intelligentie

Bij het onderwerp kunstmatige intelligentie komt steevast ook de discussie over werk-gelegenheid om de hoek kijken: leidt de inzet van kunstmatige intelligentie tot banenverlies? Voorlopig is het tekort aan cybersecurity-specialisten zo groot dat dit niet aan de orde is. Sterker nog, door de inzet van kunstmatige intelligentie zullen meer mensen sneller aan de slag kunnen in deze sector. We zullen de menselijke intelligentie en vooral interventie ook nodig blijven hebben om onze IT-infrastructuur optimaal te beveiligen en te kunnen reageren op inbreuken.
Op lange termijn voorzie ik dat de symbiotische relatie tussen mens en machine alleen maar sterker zal worden en dat we ons niet moeten blind staren op het 'kunstmatige' aan intelligentie; voorop staat de 'augmentatie' van menselijke intelligentie.

Digitaal vertrouwen

Als private sector zullen we onze innovatiekracht daarom moeten inzetten om cybersecurity-specialisten te voorzien van nieuwe hulp-middelen die helpen bij het realiseren van hun doelstellingen, en zo bij te dragen aan het vertrouwen in de digitale wereld.

Noten:

1. The 2015 (ISC)² Global Information Security Workforce Study, 2015
2. Cybersecurity In The Cognitive Era, IBM Institute Of Business Value, 2016

David Knibbe
CEO Nationale-Nederlanden
en voorzitter Verbond van
Verzekeraars

De digitalisering van onze samenleving gaat in een rap tempo. Het rapport van Herna Verhagen, dat op verzoek van de Cyber Security Raad is geschreven, constateert dat digitale technologie in bijna alle maatschappelijke sectoren het belangrijkste middel is om informatie te verwerken, te verzenden, of om een primair proces aan te sturen. “Dit is heel herkenbaar; dat zie je terug in de strategie van Nationale-Nederlanden, kort samengevat: digitaal, persoonlijk en relevant. Voordat we een nieuwe service aan klanten ontwikkelen, stellen we nadrukkelijk de vraag: kunnen we klanten de nieuwe service digitaal aanbieden?”

SAMEN ÉÉN VUIST MAKEN VOOR EEN VEILIGER MKB

Aandacht voor digitale beveiliging van bedrijven is volgens David Knibbe, CEO Nationale-Nederlanden en voorzitter Verbond van Verzekeraars, erg belangrijk. “Bedrijven worden steeds meer informatie- en ICT-gedreven. Dit betekent dat ook het top-management zich moet bezighouden met de beveiliging van kritische assets – in ons geval dus persoonlijke en financiële data van klanten. Binnen NN hebben we een overkoepelende security organisatie, die in alle bedrijfsonderdelen is geïmplementeerd. Zo is er een Chief Information Security Officer die verantwoordelijk is voor de algehele beveiliging van ons concern. En per bedrijfsonderdeel zijn er security teams, geleid door Business Information Security Officers.”

Geschikte gesprekspartner

“Centrale aansturing en coördinatie zijn cruciaal voor een effectieve aanpak. Dit betekent dat niet alleen de raden van bestuur en commissarissen zich in security risks moeten verdiepen en zich bewust moeten zijn van de verantwoordelijkheden en aansprakelijkheden. Dat geldt voor iedereen binnen het bedrijf – het zijn immers deze aspecten die na een hack of data-lek in de media volop aandacht krijgen. Een en ander betekent ook dat security officers de topbestuurders van hun bedrijf moeten voeden met actuele informatie of relevante vraagstukken. Ze dienen voor hen een geschikte adviseur en gesprekspartner te zijn. Verder houden we binnen Nationale-Nederlanden voortdurend beveiligingsscans en hanteren we security richtlijnen waar onze bedrijfsonderdelen aan moeten voldoen om data goed te beschermen. Denk aan versleuteling en aanvullende digitale bewaking. Daar waar bij grote bedrijven cyber security vaak al goed is ingericht, kunnen er bij kleinere bedrijven meestal nog wel wat slagen gemaakt worden.”

MKB aantrekkelijk doelwit

Het rapport van de Cyber Security Raad stelt dan ook dat het MKB minder goed beveiligd is en een aantrekkelijk doelwit is voor cyber criminelen. “Veel ondernemers zijn zich er sowieso niet bewust van dat ze zijn aangevallen door hackers. Deze zijn soms al maanden actief binnen in de systemen en kunnen onherstelbare schade aanrichten voordat de ondernemer daar achter komt. Het is daarom belangrijk om het MKB meer voorlichting te geven over cyber security. Overigens kun je de aanpak van een cyber veilig MKB niet alleen bij de overheid beleggen. Zelfs als die daar extra geld voor vrijmaakt. Kijk naar het resultaat van de huidige cybersecurity-subsidies: ondanks alle goede intenties kende 2016 een record aan datalekken en cybercrime-activiteiten. ‘Meer geld’ is dus

“Centrale aansturing en coördinatie zijn cruciaal voor een effectieve aanpak”

“Het MKB is gebaat bij security-oplossingen die toegespitst zijn op hun situatie”

niet altijd een remedie; er moet meer gebeuren. Alle sleutelspelers moeten samenwerken: commercieel en niet-commercieel, van multinationals tot startups. Iedereen kan bijdragen vanuit zijn eigen kracht: de één kennis, de ander een netwerk, weer een ander slagkracht. Samenwerken – daar draait het om.”

Ondersteun MKB

“Het MKB is gebaat bij security-oplossingen die toegespitst zijn op hun situatie, alsmede bij gerichte ondersteuning om uit dit aanbod een passende keuze te maken. Er komen op allerlei terreinen nogal wat veranderingen op ondernemers af. Ze werken zeven dagen per week hard en hebben soms amper tijd om de eigen ICT te controleren. Ook heeft men niet altijd financieel of menselijk kapitaal beschikbaar om in security te investeren. De wereld van een MKB-ondernemer is wat dat betreft anders dan die van een CEO binnen een internationale organisatie. De algemene richtlijn om 10% van het ICT budget voortaan aan security te besteden, is waarschijnlijk niet voor alle ondernemers in het MKB realiseerbaar. Voor het MKB draait het om laagdrempeligheid, betaalbaarheid en positieve beeldvorming rondom security awareness. Geen bangmakerij, maar heldere communicatie, met alledaagse taal en korte uitleg - met voorbeelden en zonder jargon.”

Nederlands Cyber Collectief

Eind november is het initiatief genomen om het Nederlands Cyber Collectief op te richten. Dit is een onafhankelijk platform dat in feite iedereen verbindt die er toe doet in de cyberwereld. Inmiddels hebben zich naast Nationale-Nederlanden ook Deloitte, ESET Nederland, Fox-IT, Meld Misdaad Anoniem, ThreadStone Cyber Security en Veilig Internetten bij het collectief aangesloten. Het Nederlands Cyber Collectief spoort snel nieuwe cyberaanval-methodes op, zowel via partners als direct via MKB’ers zelf. Men leert van iedere hack en gebruikt deze lessen om de rest van het MKB beter te beveiligen.
“Wij weten uit ervaring dat het MKB cyberaanvallen nog niet altijd meldt. Misschien omdat men bang is voor imagoschade, of de zwakke beveiliging niet openbaar wil maken. Hierdoor leert niemand ervan en kunnen cybercriminelen dezelfde zwakheden binnen het MKB blijven uitbuiten. Overigens, indien er zogeheten ‘bijzondere gegevens’ zijn buitgemaakt, dan moet dit worden gemeld bij de Autoriteit Persoonsgegevens (AP). En afhankelijk van het soort gegevens moet dit ook worden gemeld aan de personen waarover gegevens zijn gelekt. Uiteraard hopen wij dat het MKB, indien zij gehackt zijn, de cyberwacht bellen. Dit is een onderdeel van het Nationaal Cyber Collectief. Maar liever nog helpen we hen digitaal veilig(er) te worden.”

