



Dossier: Security tech transfer

- ◆ Wetgeving: last of lust voor tech transfer?
- ◆ COSSAS: Een open-source community voor security tech transfer
- ◆ Hoe kunnen communities en investeerders bijdragen aan succesvolle tech transfer?

PCSI maakt Nederland veiliger door gezamenlijke innovatie in cyber security.

Het Partnership for Cyber Security Innovation (PCSI) is een samenwerking tussen TNO, ABN AMRO, ING, Achmea en de Belastingdienst, gericht op het ontwikkelen van innovatieve, toepasbare security-oplossingen.

In gezamenlijke innovatieprojecten werken experts van alle partners aan concrete resultaten. De PCSI-community, met meer dan 50 Liaison Partners, speelt een grote rol bij het daadwerkelijk toepassen van deze resultaten. Security tech transfer is een belangrijk pad naar deze borging van resultaten.

Meer weten of meedoen?

Kijk op pcsi.nl



Partnership for
Cyber Security
Innovation

Transformeren versus transfereren



Chris de Vries

Mede naar aanleiding van een artikel van Reinder Wolthuis, Ruggero Montalto en Marth Breure getiteld: "Security innovation and tech transfer" (1) heb ik Reinder uitgenodigd om samen een speciale uitgave te realiseren met dat als centraal thema. Dat sprak hem aan, waarna wij een scala aan experts benaderden om daaraan deel te nemen. Samen besloten wij dat - als aanzet - de vorm te geven van een Ronde Tafel bijeenkomst. Dit nummer is het resultaat daarvan en naar mijn mening smaakt dit naar meer. Beste lezer, lid of niet lid zijnde van het Platform voor Informatiebeveiliging, spreekt je dit aan; meld je bij onze redactie en een nieuw speciaal-nummer kan het licht zien.

Wij weten dat onze wereld transformatie ondergaat, niet in de laatste plaats door twijfel aan de integriteit van onze voormalige bondgenoot de Verenigde Staten van Amerika. Wat is eigenlijk transformeren? De twee woorddelen zeggen

alles: 'trans' staat voor: naar de overkant van (hier en nu de Atlantische Oceaan!); 'formare' vertaalt zich tot 'vormen' (mogelijke vertaling: de actie van de machthebbers in de V.S. leidt tot een reactie en verandert onze Europese werkelijkheid). Transfereren bestaat eveneens uit twee woorddelen, t.w.: 'trans' (bekend: over) en 'ferre' (dragen/brengen). Dus hier gaat het om behoud van Intellectueel Eigendom, wetenschappers, onderwijs en kennis. Dat aangevuld met het overbrengen van nieuwe inzichten, innovaties, uitvindingen en steun binnen Europa (een noodzaak), én binnen het bedrijfsleven.

In de artikelen van deze uitgave komt (in)direct dat alles tot uitdrukking. Alle auteurs zijn zich bewust van de noodzaak tot aanpassing, samenwerking en deling van kennis alsook inzichten. Ieder vanuit zijn specialisme en netwerk. Dit geheel aan visie, standpunten en gevoel van urgentie maakt dat iedere lezer zich ervan bewust zal worden dat 'transfer' van technologie van levensbelang is. Maar, ook dat het belangrijk is vast te stellen waar wij als Europa staan en wat wij voor onze volgende generaties moeten doen. Ik zie onze huidige situatie meer nog als een kans, dan enkel als een bedreiging van/voor Europa. Ik ben benieuwd naar jullie reacties.

Chris

(1) Informatiebeveiliging Magazine, jaargang 24, editie 4, 'security innovation and tech transfer', auteurs: R. Wolthuis, R. Montalto en M. Breure, pagina 30 t/m 35

IN DIT NUMMER

- 03 Voorwoord - Transformeren versus transfereren
- 04 Security tech transfer: een introductie
- 07 Column Lex Borger - Innovatie is meer dan techniek
- 08 Hoe kunnen communities en investeerders bijdragen aan succesvolle tech transfer?
- 14 Krachten bundelen om onderzoek en innovatie op post-quantum cryptografie toepasbaar te maken
- 17 Tech transfer: vanuit dienstverlener naar overheid en dan naar de markt?
- 18 Cybersecurity: innovatiekansen in een veranderende wereld met nieuwe uitdagingen
- 21 Column Privacy - Genderen is nergens voor nodig
- 22 COSSAS: een open-source community voor security tech transfer
- 25 Column Nicole van der Meulen - Digitale oplichting: waarom zelfs bewust bekwaam niet immuun maakt
- 26 A tech transfer Success story - Van Dark Web Monitor tot BigPhish: Cyber Tech Transfer Successen Uitdagingen
- 28 Security en Innovatie: geen tegenspraak, maar noodzaak!
- 32 Security tech transfer en Europa?
- 36 Vergeet de "tech" in "tech transfer"
- 38 Wetgeving: last of lust voor tech transfer?



Auteurs: Reinder Wolthuis is Program manager Partnership for Cyber Security Innovation (PCSI) bij TNO. Tevens mede-initiatiefnemer voor deze 'special'. Hij is bereikbaar via reinder.wolthuis@tno.nl Chris de Vries is hoofdredacteur van InformatieBeveiliging Magazine en werkt als Zelfstandig Professional onder de naam De Vries Impuls Management. Hij is bereikbaar via impuls@euronet.nl

Security tech transfer: een introductie

Wat verstaan we onder security tech transfer en welke uitdagingen zijn er?

Innoveren in cybersecurity is essentieel om als maatschappij beschermd te blijven tegen cyberaanvallen, nu en in de toekomst. Innovatie is echter niet genoeg; om een mooie innovatie bruikbaar te maken moet het uiteindelijk landen in een bruikbaar securityproduct of een dienst. De weg van idee naar innovatie naar product of dienst is een complexe weg, met veel verschillende belangen, obstakels en betrokkenen. Deze speciale editie van het PvlB magazine is gewijd aan dit onderwerp, de 'security tech transfer'. In dit inleidende artikel definiëren we het probleem en lichten we toe wat u kunt verwachten in dit magazine.

Van idee naar innovatie naar toepassing

De weg van idee naar toepassing kunnen we toelichten aan de hand van twee zogenaamde 'Readiness Levels'. Deze niveaus zeggen iets over de fase waarin een innovatie zich bevindt:

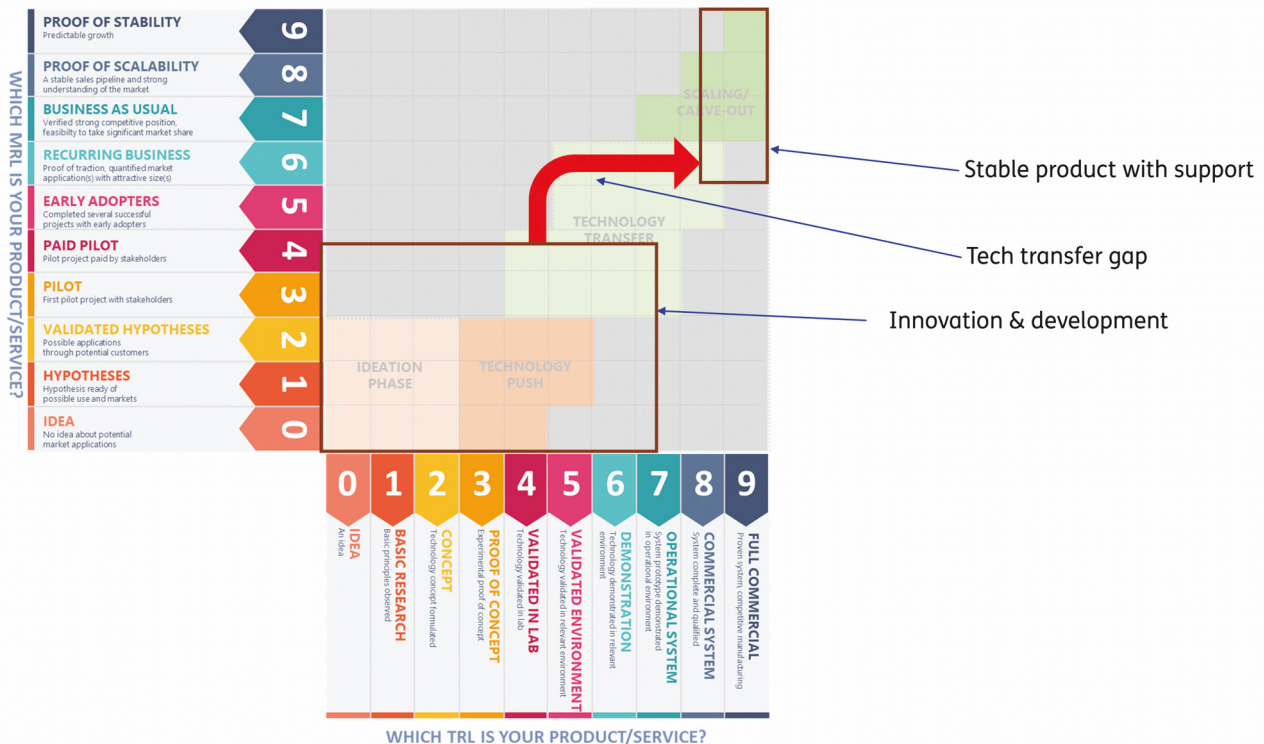
- TRL – Technological Readiness Level is een schaal die aangeeft wat de technologische volwassenheid is van een innovatie. De TRL kent 9 niveaus, die lopen van niveau 0 (alleen maar een idee) naar niveau 9 (een kant-en-klaar verkrijgbaar product of dienst, inclusief ondersteuning). Een product is marktrijp op niveau 8 of 9.
- MRL – Market Readiness Level is een schaal die aangeeft wat de commerciële/marketing volwassenheid is van een innovatie. De MRL kent 9 niveaus, die lopen van niveau 0 (alleen maar een idee) naar niveau 9 (stabiel in de markt met voorspelbare groei). Om een product commercieel verkrijgbaar te maken is niveau 6 (recurring business) voldoende.

Een bruikbaar product zou dus in de range moeten van TRL 8-9 en MRL 6-9, zie figuur 1.

We zien in Nederland en Europa een zogenoemd 'tech transfer gat', waarin innovaties ergens in de groei naar TRL 8-9 en MRL 6-9 stikken en niet tot wasdom komen. Dit gat werd ook gevoeld in het Partnership for Cyber Security Innovation (PCSI), een security innovatie samenwerking van ABN AMRO, ING, Achmea, de Belastingdienst en TNO. Met de hulp van het ministerie van EZ heeft dit geleid tot een tweetal rapporten met probleembeschrijving en mogelijke oplossingen (1), (2).

Grofweg zijn er twee grote oorzaken aan te wijzen voor het tech transfer gat:

- Een innovatie wordt vaak niet van TRL-niveau 0 naar niveau 8-9 gebracht door dezelfde mensen. Er vindt bijvoorbeeld wetenschappelijk onderzoek plaats aan de universiteit die leidt tot TRL-niveau 2-3, dat wordt opgepakt door een toegepast innovatieproject en daar verder gebracht tot niveau 5-6. Dat wordt dan vervolgens weer opgepakt door ondernemende personen in een startup, die er een product of dienst van maken. Er vinden dus overdrachten plaats, met alle bijbehorende aspecten zoals kennisoverdracht, commerciële aspecten en juridische en (geo-)politieke aspecten. Zie figuur 2.



Figuur 1: Het tech transfer gat vanuit het perspectief van TRL en MRL niveau.

- Er ligt vaak te veel focus op het verhogen van het TRL-niveau, waarbij het MRL-niveau (het marketing aspect) wordt verwaarloosd, terwijl (zoals ook uit de artikelen in deze speciale editie blijkt) het groeien van het MRL-niveau wellicht belangrijker is dan het groeien van het TRL-niveau.

De volwassenheid van het cybersecurity-ecosysteem in Nederland is best groot; er is een goed opleidingssysteem, goede research en er zijn kennisinstituten, een actieve overheid naast opsporingsdiensten en een groot aantal actieve cybersecuritybedrijven. We zien echter wel dat het moeilijk is voor innovatieve startups om tot wasdom te komen; het aantal Nederlandse cybersecurity startups is relatief laag in vergelijking met omliggende landen. De oorzaken hiervan worden in dit magazine beschreven.

Security tech transfer vanuit verschillende invalshoeken belicht

In deze special belichten we de uitdagingen op het gebied van security tech transfer vanuit verschillende invalshoeken. We zijn begonnen met het organiseren van een rondetafel event, waar veel partijen die iets hebben met security tech transfer zijn uitgenodigd om het onderwerp te bespreken. Dit werd een energiek en goed bezocht event, waarin veel kennis werd gedeeld en waar ook bleek dat er veel gemeenschappelijke gedachten zijn over het onderwerp security tech transfer. En het mooie was dat de meeste deelnemers zich bereid verklaarden om een bijdrage te leveren aan deze special, waarvan het resultaat nu voor u ligt. Voor een kijkje in de keuken van investeerders en communities hebben we Joris den Bruijnen, Aldebert Wiersinga en Reinout van der Meulen geïnterviewd. Het artikel van Folkwin Poelman geeft inzicht in subsidie. Ellen Wesselingh en Kees Stammes nemen u mee in het wetgevingsaspect, dat zowel lusten als lasten kent. Martijn Dekker licht toe hoe een CISO van een grote organisatie omgaat met security tech transfer. Ellis Brouwer beschrijft de cybersecurity-innovatie-

Het brengen van een innovatief idee naar een bruikbaar product of dienst is een lange en moeilijke reis met veel obstakels



Figuur 2: Handovers gedurende tech transfer vanuit het perspectief van TRL en MRL-niveau.

kansen in een veranderende wereld vanuit het perspectief van Cyberveilig.NL Een vorm van tech transfer is het publiceren van software als Open Source; Richard Kerkdijk beschrijft het COSSAS (Community for Open Source Security Automation Software) initiatief van TNO. We hebben twee artikelen die toelichten hoe in projecten met security tech transfer is omgegaan: Şeyma Irilmazbilek, Martijn Neef en Pieter Schneider beschrijven een post-quantum project en Sander Dorigo beschrijft een high-assurance case. En we hebben twee hele mooie beschrijvingen van praktijkervaringen van security startups: Mark van Staalduijn beschrijft de ervaringen van zijn bedrijf CFLW en Maarten Everts beschrijft de ervaringen van zijn bedrijf LinkSight.

Afsluitend

Het brengen van een innovatief idee naar een bruikbaar product of dienst is een lange en moeilijke reis met veel obstakels. We weten dat deze speciale editie van het PvIB magazine inzicht verschaft in wat er bij deze reis komt kijken en wat de tips zijn om deze reis aangenamer te maken.

Referenties

- (1) PCSI tech transfer, Improving the applicability of PCSI innovation results - Reinder Wolthuis, Marth Breure, Ruggero Montalto - 2024 - Report number TNO 2023 R11589. URL: <https://publications.tno.nl/publication/34642234/1rUnk7/TNO-2023-R11589.pdf>
- (2) Security Innovation & tech transfer in the Netherlands - Lessons learned from PCSI and more - Reinder Wolthuis, Marth Breure, Ruggero Montalto - 2024 - Report number TNO 2024 R11495. URL: <https://publications.tno.nl/publication/34643092/nxdAYi75/TNO-2024-R11495.pdf>

Lex Borger is security consultant bij Tesorion en oud-hoofdredacteur van IB Magazine. Lex is bereikbaar via lex.borger@tesorion.nl



Innovatie is meer dan techniek

De geopolitieke verhoudingen staan onder druk en verschuiven continu. De rol van internationale samenwerkingsverbanden, zoals: de Verenigde Naties (UN) en de NAVO, is in beweging. Conflicten en oorlogen spelen zich steeds dichterbij huis af en de scheidslijn tussen bondgenoten en tegenstanders is minder voorspelbaar dan ooit. Dit heeft directe gevolgen voor het digitale landschap: de herkomst van leveranciers en de locatie van dataopslag worden belangrijker.

Overigens worden supply-chain keuzes niet alleen door geopolitiek beïnvloed. Overheden en bedrijven werden door wet- en regelgeving, zoals NIS2, DORA en CER al gedwongen hun beveiligingsstrategieën te herzien en meer grip te krijgen op hun IT-ketens. En treffen ook maatregelen om ongewenste afhankelijkheden te verminderen en digitale soevereiniteit te versterken.

