

Hebben wij die nog wel in een hyper-connected wereld?

ROTTERDAM – 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.

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. Deze nieuwe technologieën zijn echter niet ontworpen met de gedachte dat zij ook misbruikt kunnen worden. De snelheid waarmee zij ontworpen worden, zorgt ervoor dat er onvoldoende aandacht is voor het security- en privacy-aspect. De wetenschap dat rond 2025 maar

lieft 7 triljoen apparaten met elkaar verbonden kunnen zijn, roept wel de vraag op of wij als samenleving niet security-eisen 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 ervan. Steeds meer organisaties doen dit al: zij delen informatie over risico's en dreigingen en er zijn bepaalde sectoren waarin bedrijven samenwerken aan *contingency*-plannen of een gezamenlijke aanpak om kwetsbaarheden op te sporen en aan te pakken. Ook delen steeds meer organisaties hun security-informatie zodat het mogelijk wordt om kenmerken of patronen vroegtijdig te herkennen.

Privacywetgeving

Er bestaan grote verschillen tussen landen als het gaat om privacywetgeving. Zo kent de VS een bijna 'laissez 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 omnibus-regeling voor gegevensbescherming; hierbij wordt alle persoonsgerelateerde data gereguleerd. Veel nationale overheden en grote handelsblokken zoals de EU herzien bestaande overeenkomsten wat betreft het delen van data

“rond 2025 zijn meer dan 7 triljoen apparaten draadloos met elkaar verbonden”



met andere landen zoals de VS, met als doel het garanderen van dezelfde mate van databescherming - de huidige databescherming in de EU is nog gebaseerd op een richtlijn uit 1995. De nationale 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 uitsluitel komt over een nieuwe Europese privacywet. 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 privacy-issues alléén oplossen. We moeten kiezen voor een samenwerkende multi-stakeholder aanpak, zelfs als dit betekent dat concurrenten in een bepaalde branche of land met een andere visie op privacy moeten samenwerken om een stabiele en veilige omgeving te creëren.

Jaap Schekkerman is Director Global Cyber Security bij CGI