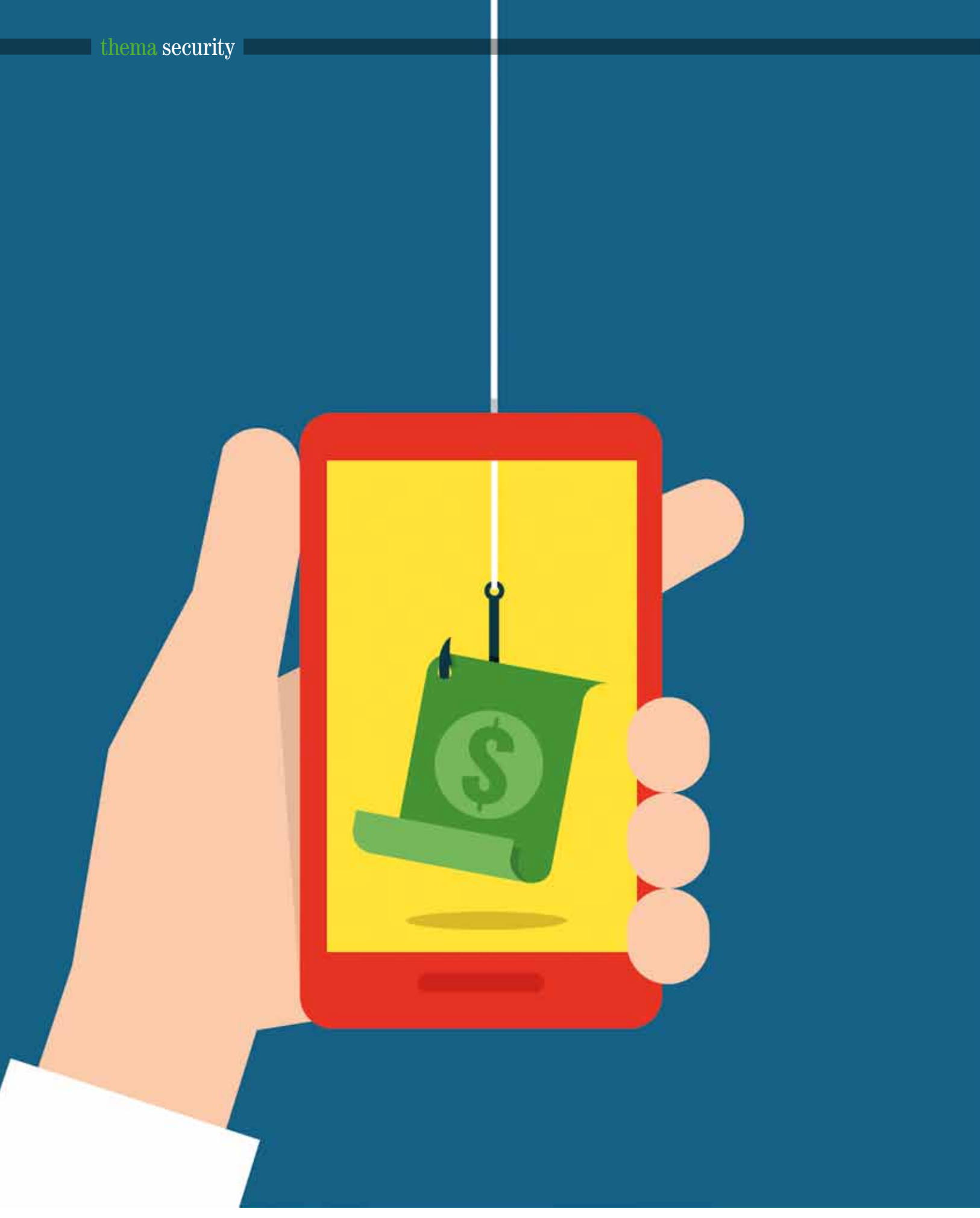

De 'hyperconnected world' maakt organisaties kwetsbaar

De toekomst van privacy en security

Onderzoekers hebben becijferd dat er in 2015 zo'n 7 triljoen apparaten draadloos met elkaar verbonden zullen zijn. Met hoge snelheid komen er op grote schaal nieuwe technologieën en functionaliteiten beschikbaar. Helaas zijn die niet allemaal ontworpen vanuit de gedachte dat ze ook zouden kunnen worden misbruikt. Daar ligt een grote uitdaging: enerzijds om nieuwe technologieën te omarmen en aan de andere kant de hieraan verbonden risico's op het gebied van databescherming en privacywetgeving te managen.

