De cyberwereld wordt niet vanzelf veilig

Marcel Spruit
Lector Cyber Security & Safety

De cyberwereld

Sinds mensenheugenis leven we in een fysieke wereld, een wereld waarin we wonen, werken en waar we andere mensen fysiek ontmoeten. Sinds de vorige eeuw is daar de cyberwereld bijgekomen. De digitale wereld, de wereld van computers en netwerken, van bits en bytes. Tegenwoordig zit iedereen in meer of mindere mate in de cyberwereld.[1] Je merkt het nauwelijks als je de cyberwereld instapt. Van het ene op het andere moment zit je erin. Bijvoorbeeld als je belt, sms't, een mail stuurt, shopt of bankiert op internet, in een winkel betaalt met een pinpas of een mobiel, of een verhuizing doorgeeft aan de gemeente.

Niet alleen privé zitten we vaak in de cyberwereld, maar dat geldt ook voor het werk. We doen veel werk achter een computer. We schrijven en lezen daarop documenten, sturen e-mails en halen informatie van het intranet en het internet, voeren administraties uit en rekenen analyses door. Als we niet achter een computer zitten, hebben we meestal wel een tablet, een PDA, of een mobieltje, om op die manier toch in de cyberwereld te kunnen komen, voor privé of voor het werk.

Veel organisaties zijn zo afhankelijk geworden van de cyberwereld, dat ze die absoluut niet meer kunnen missen. Als computers en netwerken uitvallen, stagneert de productie of dienstverlening, stromen klachten binnen en lopen klanten over naar andere dienstverleners. Was terugvallen op papieren administraties nog een tijd lang een acceptabele workaround als de computers en netwerken waren uitgevallen, in steeds meer organisaties is dat geen reëel alternatief meer. Als de uitval te lang duurt, dan valt de organisatie om.

Sommige organisaties gebruiken tegenwoordig de cyberwereld niet alleen voor informatie en administratie, maar ook om van daaruit geautomatiseerde processen, of maatschappelijk vitale objecten, zoals bruggen, sluizen, gemalen en energiecentrales, te bewaken en te besturen. Deze processen en objecten kunnen dan met minder mensen sneller en beter bestuurd worden. En dat spaart kosten. Bovendien kunnen deze processen en objecten via de cyberwereld constant gemonitord en bijgestuurd worden. En dat verhoogt de veiligheid. Zo kan een beheerder van huis uit, via het internet, met regelmatige tussenpozen controleren of een geautomatiseerde productielijn goed blijft lopen. En als de productielijn dreigt te stagneren, kan hij direct ingrijpen, zonder dat hij daarvoor bij nacht en ontij naar de productielijn hoeft te gaan.

Problemen in de cyberwereld

De cyberwereld heeft echter ook een keerzijde: ook criminelen en spionnen hebben het ontdekt.[2] Met name de groei en bloei van het wereldwijde internet was een sterke stimulans voor cybercriminelen en cyberspionnen. Voor vrijwel alle klassieke vormen van criminaliteit en spionage zijn inmiddels wel cybervarianten beschikbaar, vaak zelfs meerdere.[3,4] Vrijwel dagelijks worden nieuwe cyberincidenten in het nieuws gemeld.[5,6] Enkele voorbeelden zijn het geruchtmakende incident over onbetrouwbare certificaten van Diginotar,[7] het afluisterschandaal van de NSA en andere inlichtingendiensten,[8] de DDoS-aanvallen op banken en andere organisaties,[9] de onveilige sluisbesturing van de gemeente Veere,[10] de langdurige internationale spionage met het virus Red October[11] en de cyberaanval op een nucleaire installatie in Iran met het virus Stuxnet.[12] Daarnaast zijn er nog veel meer incidenten waar

niemand iets van verneemt. Enerzijds komt dit doordat veel slachtoffers hun incidenten niet aan de grote klok wil hangen en daarvan ook geen aangifte doen. Anderzijds worden veel cybercriminelen en cyberspionnen nooit ontdekt, omdat ze met succes hebben geprobeerd onzichtbaar te blijven, om zo lang mogelijk te kunnen profiteren van hun slachtoffers. Zo is de weinige cyberspionage die is ontdekt, amateuristisch opgezet, bij toeval ontdekt, of pas veel later ontdekt.