Eén vuist

“Het voornaamste doel van het Nederlands Cyber Collectief is om van de huidige versnippering in aanpak één geheel te maken en Nederland op het gebied van cybersecurity veiliger te maken. We zitten daarmee op dezelfde lijn als het rapport van de Cyber Security Raad. Ik doe bij deze een oproep aan alle geïnteresseerde organisaties en individuen om met het onafhankelijke Cyber Collectief samen te werken. Zo maken we samen één vuist tegen cybercriminelen. Het spreekt voor zich dat het Cyber Collectief ook wil samenwerken met, of bijdragen aan andere initiatieven vanuit de politiek en de overheid. Samenwerken, coördinatie en voorlichting – dat zijn sleutelwoorden om Nederland op korte termijn digitaal veiliger te maken.”

Nederland is een waterrijk land. Een inherent risicovolle omgeving. In die risicovolle omgeving bouwen we geen hekjes om elk riviertje, gracht of meertje. Dat is ondoenlijk, schept schijn-veiligheid en zou ook te kostbaar zijn. Nee, we sturen onze kinderen op zwemles, zodat ze leren om te gaan met de risico’s van het waterrijke land. En die aanpak moet ook model staan in ons denken over hoe om te gaan met de inherente risico’s van onze digitale omgeving.

Dick Berlijn
Cybersecurity adviseur Deloitte Nederland

WE LIJKEN ONS ONVOLDOENDE BEWUST VAN DE RISICO’S

LEER ZWEMMEN IN DE DIGITALE VIJVER

Je kunt om elk stukje data een hek zetten, maar dat is niet uitvoerbaar en creëert schijn-veiligheid. Beter is om elke Nederlander in de digitale vijver te leren zwemmen.
Westerse samenlevingen zijn in de loop der jaren meer en meer afhankelijk geworden van digitale toepassingen, netwerken en data. Pas de laatste tien jaar beginnen we ons door nieuws over de vele hacks en cybercriminaliteit meer bewust van te worden dat dit niet zonder risico is. Nu staan we aan het begin van het tijdperk van het *Internet of Things*, *big data* en *data analytics*. Wederom zijn we geneigd om ons daar helemaal in te storten en alle toepassingen gretig te omarmen. En die zijn niet gering. Maar opnieuw lijken we ons onvoldoende bewust van de risico’s.

Normstellende overheid

In mijn ogen is de grootste uitdaging het werken aan bewustwording en het daaraan koppelen van consequenties, de juiste dingen doen. Concreet betekent dat verhelderen wie waarvoor verantwoordelijkheid is, afspraken maken over wie wat doet en cybersecurity continu onder de aandacht brengen en houden. Daarin dragen verschillende partijen een verantwoordelijkheid; wij als individuele gebruikers van de digitale omgeving, het bedrijfsleven, de overheid en nog vele anderen. De overheid doet al veel, maar zou nog meer het goede voorbeeld moeten geven. Gemeenten die nog op Windows 7 draaien, dat kan niet meer. Daarnaast moet de overheid normstellend optreden en ons aanspreken op onze eigen verantwoordelijkheid. Ik denk dat we ook meer *carrots and sticks* zullen gaan meemaken: wie er met de pet naar gooit, moet dat voelen en wie er werk van maakt zal worden beloond.

Digitale verdediging

Het niveau van cybersecurity in Nederland verschilt heel erg per sector. De financiële sector heeft haar cybersecurity heel aardig op orde. Het kost ze simpelweg te veel geld als ze zich niet goed beschermen. Maar in andere sectoren is dat besef er vaak nog veel minder. Zo kom ik soms bij ziekenhuizen om te spreken over dit onderwerp. Niet altijd realiseren die ziekenhuizen dat ze op een berg data zitten. Daar kun je geweldig mooie dingen mee doen, zoals het voorspellen van ziekteverloop, onderzoek en betere resultaten boeken bij operaties. Maar de ziekenhuis omgeving is ook kwetsbaar. Iedereen kan er in- en uitlopen en gegevens worden niet altijd voldoende beschermd. Als je niet begrijpt hoe belangrijk data zijn, dan investeer je ook minder in beveiliging.

Secure

Ik pleit er zeker niet voor om alles zoveel mogelijk dicht te gooien. Daarvoor is uitwisseling van informatie te belangrijk. Maar bereid je wel zo goed mogelijk voor op eventuele hacks. Denk na over hoe je je digitale verdediging organiseert en over welke dingen je wel en welke je niet online wilt zetten. Risico’s die je niet hoeft te lopen moet je niet willen lopen. Neem daar actie op. Maar 100% veiligheid bestaat niet, en het volledig dicht zetten van alle ingangen is geen optie.

Vigilant

Is de detectiecapaciteit op orde? Kan de organisatie het waarnemen als er vreemde dingen op het netwerk gebeuren? Als dat niet het geval is, kan de organisatie ook geen maatregelen nemen. Een goede detectie capaciteit is dus essentieel.

Resiliant

De volgende stap is de reactie. Kan de organisatie adequaat reageren als er iets bijzonders gebeurt? Is er een goed opgeleid en getraind team dat goed kan reageren op het incident? En is men in staat de schade beperkt te houden? Of zaten alle eieren in het zelfde mandje? Onderzoekt men reactiemogelijkheden na een incident? Als dat het geval is, kan men ook leren van het incident en procedures desgewenst bijstellen.

“Cybersecurity is complex, maar overzichtelijk te benaderen”

Middelen

Kleinere bedrijven zullen niet altijd over de middelen beschikken om zelf alle noodzakelijke maatregelen te nemen. Maar bepaalde zaken kunnen worden uitbesteed en hoeft een bedrijf niet zelf te doen. Alle partijen, ook de kleinere, moeten de interne organisatie onder de loep nemen: hoe gebruik ik internet en welke risico’s loop ik? Kun je het niet zelf: zorg dat je hulp inroept van de experts. Die zijn er voldoende. Denk nooit dat het jou niet overkomt.

Overzichtelijke benadering

Het is een uitdaging om gelijke pas te houden met cybercriminelen. Bij Deloitte doen we er alles aan om te blijven bouwen aan onze kennis en ervaring op dit vlak. Dat betekent onder meer dat we veel aandacht besteden aan het rekruteren van – veelal jonge – experts. Om hen scherp te houden sturen we ze naar de Cyberlympics (jaarlijkse internationale cybersecurity wedstrijd), waar ze al vijf keer eerste werden. Ook onderwerpen we de eigen organisatie aan ‘self inflicted fishing campaigns’, om het bewustzijn op dat gebied hoog te houden.

Tot Slot

Cybersecurity is complex, maar is overzichtelijk te benaderen. Over welke data beschikken wij, is alle data even belangrijk, welke data mag nooit worden gecompromitteerd, hoe is die data beveiligd, hoe zit het met onze identity and access management, moet die data naar de cloud of juist niet, etc. Het begint met bewustzijn, weten dat jouw data het nieuwe goud is en dat er partijen zijn die die data graag willen bemachtigen. Goed password management, het up-to-date houden van firewalls, het op tijd patchen van software, etc. zijn allemaal belangrijke zaken die geen fortuin kosten om te implementeren.