Recent waren grote IT-plattformen, zoals: Azure, AWS, Google Cloud, Windows en Intel de vanzelfsprekende keuze. Nu worden deze monoculturen vaker ter discussie gesteld vanwege strategische afhankelijkheden en beveiligingsrisico's. De roep om een sterkere Europese positie in cybersecurity en IT-infrastructuur groeit. Europa zal fors moeten innoveren: op technologisch vlak, maar ook in processen en governance - voor een onafhankelijke en veerkrachtigere digitale infrastructuur.

Cyberdreigingen werken niet in silo's, en cybersecuritybeheer zou dat evenmin moeten doen. Bedrijven en overheden werken vaker samen, over sectoren heen, om dreigingsinformatie te delen en gezamenlijke responsstrategieën te ontwikkelen. Publiek-private samenwerkingen, zoals: threat intelligence-plattformen en cybersecurity-oefeningen, worden steeds gebruikelijker.

Overheden en brancheorganisaties ontwikkelen gestandaardiseerde raamwerken en platformen om dreigingsinformatie real-time te delen. Hierdoor worden snellere reacties op aanvallen en gezamenlijk een robuustere verdedigingslinie opgebouwd. Dit is cruciaal, omdat cybercriminelen en statelijke actoren steeds verfijndere, gecoördineerdere aanvallen uitvoeren.

Technologische innovaties, zoals: Zero Trust, AI-gedreven threat monitoring (MDR/XDR) en post-quantum cryptografie, focusen op procesmatige innovaties. Securitybeleid en compliance zijn te vaak versnipperd binnen de keten, waardoor bedrijven moeite hebben om effectieve afspraken te maken.

Veel organisaties hanteren eigen securitybeleidsdocumenten, richtlijnen en dataclassificaties, leidende tot inconsistenties binnen de supply-chain. We zien vaker dat kernonderwerpen binnen cybersecuritybeleid - zoals toegangsbeheer, incidentrespons en data-encryptie - nagenoeg universeel toepasbaar zijn. Het verschil zit vooral in hoe beleid wordt afgestemd op de specifieke bedrijfsprocessen.

Dit vraagt om een gestandaardiseerde en ketenbrede aanpak, waarbij bedrijven hun securitybeleid beter op elkaar afstemmen. Hierdoor kunnen risico's in de keten effectiever beheerst worden en wordt samenwerking binnen sectoren versterkt.

Hierdoor verschuift de rol van de Chief Information Security Officer (CISO) meer van een tactische naar een strategische functie. Beveiliging wordt niet langer gezien als een technische IT-aangelegenheid, maar als een kernonderdeel van de bedrijfsstrategie.

Een risicobaseerde governance-aanpak helpt organisaties om cybersecurity te integreren in hun zakelijke doelstellingen. Dit betekent dat beveiligingsmaatregelen niet alleen effectief moeten zijn, maar ook kostenefficiënt en afgestemd op de risicobereidheid van het bedrijf.

CISO's en securityteams werken nauwer samen met directies en raden van bestuur om cybersecurity als business enabler te positioneren in plaats van kostenpost. Dit zorgt voor betere besluitvorming en een evenwichtige balans tussen innovatie, veiligheid en bedrijfscontinuïteit.

Cybersecurity is niet langer een kwestie van technologische innovaties, maar draait om de manier waarop organisaties beveiliging integreren in hun werkprocessen, governance en cultuur.

Investering in: medewerkertraining en security-awareness, automatisering van security-operaties, risicobaseerd governance-beleid, ketensamenwerking en dreigingsinformatie-deling ontwikkelt een flexibele en robuuste cybersecuritystrategie, die meegroeit met de dreigingen van morgen.

In een wereld waarin geopolitieke spanningen, cyberdreigingen en supply-chain risico's complexer worden, zullen succesvolle organisaties niet degenen zijn die de meeste firewalls en AI-tools hebben, maar degenen die cybersecurity beschouwen als een integraal bedrijfsproces, waarin de traditionele focus op techniek verbreed wordt met de aspecten mens, proces en samenwerking.



INTERVIEW

Hoe kunnen communities en investeerders bijdragen aan succesvolle tech transfer?

Reinder Wolthuis en Chris de Vries interviewen Joris den Bruinen, Aldebert Wiersinga en Reinout vander Meulen.

We spreken met drie heren die elk een belangrijke bijdrage leveren aan security tech transfer: Joris den Bruinen, Directeur-bestuurder stichting Security Delta (HSD), Aldebert Wiersinga, oprichter en investeerder bij Value Creation Capital (VCC) en Reinout vander Meulen, investeerder bij TIN Capital.

Joris: HSD is hét nationale veiligheidscluster waarin zo'n 300 bedrijven, overheidsorganisaties en kennisinstellingen samenwerken. Het doel is het versterken van de Nederlandse economie, het creëren van werkgelegenheid en een digitaal weerbaarder Nederland. Dit door kennisdeling en samenwerking aan innovatieve veiligheidsoplossingen, die ook (inter)nationaal uitgerold kunnen worden. HSD zorgt voor toegang tot kennis, innovatie, markt, financiering en talent.

Aldebert: VCC is investeerder (meer ondernemer dan investeerder) die startup en scale-up technologiebedrijven helpt om verder te komen. Het VCC-portfolio bevat kleinere bedrijven, tussen 0,5 en 2 miljoen omzet (startup) en tussen 2 en 10 miljoen omzet (scale-up). Op de website van VCC staan alle huidige deelnemingen, bijvoorbeeld Sceptr (voormalig NetDialog). Op het topic Security & Safety heeft VCC circa 6

'exits' (het verkopen van de investering, bij voorkeur strategisch) gedaan en momenteel nog circa 10 deelnemingen in dit domein. Dit thema valt ook binnen de (nieuwe) Deep Tech fondsen van VCC.

Reinout: TIN Capital is een investeringsmaatschappij en is een aantal jaren geleden het Dutch security TechFund gestart (36 miljoen euro budget). Dit Dutch Security TechFund is nu volledig besteed met 17 investeringen. Daarom hebben zij nu het European Cyber Tech Fund opgezet (circa 100 miljoen euro) om door te kunnen investeren. De investeerders zijn zowel particulieren als professionele investeerders en het gaat om zogenoemde 'Limited Partners', die nemen geen beslissingen en zijn dus ook niet aansprakelijk. TIN Capital zoekt naar 'pareltjes', zodra gevonden dan vormt zich een investeringscomité, die advies geeft. Bij positief advies volgt investering in de startup en dat voor langere termijn, vaak 5 jaar.

Hoe kunnen startups groeien

Investeren in startups is belangrijk, maar er moet uiteindelijk ook geld verdiend worden, hoe doen jullie dat?

Aldebert: om te beoordelen of VCC een startup gaat helpen, zoeken wij naar commercieel bewijs dat het product/dienst van de startup aanslaat in de markt; dat klanten het willen kopen. Er is altijd een exit strategie: investeren op dag 1, exit op dag x. VCC investeert in onderwerpen, zoals: infrastructuur, tech, software en cybersecurity. VCC stapt in op startups die een product/dienst hebben die op Technology Readiness Level (TRL) 5-6 zitten (1). Soms zijn startups nog niet ver genoeg, dan vragen wij zo'n startup terug te komen als ze wat verder zijn en eventueel zoekt VCC mee naar de juiste propositie en/of versterking van het team. VCC is geen 'venture builder', dat zijn investeerders die meer in de tech transfer fase zitten, maar die zijn volgens Aldebert wel nodig om een brug te slaan tussen idee en Venture Capitalist (VC). Reinout: Venture builders kennen het domein waarin ze opereren goed en hebben een grote staat van dienst. Het begint vaak met het zien van een gat in de markt, dan zoeken ze daar de juiste mensen bij en stoppen er een beetje financiering in. Het bedrijf kan daarna gefinancierd worden door een 'seed investor'. Een venture builder vraagt vaak 30-40% aandeel in een bedrijf als wederdienst voor hun hulp. De ondernemers zijn veelal ingehuurd, dus geen echte founder. Een voorbeeld van een venture builder is Cyberstarts in Israël. Het succes bij een venture builder staat of valt niet met 'leading edge' technologie, maar het herkennen van de problemen.

Joris: In Nederland is het cybersecurity-ecosysteem tot op heden beperkt ontwikkeld. Er zijn allerlei deel-ecosystemen: overheid en ministeries, dcypher, PCSI, HSD, Amsec, Cyberveilig Nederland, DIVD. Tot twee jaar geleden gunden men elkaar weinig. Nu kennen partijen elkaar beter, heeft ieder op eigen kracht een plek in het gehele ecosysteem gevonden. Partijen weten meer samen te werken om Nederland en de wereld weerbaarder te maken. De eerste

Capital investeringsfondsen met een specifiek focus op cybersecurity zijn ongeveer 10 jaar geleden gestart, sindsdien is dit behoorlijk uitgebreid qua budget en aantal spelers. Nu zijn er TIN Capital en VCC en daaromheen ook spelers zoals: KPN Ventures en Innovation Quarter. HSD speelde daar een faciliterende en verbindende rol in, ook Europees bijvoorbeeld samen met ECSO (European Cyber Security Organisation) en de gezamenlijke Cyber Investor Days op de HSD Campus in Den Haag. Er moet nadrukkelijker gebruik worden gemaakt van het gehele NL/EU investeringsveld en meer worden samengewerkt. Ook in de tech transfer met TNO en universiteiten en de vroege-fase financiering. Er is voldoende potentieel, ook in deze vroege-fase financiering, met Arches, Lumo labs, Ctrl-Alt-Invest en UNIQ. Yes!Delft heeft inmiddels een



Cyber Security accelerator programma opgezet voor meerdere fases van een startup ontwikkeling. Het is goed dat we de investeringskant beter op orde hebben, maar cruciaal blijft de eerste klant; zonder klanten geen omzet en geen toekomst.

Joris: laat elke CISO in Nederland één startup helpen, wellicht organisatorisch via CISO-community NL.

RiskApp, als voorbeeld, die heeft nu een paar CISO's die hen helpen als launching customer.

Reinout: dit is een goed idee. CISO's doen soms wel 'Angel investments', vooral in de VS gebeurt dit. De eerste investeringen worden daar vaak bij CISO's opgehaald. Daar gaat het makkelijker om als jong bedrijf een CISO te vinden om een Proof of Concept (PoC) te evalueren. In de EU zijn organisaties meer risicomijdend, ze willen iets hebben dat werkt en zich bewezen heeft. Startups zijn uiteindelijk een bedrijf, ze hebben dus klanten nodig. Het grote nadeel van startups is het gemis aan trackrecords, zoals een groot bedrijf als Palo Alto wel heeft; zij zijn duur, maar wat ze leveren werkt en ze bieden uitgebreide ondersteuning. Dus voor een startup is die eerste klant van wezenlijk belang, 'word of mouth' werkt en als er één klant over de dam is ...



Aldebert: CISO als launching customer is een goede optie. Corporate bedrijven hebben vaak wel budget voor pilots, zo'n pilot kan goed helpen bij de uitrol. En via een groter bedrijf kan een product/dienst van een startup ook weer belanden bij kleinere (MKB) bedrijven; een grotere bank een product/dienst afnemende van een startup en dat vervolgens doorverkoopt aan haar MKB-klanten.

Nationale veiligheid en cybersecurity investeringen

We zien in landen als de VS en Israël een grote cybersecurity vraag vanuit nationale veiligheid en defensie, die de cybersecurityindustrie en daarmee tech transfer alsook de startup cultuur lijkt te stimuleren. Zouden we dat in Nederland ook moeten nastreven?

Reinout: de defensie-uitgaven van een land zijn een goede indicator voor de bereidheid om budget vrij te maken voor cybersecurity-industrie - ook in de private sector, dat zie je in landen als de VS en Israël. Veel securityproducten en diensten komen uit die landen. Als Nederland zijn we te klein om deze hegemonie te breken en als het gaat over cybersecurity moeten we vooral Europees denken en niet nationaal! Als Europeanen moeten we dus zoveel mogelijk Europese

producten kopen, maar dat vereist verandering. Als Frans cybersecuritybedrijf is het nu moeilijk om een product/dienst in Duitsland te verkopen.

Aldebert: eens met het Europees denken. In het huidige portfolio van VCC zit een tiental cyberbedrijven. De klanten van deze bedrijven kiezen vaak bewust voor een product/dienst dat niet Amerikaans of Israëliësch is. Dick Berlijn (redactie: voormalig commandant van de Nederlandse strijdkrachten) helpt bij de governance van een aantal VCC-deelnemingen ten einde geopolitieke afwegingen goed te kunnen maken. Als startup met een mooi product, kom je allicht voor de vraag te staan aan welke landen je jouw product/dienst wilt verkopen. Dat is een morele afweging en die kun je het beste 'protocolleren'; via een vooraf vastgesteld protocol beslissen of je wel of niet levert.

Joris: de vraag vanuit het veiligheidsdomein is een interessante. Als we naar het Operational Technology (OT) domein kijken, zien we ook de hefboom-factor voor startups via grote bedrijven bij de Nederlandse vitale infrastructuur en industrie. Er liggen kansen bij secure-by-design producten in relatie tot smart grids en de energietransitie. Daarop meeliftende zet je

De meest capabele ondernemers willen in de Champions League meespelen en die gaan dus voor een Unicorn

innovatieve cybersecurityproducten beter op de markt. Ook Dual Use producten, die ingezet worden voor zowel de civiele als de defensiemarkt, bieden kansen. Hiervoor is er recent ook meer kapitaal beschikbaar gekomen, wat benut kan worden voor een Nederlandse en Europese 'Buy & Build' fusie- en overnamestrategie!

Aldebert: ja, Dual Use is een goede hefboom. Overheids-investeerders wilden er een jaar geleden niets van weten, maar dat is omgedraaid. Opsplitsing van bedrijven, waar nodig, helpt de exit-uitdagingen bij Dual Use bedrijven beheersbaar te maken. Veel defensie gerelateerde startups kunnen bijvoorbeeld niet ongeclausuleerd buiten de EU-exit'en. Vanuit rendementsoogpunt splitsen bedrijven vaak beter op naar product/markt combinatie. Dit heeft VCC recent gerealiseerd bij optische technologie, dat ook voor de marine zeer interessant bleek te zijn.

Reinout: als de Wet veiligheidstoets investeringen, fusies en overnames (Vifo) gaat gelden dan wordt dat een probleem voor bedrijvenkopers uit de VS, die daaronder vallen. Dan lukt het dus niet om EU-kampioenen te creëren.

Aldebert: bij VCC hebben ze net een casus afgewezen omdat de aandeelhouders de exit-voorwaarden al te veel hadden geclausuleerd.

Joris: ik snap de geschetste problematiek, echter er zijn ook goede voorbeelden zoals Compumatica, dat werd een waardevolle Nederlandse exit. Joris zou opnieuw om tafel willen om dit soort exits te regelen met kapitaal uit de EU. Krijg de grote investeerders, zoals: Main Capital uit Den Haag en

Invest NL, zover om mee te doen in het domein van Cyber Security, ook met Dual Use, dan bereiken wij wellicht de gewenste combinatie van: succesvol schalen van startups, investeringen en NL/EU autonomiedoelen.

Reinout: de meest capabele ondernemers willen in de Champions League meespelen en die gaan dus voor een Unicorn (redactie: een startup bedrijf dat een waarde bereikt van meer dan 1 miljard dollar en dat in privaat eigendom is, niet aan de beurs genoteerd). Beknot op voorhand de uitkomst tot alleen de EU, dan beperk je die mogelijkheden. Succesvolle ondernemers starten hun volgende bedrijf gelijk in de VS omdat het daar gemakkelijker is om tot een Unicorn te worden.