Cyberincidenten leiden tot een enorme schadepost. Er is weliswaar geen betrouwbare registratie van dit soort incidenten en de daardoor veroorzaakte schade, maar er zijn wel schattingen. De schade door cybercrime wordt, alleen al voor Nederland, geschat op meer dan 1 miljard euro per jaar.[13,14,15,16] De schade door cyberspionage is moeilijker te schatten, maar ligt waarschijnlijk in dezelfde orde van grootte.[17]

Het grote aantal incidenten en de enorme schade is een duidelijke indicatie dat het slecht is gesteld met de veiligheid in de cyberwereld.

Een deel van de oorzaak van het grote aantal incidenten ligt in de omvang en de techniek. De cyberwereld is zo groot dat deze onbeheersbaar is. Dat is onontkoombaar. Bovendien is een belangrijk onderdeel van de cyberwereld, het internet, dat wereldwijd computers en netwerken met elkaar verbindt, nooit ontworpen om beheerst en veilig te werken.[18] Herontwerpen en opnieuw bouwen is geen reële optie (meer). Met name cybercriminelen en cyberspionnen hebben baat bij de onbeheersbaarheid en onveiligheid van het internet. Overigens heeft de onbeheersbaarheid en onveiligheid van het internet ook voordelen, want daardoor krijgen minderheden en onderdrukte groepen de mogelijkheid om vrij en ongecontroleerd met elkaar te kunnen communiceren. Zo heeft bijvoorbeeld de Arabische Lente baat gehad bij de ‘zwakheden’ van het internet.[19]

Een andere oorzaak van het grote aantal incidenten ligt in de nonchalance waarmee veel mensen in de cyberwereld vertoeven. Als het dan niet mogelijk is om de cyberwereld zelf veilig te krijgen en te voorkomen dat cybercriminelen en cyberspionnen daar rondhangen, dan kunnen we ieder geval zo verstandig mogelijk met de risico’s omgaan. Veel mensen lappen echter belangrijke beveiligingsmaatregelen aan hun laars en creëren daarmee onnodig onveilige situaties waarin van alles mis kan gaan. Organisaties verergeren dat door klakkeloos mee te bewegen met onvolwassen ontwikkelingen zoals cloud computing, Het Nieuwe Werken, Bring Your Own Device en integratie van sociale netwerken. Veel incidenten zijn te voorkomen door behoudender om te gaan met onvolwassen ontwikkelingen en consciëntieuzer om te gaan met tenminste de meest elementaire beveiligingsmaatregelen. Op dit gebied is nog genoeg ruimte voor verbetering.

Gebrek aan opvoeding

Dat zo veel mensen zo slecht omgaan met beveiliging in de cyberwereld, is vooral een gebrek aan kennis en inzicht. Kennis en inzicht ten aanzien van veiligheid in de cyberwereld is dun gezaaid. Als het over veiligheid in de fysieke wereld gaat, weet vrijwel iedereen waar het over gaat, wat er nodig is en wat de consequenties zijn als je beveiligingsmaatregelen aan je laars lapt. Zo hoef je niemand uit te leggen dat je ’s winters een jas aan moet doet om geen kou te vatten, dat je op de weg rechts moet houden om botsingen te voorkomen en dat je geen water uit de sloot mag drinken als je dorst hebt. In de cyberwereld is beveiliging minder vanzelfsprekend. Er zijn maar weinig mensen die goede antivirus op hun PDA of mobieltje hebben, die goede codes en wachtwoorden gebruiken, die hun device na gebruik vergrendelen, die alle phishing-verzoeken herkennen en naast zich neer leggen, die niet op besmette websites komen en die terughoudend omgaan met het verstrekken van allerlei gevoelige gegevens via sociale media.