In de laatste twintig jaar heeft de technologische revolutie een enorme impact gehad op hoe we leven en werken. Het heeft ons nieuwe kansen voor innovatie en verbeterde productiviteit gebracht, maar ook risico's en uitdagingen. Als gevolg van innovatieve technologieën als cloud, mobile computing en het Internet of Things staat alles en iedereen tegenwoordig in verbinding met elkaar, de zogenaamde 'hyperconnected world'. Onderzoekers denken dat rond 2025 meer dan 7 triljoen apparaten draadloos met elkaar zijn verbonden. Deze verbonden wereld zorgt voor economische en maatschappelijke groei, maar maakt organisaties ook kwetsbaar voor identiteitsdiefstal, cyberspionage en digitale oorlogsvoering.

> Nieuwe technologieën zijn niet ontworpen met de gedachte dat zij ook misbruikt kunnen worden

Privacy vs. openbaar

De uitdaging is dus om deze nieuwe technologieën aan de ene kant te omarmen en aan de andere kant de hieraan verbonden risico's op het gebied van databescherming en privacywetgeving te managen. Het echte probleem hierbij is dat al deze nieuwe technologieën niet ontworpen zijn met de gedachte dat zij ook misbruikt kunnen worden. De snelheid waarmee nieuwe technologieën en functionaliteiten ontworpen worden, betekent dat er onvoldoende aandacht is voor het security- en privacyaspect. De wetenschap dat rond 2025 7 triljoen apparaten met elkaar verbonden kunnen zijn, roept wel de vraag op of wij als samenleving niet securityeisen moeten stellen aan technologieën en apparaten. Bedrijven en overheden kunnen een deel van de risico's verkleinen en de schade beperken door beter samen te werken en zelf eisen te stellen aan het gebruik van al deze nieuwe technologieën. Steeds meer organisaties doen dit al; zij delen informatie over risico's en dreigingen en er zijn bepaalde sectoren waarin bedrijven samen werken aan contingencyplannen of een gezamenlijke aanpak om kwetsbaarheden op te sporen en aan te pakken.
Ook delen steeds meer organisaties hun securityinformatie met die van andere publieke en private partijen op basis van vertrouwen – de bankenwereld is hier een goed voorbeeld van – zodat het mogelijk wordt om kenmerken of patronen vroegtijdig te herkennen.
Er bestaan verschillende barrières voor samenwerking op het gebied van cybersecurity. Ten eerste zit het in de menselijke natuur om zwakheden te verbergen, in plaats van deze te laten zien. Organisaties laten zien wat het delen van informatie hun oplevert, vergroot de kans op deelname.

Dan de verschillen op juridisch gebied. Elk land heeft zijn eigen wetgeving als het gaat om het openbaar maken van *data breaches*. Zo verplichten de Verenigde Staten organisaties om aanvallen op de kritieke infrastructuur te melden, maar dat geldt in veel Europese landen zoals Nederland (nog) niet. Dit werpt een barrière op voor landen om informatie te delen. Daarnaast bestaat er bij sommigen een zeker wantrouwen om informatie te delen uit angst dat bedrijfsgeheimen of kwetsbaarheden openbaar worden. Wanneer organisaties de securityvolwassenheid van de andere deelnemers kennen, zullen ze eerder openstaan voor deelname. Tot slot is het moeilijk de balans tussen privacy en openbaarheid te bewaken; privacyrechten kunnen overheden beperken als het gaat om het bewaken van het democratische proces.