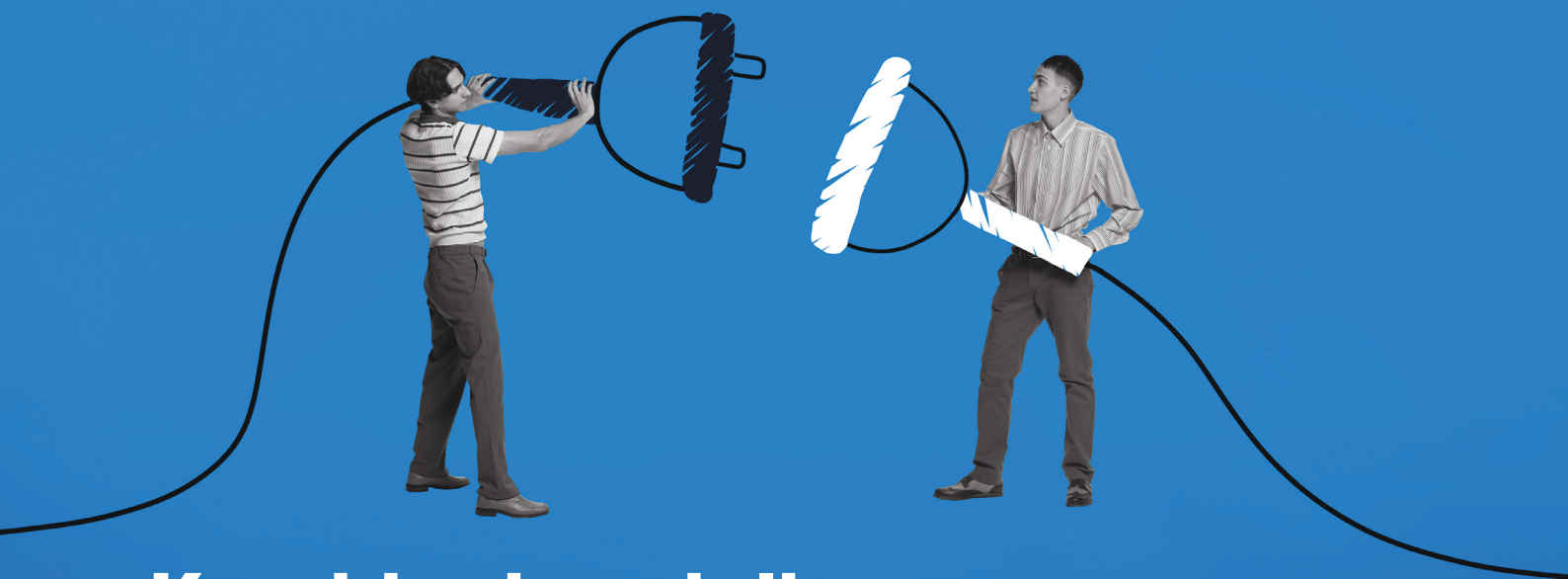
Actiegericht vervolg

Uit dit interview blijkt, dat er een aantal dingen goed gaan en dat er al best wat randvoorwaarden zijn gecreëerd voor een succesvol startupklimaat, maar dat er ook nog veel te doen is. Als concrete vervolgactie komt het idee op, om een rondetafel te organiseren tijdens de Cyber Security Week/ONE Conference. Dat met de verschillende partijen, die betrokken zijn bij de tech-transfer en investeringen op het gebied van Cyber Security en Dual Use, over hoe waargenomen obstakels uit de weg geruimd kunnen worden. Joris verklaart zich bereid om hier het voortouw in te nemen. Zo komt er een heel mooi actiegericht vervolg aan dit interessante interview!

Referentie

- (1) Technology Readiness Level:
https://en.wikipedia.org/wiki/Technology_readiness_level

Auteurs: Şeyma Irlmazbilek is Onderzoeker bij NCSC-NL, zij is bereikbaar onder research@ncsc.nl ; Martijn Neef werkt als Coördinator Kennis en Innovatie Cybersecurity bij het ministerie van Economische Zaken, hij is bereikbaar via r.m.neef@minezk.nl en Pieter Schneider is Programmamanager Quantumveilige Cryptografie bij CIO-Rijk, zijn e-mail adres luidt: QvC-Rijk@rijksoverheid.nl



Krachtenbundeling van onderzoek en innovatie: relevantie & toepasbaarheid op post-quantum cryptografie

Organisaties moeten nu in actie komen om tijdig te kunnen migreren naar quantumveilige cryptografie. Een belangrijke eerste stap hierin is om een inventarisatie uit te voeren van cryptografische middelen die een organisatie gebruikt. Maar hoe doe je dit op een juiste manier? Welke technologie kun je inzetten voor zo'n inventarisatie en zijn er al producten beschikbaar? Die vragen raken ons allemaal en zijn niet alleen actueel vanwege de dreiging van de quantumcomputer op cryptografie, maar ook door de NIS2.

In het bijzonder door maatregel 8 met betrekking tot cryptografiebeleid waarin gesteld wordt dat organisaties hun data passend moet beschermen tegen de relevante en actuele risico's. Tegelijkertijd zijn er nog veel uitdagingen waar de praktijk mee te kampen heeft bij de inventarisatie van cryptografische middelen. Het is beperkt duidelijk of de beschikbare technologie voldoende toereikend is om inzicht te krijgen in welke cryptografische middelen er in een digitale infrastructuur zitten, of welke functionaliteiten dergelijke tooling moet hebben om tot een cryptografische inventaris te komen. Om hier beter zicht op te krijgen hebben het Nationaal Cyber Security Centrum (NCSC), het ministerie van Economische Zaken (EZ) en de directie Chief Information Office-Rijk (CIO-Rijk) TNO gevraagd onderzoek te doen naar Crypto Asset Discovery & Inventory (CADI-) tooling (1). In dit onderzoek heeft TNO middels literatuuronderzoek, brainstormsessies met experts, en workshops met stakeholders en leveranciers inzicht opgebouwd over de huidige en gewenste staat van CADI-tooling.

In dit artikel belichten we ten aanzien van post-quantum cryptografie (PQC) de samenwerking tussen NCSC, EZ en CIO-Rijk in dit project, de wisselwerking tussen onderzoek en innovatie, en de wijze waarop dit onderzoeksproject een impuls kan geven aan innovatie van de Nederlandse markt.

Samenwerking tussen NCSC, EZ en CIO-Rijk

CIO-Rijk is de coördinator van Quantumveilige Cryptografie Nederland (QvC) op nationaal niveau en op internationaal niveau is CIO-Rijk de co-chair van de PQC-workstream. Dit is een Europees samenwerkingsgroep dat als doel heeft een routekaart te ontwikkelen voor de PQC-migratie, zodat de digitale infrastructuur in Europa bestendig zijn tegen de komst van quantumcomputers. Het QvC-programma heeft als doel de Rijksoverheid, medeoverheden en vitale entiteiten te helpen om de risico's van quantumtechnologie op cryptografie tijdig te beheersen. Het NCSC levert als kennisautoriteit een structurele bijdrage aan het QvC-kernteam, en houdt daarbij zicht op welke kennis ontwikkelt moet worden. De onderzoekers van het NCSC-onderzoeksteam stimuleren, coördineren, en voeren zelfstandig of in samenwerking met verschillende kennisinstellingen (co-creatie) wetenschappelijk onderzoek op het gebied van cybersecurity uit. Een belangrijk doel is dat de onderzoeken impact hebben en een bijdrage leveren aan de digitale weerbaarheid van Nederland. De nieuwe kennis en inzichten, die voortvloeien uit de onderzoeken, kunnen vervolgens onder andere als basis dienen voor innovatie. Hierin wordt nauw samengewerkt met EZ: EZ is de hefboom om innovatie naar de markt te brengen en ondersteunt diverse programma's om de (inter-)nationale positionering van

het Nederlandse kennis- en innovatiesysteem te versterken. Deze wisselwerking tussen onderzoek en innovatie stimuleert vooruitgang waarbij onderzoek innovatie aandrijft en innovatie – of poging tot innovatie – nieuwe onderzoeksvragen creëert en daarmee kennisontwikkeling.

Urgentie van PQC-migratie

Quantumcomputers zijn niet langer slechts een idee waar we later mee te maken gaan hebben. Universiteiten en grote technologiebedrijven doen grote investeringen in onderzoek en ontwikkeling. Steeds sterkere prototypes volgen elkaar in rap tempo op. Daarmee wordt de noodzaak tot het hebben van een cryptografische inventaris – inventarisatie van de cryptografische middelen die een organisatie gebruikt: de eerste stap in je risico-analyse – en het nemen van passende maatregelen. Het CADI-onderzoeksproject speelt in op deze urgentie.

Dit onderzoek brengt praktijk en wetenschap bij elkaar en levert, naast nieuwe inzichten en een marktverkenning, ook een constatering ten behoeve van innovatie, namelijk: Op welke criteria beoordeel je de doeltreffendheid van een CADI-tooling, als de gebruiksaanpak nog niet volledig bekend is? Het achterliggende doel van dit onderzoeksproject was om inzicht te krijgen in welke tooling passend is voor een PQC-migratie middels het opstellen van een evaluatieraamwerk. Er ontstaat namelijk d.m.v. dit onderzoeksproject een steeds beter beeld hoe organisaties de eerste stap, proces – de cryptografische middelen inventarisatie binnen je organisatie – kunnen doorlopen om voorbereid te zijn op de komst en dreiging van quantumcomputers voor cryptografie. Het PQC-handboek (2) is een mooi voorbeeld van een publicatie om organisaties te ondersteunen om deze dreiging te beperken. Echter, er is nog veel te leren over hoe je deze eerste stap doeltreffend en efficiënt inricht. We weten nog niet hoe de kracht van quantumcomputers zich gaat manifesteren in de toekomst, en daardoor ook niet welke informatie en technologie nodig zijn om data in een organisatie veilig te houden. Dit project heeft daarmee een schier onmogelijke taak: hoe bepaal je de doeltreffendheid van een CADI-tooling, als we wereldwijd nog niet goed weten of kunnen inschatten wat het minimaal zou moeten kunnen? Het construeren van een evaluatieraamwerk bleek dan ook een uitdaging.

Creatie van een innovatieketen op PQC-migratie

De resultaten van dit onderzoek heeft hiermee onverwacht een additionele waarde. Niet alleen de verkenning, maar ook het evaluatieraamwerk blijkt waardevol. Die vormt een vector voor innovatie: de criteria vertegenwoordigen onze visie van wat verwacht wordt van toekomstige producten en geven daarmee

leveranciers signalen en richting voor productontwikkeling. Aangezien de quantumwereld continu in verandering is, zal ook het beoordelingskader voor CADI-tooling mee moeten veranderen, net zoals beoordelingskaders voor andere producten in de PQC-keten. Dit project staat daarom niet op zichzelf, maar is een onderdeel van een grotere uitdaging: hoe vormen we een effectieve innovatieketen op PQC-migratie, waar visievorming, productontwikkeling, -gebruik en -beoordeling nauw op elkaar aansluiten, en zich wendbaar blijven ontwikkelen?”

Onderzoek en innovatie begeleiden naar producten en diensten
Het onderzoek laat zien dat de realisatie van een zowel complete als volwaardige oplossing complex is. Het wordt steeds belangrijker voor organisaties om de waarheid rond cryptografische middelen in hun IT-, OT- en IoT-omgevingen boven water te krijgen. Om dit inzicht te krijgen, wordt in het algemeen een agent ingezet. Dit is een programma dat specifiek wordt ingezet om op de achtergrond informatie te verzamelen over het netwerk- en systeemactiviteit. Er is vaak nog weerstand om software agenten hiervoor in te zetten, omdat hier veiligheids- en beschikbaarheidsrisico's aan vast zitten. In bepaalde omgevingen is het zelfs niet wenselijk of niet mogelijk om een agent in te zetten. Hoe accuraat een oplossing uiteindelijk is, is lastig in te schatten, omdat er geen grondwaarheid is voor nauwkeurigheid. In bestaande omgevingen kan de nauwkeurigheid van een tool daardoor niet goed worden bepaald. Een dergelijk tool inzetten in een zeer gecontroleerde, gesloten omgeving, kan dit inzicht mogelijk wel bieden. Er zal in zekere mate altijd onzekerheid blijven over welke cryptografische middelen binnen een organisatie actief zijn. Het niet weten wat je niet weet, is in lijn met de filosofie van risicomangement: risico's zijn niet 100% te elimineren – waardoor wendbaarheid een belangrijke rol speelt om je risico's te beheersen. Denk aan crypto-agility. Verder laat het onderzoek zien dat er hoge kosten verbonden zijn aan de inzet van dergelijke oplossingen en dat de inzet van CADI-tooling compliance-gedreven is. Daarmee wordt het inzicht verkrijgen in deze assets een dure en niet-vrijwillige exercitie. Geen wonder dat de markt hier niet warm voor loopt.

Het onderzoek laat naast uitdagingen ook kansen voor leveranciers zien. Innovatieve partijen uit Nederland en Europa kunnen nieuwe, efficiënte oplossingen ontwikkelen voor deze uitdagingen. De wens naar het beter inzicht verkrijgen in de aanwezige cryptografische middelen zal alleen maar toenemen, zeker met het oog op de transitie naar PQC wat een verantwoordelijkheid van ons allemaal is. Daarom worden de resultaten van het onderzoek publiek gemaakt, zodat zowel leveranciers als afnemers op een geïnformeerde wijze stappen kunnen zetten op

co-creatie. QvC speelt een faciliterende rol in deze co-creatie en is blijvend in gesprek binnen Rijksoverheid en met vitale entiteiten om onder andere innovatie te begeleiden naar producten en diensten. Hiernaast moeten de ontwikkelingen op het gebied van IT-asset management en standaardisering nauw gevolgd worden. Voorbeelden hiervan zijn de ontwikkelingen op het gebied van de CBOM en implementatie van de Cyber Resilience Act (CRA).

Praktijkwensen ontmoeten marktkansen

Het onderzoek laat zien dat CTO's van de Rijksoverheid niet verwachten dat een tool (of combinatie van tools) een volledig beeld van alle cryptografische middelen kan produceren. Voor de IT-omgeving wordt 60% tot 85% nauwkeurigheid gewenst voor een Minimum Viable Product. Voor de OT-omgeving is de gewenste nauwkeurigheid een stuk lager, respectievelijk tussen 30% en 60%. Maar hoe goed werkt een tool? Hoe kan je meten of een tool 85% inzicht geeft, als je op voorhand niet weet wat er 100% in de IT-infrastructuur is genesteld? Het kunnen aantonen dat een tool een bepaalde mate van nauwkeurigheid heeft, biedt de kans om een bewezen product aan te bieden en daarmee concurrentievoordeel te behalen. Het ontbreken van de grondwaarheid voor de nauwkeurigheid van dergelijke CADI-tools biedt daardoor een kans voor de markt.

Conclusie |

Wat kan ik als organisatie met dit onderzoek?

Tijdig migreren naar quantumveilige cryptografie begint bij het inventariseren van je cryptografische middelen. Deze stap kent diverse uitdagingen en CADI-tooling kan deze uitdagingen oplossen door (automatisch) je cryptografische middelen te inventariseren en bij te houden. Uiteindelijk is de PQC-migratie een verantwoordelijkheid van ons allemaal en moeten we hiermee nu aan de slag.

Indien je als organisatie een start wilt maken met een cryptografische inventarisatie, dan kan je de resultaten van dit project gebruiken om met leveranciers in gesprek te gaan over de functionaliteiten waaraan een CADI-tooling minimaal moet voldoen, en welke waardevol zijn voor de organisatie in kwestie. Zo kunnen we in Nederland effectief de eerste stap zetten om de dreiging van quantumcomputers voor cryptografie te beperken.

Referenties

- (1) CADI-tooling is een relatief jong vakgebied waardoor deze term synoniemen kent. Zie de resultaten van het onderzoek voor details.
- (2) Het PQC-migratie handboek | Publicatie | AIVD

Tech transfer: vanuit dienst-verlener naar overheid en dan naar de markt?

Bij Fox Crypto werken we dagelijks aan het mogelijk maken van veilige communicatie. We schrijven software zoals OpenVPN-NL en we maken VPN-apparatuur voor het beveiligen van de meest gevoelige gegevens. Daarbij gaat het niet alleen om de meest gevoelige bedrijfsgeheimen, ook overheidsklanten, in binnen- en buitenland, gebruiken onze apparatuur voor deze lastige opgave. Zij zijn vaak nog veeleisender. Zou het niet mooi zijn, als je de bij de overheid opgedane kennis ook kan toepassen op de eigen commerciële productportfolio?

