'*Cyber security* is vooral een kwestie van adequaat gedrag en risicobeheersing'

Verslag NWG Wageningen-lezing Jan van den Berg, hoogleraar Cyber Security (TU Delft & Universiteit Leiden) - dinsdag 2 november, WICC, Wageningen - door Gert van Maanen

"Als het gaat om *cyber security* vormt techniek wel de basis, maar nog belangrijker is 'de laag er direct omheen': het menselijk gedrag: bijvoorbeeld, klikt iemand wel of niet op een link of kiest hij/zij altijd een voldoende sterk wachtwoord? Daar overheen zit nog een laagje regels en voorschriften - *governance* van *cyberspace* -, maar die is in het digitale domein verre van uitontwikkeld. Op de weg hierheen zag ik dat alle sloten weer netjes schoon zijn gemaakt door boeren omdat dit ingeburgerde voorschriften zijn, opgelegd door de Waterschappen. Voor een internationale infrastructuur als het Internet bestaat zoiets slechts in zeer beperkte mate, mede doordat landen, inclusief de grootmachten, heel verschillende ideeën hebben over hoe het Internet moet worden ingericht. Ieder kind wordt al vroeg geleerd hoe je moet oversteken, maar over hoe je je moet gedragen op Internet, in de diverse rollen die je veelal vervult, is maar bar weinig geregeld". Die boodschap bracht *Cyber Security*-expert Jan van den Berg in zijn lezing op 2 november in het WICC in Wageningen. In een flink tempo en met veel humor en relativering laveerde hij het publiek door een hele berg informatie, vaak met Engelstalige termen, want voor ICT en Internet is dat nu eenmaal te voertaal. "Deze presentatie komt beschikbaar op de website, dus als u meer wil weten, kunt u rustig op de links klikken", zegt Van den Berg geruststellend. Een opmerkelijke aansporing die hij deze avond meerdere keren zal herhalen.

Voor veilig internetgebruik is het volgens hem altijd belangrijk zelf afwegingen te maken en risico's in te schatten. "Wat accepteerbaar is, bepaal je zelf, dan wel het bedrijf of organisatie waarvoor je werkt", aldus Van den Berg. "Daarbij maakt het natuurlijk steeds weer uit welke rol je vervult: gewone eindgebruiker, crisismanager van een bedrijf, dan wel eindverantwoordelijke van een kritieke infrastructuur. Het gaat allemaal om risicomanagement: bij *alle* gebruikte IT-toepassingen dien je de risico's te beperken tot 'de overeengekomen acceptabele niveaus'. Absolute veiligheid bestaat niet in *cyberspace*."

Hoe alomvattend informatisering en digitalisering is in de moderne samenleving illustreert Van den Berg in zijn inleiding: elektronica wordt steeds kleiner, steeds meer processen worden geautomatiseerd, er is sprake van *Big Data*, 5G-netwerken, mensen werken *real-time* in de *Cloud* en betalen kan met bitcoins en andere cryptomunten dankzij *Block Chains*. "Er is nu ook sprake van een *Internet of Things*. In 1992 waren er een miljoen computers online, maar in 2021 gaat het om zo'n 50 miljard internetaansluitingen voor allerlei apparaten", vertelt Van den Berg. "Geen wonder dat er ook steeds vaker sprake is van incidenten. Zo werd in 2016 een zogenaamde DDOS-aanval uitgevoerd van 1 Terabyte per seconde waarbij hackers gebruik maakten van 150.000 slecht beveiligde op Internet aangesloten en door hen gehackte apparaten zoals beveiligingscamera's, televisies en koelkasten. Daarnaast maken spionagediensten veelal gebruik van allerlei Internet-*scanning-software*, zoals blijkt uit de onthullingen over de Amerikaanse NSA door Edward Snowden (met codenaam: Citizenfour), die als klokkenluider asiel kreeg in Rusland. Een heel indrukwekkend voorbeeld van digitale oorlogsvoering (*Cyber Warfare)* is de Stuxnet-operatie waarmee in 2010 zo'n duizend kerncentrifuges in Iran werden stilgelegd. "Hierbij werd een computervirus als wapen ingezet om een nucleaire verrijkingsinstallatie onklaar te maken", aldus Van den Berg. Met veronderstelde betrokkenheid van Israel en de Verenigde Staten, en - zoals later bleek - ook een rol van Nederland bij het binnenbrengen van de schadelijke software in de Iranese faciliteit. "Er wordt dus ook digitaal oorlog gevoerd onder verantwoordelijkheid van de Nederlandse overheid", signaleert Van den Berg.

