01

TRENDS IN DIGITALE VEILIGHEID: IN GESPREK MET HANS DE VRIES, DIRECTEUR NCSC

Wat zijn de belangrijkste trends en ontwikkelingen om onze samenleving digitaal veilig te houden?

Trends in veiligheid kan tegenwoordig niet meer zonder de specifieke blik op trends in digitale veiligheid. In 2021 nam Hans de Vries, Directeur van het Nationaal Cybersecurity Centrum deel in de paneldiscussie tijdens de webcast Trends in Veiligheid 2021[1]. In een levendige discussie gaf hij aan dat er in het rapport meer aandacht mocht zijn voor de trends in digitale veiligheid.

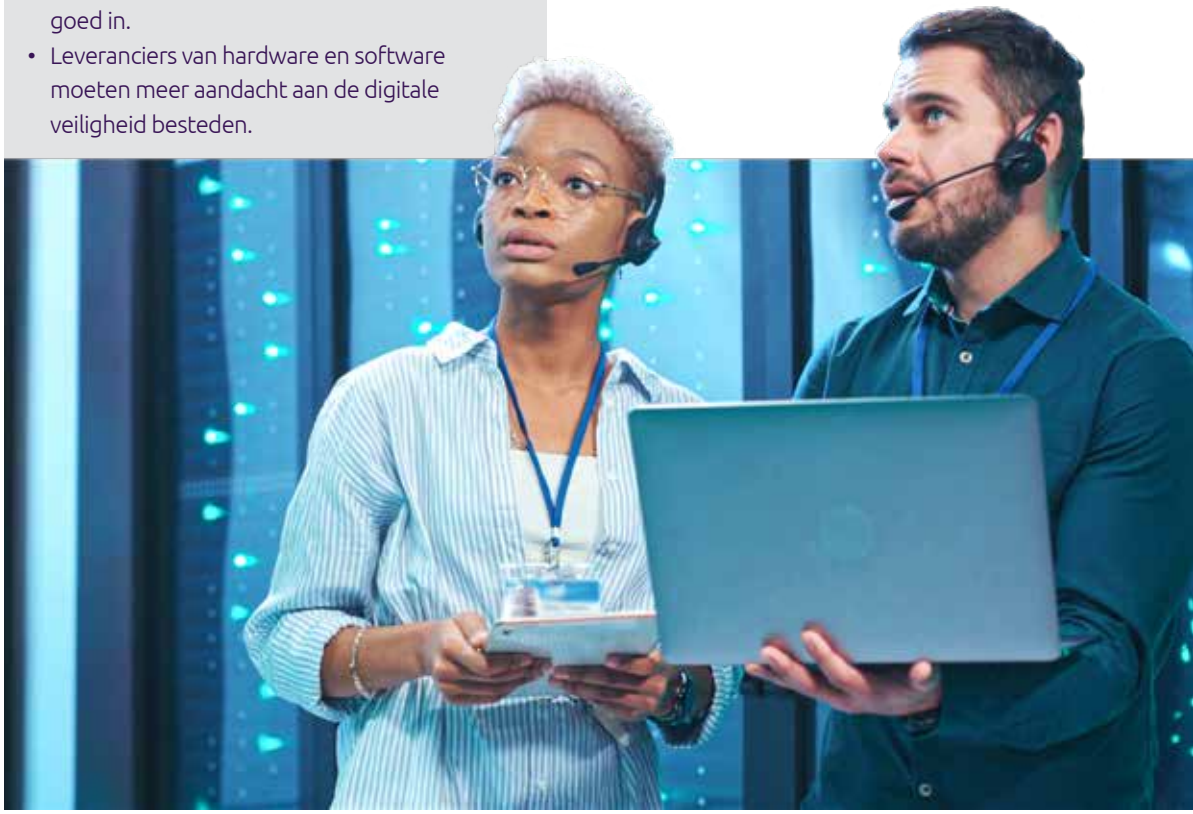
Highlights

- We werken steeds meer digitaal en gedistribueerd en de digitale veiligheid blijft achter.
- Om veiliger te worden is een stelsel met duidelijke rolverdeling tussen publiek, privaat en overheid cruciaal, het mandaat voor het NCSC moet breder.
- Voor het ontvangen van relevante informatie vanuit de overheid moet het niet uitmaken of je 'vitaal' bent of niet.
- Onze rol als digitaal knooppunt in Europa is niet alleen technisch we hebben de taak om partijen met elkaar te verbinden, daar zijn we goed in.
- Leveranciers van hardware en software moeten meer aandacht aan de digitale veiligheid besteden.