Er gebeurt al veel op het vlak van cybersecurity. De overheid is goed bezig, veel bedrijven en organisaties geven het de aandacht die het verdient, steeds meer burgers worden zich bewust van de risico’s die bij alle nieuwe mogelijkheden horen. Op die lijn moeten we verder. Cybersecurity moet gewoon een deel vormen van onze dagelijkse handelingen.

Wie waarborgt de veiligheid wanneer klanten onbewust derden toegang geven tot hun gegevens? De nieuwe kansen in de markt noodzaken tot samenwerking op het gebied van cybersecurity.

Wiebe Draijer
Voorzitter raad van bestuur
Rabobank

VEILIG EN MET VERTROUWEN ONLINE, OOK BUITEN DE BANK

“De digitalisering brengt grote economische en maatschappelijke kansen mee. Om die kansen te kunnen blijven benutten, is het noodzakelijk dat we vertrouwen hebben in de digitale wereld en ons er veilig kunnen bewegen”

Ik vind deze zin uit het rapport van Herna Verhagen heel treffend. Ons dagelijks leven wordt steeds meer digitaal ondersteund en gevormd. Cyber en fysiek zijn volledig geïntegreerd. Ook bij het denken in veiligheids-concepten is het belangrijk om je dat goed te realiseren. Teveel nadruk op woorden als ‘digitaal’ en ‘cyber’ zorgt ervoor dat dit voor veel Nederlanders een ‘ver-van-mijn-bed-show’ wordt.

Bij de discussie over veiligheid gaat het voornamelijk over technische aangelegenheden. Denk aan belangrijke vraagstukken als ‘wat voor systemen en software heb je nodig’, ‘hoe creëer je een veilig netwerk’ en ‘hoe wordt een gebruiker geïdentificeerd’.

Wanneer ik vanuit bankperspectief naar de wereld kijk dan zie ik een ander, wellicht groter, probleem. Namelijk het vraagstuk over beveiligingsbewustzijn, over bekwaam handelen in onze digitale wereld.

Oplichters zijn niet altijd ‘hightech’

Je hebt als bank het hoogst denkbare technische niveau van veiligheid ingericht, bijvoorbeeld bij het online identificeren van klanten. En dan nog gaat het soms fout. Eenvoudigweg omdat klanten door slinkse oplichters worden misleid. Het is lang niet altijd ‘hightech’ wat het oplichtersgilde toepast. Vaardigheden die in de fysieke wereld met de paplepel zijn ingegoten, behoeden ons vaak voor nare zaken als diefstal en oplichting. Helaas zien wij dat die vaardigheden vaak ontbreken als wij het internet op gaan. Met alle gevolgen van dien.

Nieuwe kansen in de markt

De nieuwe Europese Directive on Payment Services (PSD2) zal kansen bieden voor nieuwe toetreders. Een samenleving die gebaseerd is op een ‘Open Banking Model’. Dat is goed nieuws voor consumenten. Toch maak ik mij ook zorgen. Niet omdat dit de verdienmodellen van banken onder druk zet, maar omdat onze klanten extreem kwetsbaar worden wanneer zij onbewust derden toegang geven tot zijn of haar gegevens. Of zelfs toestaan om ‘buiten de bank om’ te bankieren. Wie waarborgt in dergelijke constructies de veiligheid? Wie zorgt ervoor dat de consument goed wordt beschermd tegen kwaadwillenden ? De klant zelf -zo wordt in het rapport geconstateerd- is daar niet vaardig genoeg voor. En wij als banken, wij kunnen behalve het geven van algemene waarschuwingen niets doen omdat we eigenlijk geen partij zijn.

Samenwerken om de veiligheid te verbeteren

In mijn optiek ligt hier een enorm braakliggend terrein. De publieke en private sector moeten de handen ineen slaan. Om te zorgen dat de weerbaarheid van onze burgers groot genoeg zal zijn, maar ook om te zorgen dat we adequate wet- en regelgeving hebben zonder deadlocks. Ik noem als voorbeeld de wettelijke bewaar-termijnen voor gegevens en privacywetgeving. Alleen als we al dit soort zaken in samenhang benaderen kunnen we goed bouwen aan een veilige toekomst.

Ik spreek mijn hoop en verwachting uit dat het nieuwe kabinet het belang inziet van een veilige, digitale samenleving en het dossier cybersecurity prioriteit geeft. Daarbij blijft investeren in nieuwe, gebruikersvriendelijke beveiligingstechnieken, maar ook borgt dat er voldoende gekwalificeerde security professionals in ons land zijn. En tot slot dat zij regelmatig samen met het bedrijfsleven voorlichtingscampagnes voor de ‘Online Burger’ organiseert. Dit alles, zodat we ons met vertrouwen en veilig kunnen bewegen in de digitale wereld.

Het is lang niet altijd ‘hightech’ wat het oplichtersgilde toepast

Nederland moet onveiliger worden voor criminelen. Oók in de digitale wereld. Cybercriminaliteit kost de Nederlandse samenleving naar schatting zo'n tien miljard euro per jaar. De digitalisering van veiligheid heeft het politiewerk fundamenteel veranderd.

Erik Akerboom
korpschef van politie

OOK WAAKZAAM EN DIENSTBAAR IN HET DIGITALE DOMEIN

DIGITALISERING VEILIGHEID IS TOPPRIORITEIT

De winst die we als politie afgelopen jaren behaald hebben in het fysieke domein, mag niet teniet worden gedaan door ongeziene criminaliteit in de digitale wereld. We moeten als korps fors investeren in mensen en middelen om in de pas te blijven lopen met toekomstige veranderingen. De aangiftebereidheid van burgers in dit domein moet omhoog, we moeten onze kennis doorlopend bij kunnen spijkeren en er moet extra geïnvesteerd worden in de middelen, zodat politiemensen hun werk kunnen doen.

Investeren loont

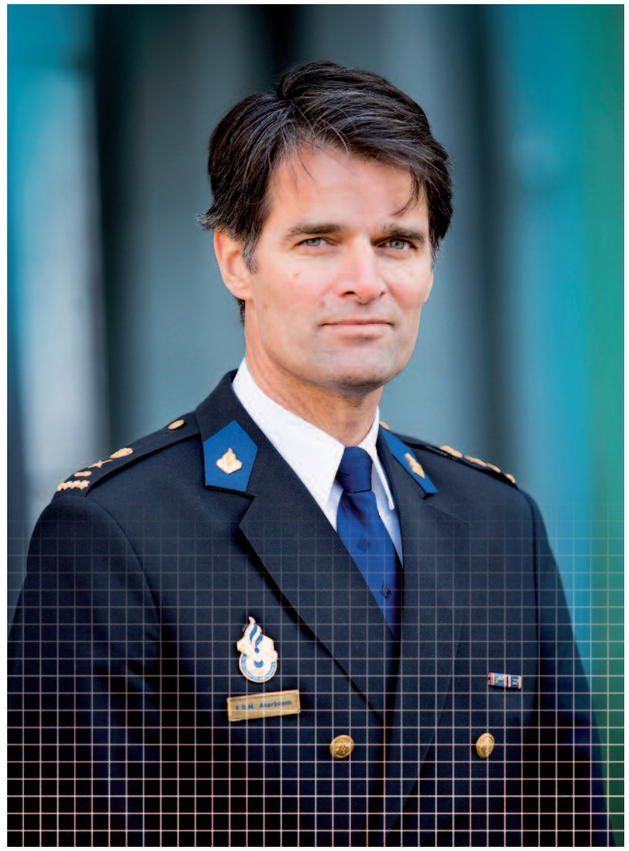
Dat een stevige investering loont, zien we aan ons Team High Tech Crime (THTC) dat sinds 2015 volledig op sterkte is. Het staat internationaal hoog aangeschreven en heeft de laatste jaren veel ervaring opgedaan met effectieve interventies en publiek-private samenwerking. Dit jaar trad het THTC onder andere succesvol op tegen een Nijmeegs bedrijf dat in het criminele circuit telefoons verkocht waarmee versleutelde berichten verstuurd konden worden. De 36-jarige eigenaar is aangehouden en Nederlandse en Canadese servers zijn in beslag genomen. Maar het bestrijden van cybercrime is niet langer uitsluitend een taak voor een team gespecialiseerde collega's. Het moet bij alle 65.000 politiemensen tussen de oren zitten. Of ze nu op straat werken, agenten opleiden, zich bezighouden met Europese aanbestedingen of met ICT: het bestrijden van cybercrime en gedigitaliseerde criminaliteit is politiewerk.