Hoe komt het dat beveiliging in de fysieke wereld zoveel vanzelfsprekender is dan in de cyberwereld?

In de fysieke wereld is het de gewoonste zaak van de wereld dat iedereen van jongs af aan wordt opgevoed in veilig handelen. Dat begint al vroeg. Als een peuter net kan lopen, leren zijn ouders hem veilig over te steken: eerst links kijken, dan rechts kijken, dan weer links kijken, en als er dan nog niets aankomt mag hij oversteken. Op de basisschool doen alle kinderen een verkeersexamen, waarin ze laten zien dat ze de verkeersregels kennen en veilig kunnen fietsen. Om auto te mogen rijden, moeten we een scala aan veiligheidsregels tot ons nemen, vervolgens uitgebreid oefenen en dan met een theorie- en een praktijkexamen bewijzen dat we veilig kunnen rijden. Anders komen we de weg niet op. En naleving van de regels wordt stringent gecontroleerd.

In de cyberwereld gaat dat anders. De eerste de beste peuter krijgt eerder vroeg dan laat een moderne mobiele device. Veelal een exemplaar dat vader of moeder net heeft afgedankt, ten gunste van een gloednieuw en nog veelzijdiger exemplaar. Peuterlief leert in no-time hoe je hiermee al vegend over het scherm spelletjes kan doen. Desgewenst helpen vader of moeder nog even, zodat het nog sneller en soepeler gaat. Niemand die met een woord rept over wat je wel en niet zou moeten doen en waar gevaren loeren. Veel kinderen krijgen als ze naar de basisschool gaan voor hun mobieltje een abonnement waarmee ze de hele wereld binnen handbereik hebben, want dan kunnen de ouders ze te allen tijde bereiken om te horen dat het nog goed met ze gaat. Weer rept niemand over de do's en don'ts. Op de basisschool en het voortgezet onderwijs worden alle leerlingen, zelfs zonder hun eigen mobiele devices, de cyberwereld ingeduwd, want dat leert zo fijn en het ontlast de leraren en docenten. Ook hier rept veelal niemand over wat je wel en niet zou moeten doen en waar gevaren op de loer liggen. Ook op vervolgopleidingen is veiligheid in de cyberwereld in het algemeen geen onderdeel van de lesstof.

Een groter contrast tussen de fysieke wereld en de cyberwereld is nauwelijks mogelijk. In de fysieke wereld wordt veiligheid er bij iedereen van jongs af aan met de paplepel ingegoten. In de cyberwereld wordt nauwelijks over veiligheid gepraat. Alleen na een incident is het even gespreksstof, waarna iedereen weer overgaat tot de orde van de dag.

Verbetertraject

Veiligheid in de cyberwereld is dus een onderwerp dat erg weinig aandacht krijgt in opvoeding en opleiding. De daaruit volgende nonchalance waarmee mensen in de cyberwereld vertoeven, is er mede de oorzaak van dat cybercriminaliteit en cyberspionage zo groeien en bloeien. En dat leidt weer tot een stroom aan cyberincidenten en een enorme maatschappelijke schade.

De oplossing moeten we zoeken in het verbeteren van de opvoeding en opleiding op het gebied van cyberveiligheid. Een probleem is dat we van ouders, die zelf nooit zijn opgevoed en opgeleid in het omgaan met de gevaren van de cyberwereld, niet mogen verwachten dat ze dit bij de opvoeding van hun kroost goed kunnen doen. Daarom is het nodig om de cyberopvoeding, met ruime aandacht voor de cyberveiligheid, dan tenminste zo vroeg mogelijk in het reguliere onderwijs onder te brengen, te beginnen bij de basisscholen en doorlopend in de vervolgopleidingen. Aangezien iedereen intensief met de cyberwereld te maken krijgt, bestaat de doelgroep uit alle leerlingen. Het probleem wordt dan echter bij de leraren van de basisscholen en de docenten van de vervolgopleidingen neergelegd, terwijl zij op dit gebied ook niet geschoold zijn. Het is dan ook nodig dat de leraren- en docentenopleidingen hier meer aandacht aan gaan besteden. Parallel daaraan zullen de zittende leraren en docenten bijgeschoold moeten worden. Iemand moet dit traject inzetten en trekken. Aangezien het hier gaat om een breed maatschappelijk probleem, ligt het voor de hand dat de centrale overheid het voortouw neemt. Hier ligt een mooie taak voor het Ministerie van Onderwijs,