Die handschoen pakken wij natuurlijk graag op in het rapport van 2022. In gesprek met Hans bespreken wij de laatste trends die hij ziet om de Nederlandse samenleving digitaal veilig te maken. Nu de meeste coronamaatregelen zijn vervallen en aan de oostgrens van Europa veel aan de hand, is dit onderwerp urgenter dan ooit tevoren.

Digitalisering en veiligheid

Afgelopen twee jaar is onze samenleving sneller gedigitaliseerd dan de vijf jaar hiervoor. In het huidige regeerakkoord is een volledige paragraaf gewijd aan 'digitalisering'. Erkend wordt dat "de huidige digitale revolutie geweldige kansen biedt voor onze samenleving en economie", maar tegelijkertijd zorgt "voor een digitale kloof en groeiende ongelijkheid in onze samenleving". Welke digitale trend was afgelopen jaar dominant voor de digitale veiligheid in Nederland? Hans: "Wat mij betreft is de dominante trend in 2021 dat door de coronacrisis gedistribueerd werken in hoog tempo is doorontwikkeld en dat digitale veiligheid hierbij achterblijft en aandacht behoeft."



Afgelopen twee jaar is onze samenleving sneller gedigitaliseerd dan de vijf jaar hiervoor. In het huidige regeerakkoord is een volledige paragraaf gewijd aan ‘digitalisering’. Erkend wordt dat “de huidige digitale revolutie geweldige kansen biedt voor onze samenleving en economie”

Waaruit blijkt dat de digitale veiligheid achterblijft bij de snelheid van digitalisering? “Dit komt onder andere tot uitdrukking in de vragen die wij van CISO’s krijgen. Zij vragen hulp om cybersecurity op de agenda van de bestuurder te zetten. Het wordt beter maar we moeten blijven benadrukken dat digitale veiligheid ‘chefsache’ is. **Cyber is veel meer dan techniek alleen.** Er wordt nog te weinig aan risicomanagement gedaan door organisaties. Te vaak zien we dat organisaties niet nadenken over de keten waarin ze zich bevinden of het wordt pas gedaan als het te laat is. Ook zijn er voldoende voorbeelden dat het updaten van software met de laatste versie (‘patch gedrag’) niet past bij de afhankelijkheid en kwetsbaarheid van digitale systemen.”

Van welk cybersecurity incident heb je afgelopen jaar het meest ‘wakker gelegen’? Hans: “Dat is de problematiek rondom kwetsbaarheden zoals in Log4j, een door IT-ontwikkelaars veelgebruikt softwareproduct. Dit product wordt gebruikt voor het vastleggen van input van buitenaf in software op een server. Bijvoorbeeld een inlogpoging. Maar dit soort software zit in vele honderden, zo niet duizenden softwareproducten en applicaties. De vergelijking met suiker wordt vaak gemaakt: bijna in ieder levensmiddel zit wel suiker, ook waar je het misschien niet verwacht. Daarom is het moeilijk om zicht te hebben op de omvang van misbruik en kan impact reusachtig zijn.“

Hoe ontwikkelt de digitale veiligheid zich in Nederland?