Sluitende aanpak cybercrime

De digitalisering van veiligheid is voor mij topprioriteit. Het is mijn sterke ambitie om een goed toegeruste organisatie neer te zetten die ook in het digitale domein waakzaam en dienstbaar is. Onze eerste stap op weg naar een sluitende aanpak van cybercrime is het inrichten van cyberteams in de eenheden. In diverse eenheden is dit al een feit, de overige volgen. Deze teams onderzoeken de reguliere cybercrime, vergroten de kennis van hun collega's in de eenheden en ondersteunen bij aangiftes van cybercrime. Zo verbeteren we onze dienstverlening aan burgers en bedrijven. De teams bereiden de organisatie in feite voor op de verdere digitalisering van ons vak. Daarnaast werven we tussen 2015 en 2018 jaarlijks honderd digitale experts die onder andere een bijdrage leveren aan de aanpak van cybercrime.

Permanente vernieuwing

Dat zijn mooie, maar wel basale stappen. Gezien de urgentie moeten we ook investeren in een toegankelijker aangifteproces, goed opgeleid personeel, een betere informatiepositie en



“Cybercrime ontwikkelt zich tot een nieuwe dienstensector”

innovatieve oplossingen. Hiervoor is het noodzakelijk dat er meer flexibiliteit komt in de nu nog in de begroting vastgezette verhouding tussen uitgaven aan personeel en middelen. Deze vaste verhouding zou ik graag willen loslaten. Daarnaast zijn extra investeringen noodzakelijk om de snelle ontwikkelingen bij te kunnen houden. Een meerjarig actieprogramma met investeringsagenda, zoals mevrouw Verhagen adviseert aan het nieuwe kabinet, past bij de aanbevelingen van de Algemene Rekenkamer over de ICT bij de politie om meer ruimte beschikbaar te maken voor permanent noodzakelijke vernieuwing.

Modern wettelijk kader nodig

Naast adequate middelen is een modern wettelijk kader een essentiële voorwaarde voor de strijd tegen cybercriminaliteit. Dit geeft ons niet alleen eigentijdse instrumenten, maar schept ook kaders waarbinnen wij democratisch gelegitimeerd kunnen optreden. De huidige wet- en regelgeving is gedateerd. Een eerste stap is de Wet Computercriminaliteit III die recent door de Tweede Kamer is aangenomen en nu bij de Eerste Kamer ligt. Voor de opsporing is deze wet essentieel.

Bijdrage overheid beperkt

Het Cyber Security Beeld Nederland laat een sterke toename van de dreiging van cybercrime zien. Met name *ransomware* en *advanced persistent threaths* nemen enorm toe. Professionele criminele samenwerkingsverbanden voeren steeds geavanceerdere aanvallen uit. En onlangs vond in de VS de eerste massale DDoS-aanval plaats met gebruik van Internet of Things-devices. Ons Team High Tech Crime heeft de handen vol aan zulke nieuwe, innovatieve vormen van cybercrime die zich vaak richten tegen de vitale infrastructuur. In dit licht is het belangrijk om te onderkennen dat de overheid zelf maar beperkt kan bijdragen aan een veilige digitale infrastructuur. Wij hebben intern nog een enorme stap te zetten, maar als we cybercrime en gedigitaliseerde criminaliteit duurzaam willen aanpakken, moeten we samenwerken met alle relevante publieke en private partijen. We moeten onze informatie delen met elkaar en iedereen moet zijn eigen instrumentarium in willen zetten in het belang van Nederland.

Kansen voor opsporing

Wat ik zorgelijk vind, is dat specialistische kennis allang niet meer nodig is voor het plegen van cybercrime. Tegenwoordig koop je op online-marktplaatsen complete pakketten waarmee je kunt hacken of een DDoS-aanval kunt uitvoeren. Inclusief goed geregelde klantenservice. Cybercrime ontwikkelt zich tot een nieuwe, criminele dienstensector. We zien ons ook steeds vaker geconfronteerd met een vermenging van criminaliteit in het fysieke en digitale domein. Op het Darkweb worden bijvoorbeeld drugs, wapens en valse identiteitsbewijzen verhandeld. Er wordt betaald met bitcoins, maar de goederen worden door pakketdiensten in de fysieke wereld afgeleverd. En de bitcoins worden weer omgezet

Foto: Grekenrooi - Nationale Beeldbank

Dreigingen van vandaag zijn de reguliere criminaliteit van morgen. Wij moeten doorlopend meebewegen. Zonder structurele aandacht voor cybersecurity en gedigitaliseerde criminaliteit is deze zich telkens vernieuwende dreiging onmogelijk bij te houden.

in euro’s. Hier liggen kansen voor de opsporing. We werken nu al samen met pakketdiensten om criminele pakketten te onderscheppen. En in onze goede samenwerking met banken liggen mogelijkheden voor de aanpak van deze vorm van witwassen.

Publiek-private samenwerking

Iedereen is verantwoordelijk voor zijn eigen digitale veiligheid. Door met burgers en bedrijven slimme interventies te ontwikkelen, wordt de aanpak pas echt effectief. Een goed voorbeeld van succesvolle publiek-private samenwerking is de Electronic Crimes Taskforce (ECTF) waarin politie, Openbaar Ministerie, grootbanken en de Betaalvereniging samenwerken. In 2016 organiseerde dit ECTF een internationale *money mule*-actie waarbij 178 arrestaties zijn verricht. En recent gingen wij een succesvolle samenwerking aan met de securitybedrijven Kaspersky Labs en Intel Security, met betrekking tot *ransomware*-aanvallen. Op de website Nomoreransom.org is informatie te vinden over het voorkomen en verhelpen van zo’n aanval. Steeds meer bedrijven sluiten zich bij dit initiatief aan. Daarnaast werkt ons Landelijke Meldpunt Internetoplichting (LMIO) intensief samen met banken en Marktplaats om fraude op online-handelsplaatsen aan te pakken. Ook houdt het meldpunt een bestand bij van verkopers over wie melding van oplichting is gedaan. ‘Check de Verkoper’ is te vinden op Politie.nl.

Structurele middelen

De ontwikkelingen op het gebied van cybercrime gaan razendsnel. Dreigingen van vandaag zijn de reguliere criminaliteit van morgen. Wij moeten doorlopend meebewegen. Zonder structurele aandacht voor cybersecurity en gedigitaliseerde criminaliteit is deze zich telkens vernieuwende dreiging onmogelijk bij te houden. Landen om ons heen hebben al flink geïnvesteerd op dit gebied. Nederland kan niet achterblijven.