Voor een veilige overdracht van door zulke overheden gerubriceerde gegevens, is meer nodig dan een veilige verbinding. De apparatuur moet getoetst zijn, er is vaak een inzetadvies nodig en op de allerhoogste niveaus zijn diverse geheime en minder geheime maatregelen genomen om de "lijn" veilig te houden. Voor ons is dat een prettig verkoopargument. Als zulke partijen het product vertrouwen om hun geheimen te bewaren, dan zal het voor uw toepassing ook wel goed zijn. Echter, niet alle van staatswege toegepaste maatregelen vinden hun weg naar de commerciële markt. Toch blijft het mogelijk om uit deze bijzondere producten kennis en kunde te extraheren, welke toe te passen zijn op 'gewone' producten.

Om te beginnen is het vaak een kwestie van zorgvuldig werken. Als de klant, net als wij, streeft naar een omgeving zonder compromissen, indien het gaat om verbindingsbeveiliging, bereik je al veel. Goede processen, een robuuste high-availability omgeving zorgt voor een groot deel van de zekerheid. Daar waar overheden soms gezien worden als "traag", ervaren wij ze vaak als "zorgvuldig". Dat is een goede gewoonte om over te nemen.

De open source softwarewereld groeit en breidt zich steeds verder uit. Een bijzonder voorbeeld is post-quantum-cryptografie. De zoektocht naar nieuwe algoritmes gebeurt geheel in het openbaar. Algoritmes, voorbeeldcodes en protocollen staan allemaal online. Fox Crypto

draagt daar een steentje aan bij. Wij bouwden (en publiceerden!) een C99-implementatie van een eXtended Merkle Signature Scheme (XMSS). Dit vond plaats onder de vlag van de Nationale Cryptostrategie. Een vruchtbare samenwerking tussen overheid en markt.

Maakt uw bedrijf hardware? Bereid die voor op een mogelijke toekomstige commerciële lancering door modulaair te werken. Een modulaire opbouw zorgt ervoor dat chips makkelijk te upgraden zijn en software-patches functies toevoegen. Dat maakt het eenvoudiger om een commerciële variant van een apparaat te produceren. Dat kan ook in de software. De door Fox Crypto geleverde Bittium telefoon is hiertoe in staat. Naast de diverse fysieke varianten, kan de software - afhankelijk van de wensen van de klant - worden uitgerust mét of zonder afhankelijkheid van Google.

Meer dan ooit publiceert de overheid handreikingen, gidsen en flyers over allerlei onderwerpen. Recentelijk over AI en post-quantum-cryptografie. In samenwerking met TNO schreef de AIVD bijvoorbeeld een nieuw handboek voor de post-quantum-migratie. Vanuit Fox Crypto leverden we zo een kleine bijdrage aan en onderzoekskennis terug naar de markt.

Veel overheden vereisen strenge geheimhouding als het gaat om de voor hen ontwikkelde producten. Maar in goede samenwerking kan deze kennis terugvloeien naar de rest van het productportfolio. Daar hebben alle partijen veel baat bij. Zoek daarom naar de mogelijkheden.

Auteur: Ellis Brouwer is relatiemanager binnen Cyberveilig Nederland; de belangenvereniging van de cybersecuritysector. Naast haar werkzaamheden voor Cyberveilig Nederland werkt Ellis bij Hogeschool Saxion waar ze als docent-onderzoeker lesgeeft aan studenten van de opleiding Security Management. Zij is bereikbaar via 'e-mail': ellis@cyberveilignederland.nl

Innovatie door Cyberdreigingen

- Onze maatschappij is in een hoog tempo afhankelijk geworden van digitale netwerken. Recente IT-storingen en -incidenten benadrukken hoe afhankelijk onze samenleving is geworden van digitale netwerken, maar ook van een digitale overheid. In het verlengde daarvan wordt ook onze afhankelijkheid van digitale computernetwerken met technologie van buiten Europa steeds groter. Veel IT-oplossingen worden ingekocht bij leveranciers uit bijvoorbeeld China en de Verenigde Staten. Tegelijkertijd is er een geopolitiek landschap ontstaan, waarin het vertrouwen in de landen waar we deze oplossingen inkopen, is afgenomen. Bevriende naties van vandaag kunnen morgen risico's vormen voor onze nationale veiligheid én daarmee ook voor onze (IT-)systemen.

Loading...

80%

Deze veranderende, geopolitieke situatie geeft nieuwe uitdagingen en risico's die volgen uit de afhankelijkheid van de gehele Nederlandse maatschappij ten aanzien van andere mogelijkheden en actoren, oftewel onze digitale soevereiniteit. Aan de andere kant belichten deze uitdagingen en risico's ook de urgentie voor nieuwe oplossingsrichtingen en biedt het nieuwe kansen voor Europese cybersecurity-innovatie. Vanuit Cyberveilig Nederland (CVNL), de brancheorganisatie van cybersecuritybedrijven in Nederland, geven we alvast een voorzet.

Digitale soevereiniteit: wat is haalbaar?

Het Draghi-rapport van september 2024 (1) bevestigt dat Europa in de afgelopen jaren steeds verder afhankelijk is geworden van leveranciers buiten Europa. Of het nou gaat om maak-, IT-, of defensie-industrie: we zijn onvoldoende in staat geweest om goede competitieve tegenhangers tegenover veelal Chinese en Amerikaanse bedrijven te zetten. Hoewel twee hoogleraren economie in het FD nog pleitten voor het terughalen van toeleveranciersketens (2), zien wij het als onhaalbaar om in Europa een volledig concurrerende IT-industrie op te bouwen. Dat is veel te duur en tijdrovend en daar hadden we al jaren geleden mee moeten beginnen.

In plaats van het streven naar een eigen industrie die gericht is op het produceren van Europese IT-systemen, moeten Nederland en Europa zich naar onze mening richten op het vergroten van controle over bepaalde aspecten van ons IT-landschap. Dit sluit aan bij de definitie van digitale soevereiniteit die TNO geeft in haar rapport over dit onderwerp uit 2024:

Digitale soevereiniteit betekent dat men de digitale capaciteiten en mogelijkheden heeft om digitale goederen, diensten en infrastructuren te produceren, te leveren en te gebruiken en dat men de controle hierover heeft om de soevereiniteit te beschermen (3).

Vergroting van digitale soevereiniteit

Voor wat betreft het vergroten van controle over delen van het IT-landschap ziet CVNL vanuit cybersecurityperspectief een

aantal mogelijke oplossingen, waaronder risicospreiding door een aangepaste inkoopstrategie, fallback-oplossingen bij uitval, betere bescherming van gevoelige data, inzet van Europese en Nederlandse regulering, fysieke bescherming van de Nederlandse digitale infrastructuur en het versterken van human capital. Een aantal van deze mogelijke oplossingen behoeven aanpassingen of nieuwe ontwikkelingen en bieden daarom kansen voor innovatie.

Risicospreiding en inkoopstrategie

Bij het inrichten van een IT-landschap hebben organisaties veel mogelijkheden als het gaat om de keuze voor toeleveranciers. Vanuit het perspectief van beheersbaarheid, gemak en kosten kan de keuze vallen op een beperkte set van toeleveranciers voor onderdelen in het IT-landschap zoals hardware, netwerkcomponenten en software. Belangrijk bij inkoop van IT-oplossingen is echter dat ook het perspectief van digitale soevereiniteit wordt meegewogen. Risico's op dit gebied kunnen ontstaan door bijvoorbeeld veel oplossingen in te kopen bij dezelfde leverancier, maar ook door de oplossingen in te kopen bij meerdere leveranciers uit hetzelfde land. In plaats daarvan zouden inkoopstrategieën gericht moeten zijn op spreiding, zowel geografisch als wat de keuze van verschillende toeleveranciers betreft.

Op deze manier inkopen maakt een organisatie minder kwetsbaar als geopolitieke spanningen ervoor zorgen dat je moet of wilt veranderen van (toe)leverancier. Zo'n slimme inkoopstrategie is haalbaar voor met name vitale organisaties en de Rijksoverheid, maar is voor kleinere (MKB-)organisaties veel moeilijker te realiseren. Deze organisaties willen vaak off-the-shelf oplossingen en beschikken meestal over minder specialistische kennis om hierin weloverwogen keuzes te maken. Omdat digitale soevereiniteit vaak niet wordt meegenomen in strategische afwegingen, is het raadzaam dat er in de toekomst wellicht nieuwe leveranciers ontstaan. Zij kunnen dan deze inkoopstrategie als dienst leveren en als het ware off-the-shelf een goede leveranciersmix samenstellen en aan kleine bedrijven aanbieden. Wel is het concurrentievermogen van dit soort inkoopleveranciers een punt van zorg, omdat dit soort diensten kostbaar kunnen zijn. Een mogelijkheid om dit tegen te gaan zou bijvoorbeeld het tijdelijk verlagen van de BTW voor dit soort diensten of andere financiële prikkels vanuit de overheid kunnen zijn.

Zo staat Nederland binnen Europa bekend om zijn cryptografische kennis en -toepassingen

Beter beschermen van gevoelige data

Voor het beschermen van data wordt veel gebruik gemaakt van encryptiestandaarden. Als data versleuteld wordt opgeslagen, is het lastiger (zo niet onmogelijk) voor derden om zonder een geldige sleutel daar toegang toe te krijgen. In het kader van digitale soevereiniteit, maar ook vanwege de ontwikkelingen rondom quantum computing, is het van belang om zoveel mogelijk dit proces onder eigen controle te houden. Denk bijvoorbeeld aan het in Nederland (of Europa) produceren van encryptiesleutels, maar ook aan het verder stimuleren van een Nederlandse (en Europese) crypto-industrie en het toepassen van concepten zoals bring-your-own-key, waardoor je altijd de controle behoudt over encryptiesleutels omdat leveranciers er niet bij kunnen.

Hierop voortbordurend kunnen we vaststellen dat de cybersecurity-industrie nog volop in beweging is en er, in tegenstelling tot de IT-industrie, nog genoeg kansen liggen voor ontwikkeling en innovatie van cybersecurity-oplossingen in Nederland en Europa. Het is belangrijk om te kijken naar de cybersecurity-oplossingen die al voorhanden zijn en waar nog extra in geïnvesteerd moet worden. Daarin de samenwerking opzoeken is minstens zo belangrijk. Hierin zou dan wel fors moeten worden geïnvesteerd en de perverse prikkels - waardoor ieder (Europees) land zijn eigen encryptie-industrie probeert te ontwikkelen - moeten worden weggenomen. Het overdragen en/of verspreiden van nieuwe technologie van en tussen Europese landen kan juist de sleutel zijn tot nieuwe uitdagingen op het gebied van digitale autonomie: 1. het omzetten van uitvindingen en wetenschappelijke resultaten in nieuwe producten alsook 2. diensten leveren voor de vergroting van de cyberweerbaarheid en digitale autonomie. Dat is nu meer dan nodig. Er bestaan tussen Europese landen verschillende specialisaties en innovatieve oplossingen voor de vergroting van de digitale weerbaarheid. Het onderzoeken en verkennen van samenwerkingsmogelijkheden voor

het uitwisselen van ontwikkelingen en ervaringen zou centraal moeten staan. Zo staat Nederland binnen Europa bekend om zijn cryptografische kennis en -toepassingen. We kunnen van elkaar leren en daarnaast de volgende stap zetten, dit is het realiseren van de concrete producten en diensten ten behoeve van de cyberweerbaarheid. De Europese overheden zouden hierin vaker als launching customer op moeten treden en de toegang tot het (investerings)kapitaal moet worden verbeterd.

Versterken van human capital

Voorgaande oplossingen zijn niet uitvoerbaar zonder te werken aan het kwalitatieve en kwantitatieve tekort aan cybersecurity-professionals. Hierover zijn in Nederland al verschillende rapporten (4,5) verschenen en acteert al het ministerie van Economische Zaken, die dit vanuit een multi-stakeholder principe heeft opgepakt. Echter, het welslagen hiervan vraagt ook politiek commitment én voldoende investeringsbereidheid. Dit is geen uitsluitend Nederlands probleem, want dit speelt wereldwijd. Investeren in digitale geletterdheid bij onze kinderen is hierbij een begin. Voldoende onderzoeks- en innovatiemiddelen om het talent hier te houden, in plaats van aan de overzijde van de grote oceaan, is een andere vereiste. Immers, toegang tot talent is en blijft een cruciale voorwaarde voor veiligheid om gelijke tred te houden met veranderende bedreigingen en tegelijkertijd economische kansen in een digitaliserende samenleving tot volle wasdom te brengen.

Referenties

- (1) https://commission.europa.eu/topics/eu-competitiveness/draghi-report_en
- (2) <https://fd.nl/politiek/1542754/het-oude-model-van-open-grenzen-werkt-niet-meer-als-de-wereld-voor-iets-anders-kiest>
- (3) <https://publications.tno.nl/publication/34642268/o5remY/TNO-2024-R10300.pdf>
- (4) https://intgovforum.org/en/filedepot_download/56/28580
- (5) <https://www.rijksoverheid.nl/documenten/rapporten/2024/05/15/bijlage-onderzoeksrapport-adviesrapport-onderwijs-en-arbeidsmarkt-cybersecurity-ptvt>



COLUMN PRIVACY

Mr. Rachel Marbus

Genderen is nergens voor nodig

Wie bovenstaande kop leest, krijgt gezien alle politieke stemmingmakerij rondom genders van mensen, vast de indruk dat dit een bijzonder activistische column gaat worden. "Transrechten zijn mensenrechten!", hoort u mij in gedachten al roepen. En het schepje daarbovenop: "Een transvrouw is een vrouw en een transman is een man!". Nu is dat allemaal reuze waar, maar daar gaat deze column helemaal niet over. Deze column gaat namelijk over dataminimalisatie en wat het Europese Hof van Justitie daarvan vindt.

Wat wil het geval? De Franse spoorwegvervoerder (SNCF) biedt klanten de mogelijkheid om online een kaartje te kopen. Daarbij is het verplicht om in te vullen of je aangesproken wilt worden met 'meneer' of 'mevrouw'. Nu kun je van alles vinden over het feit dat dit al weinig inclusief is, maar ook daar gaat het in dit geval niet over. De Franse belangenvereniging Mousse beklagde zich bij de spoorwegvervoerder: het zou geheel overbodig zijn om hier überhaupt naar te vragen en daarmee in strijd met de AVG en het dataminimalisatiebeginsel. SNCF wilde daar niet van horen en wees de klacht af. De gang naar de rechter volgde.

Het Europese Hof boog zich over de zaak en toetste of het vragen naar dergelijke gegevens objectief noodzakelijk is om het kaartje te kunnen kopen, en dat vindt het Hof niet het geval. "the Court finds that personalisation (...) based on presumed gender identity (...) does not appear to be objectively indispensable in order to enable the proper performance of a rail transport contract". Met andere woorden: wie met de trein wil reizen, moet dat kunnen doen zonder allemaal persoonlijke gegevens te delen.

Het Hof voegde eraan toe dat het niet moeilijk is om op een genderneutrale en inclusieve manier te communiceren en dat een vooronderstelde genderidentiteit helemaal niet nodig is als je tegen een klant praat. In Nederland weten we dat natuurlijk al wel een tijdje langer. Wie weleens met de trein reist, hoort daar al sinds 2017 de woorden "beste reiziger", NS riep toen al andere vervoerders op dit voorbeeld te volgen. De toenmalig president-directeur sprak daarbij de woorden: "Onze mensen op de trein willen graag dat iedereen zich welkom voelt. (...) Iedere reiziger is ons even lief."