> "We will continue to lose privacy one degree at a time, until there is none left at all"

Geografische verschillen in privacywetgeving

Wereldwijd gezien is er sprake van een spectrum voor privacywetgeving; deze gaat van sector- of situatiespecifieke wetten tot omnibusframeworks. Bedrijven geven de voorkeur aan landen waar de privacywetgeving duidelijk gedefinieerd en transparant is. Vergeleken met internationale standaarden kent de Verenigde Staten op het gebied van privacywetgeving een bijna laisser faire sectorspecifieke aanpak, gericht op een aantal specifieke gebieden van datamanagement (medische en financiële gegevens et cetera). In tegenstelling tot deze aanpak maken Canada en de EU gebruik van een omnibusregeling voor gegevensbescherming; hierbij worden alle persoonsgerelateerde gegevens gereguleerd. Deze wetgeving is zo uitgebreid dat ze zelfs betrekking heeft op schijnbaar onschuldige databases zoals telefoonboeken, reserveringssystemen van restaurants en persoonlijke blogs. En ze hebben invloed op alle belangrijke aspecten van de bedrijfsvoering zoals facturatie, medewerkers- en klantgegevens. Het verschil tussen de Amerikaanse privacyregelgeving en omnibuswetgeving inzake gegevensbescherming heeft voor een groot deel te maken met de Amerikaanse grondwet. Het eerste amendement van de Amerikaanse grondwet geeft mensen in de VS een expliciet recht om de meeste informatie die beschikbaar is over anderen te bespreken, af te drukken of online te plaatsen zonder dat er een uitzondering wordt gemaakt als iemands privacy in het geding is. Dit betekent dat het recht op vrijheid van meningsuiting belangrijker wordt gevonden dan het recht op privacy. Europa, Canada en andere rechtsgebieden met grondwettelijke bescherming van de privacy en uitgebreide wetten voor gegevensbescherming kijken vanuit een heel ander perspectief naar deze kwestie. In plaats van het belang van privacy op te wegen tegen vrijheid van meningsuiting maken zij een vergelijking tussen het recht op privacy en het recht op intellectueel eigendom. Als de overheid bedrijven helpt met exploiteren van merknamen en handelsmerken, dan moet de wet de burger beschermen tegen het verhandelen van persoonlijke informatie zoals hun financiële en medische geschiedenis. Ook buitenlandse bedrijven die in de EU gevestigd zijn of daar handel willen drijven, moeten voldoen aan de strikte standaarden van de EU. Veel nationale overheden en grote handelsblokken zoals de EU herzien bestaande overeenkomsten wat betreft het delen van gegevens met andere landen zoals de Verenigde Staten met als doel het garanderen van dezelfde mate van gegevensbescherming. De huidige gegevensbescherming in de Europese Unie is nog gebaseerd op een richtlijn uit 1995 die als gedateerd wordt beschouwd. De betrokken ministers van alle EU-landen kijken momenteel naar het voorstel van de Europese Commissie dat op enkele kleine aanpassingen na in maart 2014 is aangenomen door het Europees Parlement. De verwachting is dat er dit jaar uitsluitsel komt over een nieuwe Europese privacywet.

Samenwerken aan privacy

Onze toenemende afhankelijkheid van connectiviteit zorgt ervoor dat gegevensbescherming een kritieke factor is voor ons allemaal. De vraag is of de nieuwe Europese regelgeving voldoende waarborgen biedt in een 'hyperconnected wereld' en wat wij er zelf als samenleving aan kunnen doen. Geen enkele regelgeving of samenleving kan gegevensbescherming en privacyissues alléén oplossen. We moeten kiezen voor een samenwerkende multistakeholderaanpak, zelfs als dit betekent dat concurrenten in een bepaalde branche of landen met een andere visie op privacy moeten samenwerken om een stabiele en veilige omgeving te creëren.
Dit alles roept de vraag op of er rond 2025 nog wel sprake kan zijn van het begrip 'privacy' als alles en iedereen met elkaar verbonden is en als autonome systemen beslissingen kunnen nemen zonder tussenkomst van de mens. Een aantal recente uitspraken van gerenommeerde auteurs spreken voor zich. Privacy in 2025: "*It will be similar to the (mythical) boiling frog – we will continue to lose privacy one degree at a time, until there is none left at all*", aldus Jeremy Epstein, Senior Computer Scientist bij SRI International.

Jaap Schekkerman is Director Global Cyber Security bij CGI.