“Landen om ons heen investeren flink, Nederland kan niet achterblijven”

Met de toenemende digitalisering van de samenleving wordt de kwetsbaarheid van consumenten steeds groter. Om de consument te beschermen is het daarom noodzakelijk om regels op te stellen. We hebben immers ook regels die gelden voor de fysieke veiligheid van producten; onze digitale veiligheid is in essentie niets anders.

Bart Combée
Algemeen Directeur
Consumentenbond

CONSUMENTEN MOGEN OOK DIGITAAL VEILIGE PRODUCTEN VERWACHTEN

Uit onderzoek van de Consumentenbond blijkt dat consumenten identiteitsdiefstal – wachtwoorddiefstal, *phishing*, kopie van het paspoort – als hét grootste cybersecurity-issue ervaren. Dat blijkt ook uit het aantal meldingen van slachtoffers van identiteitsdiefstal. Met name de steeds verdergaande professionalisering van cybercrime is daar debet aan: het wordt voor de leek steeds ingewikkelder om verschillende vormen van cybercrime te herkennen. De tijd van de overduidelijke phishing-mail vol met spelfouten is voorbij.

Kennis ontbreekt

Consumenten zijn zich goed bewust van de problemen en gevaren rond cybersecurity. Toch is het voor consumenten vaak moeilijk om zelf zorg te dragen voor bescherming omdat de concrete kennis ontbreekt. Daarvoor verandert er eenvoudig te veel en is de materie te complex. Dat ontslaat consumenten overigens niet van hun eigen verantwoordelijkheid voor hun veiligheid. Ze moeten bijvoorbeeld wel updates installeren, sterke wachtwoorden gebruiken, en back-ups van hun data maken. De Consumentenbond geeft hier tips en informatie over.

Techneutrale wetgeving

Met het Internet of Things (IoT) gaan de ontwikkelingen zo snel dat je niet van consumenten kan verwachten dat ze alles bij kunnen houden en doorgronden. Een incident zoals recent met *smart toys* die stiekem geluid opnemen, dat mag niet gebeuren. Ook zien we een waterbed-effect in de cybercriminaliteit: zodra een bepaalde sector zich goed beveiligt, zoals de bankensector, richten cybercriminelen zich op andere sectoren.
Omdat technologie en criminaliteit zich razendsnel ontwikkelen, hebben juist het bedrijfsleven en de overheid een extra verantwoordelijkheid. Daarom moet de overheid over de hele linie techneutrale regelgeving invoeren. Een volgend kabinet moet de handschoen oppakken en een sterk wetgevend kader hoog op de politieke agenda zetten. Een type eis kan bijvoorbeeld zijn dat gedurende de levensduur van het product de software, de beveiliging, en de functionaliteit vanuit de fabrikant op orde moet blijven.

Verplichte normen

Om het bovenstaande te realiseren kan de overheid het bedrijfsleven de verplichting opleggen om zelf normen in te stellen. Een dergelijke verplichting is niet gek: je mag immers ook niet zomaar een bank beginnen zonder vergunning en ook aan fysieke producten stellen we allerlei eisen. Het is niet realistisch dat bedrijven dit zonder druk van de overheid zelf oppakken. Ten eerste kost het bedrijven geld om een dergelijk systeem op te stellen zonder dat de opbrengsten hoger worden, waardoor de prikkel minder aanwezig is. Ten tweede is er bij een niet-verplicht systeem het compliance probleem, dat niet alle bedrijven aan een normaliseringssysteem willen deelnemen. Dan regel je alleen de bovenkant van de markt en niet de onderkant, terwijl dat juist wel nodig is als we de problemen rondom cybercrime de baas willen blijven. Als gebruiker heb je net als bij fysieke producten namelijk recht op een goed werkend en veilig product.

Gegarandeerde veiligheid

Vanuit het gebruikersperspectief ben ik het niet eens met de 10% maatstaf waarvoor in het rapport Verhagen wordt gepleit: een consument hoeft niet 10% budget te investeren in beveiliging. Als consument in een moderne economie mag je er van uitgaan dat er alleen maar veilige producten de markt op komen. Dat is niet wezenlijk anders dan bij de fysieke veiligheid: je mag geen giftige producten verkopen waarbij de consument er zelf maar voor moet zorgen dat het niet meer giftig is.

> “Een volgend kabinet moet de handschoen oppakken”

Piet Mallekoote
Algemeen directeur
Betaalvereniging Nederland

Een veilig betalingsverkeer is cruciaal voor een efficiënte afhandeling van transacties in de economie. Indien de veiligheid in het geding komt, kan dit leiden tot een verlies aan vertrouwen in het betalingsverkeer.
Dit gaat gepaard met hogere maatschappelijke kosten en kan in het ergste geval een economische crisis inluiden, die vergelijkbaar is met de krediet- en schuldencrisis van de afgelopen jaren.[1]

CYBERSECURITY BELANGRIJK VOOR VERTROUWEN IN BETALINGSVERKEER

ZORG VOOR WERKBARE WETTEN EN REGELS

De digitalisering van het betalingsverkeer in Nederland is al vele jaren gaande. Nederland behoort op dit gebied tot de koplopers in Europa en de digitalisering heeft er toe bijgedragen dat ons land behoort tot de landen met de laagste maatschappelijke kosten van het betalingsverkeer in Europa[2]. Dit kan niet zonder voldoende vertrouwen in het fiduciaire karakter van het geld. Cybersecurity is dan ook van groot belang om dit vertrouwen niet in de waagschaal te stellen. Onder cybersecurity wordt volgens de definitie in de Nationale Cyber Security Strategie verstaan 'het streven naar het voorkomen van schade door verstoring, uitval of misbruik van ICT en, indien er toch schade is ontstaan, het herstellen hiervan.' Met voortgaande digitalisering en innovaties in het verschiet, blijft een grote aandacht voor cybersecurity door alle stakeholders in het betalingsverkeer topprioriteit.

"Het aanmaken en onthouden van verschillende toegangscodes gaat tot het verleden behoren"

Niet van deze tijd

Veiligheid is een thema waarvoor alle partijen die in betaalketens actief zijn – aanbieders, ondersteunende dienstverleners en eindgebruikers – een eigen verantwoordelijkheid hebben. Dat komt niet vanzelf. In dit kader helpen de Betaalvereniging en haar leden consumenten meer bewust te maken van internetfraude en wat zij zelf kunnen doen om die te voorkomen. Bekend is in dit verband de nationale (televisie) voorlichtingscampagne 'Hang op, Klik weg, Bel uw Bank'. Ondernemers kunnen zelf ook nog veel meer doen om hun klanten veiliger te laten betalen. Zo bieden veel e-commerce bedrijven en nutsbedrijven consumenten de gelegenheid in hun internetomgeving een incassomachtiging af te geven via een 'vinkje'. Deze werkwijze, hoewel goedkoop en efficiënt, is vanuit cybersecurity oogpunt niet langer van deze tijd. Dit omdat de identiteit van diegene die de machtiging verstrekt, niet is vastgesteld. Daarom heeft de Betaalvereniging met haar leden hiervoor een aparte beveiligde dienst opgezet (Digitaal Incassomachtigen)[3]. Deze wordt door ondernemers tot nu toe nog maar beperkt aangeboden. Vaak wordt nog onvoldoende beseft dat veiligheid ons allen aangaat en we die echt samen (moeten) organiseren vanuit ieders eigen verantwoordelijkheid.

