In korte tijd is het Nederlandse cyber security onderzoek uitgegroeid van een nicheterrein tot een volwassen onderzoeksgebied. De komst van het Nationaal Cyber Security Centrum, de Cyber Security Raad en het Nationaal Cyber Security Research Programma laten een gedegen maatschappelijk inbedding zien. Dat verdient het onderwerp ook wel, zo maken prof. dr. Herbert Bos van de VU en prof. dr. Bart Jacobs van de RU duidelijk. De bedreigingen zijn serieus. *Door Leendert van der Ent*

Nederland maakt werk van Cyber Security

'Cyber Security dateert van de jaren zeventig. Destijds waren er "phone freakers" zoals Steve Jobs en zijn Apple-collega Steve Wozniak', vertelt Bos. 'Ze deden dat in navolging van Captain Crunch, oftewel John Draper. Die trof in 1972 een gratis fluitje bij de Captain Crunch cornflakes aan. Dat bleek geschikt om modemgeluiden te imiteren, waarmee het mogelijk werd gratis *long distance* te bellen. Tamelijk onschuldig dus, allemaal.' In de jaren tachtig en negentig nam de overlast echter toe. 'Maar het bleef tot aan het begin van het nieuwe millennium bij "liefhebbers" die door middel van grote wormen indruk wilden maken. Daarmee kon het internet worden platgelegd.'

Het waren kwajongensstreken, in vergelijking met de grimmige vormen die het hacken daarna aannam. Er ontstonden professionele, winstgedreven criminele organisaties. Ze kregen interne specialisaties: het hacken, het zo duur mogelijk verkopen van gehackte informatie, botnet-beheer, noem maar op. Daarnaast kwam de cybercriminaliteit vanuit staten op, zo wezen steeds meer incidenten uit. Vaak is daarbij met een beschuldigende vinger naar China gewezen. Bos: 'Analyse van de Stuxnet-cyberaanval op een Iraanse atoominstallatie leert dat die bijna alleen van een staat kan zijn gekomen – en waarschijnlijk niet China. Tegenwoordig is wel duidelijk dat ook Westerse landen behalve aan defensieve technologie eveneens geld uitgeven aan offensieve cyber security technologie.' Informeel vindt er binnen de Westerse wereld veel uitwisseling en samenwerking plaats tussen cyber security onderzoekers, zo geeft Jacobs aan.

Opschieten graag

De Nederlandse wetenschap heeft in korte tijd een behoorlijke omslag doorgemaakt, vertellen Bos en Jacobs. 'Tot voor kort was de Nederlandse wetenschappelijke cyber security gemeenschap erg klein, met een duidelijke specialiteit in cryptografie. Nederland en Europa zijn traditioneel sterk in de theoretische kant. Maar de meeste incidenten zijn niet cryptografie-gerelateerd.'

De laatste jaren is er dan ook veel meer aandacht voor de systeemkant gekomen, het dichten van mazen in de beveiliging. Bos: 'Inmiddels zijn er flink wat universitaire onderzoeksgroepen en een half dozijn hoogleraren die zich breed met cyber security profileren.' Jacobs: 'Elke universiteit en groep heeft zijn eigen specialisaties en zwaartepunten, zoals besturingssystemen, malware of smartcards.' De aanwezigheid op conferenties en het aantal wetenschappelijke publicaties wijzen erop dat Nederland tegenwoordig meedraait met de wereldtop. 'Het is een serieus vakgebied geworden', concludeert Bos dan ook. 'Er is echt een veiligheids-issue en die boodschap is politiek-maatschappelijk overgekomen.' (zie kader)

Het DigiNotar-incident maakte duidelijk hoe groot de risico's zijn

Jacobs belicht die politiek-maatschappelijke kant: 'Deze regering heeft cyber security als speerpunt. Minister Opstelten zit er bovenop. De Tweede Kamer betoonde zich voor de zomer van 2011 uiterst kritisch: "Overdrijft u niet, minister?" Toen kwamen DigiNotar en "lektober" (de maand van het privacylek) – waarbij overheidssites "lek" bleken – en werd voor een breder

Prof. dr. Herbert Bos werd op 1 februari 2012 benoemd tot hoogleraar aan de VU. Hij is betrokken bij het IIP Veilig Verbonden en medeopsteller van de Nationale Cyber Security Research Agenda

Prof. dr. Bart Jacobs, hoogleraar computerbeveiliging aan de RU, onder andere bekend van de perikelen rond de OV-chipkaart en lid van de Cyber Security Raad

publiek duidelijk wat de risico's zijn. De Tweede Kamer bleef kritisch, maar inhoudelijk compleet omgekeerd. De boodschap is nu: "Kunt u niet wat opschieten?"'