Hans: “Zoals gezegd, als gevolg van COVID-19 is de digitalisering van de maatschappij versneld. Dat betekent dat nog meer dan voor de pandemie een zwaar beroep wordt gedaan op de digitale ruimte. Digitalisering biedt onze maatschappij volop kansen en oplossingen, maar zorgt ook voor een groter aanvalsoppervlak waarin criminelen en statelijke actoren snel kunnen inspelen op het uitbuiten van nieuwe kwetsbaarheden.”
Wat betekent dit voor de digitale risico’s? “De digitale risico’s zijn onverminderd groot: denk daarbij aan spionage en sabotage door andere landen maar ook ransomware aanvallen door criminelen. Dit kan maatschappelijk ontwrichtende gevolgen hebben. De digitale dreiging blijft zich ontwikkelen, de impact van cyberaanvallen neemt toe en de weerbaarheid is nog onvoldoende.”

Hoe gaat het bedrijfsleven en onze vitale infrastructuur hiermee om?

“Er zijn er grote verschillen in weerbaarheid tussen bedrijven die kunnen investeren in kennis en kunde op het gebied van cybersecurity en (veelal kleine) bedrijven die niet de middelen hebben om de weerbaarheid naar een hoger plan te tillen. In het bedrijfsleven is cybersecurity nog steeds onvoldoende onderdeel van volwassen risicomanagement en daardoor blijven investeringen uit die dat risico reflecteren. Toch is er goed nieuws: tijdens Log4j zag je dat organisaties, ook buiten de ICT-afdeling, meteen op scherp stonden en hebben gehandeld. Een inhaalslag is nodig om Nederland weerbaarder te maken. Het is tijd om naast de fysieke infrastructuur (weg, spoor, water en lucht) ook de digitale infrastructuur waar Nederland van afhankelijk is op orde te brengen.”

Vanuit de overheid zetten we nu volop in op een ‘landelijke dekkend stelsel’ om potentiële slachtoffers van cyberaanvallen tijdig te informeren, maar tegelijkertijd merken we dat we daar nog niet zijn en het landschap nog te versplinterd is. Goede nationale coördinatie is echt nodig in cybersecurity en daarbij moet het NCSC de spilfunctie in het midden vervullen.

Structurele samenwerking

In het huidige regeerakkoord wordt gepleit om het bedrijfsleven beter te beschermen en beter informatie te delen, door middel van een structureel samenwerkingsverband en een meerjarige cybersecurity-aanpak.
Hoe ziet deze meerjarige cybersecurity aanpak er idealiter voor jou uit?
“We moeten als Nederland voldoende slagkracht organiseren om de toenemende dreiging het hoofd te kunnen bieden. Dat betekent: de vrijblijvendheid is voorbij en geen versplintering in de aanpak, maar juist samenhang. Belangrijk daarbij is samenwerking tussen publiek en privaat binnen overheid, een stelsel met duidelijke rolverdeling en groter mandaat voor NCSC (dus niet alleen meer overheidsorganisaties en Vitale infrastructuur, maar een bredere doelgroep).”

Ook volgens de Cyber Security Raad (CSR) moet Nederland de krachten bundelen om te komen tot een integrale aanpak van onze cyberweerbaarheid en werken aan één cyberweerbaarheidsstrategie met een meerjarenprogramma en dekkende financiering. Zij pleiten voor een bijbehorende investering van € 833 miljoen. Besteedt Nederland voldoende aan digitale veiligheid? Is er een verbetering zichtbaar in de budgetten voor het veiliger maken van onze huidige digitale wereld?
Hans: “Het wordt beter, maar we hebben nog wel echt een weg te gaan. Het is fijn dat er meer middelen beschikbaar komen naar aanleiding van het coalitieakkoord. Dat is enorm nodig. Het is misschien niet de € 833 miljoen waar de CSR om vroeg maar met het geld dat er wel extra komt voor cybersecurity kunnen we ook al belangrijke dingen gaan doen, ook bij het NCSC. Ten behoeve van ons allemaal.“