Cultuur en Wetenschap, zo mogelijk in samenwerking met andere instellingen, zoals ECP, die al meer ervaring hebben op dit gebied.[20]

Naast de algemene kennis over cyberveiligheid, die voor iedereen van belang is, is er in de maatschappij ook meer specialistische kennis nodig over het beveiligen van de cyberwereld en de interactie tussen de cyberwereld en de fysieke wereld. Hiervoor zijn goed opgeleide mensen nodig. En die hebben goede specialistische opleidingen nodig. Er is daarbij behoefte aan reguliere opleidingen op mbo-, hbo- en wo-niveau, maar ook aan verdiepende opleidingen en cursussen. Er zijn zowel opleidingen nodig in de technische hoek (de cyberwereld is nu eenmaal technisch), als in de beheersmatige hoek (de cyberwereld wordt gebruikt door mensen en organisaties). Om transparant te maken wie welke opleiding heeft genoten, en wellicht daarop voortbordurende vervolgopleidingen of cursussen, is het nuttig om een kwalificatiestelsel in te voeren waarmee professionals kunnen laten zien welke kwalificaties ze op het gebied van cyberveiligheid hebben.

De Haagse Hogeschool

De Haagse Hogeschool is al een aantal jaren bezig met de hierboven geschetste problematiek. De inspanningen richten zich met name op het uitvoeren van onderzoek ten behoeve van het veilig maken van de cyberwereld en de interactie met de fysieke wereld, alsmede op het aanbieden van specialistisch onderwijs op hbo-niveau op het gebied van cyberveiligheid.

Het onderzoek wordt uitgevoerd door het lectoraat Cyber Security & Safety (CSS). Bij het onderzoek zijn docenten en studenten van verschillende hbo-opleidingen betrokken. Bovendien wordt voor dit onderzoek samengewerkt met externe kennispartijen. De volgende onderzoekslijnen zijn in het kader van dit artikel relevant:

- *Cyber security awareness*. De sterke toename van interactieve en mobiele media in thuis-, straat- en werkomgeving en de vlucht die de sociale netwerken hebben genomen, vraagt om een toenemende awareness op het gebied van veiligheid in de cyberwereld. Het onderzoek zoekt manieren waarmee deze awareness van mensen gemeten en verbeterd kan worden.
- *Cyber security governance*. Organisaties zijn in hoge mate afhankelijk van de cyberwereld. Het voortbestaan van organisaties hangt af van de veiligheid van hun cybercomponent. Onder meer het management speelt hierin een cruciale rol, maar realiseert zich dat niet altijd voldoende. Het onderzoek zoekt manieren om de perceptie en de attitude van het management ten aanzien van cyberveiligheid te verbeteren.
- *Serious games voor cyber security*. Het beïnvloeden van de awareness ten aanzien van cyberveiligheid is lastig te realiseren. Serious games kunnen daar een effectief hulpmiddel bij zijn. Het is dan de bedoeling dat de awareness spelenderwijs positief wordt beïnvloed. Het onderzoek analyseert welke spellen nuttig zijn en hoe die opgebouwd en gerealiseerd kunnen worden.

Op het gebied van onderwijs heeft De Haagse Hogeschool een aantal specialistische opleidingen op het gebied van cyber security. Het gaat onder meer om een vierjarige bacheloropleiding en verscheidene minoropleidingen met doorlooptijden van één tot drie kwartalen. Daarnaast zijn in een aantal opleidingen onderwerpen opgenomen op het gebied van veiligheid in de cyberwereld.