En ik herhaal graag het eerst gehoorde 'nieuwe' omroepbericht: *Beste reiziger, dit is een genderneutraal bericht. De trein is beschikbaar voor ieder mens met een geldig vervoerbewijs, ongeacht geslacht en genderidentiteit en of die nu met elkaar in overeenstemming zijn of niet. Of u zich nu mannelijk voelt of vrouwelijk of iets er tussenin, de NS rijdt voor alle mensen. Zoals u weet zijn de toiletten in de trein al jaren genderneutraal. Zo willen wij u voortaan ook aanspreken.*

Rachel



Auteur: Richard Kerkdijk is Senior Cybersecurity Consultant werkzaam zijnde bij TNO en hij is bereikbaar via richard.kerkdijk@tno.nl



OPEN SOURCE

COSSAS

Een open-source community voor security tech transfer

Cybersecurity-innovatieprojecten resulteren met enige regelmaat in experimentele (proof-of-concept) software-oplossingen die ook van waarde kunnen zijn voor partijen die niet direct bij de ontwikkeling betrokken zijn geweest. Dit is zeker het geval voor software die automatisering van operationele securityprocessen faciliteert. Enerzijds omdat dit een belangrijk thema is voor SOC-, CERT- en CTI-teams en anderzijds omdat deze teams vaak voortdurend op zoek zijn naar vernieuwing van hun instrumentatie. Het COSSAS (Community for Open Source Security Automation Software) initiatief is in 2021 door TNO gelanceerd om conceptuele software voor cybersecurity-automatisering structureel als open source aan geïnteresseerde security professionals beschikbaar te stellen. Deze specifieke vorm van technology transfer heeft vooral als doel om (door-) ontwikkeling en adoptie van vernieuwende oplossingen voor cybersecurity-automatisering te stimuleren.

De waarde van open source

Open source software – software waarvan de broncode publiek beschikbaar wordt gesteld en die door iedereen kan worden bekeken, verbeterd en gebruikt – speelt een belangrijke rol in de ontwikkeling van moderne technologie. Studies wijzen uit dat veel software-oplossingen voor een aanzienlijk deel uit open source code bestaan en dat open source initiatieven een belangrijk effect hebben op de mondiale economie (1). Ook TNO zet in toenemende mate in op open source, met name omdat hiermee het bereik en de maatschappelijke impact van haar technologische innovaties aanzienlijk wordt vergroot. Van oudsher werd proof-of-concept software die voortkwam uit innovatieprojecten uitsluitend met de direct betrokken partijen gedeeld. Door het als open source aan een breder publiek beschikbaar te stellen, wordt zowel verdere doorontwikkeling als de daadwerkelijke operationele toepassing beter geborgd. Voor TNO is open source dan ook vooral een instrument om innovatie en open samenwerking te stimuleren.

Het COSSAS initiatief

Automatisering van (operationele) cybersecurityprocessen is voor TNO een belangrijk innovatiegebied waaraan in verscheidene (nationale en Europese) projecten wordt gewerkt. Het COSSAS-initiatief dient als kanaal om hieruit resulterende (vernieuwende) softwarecomponenten met een breder publiek van cybersecurityprofessionals te delen. Als vertrekpunt is van twee belangrijke principes uitgegaan:

- Thematische focus. Het succes van open source wordt ultimo gemaakt door een actieve community van professionals die de software omarmt en actief bijdraagt aan verdere ontwikkeling. Een specifieke en consistente focus op automatisering van cybersecurityprocessen bakent deze community eenduidig af, in dit geval naar een doelgroep van SOC-, CERT- en CTI-professionals. Dit bevordert de mogelijkheden voor gerichte communicatie en community ontwikkeling.
- Eenduidige kwaliteitsgaranties. Om aantrekkelijk te zijn voor ontwikkelaars en eindgebruikers moeten softwarecomponenten die vanuit COSSAS worden vrijgegeven aan consistente kwaliteitsvereisten voldoen. Daarbij gaat het niet alleen

om de kwaliteit van de daadwerkelijke code, maar ook om ondersteuning van relevante open standaarden en beschikbaarheid van bruikbare en actuele documentatie. Op een dergelijke quality assurance wordt gericht gestuurd.

De kwaliteit van COSSAS-software wordt gereguleerd met een zogeheten Continuous Integration (CI-)pipeline die geautomatiseerde controles op veiligheid en bouwkwaliteit omvat. Deze pipeline omvat een breed palet aan erkende (eveneens als open source beschikbare) scan- en evaluatietools waaraan vastomlijnde (minimaal te behalen) metrics zijn gekoppeld. Een softwarecomponent (of wijziging daaraan) wordt slechts vrijgegeven als alle controles met succes zijn doorlopen.

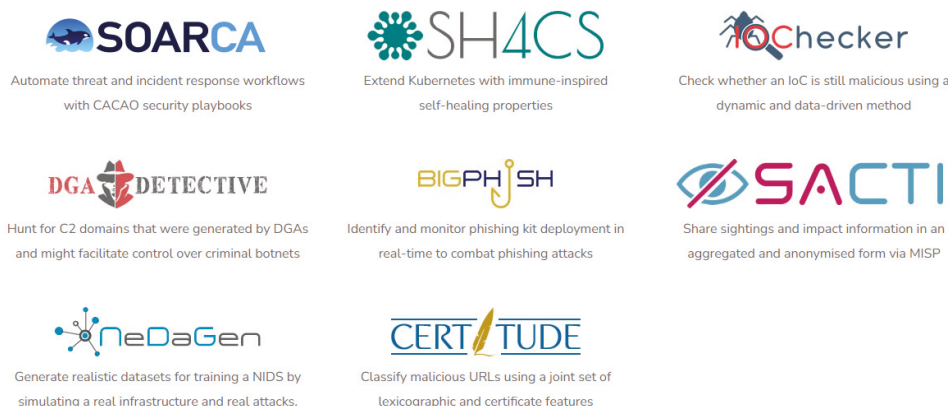
Het softwareportfolio

Een belangrijk kenmerk van het COSSAS-initiatief is dat het niet één specifieke software-oplossing maar juist een almaar groeiend portfolio van softwarecomponenten onderhoudt. In de regel zijn dit geen volledig uitontwikkelde software-oplossingen maar innovatieve bouwblokken waarmee geïnteresseerde professionals in hun eigen werkomgeving kunnen experimenteren. Bij de lancering zijn al meteen vier softwarecomponenten vrijgegeven en inmiddels bestaat het portfolio uit acht open source componenten voor cybersecurity-automatisering (zie figuur). De intentie is om dit de komende jaren nog verder uit te breiden. Elke softwarecomponent wordt zowel op GitHub als op GitLab (de twee grootste online ontwikkelplatformen voor open source software) gepubliceerd. Verder wordt op de COSSAS-website van elke softwarecomponent een showcase pagina onderhouden met achtergrondinformatie, technische documentatie en verwijzing naar relevante artikelen, webinars en demonstratievideo's.

Het succes van open source

Een prominent en succesvol voorbeeld van een COSSAS open source release is SOARCA, een open security orchestrator (ook wel SOAR) die TNO (mede) in Europees onderzoek heeft ontwikkeld. SOARCA ondersteunt cyber incident response processen door de hiertoe gedefinieerde workflows (vastgelegd

COSSAS: een open-source community voor security tech transfer



Figuur: Huidig COSSAS softwareportfolio

in cybersecurity playbooks) geautomatiseerd uit te voeren. SOARCA onderscheidt zich van veel marktproducten doordat het gestandaardiseerde formats en technologieën ondersteunt (waaronder de technologieën CACAOv2 (2) en OpenC2 (3), beide gespecificeerd door OASIS Open) en naar behoefte aanpasbaar is (bijvoorbeeld voor onderzoeksdoel-einden). SOARCA kreeg al snel na de lancering aandacht uit binnen- en buitenland en is inmiddels met een aantal aanpa-lende (open source en commerciële) software-oplossingen geïntegreerd (4). Deze mate van tractie en adoptie was bij een gesloten ontwikkelmodel niet mogelijk geweest en SOARCA onderstreept dan ook nadrukkelijk de potentie van open source als instrument om het bereik van nieuwe technologie aanzienlijk te vergroten.

De ambitie

COSSAS beoogt een duurzaam platform en een herkenbare brand voor open source cybersecuritysoftware te bieden. Daartoe wordt bewaakt dat de onderliggende projecten actief worden onderhouden en dat contributies en suggesties tijdig in behandeling worden genomen. Het grotere doel is zowel de (door-)ontwikkeling als de daadwerkelijke inzet van vernieu-wende software voor cybersecurity-automatisering een positieve impuls te geven. Ook richting de toekomst zullen daarom met enige regelmaat nieuwe softwarecomponenten aan het portfolio worden toegevoegd. Daarnaast is de ambitie om de community van analisten, onderzoekers en ontwikkelaars rondom COSSAS verder te verstevigen. Het laatste vraagt tijd en aandacht, maar bepaalt voor deze vorm van technology transfer uiteindelijk wel het succes.

Referenties

- (1) Manuel Hoffmann, Frank Nagle en Yanuo Zhou, The Value of Open-Source Software, Harvard Business School, januari 2024
- (2) OASIS Open, CACAO Security Playbooks v2.0
<https://www.oasis-open.org/standard/cacao-security-playbooks-v2-0/>
- (3) OASIS Open, Open Command and Control (OpenC2) Language Specification Version 2.0
<https://docs.oasis-open.org/openc2/oc2ls/v2.0/oc2ls-v2.0.html>
- (4) Onder meer met de open source playbook editor CACAO Roaster (5) die sterk complementair is aan de SOARCA-tool.
- (5) Open Cyber Security Alliance, CACAO Roaster (playbook editor tool)
<https://github.com/opencybersecurityalliance/cacao-roaster>

Meer informatie

COSSAS-website

<https://cossas-project.org/>

COSSAS op GitHub

<https://github.com/COSSAS>

COSSAS op LinkedIn

<https://www.linkedin.com/company/cossas>

dcypher meetup over open-source software en COSSAS-lancering

<https://www.youtube.com/watch?v=C8B6cLK7GzE&t=106s>

Digitale oplichting: waarom zélf bewust bekwaam niet immuun maakt

Je denkt dat je het doorhebt. Dat jij weet hoe digitale oplichting werkt. Tot het jou overkomt; snel, geraffineerd, als je even niet oplet. Dat is het probleem: bewustzijn en bekwaamheid zijn geen garantie. Sterker nog, zelfs wie bewust bekwaam is, is niet immuun. Jaren geleden schreef ik, als onderdeel van mijn proefschrift, over het fundamentele verschil tussen bewustzijn en bekwaamheid. De bekende ladder van bekwaamheid beschrijft hoe mensen zich ontwikkelen van onbewust onbekwaam naar bewust bekwaam: een traject van groei door oefening en ervaring.

Hoewel dit model op veel terreinen werkt, geloof ik dat het op het gebied van digitale oplichting een hardnekkige misvatting in stand houdt: dat bewustzijn en bekwaamheid automatisch leiden tot betere bescherming. Ik ben geen tegenstander van bewustwordingscampagnes. Ze zijn waardevol, maar moeten wel beoordeeld worden op hun effectiviteit. In de tijd van man-in-the-middle-aanvallen en drive-by downloads wapent bewustzijn op zichzelf gebruikers onvoldoende. Die dreigingen waren onzichtbaar, en daarmee moeilijk of zelfs onmogelijk te herkennen, ook voor wie bewust was van het risico.

Nu zie ik diezelfde valkuil opnieuw, met nog verfijndere middelen. Generatieve AI kan stemmen felloos nabootsen en gezichten overtuigend imiteren. Toch verwachten we van gebruikers dat zij het echte van het neppe onderscheiden. Dat is niet alleen onrealistisch, het is onhoudbaar. Veel mensen zijn onvoldoende bewust en toegerust om digitale dreigingen te begrijpen of te herkennen. Criminelen spelen daar geraffineerd op in. Ze combineren urgentie, subtiele sociale druk en emotionele manipulatie tot een cocktail waar zelfs de meest alerte gebruiker moeite mee heeft.

In het eerste kwartaal van dit jaar ontving de Fraudehelpdesk bijna 10.000 meldingen van neptelefoontjes, drie keer zoveel als in dezelfde periode vorig jaar. Maar confronterender is het besef dat niemand onaantastbaar is. Ook ik niet. Het tweede bericht van de Fraudehelpdesk lezende over oplichting rond het nieuwe Britse reisdocument, de ETA, voelde ik een pijnlijke herkenning. Wie via Google zoekt naar een ETA, komt al snel op websites van tussenpartijen die veel geld vragen zonder duidelijk te maken dat ze geen officiële instantie zijn. Zelf ben ik op soortgelijke wijze misleid bij het aanvragen van een ESTA voor de VS. Ik was druk, wilde het snel regelen, en klikte akkoord zonder echt te controleren met wie ik zaken deed. En dat terwijl ik mezelf als bewust én bekwaam beschouw. Maar zelfs dan ben je niet immuun—zeker niet op momenten van haast of verminderde alertheid.

En daar zit precies het probleem: het is niet redelijk om te verwachten dat gebruikers altijd scherp en waakzaam zijn. Niet alleen omdat mensen nu eenmaal fouten maken, maar omdat onzichtbare dreigingen bestaan. Ik zag niet welk bedrag ik goedkeurde, de oplichting zat subtiel verstopt in de interface. En bij een nagebootste stem of overtuigend nepverzoek is er soms niets te zien of horen om alarm te slaan. Je moet het doen met je intuïtie, met vage signalen: de toon van een bericht, de timing van een verzoek, een onderbuikgevoel dat iets niet klopt, maar dat is een oneerlijke opgave. Het vraagt van mensen dat ze elke dag, op elk moment, in elke context, op hun scherpst zijn—terwijl de aanvaller maar één moment nodig heeft waarop jij het níet bent. Wat je niet kunt waarnemen, kun je ook niet weren. Zo simpel is het.

Dr. Nicole van der Meulen is expert op het gebied van cybersecurity en emerging technologies en werkzaam bij SURF als Cybersecurity Innovation Lead, ns.vandermeulen@gmail.com



Cyber Tech: van Dark Web naar BigPhish

In 2013 maakte ik, Mark van Staalduinen, destijds onderzoeker bij TNO en nu Managing Director van CFLW Cyber Strategies (CFLW), voor het eerst kennis met het Dark Web. Dit is dat deel van het internet waar men in technische anonimiteit kan opereren. De onderliggende encryptietechnologie is essentieel voor internet toegang in landen met minder vrijheden dan de onze, maar ook een technologie die wereldwijd door criminelen wordt misbruikt voor illegale doeleinden.

Binnen TNO waren we een Dark Web-programma gestart dat later is opgenomen in het cybercrime-programma. Rond 2014 is een eerste concept van de Dark Web Monitor ontwikkeld, waarmee we probeerden een breed inzicht te krijgen in alle Onion-services. Dit zijn websites die binnen het Tor-netwerk bestaan en die zonder IP-adres te bereiken zijn, waardoor de locatie van de servers onbekend blijft. Sommige websites groeiden uit tot platforms waar onder andere: drugshandel plaatsvindt, kindermisbruikbeelden worden gedeeld of ransomwaregroepen gestolen gegevens lekken. Deze laatste groep is de angst van iedere professional op het gebied van informatiebeveiliging, omdat in het ergste geval gevoelige gegevens op het Dark Web terechtkomen. Helaas wordt Tor-technologie vandaag de dag nog steeds veelvuldig misbruikt voor dergelijke illegale doeleinden.

Dark Web Monitor

Dark Web Monitor is beschikbaar als product via CFLW, een spin-out van TNO die in 2019 werd opgericht. Na stevige onderhandelingen met TNO werd het proces gestart om de proof of concept om te zetten in een product dat handelingsperspectief biedt aan verschillende diensten. Het primaire gebruik van deze operationele cybertechnologie is voor politie en justitie, maar ook verschillende use cases buiten de justitiële keten worden ondersteund. Denk aan het kwalificeren van Bitcoin-adressen op basis van de illegale context waarin ze worden aangetroffen.

Launching Customer

Met de steun van onze launching customer: het Openbaar Ministerie Beieren (Zentralstelle Cybercrime Bayern, ZCB) en TNO is de Dark Web Monitor doorontwikkeld tot operationele technologie. In die fase is het concept zelf niet veel veranderd, maar moest alles schaalbaar worden gemaakt en moest er een businessmodel worden ontwikkeld. Dat hebben we in nauwe samenwerking gedaan. Onze launching customer realiseerde zich heel goed dat deze technologie eigenlijk beschikbaar moet zijn voor elke digitaal of cyber rechercheur. Daarom hebben we een flat fee-model ontwikkeld, waarbij alle gebruikers binnen één organisatie met één overeenkomst toegang krijgen en niet alleen de "happy few". Die nauwe samenwerking loont. Steeds meer organisaties sluiten licentieovereenkomsten voor meerdere jaren af. Ondertussen gebeurt dit wereldwijd in meer dan 20 landen: van Azië tot een federale instantie in de VS waarmee we sinds vorig jaar een overeenkomst van vijf jaar hebben.