Intensieve informatie-uitwisseling

Banken investeren continu in de veiligheid van het elektronische betalingsverkeer door het verbeteren van fraude- en detectie-maatregelen. Samenwerking tussen betrokken partijen op het gebied van fraudepreventie speelt hierbij een zeer belangrijke rol. Door een gezamenlijke intensieve informatie-uitwisseling over dreigingen, kwetsbaarheden en incidenten kunnen financiële instellingen vooraf adequate maatregelen treffen. Deze samenwerking verloopt via de Betaal-vereniging en via publiek-private samen-werking, zoals met het Nationaal Cyber Security Centrum (NCSC). Met deze in Nederland gekozen vorm van samenwerking loopt ons land voorop in Europa. Onder invloed hiervan en ook door de toegenomen bewust-wording bij het publiek van fraudepreventie is de schade door fraude in het betalingsverkeer teruggelopen van 82 miljoen euro in 2012 naar minder dan 18 miljoen in 2015. De schade door phishing liep in dezelfde periode terug van ruim 10 miljoen naar 3 miljoen euro[4]. In 2016 is de fraude verder afgenomen (cijfers komen binnenkort beschikbaar).

Beveiliging van data

In de maatschappij worden steeds meer gege-vens digitaal opgeslagen en uitgewisseld. Hieraan kleven risico's. Voor een verdere digitali-sering is een adequate beveiliging van data dan ook van cruciaal belang. Banken wisselen geen gegevens met derden uit. Zo bestaat het online-betaalsysteem iDEAL -uniek in Europa- inmiddels al meer dan tien jaar en is de veiligheid van dit betaalproduct niet in het geding geweest. Dit mede doordat de daarvoor benodigde persoon-lijke gegevens binnen de veilige bankomgeving blijven[5]. Gebaseerd op deze ervaringen hebben banken, mede vanuit hun maatschappelijke rol, besloten een digitale identificatie- en inlogdienst op te zetten. Eind 2016 is deze dienst, iDIN, op de markt geïntroduceerd. Met iDIN kunnen parti-culiere rekeninghouders zich online identificeren en inloggen bij aangesloten organisaties (accep-tanten) met de vertrouwde inlogmiddelen van hun bank[6]. Het aanmaken en onthouden van verschillende toegangscodes voor websites gaat hierdoor tot het verleden behoren. Dat brengt niet alleen meer veiligheid, maar bespaart ook vaak veel ergernis voor gebruikers. Acceptanten krijgen met iDIN zekerheid over hun online klan-ten omdat banken hun klanten zorgvuldig hebben geïdentificeerd.

Principle based toetsingskader

Ook de overheid kan met iDIN een versnelling in de gewenste veilige digitalisering van haar dienstverlening tot stand brengen. Het kabinet heeft in dit kader besloten tot een multi-middelenaanpak, waarbij naast publieke ook private inlogmiddelen in het overheidsdomein gebruikt kunnen worden. Daartoe heeft het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties inmiddels een uniforme set van eisen gepubliceerd en de voorgenomen Wet Generieke Digitale Infrastructuur ter consultatie aangeboden. Helaas heeft het ministerie in plaats van een toetsingskader gebaseerd op relevante principiële uitgangspunten (principle based) gekozen voor een set uiterst gedetailleerde regels inclusief technische specificaties (rule based), die in de markt niet gangbaar zijn en waarmee tot nu toe ook geen ervaring is opgedaan. Een dergelijke aanpak bevreemdt niet alleen in internationaal perspectief en vergeleken met andere sectoren zoals het betalingsverkeer. Een dergelijke gedetailleerde uitwerking remt ook innovatie door het veel te strakke kader. De werkbaarheid hiervan zal in de praktijk bij private partijen tot problemen leiden en de beoogde versnelling van de digitalisering van de overheidsdienstverlening zal vertragen of niet tot stand komen.
De overheid zou er verstandig aan doen deze aanpak en de voorzienbare gevolgen ervan nog eens goed te overdenken en te kiezen voor een meer 'principle based' benadering met voldoende ruimte voor eigen invulling en techniek door private partijen. Overheid, zorg voor werkbare wetten en regels en betrek marktpartijen daarbij. Dat komt de veiligheid en privacy ten goede.

Partnerschap

De Betaalvereniging en de banken werken al vele jaren in partnerschap met de overheid samen, bijvoorbeeld met het NCSC. Dat gebeurt onder meer in de FI-ISAC (Financial Institutes-Information and Sharing Analysis Centre). Kern hiervan is dat cyberdreigingen en incidenten tussen de deelnemende partijen snel en succesvol worden gedeeld en de sector weerbaar blijft. Voorts is er sinds enkele jaren een speciale banken-liason die op dagelijkse basis de contacten tussen de financiële sector en het NCSC onderhoudt. Dit brengt veel voordelen met zich mee en leidt er onder meer toe dat gezamenlijke projecten, die ertoe doen, worden opgezet, zoals deelname van de banken aan het Nationaal Detectie Netwerk en het Nationaal Response Netwerk. Deze werkzaamheden zijn van grote waarde voor een veilige financiële sector. Het advies aan de overheid op dit punt is dan ook hieraan de komende jaren voldoende prioriteit te blijven geven.

Noten:

1. Butter, Frank den en Mallekoote, Piet (2016) Vertrouwen in het betalingsverkeer: de rol van transactiekosten. Econo-misch Statistische Berichten nr 4740, 11 augustus 2016.
2. DNB (2012) Kosten Nederlands betalingsverkeer behoren tot de laagste in de EU. DNB persbericht 20 december 2012.
3. www.incassomachtigen.nl
4. Betaalvereniging, Jaarverslag 2015, ww.betaalvereniging.nl
5. www.ideal.nl
6. www.idin.nl
7. Brief minister BZK aan Tweede Kamer, 21 december 2016

Cybercrime en gedigitaliseerde criminaliteit maken een steeds groter onderdeel uit van het werk van het Openbaar Ministerie (OM). Wij denken dat over vijf jaar ongeveer 50% van de criminaliteit een digitale component heeft. Het strafrecht wordt hierbij – uiteraard op basis van rechtstatelijke uitgangspunten – ingezet als 'optimum remedium': een instrument dat in verbinding staat met andere vormen van handhaving en toezicht. Strafrecht kan alleen effectief zijn in een keten waarbij burgers, bedrijven en overheid samenwerken aan preventie, bewustwording en bereidheid om over de volle breedte te investeren in cybersecurity.

Gerrit van der Burg
lid van het College van procureurs-generaal

STREEF KETENSAMENWERKING NA

CYBERSECURITY MOET VANZELFSPREKEND ZIJN

Foto: Frank Groeliken

Begin dit jaar legde het gerechtshof Den Haag in hoger beroep forse celstraffen op aan twee mannen: respectievelijk 4,5 jaar en 45 maanden. De feiten waarvoor ze veroordeeld werden? Computercriminaliteit, voornamelijk het vervaardigen en inzetten van zogenaamde *webinjects*: malware om bankrekeningen digitaal te plunderen. In deze zaak komt goed naar voren dat rechters de ernst van cybercriminaliteit inzien. Het gaat niet om een eenzame criminele hacker op een zolderkamertje die een misstap begaat. Het gaat om feiten waardoor reëel gevaar ontstaat voor ontwrichting van het online betalingsverkeer. De daders kochten op internet kant-en-klare software en lieten die geheel naar wens aanpassen. *Cybercrime-as-a-service*, een trend die we tegenwoordig vaker zien. In deze zaak werd samengewerkt met partijen in het ECTF, het samenwerkingsconvenant van politie, OM en financiële instellingen. Het illustreert de noodzaak om bij de bestrijding van dit soort cybercriminaliteit een ketensamenwerking na te streven.