Stap voor stap beter in digitale veiligheid

In het OVV Rapport ‘Kwetsbaar door software’ stelt haar voorzitter Jeroen Dijselbloem: “Aanpak digitale veiligheid moet anders”: De Nederlandse aanpak van digitale veiligheid moet snel en fundamenteel veranderen om te voorkomen dat de maatschappij ontwricht raakt door cyberaanvallen. Uit de casus ten aanzien van de kwetsbaarheden in software van Citrix concludeert de OVV dat Nederlandse overheidsorganisaties en bedrijven zeer kwetsbaar zijn voor cyberaanvallen en dat er geen nationale structuur is waarbinnen alle potentiële slachtoffers van cyberaanvallen tijdig worden gewaarschuwd.” Wat kan er aan de waarschuwing verbeteren en hoe kan publiek-private samenwerking hieraan bijdragen?
Hans: “Waar ik heel blij mee ben, is de al bestaande samenwerking tussen publiek, privaat, wetenschap en non-profit. Denk aan bijvoorbeeld onze samenwerking met Cyberveilig Nederland of DIVD, partijen die hun eigen verantwoordelijkheid willen nemen als het gaat over onze digitale veiligheid. Zij weten ons te vinden en te informeren en vice versa. Ik ben trots op deze publiek-private samenwerking in Nederland. Dit is iets wat je in andere landen echt met veel meer moeite van de grond ziet komen. Maar ook in Nederland kan het intenser.“

Welke andere acties worden genomen?

“Vanuit de overheid zetten we nu volop in op een ‘landelijke dekkend stelsel’ om potentiële slachtoffers van cyberaanvallen tijdig te informeren, maar tegelijkertijd merken we dat we daar nog niet zijn en het landschap nog te versplinterd is. Goede nationale coördinatie is echt nodig in cybersecurity en daarbij moet het NCSC de spilfunctie in het midden vervullen. Het NCSC zou daarbij meer mandaat moeten hebben om organisaties te waarschuwen als dat nodig is. Een eerste stap is daarvoor het wetsvoorstel dat binnenkort in het parlement behandeld wordt waarmee de mogelijkheden voor het NCSC om informatie te delen worden vergroot. Als het voorstel uiteindelijk wetgeving wordt, zal het NCSC meer dreigingsinformatie kunnen delen met organisaties die niet onder de ‘vitale infrastructuur’ worden geschaard. Daarnaast is ook een wetsvoorstel ingediend dat het Digital Trust Center voorziet van een wettelijke grondslag om dreigingsinformatie, inclusief persoonsgegevens, te gaan delen met het niet-vitale bedrijfsleven. Voor het ontvangen van informatie vanuit de overheid die voor jouw organisatie van belang is, moet het mijns inziens niet uitmaken of je ‘vitaal’ bent of niet.“

Op welke wijze gaat de overheid organiseren dat overheden, bedrijfsleven, ‘vitaal’ en ‘niet-vitaal’ digitale veiligheid beter op orde hebben?

“Er zijn natuurlijk al allerlei normen zoals BIO, NEN 7510, et cetera en bestaande wetten zoals WBNI en de AVG. Een grote verandering is wel aanstaande met de vernieuwde Europese NIS2-richtlijn. De huidige wetgeving is voornamelijk georiënteerd op vitale, of essentiële, sectoren en organisaties, maar daar gaat dus verandering in komen. Als de verbreding van de NIS2 doorgaat en organisaties van zowel de categorie ‘essential’ als ‘important’ moeten voldoen dan is deze scope veelvoudig van wat het nu is. Al deze partijen gaan te maken krijgen met een verzwaard toezicht op het naleven van cybersecurity eisen en standaarden. Ik zeg wel vaker dat we de vrijblijvendheid voorbij moeten en deze Europese wetgeving biedt daar een goede basis voor. We moeten ook meer de durf hebben om te zeggen: hier moet je je echt aan houden. We moeten de druk op opvoeren om de weerbaarheid bij zowel publiek als privaat naar een nieuw niveau te tillen.”

Nederland is een Europees digitaal knooppunt

Nederland is ambitieus. Alle delen van het land moeten robuust, veilig en supersnel internet krijgen om het digitale knooppunt van Europa te worden. Onze regering wil het voortouw nemen en zet op Europees verband in op ‘versterking van de samenwerking tussen lidstaten op het gebied van digitalisering, onder meer op mensgerichte inzet van kunstmatige intelligentie, digitale ethiek, ontwikkeling van digitale identiteit en cybersecurity en ‘open source’.’ Wat moet er nog gebeuren om een veilig digitaal knooppunt van Europa te worden?