BigPhish

Naar aanleiding van het succes van Dark Web Monitor heeft TNO ons gevraagd om een vergelijkbaar traject te starten voor BigPhish. Dit is een anti-phishingtool die ingrijpt in de economische principes die criminelen hanteren in hun phishing praktijken en die door de inzet van deze technologie verstoord kan worden; zeker als deze technologie wereldwijd wordt ingezet. Momenteel werken we dagelijks hard aan de omzetting naar operationele technologie. Tegelijkertijd worden de eerste operationele successen al geboekt door nauwe samenwerking met onze launching customer.

Lessons learned

- Proof of Concept is geen product. Het proof of concept is het essentiële resultaat van onderzoek en innovatie. Het technisch schaalbaar maken, het ontwikkelen van de markt en businessmodellen zijn essentieel. Die vervolgstappen vereisen dan ook andere vaardigheden, zoals: ondernemerschap en sustainable software development.
- Co-creër samen met een launching customer: operationele requirements zijn essentieel, daarnaast ontvangt een launching customer een product dat veel meer in lijn is met zijn wensen: win-win.
- Intellectueel eigendom is en blijft een grote uitdaging. Als concepten voor nationale veiligheid zijn ontwikkeld met belastinggeld, dan is het ethisch onverantwoord om alleen te focussen op intellectuele eigendomsrechten, maar brengen deze rechten ook verplichtingen met zich mee. Bijvoorbeeld inzet om het concept daadwerkelijk op het bureau van de veiligheidsprofessionals te krijgen. Het open source platform COSSAS is een uitstekende route voor technologie transfer en uniek in Europa!

Conclusie

Tot slot is het natuurlijk prachtig om nieuwe overeenkomsten te ontvangen vanuit nieuwe landen of organisaties. Maar wat we nog meer waarderen is wanneer we op de hoogte worden gebracht van operationele successen, waarbij onze technologie een sleutelrol heeft gespeeld. Dat motiveert ons het meest om onze techniek elke dag verder te verbeteren!

Cybersecurity en informatiebeveiliging worden de komende jaren door alle nieuwe technologieën en tegelijkertijd steeds specifiekere regelgeving eerder complex dan eenvoudiger. Laten we samen werken aan nieuwe security producten, op basis van degelijk onderzoek, die Nederland veiliger maken en tegelijkertijd internationaal economische waarde creëren.



Auteur: Prof. dr. Martijn Dekker, ABN AMRO Bank, werkzaam als CISO.
Hij is bereikbaar via: martijn.dekker@nl.abnamro.com



Security en Innovatie:

geen tegenspraak, maar noodzaak!

We leven in een wereld waar ontwikkelingen steeds sneller gaan. Nieuwe technologieën, nieuwe producten en processen, nieuwe verwachtingen of nieuwe eisen van gebruikers en nieuwe businessmodellen vragen hoge wendbaarheid van organisaties. Beveiligers weten dat elke effectieve securitystrategie moet aansluiten bij de strategie van de organisatie. Dit betekent dat snelheid en proactiviteit dus ook belangrijke pijlers zijn van die securitystrategie. Naast aansluiting op de business strategie, is het dreigingslandschap de andere bepalende factor in de securitystrategie en daar zien we ook een verhoging van snelheid, vernieuwing en volatiliteit.

Hoe ga je als CISO om met snelheid, vernieuwing, en onbekende uitkomsten terwijl je tegelijkertijd moet opereren in een strak georganiseerde operatie waar budgetten en uitkomsten scherp geformuleerd dienen te zijn? De genoemde ontwikkelingen dwingen securityleiders innovatief te zijn en vaak “early-adoptors” van nieuwe technologie.

Innovatie combineren met de strakke beheersing, die veel organisaties vragen, is lastig. Er zijn meerdere verschillen te overbruggen. We noemen er drie: het omgaan met snelheidsverschillen tussen de partijen die samenwerken, het feit dat innovatie onbekende uitkomsten heeft waar organisaties graag sturen op een goed gedefinieerde uitkomst, en het feit dat innovatie bijna per definitie gepaard gaat met het gebruiken van technologie die nog niet bewezen is. We zullen zien dat hiervoor volwassen leiderschap nodig is dat in staat is risico afwegingen te maken die een hoge mate van onzekerheid kennen in zowel kans als impact. Dit is een uitdaging voor securityleiders, want het vergt relatie en moed. Het vergt relatie omdat het risico-acceptatie en budgetallocatie betreft, en dus een goede relatie met bestuurders benodigd. Het vergt moed omdat een risico genomen moet worden door een leider die als doel heeft risico te beheersen.

Verskillende snelheden

Er is een verschil tussen wendbaarheid en snelheid. In het algemeen kan gesteld worden dat onderzoekscentra, startups en uitvinders hogere wendingsnelheid hebben en veel organisaties en bedrijven hogere voortgangssnelheid. Onderzoekers zijn wendbaarder dan commerciële organisatie of publieke organisaties van enige omvang. Iets is wendbaar als er snel koers gewijzigd kan worden en als er gemakkelijk gereageerd kan worden op nieuwe informatie. Juist bij innovatie is wendbaarheid dus nuttig, en ook mogelijk, want er is vaak geen vooraf vastgesteld doel en koersvastheid is dan niet nodig. Voortgangssnelheid is de snelheid waarmee de organisatie draait, de kloksnelheid en de efficiëntie. Organisaties met goede interne beheersing of bedrijven met grote commerciële belangen, of urgentie voor “time to market”, hebben vaak een hoge voortgangssnelheid. Die is ook nodig om te kunnen blijven concurreren.

Om te innoveren in een organisatie moet een goede mix gevonden worden van deze twee soorten snelheden, ofwel van wendbaarheid en voortgang. Voortgang in de organisatie komt vaak voort uit strak georganiseerde processen en hoge mate van standaardisering. Om wendbaarheid te verhogen, moeten deze omgevingsfactoren aangepast worden, en dit

Om te innoveren moeten securityleiders leren om te gaan met de onzekerheden die dit met zich meebrengt

introduceert risico. Zo moeten bijvoorbeeld afwijkingen van standaard technologieën of standaardprocessen worden toegestaan. Ook kan het nodig zijn om een ontkoppeling toe te staan tussen de standaard IT-omgeving en de “innovatie omgeving” van de organisatie. Dit introduceert extra kosten. Besluiten over kosten en risico’s worden vaak hoog in een organisatie genomen, en als securityleiders willen innoveren, moeten zij dus in een positie zijn om die besluitvorming te beïnvloeden. Dit kan een positie in de hiërarchie van de organisatie zijn, met bijbehorende mandaten, of een positie die invloed op besluitvorming geeft. Reputatie en relaties spelen dus een minstens zo belangrijke rol als rapportagelijijn. Onderzoekers zullen op hun beurt hun partners en bedrijven waar ze mee samenwerken, een mate van transparantie en besturing moeten gunnen. Het publiceren van wetenschappelijk werk kan jaren duren en dat is een termijn die voor bedrijven onacceptabel is omdat zij vaak in termen van maanden of kwartalen plannen. Transparantie over tussenresultaten en bestuurbaarheid van tussenstappen is dus nodig, waarbij de samenwerkende partijen oog moeten hebben voor elkaars belangen.

Onbekende uitkomsten

Naast snelheidsverschillen zijn uitkomstenverschillen een andere kloof die een innovatieve securitystrategie moet overbruggen. Uitkomsten van innovaties zijn vaak vooraf onbekend en het is daarom ook onbekend wanneer iets geleverd zal worden of tegen welke kosten. Ook kan het zijn dat gedurende het proces, andere mensen en vaardigheden gevraagd worden dan eerder gedacht. Dit vereist een besturing die anders is dan het besturen van veel andere processen en vergt een andere stijl van leiderschap. Hier is moed voor nodig. Bestuurders verdelen schaarsen zoals aandacht, tijd en andere middelen binnen hun portefeuille en met andere bestuurders. Iedereen herkent het fenomeen dat een idee dat uitlegbaar en concreet is, sneller prioriteit krijgt dan een idee dat vaag is of ongrijpbaar. Om bij schaarheid, allocatie van middelen te verkrijgen voor vage

security-innovatie ideeën, helpt een sterke reputatie van de securityleider. Andere bestuurders moeten namelijk vertrouwen hebben in de visie, expertise en executiekracht van de securityleider. Het opbouwen van die reputatie kost moed en tijd of het vraagt sterke rugdekking van de hogergeplaatste. Een effectieve manier om geloofwaardig innovaties te starten is samenwerking met een erkende innovatieve organisatie zoals een universiteit, TNO of een commercieel bedrijf met innovatieve reputatie met bewezen methodologieën. Aan dergelijke partnerships kan de securityleider onmiddellijk geloofwaardigheid en moed ontfangen voor een innovatieve securitystrategie.

Adoptie van onbewezen technologie

Als een idee na testen en ontwikkeling vruchtbaar blijkt, wordt het een innovatie als het daadwerkelijk geïmplementeerd en gebruikt wordt. Tijdens de ontwikkeling van een idee kijkt men veelal alleen naar functionaliteit. “Technology adoption” is lastig omdat dan ook operationele zaken als schaalbaarheid, integratie, interoperabiliteit en prestaties een rol gaan spelen. Ook zal niet langer de ontkoppeling tussen de innovatie-omgeving en de standaard IT-omgeving benut kunnen worden en zal er in de staande organisatie een “eigenaar” van het nieuwe product of systeem benoemd moeten worden. De acceptatieprocessen van een nieuw systeem kennen vaak criteria, die op gespannen voet staan met de aard van een innovatief systeem; zoals criteria voor beheersbaarheid en bekendheid van de onderliggende technologie. Vaak zijn dit criteria die nota bene door de securityleider zelf zijn opgesteld. Ook kan het ‘not invented here’ syndroom een rol spelen bij de mate van acceptatie van de nieuwe oplossing. Een voortvloeisel daarvan dat veel innovaties ontstaan in een ontkoppelde omgeving en daarmee door sommigen gezien worden als “externe” ontwikkelingen. Net zoals in de vorige twee secties, is hier doorzettingskracht van de securityleider nodig om de weerstand te overwinnen. Doorzettingskracht kan bijvoorbeeld voortkomen uit effectief managen van relaties en

verwachtingen. Relatie en moed geven doorzettingsmacht, maar ook sterke positiemacht kan natuurlijk helpen. Het is belangrijk dat een securityleider op een geloofwaardige manier effectief kan beïnvloeden dat nieuwe en onbewezen technologieën toch geïmplementeerd worden, omdat het de veiligheid van de organisatie juist vooruithelpt.

Portfolio en personeel

In de portfolio van activiteiten en projecten van een CISO zitten altijd werkzaamheden die nodig zijn om aan wet- en regelgeving te voldoen. Ook zijn er altijd zaken die direct invulling geven aan business prioriteiten en waar er een duidelijk vragende partij voor is. Voor veel innoverende trajecten is er vaak geen andere vragende partij dan de securityorganisatie zelf. En voor deze onderwerpen geldt dat er de optie is om het niet te doen: er zal dan niet direct een probleem ontstaan in de organisatie. Het is belangrijk om te borgen dat innovatie toch altijd onderdeel is van de portefeuille. Innovatie is nodig, zoals gezegd, om het snel veranderende dreigingslandschap bij te benen en om proactief te kunnen zijn in de ondersteuning van de business strategie van het bedrijf. Het is de rol van de CISO om security-innovatie te prioriteren, juist omdat niemand anders dat zal doen.

Een andere belangrijke reden om security-innovatie altijd een plek te geven, is dat consequent blijven innoveren, de security-afdeling een sterke reputatie en positie geeft én daarmee helpt met het aantrekken en vasthouden van talent(en). Er is een groot tekort aan security experts in de arbeidsmarkt. Het werken aan een sterke reputatie als vernieuwende organisatie helpt om medewerkers aan te trekken. Maar minstens net zo belangrijk is de bijdrage die een dergelijke, sterke security-organisatie levert aan de arbeidsmarkt doordat haar medewerkers, juist door te kunnen werken aan vernieuwing, zich ontwikkelen en beter worden. Een innoverende CISO beveiligd zo niet alleen de eigen organisatie maar levert ook een grote bijdrage aan de veiligheid van de maatschappij.

Conclusie

Om een effectieve securitystrategie uit te voeren in de snel veranderende omgeving waarin organisaties zich tegenwoordig bewegen, is innovatie een onmisbaar element. Om te innoveren moeten securityleiders leren om te gaan met de onzekerheden die dit met zich meebrengt. Ook zullen zij de nodige middelen moeten weten te verkrijgen door effectief relatiemanagement en het opbouwen van een sterke reputatie als moedige leider met visie. CISO's moeten zich steeds meer manifesteren als volwassen en strategische senior leiders in de organisatie. Dit kan doordat hier stapsgewijs, en over een langere periode consequent aan gewerkt wordt, of het kan door het aangaan van partnerships met partijen die dit al bewezen hebben. En dat laatste is goed nieuws. Innovatie in het security domein is noodzakelijk maar lijkt soms haaks te staan op de beheersing en controle focus die het security domein kenmerkt. Samenwerking is juist een van de sterkste eigenschappen van de securitygemeenschap, waarbij securityleiders gewend zijn om met anderen, voorbij de grenzen van hun eigen organisatie, samen te werken.

Innovatie in security is noodzakelijk. Het is geen tegenspraak met de doelen van controle en beheersing, maar juist een katalysator daarvan. Samenwerking met anderen of deelname in innovatiepartnerships is daarom een onmisbaar element in elke effectieve securitystrategie. Voorbeelden van dergelijke partnerships en platforms zijn Partnership for Cyber Security Innovation (PCSI), AMSec of dCypher. Nadat securityleiders zijn gaan beseffen dat absolute veiligheid niet bestaat, hebben ze risicomanagement toegevoegd aan hun strategieën. Om het hoofd te bieden aan de snelle, veranderende wereld en dreigingen, is het tijd om de onzekerheden van innovatie te omarmen. Ze beveiligen daarmee niet alleen de eigen organisatie, maar dragen ook bij aan een veiliger samenleving.



Auteur: Folkwin Poelman is werkzaam als Programmacoördinator bij NCC-NL. Hij is bereikbaar onder folkwin.poelman@rvo.nl



Security tech transfer en Europa?

Vanuit Europa is er veel geld beschikbaar voor onderzoek, ontwikkeling en implementatie voor cybersecurity. Er is een duidelijke behoefte om een sterke, Europese cybersecuritysector te creëren. In theorie zou de combinatie van kapitaal en deze ambitie het gat van de security tech transfer moeiteloos moeten opvullen. Toch blijkt in de praktijk dat veelbelovende innovaties stranden voordat ze tot daadwerkelijke implementatie en brede opschaling leiden. Om deze kloof te overbruggen, is niet alleen financiering nodig, maar ook toegang tot netwerken en expertise die implementatie en opschaling ondersteunen. Wat is er nodig om dit proces te versnellen en welke ondersteuning is hiervoor beschikbaar?

Europese fondsen en stimulering

Hoewel er meerdere Europese fondsen zijn met daarin vele miljarden ligt de focus voor cybersecurity voornamelijk binnen Horizon Europe en het Digital Europe Programme (DEP). Horizon Europe financiert voornamelijk onderzoeks- en innovatieprojecten en richt zich op de lagere TRL's. Het Digital Europe Programma financiert projecten in de hogere TRL's en is erop gericht de stap te maken naar implementatie en opschaling. Daarmee is Digital Europe potentieel een krachtig instrument om de kloof in security tech transfer te overbruggen, maar hoe kan je die potentie benutten als Nederlandse private of publieke organisatie? En welke ondersteuning is daarvoor beschikbaar?

Naast financiering speelt ook beleidsontwikkeling een grote rol in de mogelijkheden voor cybersecurity-innovatie. Europese wetgeving, subsidieprogramma's en prioriteiten veranderen voortdurend en het is belangrijk dat Nederlandse partijen goed op de hoogte blijven en actief inspelen op deze ontwikkelingen.