Een interessant geval van *Cyber Crime* is volgens hem de zogeheten Silk Road, een soort zwarte markt op

het *Darkweb* waar mensen vanaf 2011 anoniem met een TOR-browser hun inkopen konden doen. Silk Road werd in 2013 opgerold door de FBI en de oprichter Dread Pirates Roberts (pseudoniem van Ross Ulbricht) werd veroordeeld tot twee keer levenslang. De illegale handel op het *Darkweb* is daarmee niet stilgelegd, zo bewijzen recentere affaires rond AlphaBay en Hansa . ”Wapens, porno, eigenlijk alles wat verboden is, kun je daar kopen. Het *Darkweb* toont een keerzijde van het gebruik van Internet: anonimiteit doet rare dingen met mensen”, aldus Van den Berg.
Ook gerenommeerde bedrijven kunnen betrokken raken bij *Cyber Crime* zo illustreren de hack bij ASML in 2015 en de verdenkingen van bedrijfsspionage door Huawei in 2019. Hacks kunnen grote maatschappelijke gevolgen hebben, zoals het platleggen van bijna de complete stroomvoorziening in Oekraïne (2015), een digitale bankroof van bijna een miljard dollar bij de centrale bank van Bangladesh (2016), de wereldwijde Wanna Cry-aanval (2017) op Microsoft-computers en – dichter bij huis – het stilleggen van de Maersk-terminal in Rotterdam (2016-2017) met wereldwijde gevolgen en bijna 300 miljoen euro schade. *Hacks* waarbij criminelen *Randsom Software* installeren en het betalen van losgeld in bitcoins eisen, zijn gemeengoed geworden, constateert Van den Berg.

Hoe kunnen we Cyber Security risico’s beheersen in de thuissituatie, voor bedrijven en in de maatschappij? Dit is inzichtelijk te maken met het klassieke ‘vlinderdas’(bowtie)-model voor risicomanagement, waarin zowel de mogelijke *bedreigingen* en *impact* van bedreigingen worden weergegeven als de mogelijkheden om via *preventie* en *repressie* de schade van een incident te minimaliseren. ”In essentie gaat het erom om de cyberrisico’s te reduceren tot *acceptabele niveaus*”, aldus Van den Berg. ”Dat kan door technische maatregelen, aanpassingen in gedrag en het instellen van wetten en regels.“ Als voorbeeld noemt hij het voorkomen van infectie met *malware*, schadelijke software zoals computervirussen. Dat kan door bij ieder gebruik van een usb-stick een viruscheck te laten plaatsvinden dan wel usb-stick-gebruik technisch onmogelijk te maken, door gewoon niet zomaar te klikken op links in e-mails, of door als bedrijf/organisatie het klikken op links simpelweg te verbieden. ”Uiteindelijk is het beheersen van risico’s een zoektocht naar een balans, naar de afweging tussen het reduceren van de kans dat er incidenten plaatsvinden en het minimaliseren van de impact die het heeft als het misgaat. Wat daarbij een acceptabel risico is, bepalen we zelf”, aldus Van den Berg.

De momenteel drie belangrijkste uitdagingen voor *Cyber Risk Management* zijn volgens Van den Berg het creëren van bewustwording, het ontwikkelen van een gebalanceerd pakket aan (preventieve en repressieve) veiligheidsmaatregelen en het implementeren van adequate publiek-private samenwerking op dit gebied. Zijn hoofdconclusie: ”Als we eerlijk zijn is dat *cyber*-risicomanagement momenteel nog vrijwel nergens goed op orde.”