Hans: "Met AMS-IX heeft Nederland letterlijk een belangrijk internetknooppunt van Europa binnen haar grenzen. Hier moeten we er dus zorg voor dragen dat er niet alleen sprake is van snel, maar ook vooral van veilig internet. Ik zou onze NCSC-rol als digitaal knooppunt wel veel breder willen trekken. Dit gaat onder andere om de taak die we hebben om partijen met elkaar te verbinden, iets waar we in Nederland goed in zijn en dus ook in Europa het voortouw in kunnen nemen. Er ligt een evidente meerwaarde in Europese samenwerking, we zijn immers

met elkaar verbonden. Tegelijkertijd is betere en strakke coördinatie op Europees niveau in tijden van crisis nodig en ook dat is iets waar wij aan kunnen bijdragen. We laten vaak genoeg zien dat we als Nederlanders weten hoe we samenwerkingsverbanden kunnen optuigen, ook als er zowel publieke en private partijen betrokken zijn. Daarnaast hebben we ook genoeg kennis en expertise in huis die we kunnen inbrengen en ontsluiten, denk bijvoorbeeld aan onze ervaring met ISACs of ons Coordinated Vulnerability Disclosure beleid. Overigens gaat dit allemaal verder dan alleen Europa, het is ook van belang om de mondiale samenwerking op te zoeken en bijvoorbeeld bij te dragen aan capaciteitsopbouw in minder ontwikkelde landen. Ook op dit niveau geldt dat we zo sterk zijn als de zwakste schakel. Ten slotte mag de Nederlandse slagkracht om te kunnen acteren tegen statelijke actoren en criminelen best versterkt worden. Dit is niet voor het NCSC weggelegd, maar de digitale slagkracht om onze nationale belangen te verdedigen mag een belangrijk onderdeel worden van een nieuwe cybersecurity aanpak."

Welke trends in digitale veiligheid mag vooral niet onbenoemd blijven om een goed voorbereid te zijn op de steeds verdergaande digitalisering.

"De belangrijkste overkoepelende trend is dat we door de coronacrisis versneld afhankelijk zijn geworden van de digitale levensader. Het is belangrijk hierbij voldoende aandacht aan de digitale veiligheid te besteden. Ik hoop dus in de eerste plaats dat bij iedereen en misschien wel vooral bij leveranciers (van hardware en software) het besef doordringt dat het gebruik van digitale functies van al onze apparaten onlosmakelijk verbonden is met het zorgdragen voor de veiligheid daarvan. Het is zo een integraal onderdeel van ons 'zijn' geworden dat je daar op die manier naar moet kijken, handelen en durven te acteren. Dit vereist een fundamentele andere kijk. Het gebruik van een 'Software Bill of Material' (beschrijving welke software er in een product zit) is hierin een goede ontwikkeling."

"Andere trends om in de gaten te houden zijn de mogelijke effecten van grondstoffen schaarste en van klimaat/ duurzaamheid maatregelen op de beschikbaarheid en inzet van ict-middelen. De recente ontwikkelingen in Oekraïne laten ook weer zien dat het risico op de inzet van digitale middelen in conflicten met bovenregionale uitstraling reëel is."

Over de auteurs

Roeland de Koning

Director Public Security

Roeland is gespecialiseerd in nationale en internationale ISACs samenwerkingsvraagstukken tussen organisaties die werken aan digitale veiligheid en cybersecurity.

roeland.de.koning@capgemini.com

Fokko Dijksterhuis

Managing Consultant Cybersecurity

Fokko is gespecialiseerd in (internationale) samenwerking en cyber crisismanagement in het digitale veiligheidsdomein. Fokko houdt zich daarnaast bezig met beleidsmatige, organisatorische en gedragsmatige vraagstukken binnen cybersecurity.

fokko.dijksterhuis@capgemini.com

[1]https://www.trendsinveiligheid.nl/live-webcast/