Om organisaties binnen Europa te ondersteunen bij het ontwikkelen en implementeren van cybersecurity-oplossingen heeft de Europese Unie in 2021 het **European Cybersecurity Competence Center (ECCC)** opgericht. De doelstelling van het ECCC is om cybersecurity-innovatie te stimuleren om daarmee een sterke en competitieve Europese cybersecuritysector te creëren. Het ECCC wordt hierbij ondersteund door een netwerk van Nationale Coördinatie Centra (NCC's). Elke Europese lidstaat, ook Noorwegen en IJsland, heeft een NCC. Deze zijn herkenbaar aan de landencode; in Nederland is dat dus NCC-NL. NCC-NL staat met één been in Nederland en met het andere been in Europa. Het ECCC en het netwerk van NCC's richten zich niet op de cybersecurity van vandaag, maar stimuleren juist de ontwikkeling en implementatie van de oplossingen voor overmorgen. Sinds eind 2024 is het ECCC formeel verantwoordelijk voor het werkprogramma Cyber van het **Digital Europe Programme (DEP)**.

Europese beleidsontwikkelingen

We blijven nog even in Europa. In de afgelopen periode zijn er meerdere interessante ontwikkelingen geweest die een positieve invloed hebben op de beschikbaarheid van Europese finan-

ciering voor cybersecurity. In september 2024 werd het Draghi-rapport uitgebracht. In dit rapport geeft Mario Draghi aan wat er nodig is om Europa competitief en veilig te houden en pleit voor meer Europese financiering. Eind november 2024 is de Europese Commissie (EC) onder Ursula von der Leyen geïnstalleerd en bleek dat deze nieuwe Europese Commissie zowel cybersecurity en financiering voor innovatie deel liet uitmaken van de prioriteiten. Dit blijkt ook uit het Competitive Compass, uitgebracht door de EC in januari 2025 waarin invulling wordt gegeven aan de aanbevelingen uit het Draghi-rapport, onder meer om innovatie te stimuleren.

Dat de EC-cybersecurity belangrijk vindt, blijkt ook uit hun twee recente actieplannen. Zo publiceerde de Europese Commissie in januari van dit jaar een actieplan om de cyberweerbaarheid van ziekenhuizen en de gezondheidszorg te vergroten. In februari publiceerde de EC een Joint Action Plan voor veiligheid van onderzeese kabels. Hierin wordt voorgesteld om budget vrij te maken vanuit het Cyber werkprogramma van Digital Europe Programme specifiek voor toepassing in het zeekabel domein.

Ondersteuning

Nu we weten dat er Europees budget beschikbaar is én dat cybersecuriteitspolitiek beleidsmatig de volle aandacht heeft, komt de vraag naar voren hoe Nederlandse partijen dit aan kunnen wenden om de security tech transfer mogelijk te maken. Het eenvoudige antwoord is: dien een projectvoorstel in. Echter, de werkelijkheid is weerbarstiger; wie heeft immers de tijd om continu te monitoren welke financieringsmogelijkheden zich aandienen en of deze aansluiten bij de projectideeën? En als je een geschikte call hebt gevonden, moet je vaak ook nog een grensoverschrijdend consortium vormen alsook natuurlijk een projectvoorstel schrijven en indienen. Daarvoor is ondersteuning nodig en die ondersteuning is er.

Nederlandse organisaties die willen profiteren van Europese financieringskansen kunnen aankloppen bij het **Nederlands Cybersecurity Coördinatie Centrum (NCC-NL)**. NCC-NL biedt bedrijven, kennisinstellingen en publieke organisaties ondersteuning bij het vinden en aanvragen van nationale en Europese

Een effectieve inzet van Europese mogelijkheden om projecten te financieren kan een krachtig instrument zijn om de kloof van de security tech transfer te verkleinen

cybersecuritysubsidies. Daarnaast begeleidt NCC-NL organisaties bij het vormen van consortia voor EU-subsidieaanvragen, zodat zij de juiste samenwerkingspartners vinden voor hun project. Ook kunnen partijen via NCC-NL invloed uitoefenen op de richting van Europese subsidieprogramma's en beleidsontwikkelingen, door deel te nemen aan consultaties en feedbackrondes.

Aan de slag

Voor organisaties die hun oplossingen naar de markt willen brengen, is het cruciaal om vroegtijdig in te spelen op financieringskansen en strategische samenwerkingen. Drie tips om zelf aan de slag te gaan:

- Oriënteer op Europese subsidiemogelijkheden: programma's zoals: Horizon Europe en Digital Europe bieden financiering voor zowel onderzoek en ontwikkeling, maar ook implementatie en opschaling. Up-to-date blijven over nieuwe calls vergroot de kans op een tijdige start en daarmee een succesvolle aanvraag. Via het Cybersecurity Funding Portal kunnen organisaties een overzicht vinden van zowel Europese als Nederlandse subsidies voor cybersecurity-innovaties. De subsidie calls zijn geanalyseerd en worden op het Cybersecurity Funding Portal samengevat, zodat Nederlandse partijen eenvoudiger kunnen beoordelen of een specifieke call relevant is. Het Cybersecurity Funding Portal is ook de ingang om maatwerkadvies te krijgen van adviseurs die een goed beeld hebben van de subsidiemogelijkheden en praktisch advies kunnen bieden voor het vinden van partners en het schrijven van een kwalitatief goede aanvraag.
- Vorm sterke consortia: Europese subsidies vereisen vaak samenwerking tussen bedrijven (ook startups en MKB), onderzoeksinstellingen en publieke organisaties. Door samen te werken in een consortium, kunnen verschillende partijen hun

sterke kanten bundelen. Dit maakt het consortium niet alleen een krachtig middel voor financiële ondersteuning, maar ook een manier om toegang te krijgen tot een breder netwerk van kennis en ervaring. Samen zet je een stap richting projectimplementatie en schaalbaarheid. Deelname aan een consortium building sessie kan helpen om geschikte partners te vinden.

- Draag bij aan Europees beleid en subsidiemogelijkheden: Europese financieringsprogramma's zoals Horizon Europe en Digital Europe worden mede gevormd door input uit de sector. Het Cyber-werkprogramma wordt door het ECCC geschreven en bepaalt de koers voor de komende jaren, dus hoe beter organisaties weten waar zij over een paar jaar willen staan, des te beter kan er op de koers worden bijgestuurd. Door deel te nemen aan consultaties en feedback te geven, kunnen Nederlandse organisaties meedenken over de richting van nieuwe subsidieprogramma's. Hoe beter organisaties hun behoeften en ambities kenbaar maken, hoe beter het Europese beleid aansluit op hun innovatieplannen.

Europa als oplossing?

Een effectieve inzet van Europese mogelijkheden om projecten te financieren kan een krachtig instrument zijn om de kloof van de security tech transfer te verkleinen. Daarvoor is het belangrijk dat Nederlandse organisaties goed bedenken welke ambities zij in de komende jaren hebben om hun oplossingen op een hoger niveau te krijgen en daarmee de stap naar opschaling te zetten. Hoe concreter de plannen zijn, hoe eenvoudiger het wordt om de juiste (Europese) financieringskansen en samenwerkingspartners te vinden. Europa is niet de enige oplossing, maar biedt in toenemende mate kansen om innovaties naar een hoger niveau te brengen en daarmee het gat van de security tech transfer te verkleinen. Er is ondersteuning beschikbaar om de stap te nemen, dus het is tijd om samen die stap te nemen!

Hoe stuur jij op security in de board room?

Kijk op [cisomasterclass.nl](https://www.cisomasterclass.nl) om uit te vinden hoe je daar grip op krijgt en schrijf je in voor de masterclass op 22, 23 en 24 september 2025.

Kennis brengt je naar de top,
skills zetten je aan het stuur!



www.cisomasterclass.nl



info@cisomasterclass.nl



079-360 4268



COLOFON

IB Magazine is het huisorgaan van het Platform voor Informatiebeveiliging (PvIB) en bevat ontwikkelingen en achtergronden over onderwerpen op het gebied van informatiebeveiliging.

HOOFDREDACTEUR

Chris de Vries

REDACTIE

Alex Dingemanse
Marcel Feenstra
Maarten Hartsuijker
Fook Hwa Tan
Lillian Knippenberg
Leo van Koppen
Rachel Marbus
Chris de Vries

BLADMANAGEMENT

Congres- en Organisatiebureau Interactie BV
Zeynep Turkan
ibmagazine@pvib.nl

VORMGEVING

Neverseen Art & Design
Dimitri van den Berg

DRUK

Veldhuis Media, Meppel

UITGEVER

Platform voor Informatiebeveiliging (PvIB)
Horapark 9
6717LZ Ede
+31 85 799 0233
secretariaat@pvib.nl
www.pvib.nl

*Heb je vragen, opmerkingen of
suggesties, mail dan naar
ibmagazine@pvib.nl*

ABONNEMENTEN

De abonnementsprijs in 2025 bedraagt
€ 118,50 (exclusief btw), prijswijzigingen
voorbehouden.

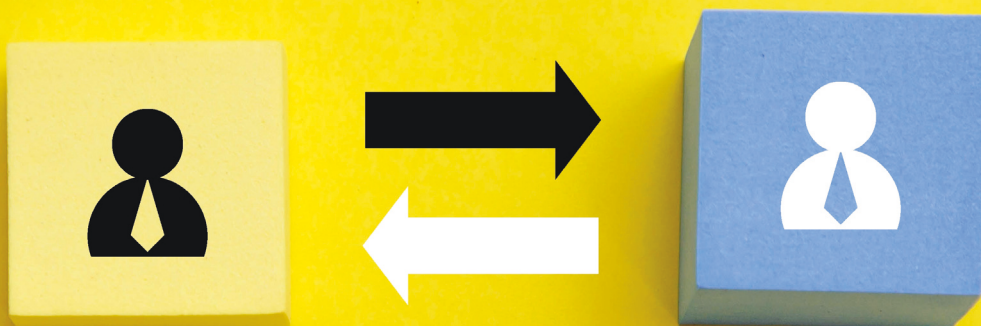
ABONNEMENTENADMINISTRATIE

Platform voor Informatiebeveiliging (PvIB)
Postbus 1058
3860 BB NIJKERK
secretariaat@pvib.nl



Tenzij anders vermeld valt de inhoud van dit
tijdschrift onder een Creative Commons
Naamsvermelding-gelijkeDelen 3.0 Nederland
Licentie (CC BY-SA 3.0)
ISSN 1569-1063

Auteur: Maarten Everts is medeoprichter van het bedrijf Linksight en aldaar actief als Chief Technology Officer. Daarnaast is hij assistent professor in toegepaste cryptografie aan de Universiteit Twente en hij is bereikbaar via: maarten@linksight.nl



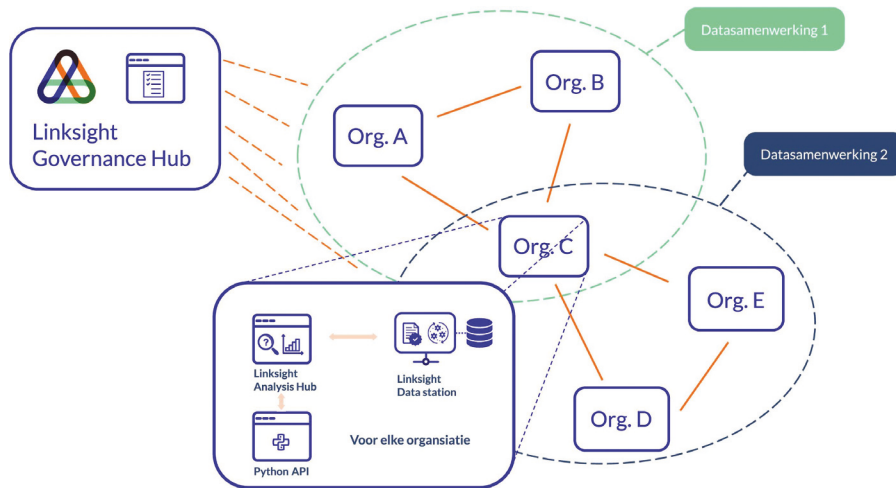
Vergeet de “tech” in “tech transfer”

Nieuwe security innovaties naar de markt brengen door middel van een “tech-transfertraject”, dat klinkt prachtig. Maar hoe werkt dat nou in de praktijk? Maarten Everts, CTO van Linksight, kwam er al snel achter dat voor een startup de focus niet moet liggen op de technologie maar op de toegevoegde waarde voor klanten. In geval van Linksight: datasamenwerkingen met een hoge mate van privacy- en vertrouwelijkheidsbescherming en het behouden van controle over je eigen data.

De technologie

Om die veilige datasamenwerking mogelijk te maken, maken we bij Linksight gebruik van Multi-Party Computation (MPC) en homomorphe vercijfering. Deze vormen van geavanceerde cryptografie maken het mogelijk om te rekenen met data, terwijl deze vercijferd blijft. Door deze bijzondere eigenschap kunnen meerdere organisaties met behulp van deze technologie samenwerken en hun gegevens combineren, zonder dat ze elkaars gegevens kunnen inzien of dat deze naar één partij wordt gebracht. Zo verkrijgt je wel inzichten maar deel je geen data.

Alleen, technologie is maar technologie. Het moet wel passen binnen de processen van je potentiële klant voordat de innovatie echt toegepast kan worden. Voor ons betekende dat naast de toepassing van de innovatieve technologie dat ook het proces van samenwerken ondersteund moest worden. Dit heeft geleid tot de ontwikkeling van het concept van data collaboration governance. Deze data collaboration governance stelt organisaties in staat om hun datasamenwerkingen te beheren door regels in te stellen en af te stemmen. Aanpassingen in de regels zijn pas actief wanneer betrokken partijen ingestemd hebben met de wijziging en alle mutaties worden vastgelegd in een onveranderbaar



“Gedecentraliseerde architectuur van het Linksight platform”

auditlog. Kortom, iedere organisatie in de datasamenwerking behoudt volledige controle over het gebruik van hun gegevens. Deze combinatie van de Privacy Enhancing Technology (PET) en de data collaboration governance is nu een onderscheidend aspect van onze propositie.

Gebruik in de praktijk

Voor de gemiddelde lezer van dit blad zullen de impact en de toepassingsmogelijkheden van PET's voor de hand liggen. Potentiële klanten hebben echter vooral interesse in concrete toepassingen en de toegevoegde waarde. Momenteel concentreren we ons op de zorgsector. Binnen deze sector zijn grote hoeveelheden data decentraal opgeslagen en is er de behoefte om zorg te verbeteren door gegevens van meerdere zorgverleners te combineren. Concrete voorbeelden van use cases in de zorg zijn effectiviteitsberekeningen over de zorgketen, inzichten in dubbelingen van personen op wachtlijsten van de GGZ en fraudebestrijding. Bovendien is het mogelijk om met ons product gezamenlijk AI-modellen te trainen. Oftewel, allemaal samenwerkingen rondom data, waarbij de te gebruiken onderliggende technologie slechts een middel is. En hoewel we ooit zijn gestart met homomorfe vercijfering, ondersteunt ons product nu bijvoorbeeld ook secret sharing en federated learning; we gebruiken wat het beste past bij de case.

Wat we tot nu toe geleerd hebben

Allereerst hebben we als TNO spin-off een stevige start gemaakt dankzij het TNO tech-transfertraject. Het tech-transfer team weet hoe de startup-wereld werkt en heeft ons klaargestoomd om deze security-innovatie in de markt zetten. De vele clichés over startups

blijken ook gewoon waar te zijn. Zo is valideren van nieuwe functionaliteit met bijvoorbeeld mock-ups – zoals beschreven in vrijwel elk startup-boek – inderdaad erg belangrijk om te voorkomen dat je dingen bouwt die niemand wil hebben. Net als weten met wie je moet praten, waarbij je verhaal goed afgestemd moet worden op je publiek. Een innovatiemanager is immers geïnteresseerd in andere aspecten van het product dan een inkoper of een CISO. En ten slotte nogmaals: concentreer je op de toegevoegde waarde, niet de technologie, dat is slechts het middel. Met Linksight zijn we nu bezig met onze volgende investeringsronde, zodat we met onze technologie op meer plekken en in meer domeinen deze waarde kunnen toevoegen en van dit tech-transfertraject een nog groter succes te maken.