Nieuwe scheurtjes in firewall

De hack van de democratische partij in de Verenigde Staten heeft geleid tot hernieuwde aandacht voor de beveiliging van data en systemen. Deze aandacht is in mijn ogen gerechtvaardigd. We zien dat criminelen continu inspelen op en gebruik maken van de laatste technologische ontwikkelingen. *Phishing* wordt steeds professioneler, *ransomware* maakt steeds meer slachtoffers onder burgers en het midden- en kleinbedrijf wordt steeds vaker gedupeerd door *Remote Access Trojans* (RAT). *Advanced persistent threats* zijn een gevaar voor bedrijven en vitale infrastructuur. Maar ook nieuwe vormen van cybercriminaliteit dienen zich aan. Steeds meer apparaten worden halve computers met een eigen verbinding met internet. Onze wekker praat straks met onze auto, zodat die in de winter al wordt voorverwarmd. Onze koelkast met de automatische bezorgservice van de supermarkt. Met elke slim apparaat als onderdeel van 'the internet of things', creëren we een scheurtje in onze 'firewall'. Want elke interactie met de buitenwereld biedt kansen voor hackers om het systeem binnen te komen en levert nieuwe uitdagingen op voor de opsporing.

Cybercrime-as-a-service

Een andere ontwikkeling die wij zien is dat het zonder diepgaande technische kennis steeds eenvoudiger wordt om cybercrime te plegen. Je kunt je malware in pakketjes kopen voor 50 tot 150 dollar en daarmee vrij eenvoudig bedrijven en burgers aanvallen. Aanbieders van DDoS-aanvallen adverteren op YouTube. Een paar muisklikken en het is geregeld. *Ransomware* is al voor 100 dollar op het Darkweb te koop. En op Youtube staan honderden instructiefilmpjes hoe je moet hacken en hoe je jezelf daarbij kunt afschermen voor de politie. Het hoeft geen betoog dat deze dienstverlening een toename van risicovolle cybercriminaliteit tot gevolg heeft.

Toenemend belang cybersecurity

Tegenover de toenemende laagdrempeligheid door 'cybercrime-as-a-service', wil ik graag het toenemende belang van cybersecurity zetten. We vinden het normaal dat kinderen leren zwemmen en de verkeersregels leren. Maar het aanleren van cybersecurity staat nog in de kinderschoenen. Toen in 1959 in auto's de driepuntsgordel op de markt kwam, werd dat met scepsis ontvangen. Een auto is immers een voorbeeld van vrijheid, daarin laat je je toch zeker niet vrijwillig vastmaken? Inmiddels staat het dragen van een gordel in een auto niet meer ter discussie. Zo zou het naar mijn mening ook met cybersecurity moeten zijn. Het moet niet gek voelen, maar als een vanzelfsprekendheid. Als je online gaat, doe je automatisch je digitale gordel om.

Zorgplichten

Het automatisme om je zelf of je organisatie van goede cybersecurity te voorzien, hiervoor moeite en investeringen te doen, is een situatie waarnaar wij met zijn allen moeten streven. Het rapport van mevrouw Verhagen spreekt in dit kader van 'zorgplichten'. Burgers, bedrijven en overheid hebben een eigen verantwoordelijkheid, zowel ten opzichte van andere bedrijven als ten opzichte van consumenten. Immers, de almaar toenemende digitalisering zorgt ervoor dat gebrekkige cybersecurity grote gevolgen kan hebben. Een gebrek in de beveiliging kan er bijvoorbeeld toe leiden dat bedrijfsgeheimen en persoonsgegevens door een hack of menselijke fout op straat komen te liggen, of als gevolg hebben dat de *business continuity* van een bedrijf in gevaar komt. Zorgplichten gaan wat mij betreft ook over het aanspreken van bedrijven die apparaten maken die verbonden zijn met het internet. Veilige software en regelmatige updates kunnen het risico van cybercrime doen afnemen.
Dat gebrekkige cyberbeveiliging in deze tijd – terecht – onder een vergrootglas ligt, is te zien aan de recente politieke en media-aandacht voor gebrekkige beveiliging van overheidssystemen. Steeds meer raken we ervan bewust dat ontoereikende cybersecurity het vertrouwen in het functioneren van de overheid kan beschadigen. Overheidsinstellingen zouden het goede voorbeeld moeten geven als het om zorgplichten gaat. Dit vraagt evenwel om aanzienlijke investeringen.

Wettelijke bevoegdheden

Criminelen maken steeds meer gebruik van digitale (versleutelings)technieken, diensten en tools om zich af te schermen van justitie en om de opsporing te bemoeilijken. Wil de opsporing in staat worden gesteld om gelijke tred te houden met moderne cybercriminelen, dan zijn ook andere randvoorwaarden noodzakelijk, zoals adequate wettelijke bevoegdheden.
Het is voor het OM en de politie dan ook heel belangrijk dat de wet Computercriminaliteit III wordt aangenomen om de opsporing en vervolging van cybercriminelen te versterken. De wet, in de volksmond – overigens onterecht – de 'hackwet' genoemd, geeft opsporingsambtenaren bevoegdheden om ernstige strafbare feiten op te sporen door communicatie van verdachten te onderscheppen, voordat deze versleuteld is. Het gebruik van encryptie en afschermingstechnieken – voor weinig geld makkelijk te verkrijgen – bemoeilijkt immers niet alleen de aanpak van cybercrime, maar ook van liquidaties, terrorisme, kinderporno, outlaw motorcycle gangs en drugscriminaliteit.
Ransomware kan 'geplaatst' worden door uw buurman, maar net zo gemakkelijk door iemand aan de andere kant van de wereld. Cybercrime is internationaal; kent eigenlijk geen vaste plaats en tijd. Investeren in harmonisatie van

"Cybercrime is internationaal; Investeren in harmonisatie van internationale wet- en regelgeving is daarom van belang."

Foto: Felix Riemersma - Nationale Beeldbank

We vinden het normaal dat kinderen leren zwemmen en de verkeersregels leren. Maar het aanleren van cybersecurity staat nog in de kinderschoenen.

internationale wet- en regelgeving is daarom van belang.
Onbereikbare daders uit het buitenland, encryptie en de technische complexiteit maken dat het OM, samen met partners, ook inzet op het versterken van de informatiepositie, opbouw van kennis en expertise en alternatieve interventies. Door preventieve of verstorende maatregelen te nemen richting cybercriminelen, digitale infrastructuur of *facilitators*, kan cybercriminaliteit worden tegengegaan en schade worden voorkomen.

Strafrecht als optimum remedium

Het rapport van mevrouw Verhagen adviseert de publiek-private samenwerking op het gebied van cybersecurity te versterken. Verhagen wijst daarbij op het belang van onderwijs, het benadrukken van zorgplichten en het stimuleren van bewustwording. Het OM streeft met zijn (internationale) partners naar een situatie waarin de samenleving kan vertrouwen op de veiligheid van het digitale domein, waarbij Nederland onaantrekkelijk is voor cyber-criminelen, omdat zichtbaar en effectief wordt opgetreden tegen cybercrime en gedigitaliseerde criminaliteit. Cybercrime bestrijden is niet alleen een taak van het OM en politie. Cybersecurity moet een prioriteit zijn van de burger, van bedrijven en van de overheid. De *core business* van het OM is natuurlijk het strafrecht, maar ik zie het strafrecht binnen het zich snel ontwikkelende speelveld van cybercrime en cybersecurity als 'optimum remedium'. Oftewel: opsporing en vervolging moeten in verbinding staan met andere vormen van handhaving en toezicht. De inzet van het strafrecht dient – altijd op basis van rechtstatelijke uitgangspunten – een bijdrage te leveren aan de versterking van de veiligheid en veerkracht van de digitale samenleving. Hiervoor is samenwerking, bewustwording, urgentie en investering in de gehele keten noodzakelijk. Nationaal en Internationaal.