Daarnaast werkt het lectoraat CSS in samenwerking met aantal andere organisaties, waaronder brancheorganisaties, banken, adviesbedrijven en overheidsinstellingen, aan het ontwikkelen van een kwalificatiestelsel voor professionals op het gebied van cyberveiligheid. In dit stelsel wordt geformuleerd welke beroepen (functies) op dit gebied worden onderkend en welke eisen aan deze beroepen worden gesteld. Het kwalificatiestelsel gaat competentie- en opleidingsprofielen bevatten

waarmee de opgeleide professionals kunnen laten zien welke kwalificaties ze gehaald hebben en in hoeverre zij hun kennis en ervaring steeds hebben bijgehouden. De werkgevers kunnen het kwalificatiestelsel gebruiken om hun werving en selectie op af te stemmen en zo de geschikte professionals te vinden. De Haagse Hogeschool en andere opleidingsinstellingen kunnen het tenslotte gebruiken om te bepalen welke competenties in de opleidingen op het gebied van cyberveiligheid aangeleerd moeten worden zodat ze op basis daarvan hun opleidingen kunnen inrichten.

Conclusie

De cyberwereld is van iedereen, en mensen en organisaties zijn er met handen en voeten aan gebonden. Het is echter wel een heel onveilige wereld. Aan de ene kant kunnen we daar niets aan doen, omdat grote delen van de cyberwereld onbeheersbaar en onveilig opgezet zijn en dat is nu niet meer te veranderen. Aan de andere kant gaan de meeste mensen in de cyberwereld wel erg nonchalant met de veiligheid om. Daardoor gebeuren ongelukken en daar is wel wat aan te doen. Het veiliger maken van de cyberwereld is een grote complexe operatie, waarbij de overheid het voortouw zou moeten nemen. Nu zitten we opgescheept met een schade van meer dan een miljard euro per jaar, alleen al in Nederland. Hoe langer we wachten met het veiliger maken van de cyberwereld, hoe groter de maatschappelijke schade wordt.

Referenties

[1] H. Seybert, *Internet use in households and by individuals in 2012*, Eurostat, 50/2012.
[2] *Cybersecuritybeeld Nederland CSBN-3*, Nationaal Cyber Security Centrum, 2013.
[3] L. Marinos & A. Sfakianakis, *ENISA Threat Landscape*, ENISA, 2012.
[4] *Internet Security Threat report 2013*, Symantec Corporation, 2013.
[5] P. Neumann, Illustrative risks to the public in the use of computer systems and related technology, http://www.csl.sri.com/users/neumann/illustrative.html
[6] https://www.security.nl/
[7] *Evaluatie van de rijkscrisisorganisatie tijdens de DigiNotar-crisis*, Inspectie Veiligheid en Justitie, 2012.
[8] http://nos.nl/artikel/566651-nsa-luisterde-35-wereldleiders-af.html
[9] http://www.nu.nl/tech/3635471/jaar-39-ddos-aanvallen-in-nederland.html
[10] http://www.eenvandaag.nl/binnenland/39770/sluizen_gemalen_en_bruggen_slecht_beveiligd
[11] http://www.kaspersky.com/nl/about/news/virus
[12] Amr Thabet, *Stuxnet malware analysis paper*, http://www.codeproject.com/
[13] J. Lewis & S. Baker, *The economic impact of cybercrime and cyber espionage*, McAfee/CSIS, 2013.
[14] *The cost of cyber crime*, Detica and The Cabinet Office, 2011.
[15] *2010/2011 Computer Crime and Security Survey*, CSI, 2011.
[16] *ICT Barometer over cybercrime*, Ernst & Young, 2011.
[17] http://www.kaspersky.com/about/news/virus/2013/nettraveler_is_back_with_new_tricks
[18] W. Stallings, *Data and computer communications*, Pearson Prentice Hall, Upper Saddle River, 2011.
[19] J. Wihbey, *The Arab Spring and the Internet: Research roundup*, the Journalist's Resource project, http://journalistsresource.org/studies/international/global-tech/research-arab-spring-internet-key-studies#
[20] https://www.digivaardigdigiveilig.nl/