TNO spin-off

Een TNO spin-off is een bedrijf dat is voortgekomen uit onderzoek of technologie ontwikkeld bij TNO (de Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek). Bij een spin-off wordt kennis of innovatie die binnen TNO is ontstaan, omgezet in een commercieel product of dienst via een nieuw, zelfstandig bedrijf. Het doel is om de impact van wetenschappelijke en technologische innovaties te vergroten door ze naar de markt te brengen, vaak in samenwerking met ondernemers, investeerders en andere partners. Zo draagt het bedrijf bij aan economische groei en maatschappelijke vooruitgang.



Auteurs: Ellen Wesselingh is senior architect bij Fox Crypto B.V. Zij focust zich op de evaluatie en certificering van de producten die Fox Crypto ontwikkelt. Zij kan worden bereikt op ellen.wesselingh@foxcrypto.com. Kees Stammes is Managing Director bij Securify. Hij focust zich op strategie, innovatie, certificeringen en compliance van de offensieve security diensten die het bedrijf ontwikkelt en aanbiedt. Hij kan worden bereikt op kees.stammes@securify.nl

Wetgeving: last of lust voor tech transfer?



Tech transfer - van prototype naar de markt

In dienst- en productontwikkeling zit een zogeheten valley of death tussen de ontwikkelfases en het daadwerkelijk op de markt kunnen brengen van de ontwikkelde dienst of product. Tech transfer is het proces om die stap te kunnen maken. Grote marktpartijen of publieke organisaties kunnen die stap zelf maken. Voor midden- en klein bedrijf is het een stuk lastiger. Belemmeringen zoals complexe wet- en regelgeving, hoge compliance kosten en intellectueel eigendomsvraagstukken spelen hierbij een grote rol.

Overheden kunnen tech transfer voor midden- en kleinbedrijf faciliteren of frustreren. Faciliteren door een ecosysteem met ondersteuning in geld, middelen en kennis aan te bieden. Maar ook: frustreren met nodeloos ingewikkelde regels. In dit artikel beschrijven wij de voor- en nadelen van de aankomende wetgeving die er op Europees en nationaal niveau op ons afkomt in de ICT-industrie in relatie tot tech transfer. Vervolgens dragen we een aantal oplossingen aan om tech transfer een grotere kans van slagen te geven.

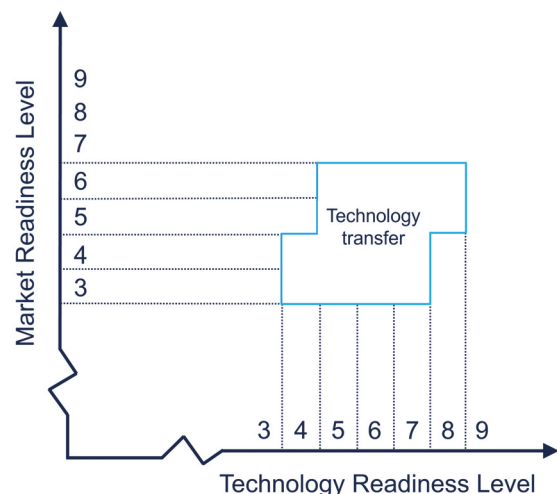
In dit artikel bekijken we het vraagstuk vanuit het perspectief van een kleine dienstenontwikkelaar en -verlener (plusminus 50 medewerkers) en een middelgrote productontwikkelaar (plusminus 150 medewerkers). Beide bedrijven zijn werkzaam in de high assurance industrie en doen veel voor de Nederlandse overheid.

Wat komt er aan wetgeving op de industrie af als het gaat om (cyber)security? Dat is veel, te veel om in een paar pagina's uit te werken. We focussen daarom op de **Network en Informatiesystemen Security (NIS2)** richtlijn, de **Digital Operational Resilience Act (DORA)** en de **Cyber Resilience Act (CRA)**. De eerste twee richten zich vooral op organisaties en hun cyberveiligheidsprocessen, de laatste op de veiligheid van producten met digitale elementen die op de markt komen. Deze wetten bieden zowel uitdagingen als kansen voor security tech transfer.

Door een goed evenwicht te vinden tussen regelgeving en stimulansen, kan Europa een veerkrachtiger en innovatiever cybersecurity landschap creëren.

De rol van Technology Readiness Levels in tech transfer

Een belangrijk raamwerk in de tech transfer is het Technology Readiness Level (TRL)-model. De TRL's geven de mate van ontwikkeling van een technologie aan, waarbij TRL 1 staat voor technologie aan het begin van de ontwikkeling en TRL 9 voor technologie die technisch en commercieel gereed is. Dus klaar om naar de markt te gaan. We gebruiken de EARTO-definities (1) van Technology Readiness Level (TRL).



De stappen van TRL 4 tot en met 8 zijn hierin cruciaal. MKB'ers bevinden zich vaak in deze fases wanneer ze hun technologie van een proof-of-concept (PoC) naar een commercieel product brengen. Hier is wet- en regelgeving een bepalende factor: het kan innovatie belemmeren als compliance kosten te hoog zijn, maar het kan juist ook een stimulans zijn als regelgeving leidt tot markttoegang en standaardisatie.

Een bestuurder kan weliswaar nog steeds advies van de CISO negeren, maar moet dat beargumenteerd en gedocumenteerd doen

De impact van Europese wetgeving op security tech transfer

De ontwikkeling van diensten en producten ten behoeve van digitale veiligheid is van oudsher vooral aan de markt overgelaten en minder gereguleerd. Alleen specifieke maatschappelijke sectoren hebben al enige tientallen jaren te maken met strenge toelatingsregels. Maar met de introductie van NIS2 en CRA gaat over de hele linie de lat omhoog. De wetgevingen brengen nieuwe verplichtingen met zich mee, zoals strengere eisen aan security-by-design, verplichte meldingen van kwetsbaarheden en het testen van hard- en software. We zien veel uit de EU op ons afkomen, maar ook nationale overheden stellen bijvoorbeeld bij aanbestedingen tegenwoordig eisen aan kwaliteit en veiligheid.

“Regels bestaan niet om innovatie te remmen of ondernemers te pesten, maar om ons te beschermen tegen ongewenste ontwikkelingen en excessen.” – citaat Hannes Cools in NRC (2).

Voordelen

Nu al is de markt onderhevig aan regels. Het is goed dat deze spelregels er zijn, om het gerealiseerde niveau van digitale veiligheid te kunnen toetsen en waar nodig te kunnen handhaven. De vele cyberincidenten van de laatste jaren tonen aan dat de markt het niet alléén kan oplossen.

Regels hebben nog meer voordelen: door de regels op EU-niveau vast te stellen, wordt de potentiële markt groter. Hierdoor gaan de kosten onvermijdelijk omhoog, maar de potentiële baten ook. Tenminste: voor die ondernemers die de regels slim weten te

implementeren om zo een marktvoordeel te behalen. Wie voldoet aan EU-wetgeving kan producten en diensten immers eenvoudiger in meerdere lidstaten aanbieden.

Voldoen aan regelgeving levert een certificaat op. Een certificaat kan ook helpen: je verkoopt vertrouwen dat jouw dienst of product van goede kwaliteit is op het gebied van digitale veiligheid. Een garantie op veiligheid en naleving. Het is immers door een onafhankelijke expert beoordeeld. Dit kan een concurrentievoordeel opleveren, doordat een level playing field wordt gecreëerd voor aanbieders die goede beveiliging willen leveren. Die aanbieders zullen nu minder snel in het nadeel zijn ten opzichte van aanbieders die veiligheid niet serieus nemen en zo goedkoper kunnen aanbieden.

Betekent de aankomende wetgeving op het gebied van (cyber)security, nog veel voor de rol van de CISO? Op papier niet, PvIB en anderen pleiten al jaren voor de CISO als boardroom functie. In de praktijk zou het wel eens zo kunnen zijn dat de regels, die expliciet verantwoordelijkheid voor risicomanagement bij het hoogste bestuursniveau leggen, de adviesfunctie van de CISO beter borgen.

Een bestuurder kan weliswaar nog steeds advies van de CISO negeren, maar moet dat beargumenteerd en gedocumenteerd doen. Met de persoonlijke aansprakelijkheid van die bestuurder onder NIS2 en de CRA krijgt de CISO met een beetje geluk eerder het voordeel van de twijfel om te investeren in een gedegen cybersecurityprogramma. Digitale veiligheid wordt een nieuwe loot aan de risicomanagementboom.

Alleen maar voordelen ... not!

De vele nieuwe wetten hebben ook nadelen en kunnen knellen, om zo uiteindelijk de innovatie en dus tech transfer af te remmen. Bijvoorbeeld als ze veel extra administratieve lasten geven zonder dat daar een daadwerkelijk betere veiligheid tegenover staat (of bredere markttoegang). Vooral de hoeveelheid aan wetgeving die op ons afkomt kan voor kleine organisaties veel tijd en middelen vergen. Grote organisaties hebben vaak de middelen om snel te voldoen aan nieuwe wetgeving, waardoor er een oneerlijk speelveld ontstaat. Een onderzoek van ENISA naar Cybersecurity investeringen met betrekking tot NIS2 (3) geeft aan dat 34% van de MKB'ers het nodige budget om aan de NIS2 te kunnen voldoen niet hebben. Dit kan leiden tot een markt waarin grote bedrijven de standaard zetten en kleine, innovatieve spelers moeite hebben om door te breken.

Ook zien wij het risico dat wet- en regelgeving vertragend of blokkerend kan zijn voor innovatie. Regelgeving die te rigide is kan de flexibiliteit wegnemen die nodig is voor snelle innovaties. Wetgeving moet daarom ruimte bieden voor nieuwe technologieën en modellen zonder de innovatie te verstikken.

Daarnaast kost het tijd en cultuurverandering om nieuwe wet- en regelgeving te implementeren. Medewerkers vinden veranderen lastig en als organisatie moet je ze wel zien mee te krijgen in dat proces. De administratieve lastendruk wordt hoger, wat ook hier weer ten koste kan gaan van de innovatie en de moraal bij het personeel, dat immers wil innoveren. Hoe kan het midden- en kleinbedrijf ondersteund worden bij deze transitie? Dat werken we hieronder uit.

Vooruit naar oplossingen

Hoewel regelgeving soms als een obstakel voelt, kan deze ook op een slimme manier worden ingezet om security tech transfer te versnellen en verbeteren. Wij, als midden- en kleinbedrijf, kunnen vol in de weerstand gaan en vooral alle nadelen benadrukken. Maar de eerste oplossing om vooruit te komen is een open houding en de verandering omarmen. Het ENISA-onderzoek naar cybersecurity-investeringen met betrekking tot NIS2 toont aan dat entiteiten die onder de NIS vielen, aanzienlijk beter scoren op cybersecurity governance, risk en compliance metrics dan nieuwe entiteiten onder de NIS2.

Dit onderzoek benadrukt de positieve impact die de eerste NIS-richtlijn heeft gehad op de sectoren die al binnen het bereik vallen. Aanvaard het nieuwe speelveld, zie het als een kans en ga er op een pragmatische manier mee om. Papier is goedkoop dus schrijf op hoe jouw huidige maatregelen zijn en hoe die zich verhouden tot de nieuwe wet- en regelgeving. Dat kost niet al te veel tijd en middelen en is een goed startpunt om vervolgens aan verbetering te werken met een Plan, Do, Check, Act (PDCA) cyclus.

Overheid en kennisinstituten kunnen ook een rol in de oplossing spelen. Het stimuleren van publiek-private samenwerking kan bijvoorbeeld door het faciliteren van kennisdeling. Deze publicatie is een mooi voorbeeld van kennisdeling. Organisaties zoals TNO of universiteiten kunnen ook fungeren als een stimulerende omgeving waarin problemen uit de markt worden onderzocht en gebracht tot een volwaardig Proof of Concept (POC) (TRL 5).

Vanuit de POC kan dan onderzocht worden hoe slimme technieken breder in de markt kunnen worden gebruikt (TRL 6 t/m 9), zonder eerst een lange discussie over intellectueel eigendoms-

Security tech transfer is een complexe uitdaging waarin wet- en regelgeving zowel een belemmering als een stimulans kan zijn

recht te voeren. Veel van het werk is immers bekostigd uit publiek geld en wat is er dan mooier dan dat het de maatschappij als geheel ten goede komt? Publiek-private initiatieven zouden innovatie niet moeten belemmeren door starre regels rondom intellectueel eigendom. Open innovatie en samenwerking kunnen ervoor zorgen dat technologieën sneller worden doorontwikkeld en breed toegepast.

Wij zien ook wel wat in een (virtuele) omgeving voor kleine marktpartijen waar zij de levensvatbaarheid van een POC kunnen testen. Een testomgeving waarin MKB'ers hun innovaties kunnen uitproberen zonder direct aan alle wetgeving te moeten voldoen. Dit biedt startups de kans om hun technologieën in realistische omstandigheden te testen, voordat ze grote investeringen moeten doen. Denk hierbij aan een marktplaats om de adoptie van een product te testen. Een ander gebruik van een testomgeving zien wij bijvoorbeeld door een POC te kunnen laten pentesten. Dat geeft dan een leereffect als het product niet veilig blijkt. Er kunnen naar aanleiding van de resultaten van de pentest vroegtijdig aanpassingen aan het product gemaakt worden. Hierdoor kunnen MKB'ers tegen relatief lage kosten veilige digitale producten op de markt brengen.

Als laatste zien wij ook een samenwerking tussen grote en midden- en klein bedrijven als mogelijke oplossing. We zien dat op het gebied van Cybersecurity grote organisaties zoals ASML hulp bieden aan leveranciers. Ook hier kan dit door middel van kennisdeling en samenwerkingsverbanden. Dit verkleint de kloof tussen regelgeving en implementatie.

Conclusie: balans tussen regelgeving en innovatie

Security tech transfer is een complexe uitdaging waarin wet- en regelgeving zowel een belemmering als een stimulans kan zijn. Door regelgeving slimmer vorm te geven – met aandacht voor publiek-private samenwerkingsverbanden, testomgevingen en realistische nalevingseisen – kan de EU een sterke basis leggen voor innovatie in de cybersecuritysector én de gehele maatschappij weerbaarder maken. Het MKB speelt hierin een cruciale rol en heeft baat bij een ecosysteem waarin compliance niet alleen een last is, maar ook een kans biedt om internationaal op te schalen. Aan het MKB om zelf ook een open houding aan te nemen en de kansen te zien. Pak het pragmatisch op en zoek aansluiting of hulp waar nodig.

Referenties

- (1) European Association of Research and Technology (EARTO) Recommendations. The TRL Scale as a Research & Innovation Policy Tool. April 2014. https://www.earto.eu/wp-content/uploads/The_TRL_Scale_as_a_R_I_Policy_Tool_EARTO_Recommendations_-_Final.pdf
- (2) Hannes Cools, universitair hoofddocent Human Factor in New Technologies aan de UvA. <https://www.nrc.nl/nieuws/2025/02/18/de-ai-race-heeft-geen-finish-a4883525>
- (3) European Union Agency for Cybersecurity (ENISA) Navigating cybersecurity investments in the time of NIS 2. <https://www.enisa.europa.eu/news/navigating-cybersecurity-investments-in-the-time-of-nis-2>



Recht in de doelgroep

100% veilig. 0% spam.

Uw merk, product of dienst onder de aandacht brengen bij dé professionals in de intersectorale branche?

IB-Magazine is hét betrouwbare platform met een sterke, betrokken lezerskring. Geen ruis, geen verspilling — alleen zichtbaarheid waar het telt.

Meer weten?

Mail naar ibmagazine@pvib.nl



Praktisch toepasbare kennis!

Bent u klaar voor de toekomst van cryptografie?

De opkomst van de quantumcomputer vormt een fundamentele bedreiging voor de huidige cryptografische standaarden. Organisaties die hier niet op anticiperen, lopen nu al grote risico's!

Leer in één dag hoe u uw systemen quantumveilig maakt.

Onze cursus *Quantumveilige Cryptografie Essentials* biedt u:

- Inzicht in de impact van quantumcomputers op cryptografie
- Praktische handvatten voor migratie
- Actuele kennis van experts
- Het PQC-migratiehandboek

Scan de QR code voor meer informatie.
Of ga naar: www.securityacademy.nl