The UK Government has set out its ambition and goals with regards to cyber security in the National Security Strategy (November 2015) and the National Cyber Security Strategy (NCSS) (November 2016). Our vision, as set out in the NCSS is that: the UK is secure and resilient to cyber threats, prosperous and confident in the digital world.

Nicholas J. Alexander
Cyber and Government Security Directorate
(author of the National Cyber Security Strategy 2016-2021)
Cabinet Office, UK

CYBER AS A TOP TIER ONE RISK TO UK INTERESTS

POLITICAL DIALOGUE AND UNDERSTANDING BETWEEN GOVERNMENTS IS KEY

This ambition reflects our determination to ensure we make the most of the opportunities that digitalisation affords our society and economy while ensuring that we do our utmost to manage and mitigate the associated risks and threats. The NCSS 2016-2021 is the second national strategy and is supported by £1.9 billion of transformational investment over five years. This investment contributes towards a range of measures including the establishment of the National Cyber Security Centre.

Vision

To realise the vision set out above we will work to achieve the following objectives:

- *Defend*
  We have the means to defend the UK against evolving cyber threats, to respond effectively to incidents, to ensure UK networks, data and systems are protected and resilient. Citizens, businesses and the public sector have the knowledge and ability to defend themselves.
- *Deter*
  The UK will be a hard target for all forms of aggression in cyberspace. We detect, understand, investigate and disrupt hostile action taken against us, pursuing and prosecuting offenders. We have the means to take offensive action in cyberspace, should we choose to do so.
- *Develop*
  We have an innovative, growing cyber security industry, underpinned by world-leading scientific research and development. We have a self-sustaining pipeline of talent providing the skills to meet our national needs across the public and private sectors. Our cutting-edge analysis and expertise will enable the UK to meet and overcome future threats and challenges.

Foto: Marco Govel - Hollandse Hoogte

The UK National Cyber Security Strategy 2016-2021 is the second national strategy and is supported by £1.9 billion of transformational investment over five years.

Investing in partnerships
Underpinning these objectives, we will pursue international action and exert our influence by investing in partnerships that shape the global evolution of cyberspace in a manner that advances our wider economic and security interests. By its very nature cyberspace is without borders. The UK is committed to working with all states to develop a common understanding in the benefits of a free, open, peaceful and secure cyberspace. This will involve building confidence and trust with all nations, maximising the mutual advantages that cyberspace has to offer while also enhancing our collective security online.

One of the key aspects of the strategy is the important role we identify for government. Good cyber security will always depend on cooperation between the citizen, industry and the state. But we believe that there is a particular and leading role for the Government to play. As we set out in the NCSS: 'The Government must set the pace in meeting the country's national cyber security needs. Only Government can draw on the intelligence and other assets required to defend the country from the most sophisticated threats. Only Government can drive cooperation across the public and private sectors and ensure information is shared between the two. Government has a leading role, in consultation with industry, in defining what good cyber security looks like and ensuring it is implemented'. But government cannot do this alone: everyone has role to play.

Risk to UK interests
The UK's 2015 National Security Strategy, reaffirmed cyber as a top tier one risk to UK interests – highlighting cyber threats as one of the key challenges to drive the UK security priorities for the coming decade. The scale and scope of the threat continues to evolve. The UK Government therefore drew up the Strategy and the Programme that 'will ensure that we have in place all the necessary components to defend the UK from cyber-attack. These include capabilities that allow us to understand and tackle the most advanced threats, law enforcement capabilities to deal with cyber crime, support for businesses particularly in the UK's CNI, and the skills and innovation needed for the long term'.
All governments make decisions on spending according to the priorities they set themselves. The UK Government, recognising the risk associated with cyber, decided it was appropriate to set aside a dedicated amount for trans-formational investment to increase our capacity across the public and private sector.

Criminal exploit
Digitalisation will continue to shape our economy and our society as new technologies come on stream or evolve. Unfortunately, the ingenuity of those who seek to exploit those technological developments for criminal purposes is likely to evolve just as rapidly. Exploitation of the Internet of Things has been such a technological evolution that some have sought to exploit for criminal ends. That said, there are also many governments, companies and gifted individuals who are working hard to protect us from those threats and thwart the criminals. While there will always be those who use the internet for criminal purposes, we can and will have the means to protect ourselves and bring those criminals to justice.

Opportunities
The greatest opportunities arise from the cooperation of governments and industry to afford greater protection to the citizen so that we can all go about our business online in safety and security. Some very clever minds are already doing some great work in this space, in a manner which could eventually change the balance of risk in favour of the individual, law-abiding citizen and against the criminal. Cooperation between governments remains an important opportunity. Better sharing of information and technical understanding between national Computer Security Incident Response Teams (CSIRTs) is one way. Political dialogue and understanding between governments is also key, and we look forward to the meeting of the Global Conference on Cyberspace in India later this year to further this goal – the latest iteration in the process launched by the UK in 2011 and last held in The Hague in 2015. Raising global standards of cyber security through targeted capacity building work is another opportunity we will continue to pursue this year. The Global Forum on Cyber Expertise launched by the Dutch in 2015 provides an important platform for coordinating these efforts and I commend the leadership demonstrated by the Government of the Netherlands in this regard.

Tackle the threat
I know from personal experience, from having spent four years living in The Hague that the Netherlands is amongst the most advanced digital nations, with a robust National Cyber Security Strategy and structure of its own. In preparing for an eventual third Dutch NCSS, it will be worth considering where government and private sector skills and resources could be even better joined up to tackle the threat to the country's core interests.

Digital Golden Age
From my reading of the summary of the Verhagen report, there appear to be many features or issues raised which coincide with the UK and other similar national strategies. Advanced societies and economies like our own all share many of the same fundamental challenges in the field of cyber security – how to best protect ourselves while preserving and protecting individual rights and without stifling the innovation that is key to our digital futures. As noted above, one of the keys to success lie in a fruitful and cooperative relationship between the public and private sectors – something which I note features strongly in the report. The Netherlands, like the UK, is in many ways a digital leader, a major hub and centre of innovation, and an influential voice on cyber security. Maintaining and reinforcing cyber security will safeguard our future digital prosperity. Just as the Netherlands revolutionized global trade in the Golden Age, so I am confident that the Netherlands, by working closely with its oldest allies in the UK, will continue to set the pace of this Digital Golden Age.

"Good cyber security will always depend on cooperation"

Foto: Hollandse Hoogte

Political dialogue and understanding between governments is also key.

Colofon
Opdrachtgever: Cyber Security Raad Nederland
Hoofdredactie: Elly van den Heuvel (secretaris) • **Concept en (eind)redactie:** Martin Bobeldijk (Turnaround Communicatie)
Met dank aan: Andrea Bakker, Martine Spaans en Siep van Sommeren
Fotografie: Arenda Oomen, Adriaan van Zijp, Nationale Beeldbank en Hollandse Hoogte • **Illustraties:** Jasper Rietman
Opmaak en redactie: BKB • **Drukwerk:** Xerox/OBT

Maart, 2017

CSR
Cyber
Security
Raad