Verse stoottroepen

De oprichting van het Nationaal Cyber Security Centrum (NCSC) op 12 januari 2012 geeft aan hoe serieus het onderwerp wordt genomen. Jacobs: 'Daarvóór was er al een decennium het Government Computer Emergency Response Team (GovCERT). Binnen het NCSC werken de universiteiten, defensie, andere overheidsorganisaties en sleutelbedrijven zoals KPN samen om cybercalamiteiten het hoofd te bieden. Behalve onderlinge contacten was er ook internationale samenwerking. Het NCSC is daar nu een uitbreiding van. In het NCSC zitten als het ware de stoot- en verbindingstroepen in de digitale loopgraven. Ze staan paraat om de eerste klappen op te vangen, alle relevante partijen te mobiliseren en zo snel mogelijk te achterhalen waar een digitale aanval vandaan komt en wat daarvan de aard is.'

Het DigiNotar-incident benadrukte het belang van korte lijnen en elkaar persoonlijk kennen nog eens. Het maakte ook duidelijk hoe groot de risico's zijn. Jacobs: 'Er werden tijdens de inbraak valse certificaten aangemaakt. Het had veel erger kunnen zijn wanneer alle geldige certificaten op de zwarte lijst geplaatst waren. Heel veel digitale processen waren dan spaak gelopen. Een cyberaanval kan zodanig ontwrichtend werken, dat de VS hebben aangegeven het als een "act of war" te kunnen opvatten. Elk militair antwoord daarop achten ze geoorloofd.'

NWO en Cyber Security

De snelle wetenschappelijke ontwikkeling van cyber security in Nederland is volgens Bos gedeeltelijk te herleiden naar het Sentinels-programma van STW, NWO en ICTRegie. Dat succesvolle programma droeg ertoe bij dat wetenschappers in het wereldje elkaar beter konden vinden en dat het veel nauwer verweven raakte met bedrijfsleven en overheid. Vanuit het ICT-Innovatieplatform (IIP) Veilig Verbonden is het initiatief genomen voor Sentinels II, later de Nationale Cyber Security Research Agenda. Die agenda is geschreven door prof. dr. Herbert Bos, prof. dr. Sandro Etalle en dr. Erik Poll, in samenwerking met het bestuur van het IIP (te downloaden via *www.iipvv.nl*). Het Nationale Cyber Security Research Programma is daar nu uit voortgekomen.

Herbert Bos: 'Er is een schreeuwend tekort aan mensen met verstand van cyber security'

Cyber Security Raad en Research Programma

Voorafgaand aan de oprichting van het NCSC, vlak voor de zomer van 2011, stelde minister Opstelten de Cyber Security Raad in. Jacobs maakt daar deel van uit: 'Het NCSC doet veel vertrouwelijk operationeel werk, waarbij wetenschappers geen actieve rol spelen. Met de Raad staan we voor minder hectische, maar meer strategische opgaven dan het NCSC. Topmensen uit bedrijfsleven, overheid, defensie en wetenschap bevorderen via polderen de digitale veiligheid. Dat doen we onder andere via rechtstreekse adviezen aan het kabinet. Ons doel is het bewustzijn te verhogen, het onderwerp hoog op de agenda te krijgen binnen organisaties en strategische adviezen te verstrekken. De Raad heeft een sturende rol met betrekking tot cyber security onderzoek en de topsectoren, waarbinnen NWO onderzoeksgeld te verdelen heeft. Daarbij is het prettig dat het onderwerp cyber security het tij mee heeft. Alle activiteiten bij elkaar leiden tot een duidelijker beeld van wat er speelt rond cyber security en wat er nodig is.' >>

De Raad heeft bijvoorbeeld de Nationale Cyber Security Research Agenda omarmd. Deze vormt het kader voor de verdere onderzoeksprogrammering. Nu is het zaak dit ook echt gefinancierd te krijgen, merkt Jacobs op. Bos: 'De insteek is drieledig. Opgave één is om ervoor te zorgen dat de burger, de infrastructuur en de economie zo goed mogelijk preventief en reactief beschermd zijn. De tweede opgave sluit daarbij aan: opgave één omzetten in economische activiteit. Daar liggen grote kansen. Tot slot draagt het programma bij aan de ontwikkeling van strategische kennis die je als land paraat wilt hebben. Sommige problemen zijn sterk cultuurgebonden, zoals het EPD en het paspoort. Daarvoor moet je niet afhankelijk zijn van buitenlandse experts.'

Bredere opzet

Behalve aan ICT besteedt het onderzoeksprogramma ook aandacht aan belangrijke gerelateerde onderwerpen. Daartoe behoren juridische aspecten zoals privacy en informatiediefstal: wanneer kun en mag je wat doen? Daarnaast zijn er de organisatorische aspecten – hoe richt je een bedrijf goed en veilig in. Voorts zijn er de psychologische en economische aspecten die een plek hebben gekregen in het programma. Hoe verdient een criminele organisatie aan cybercrime? Hoe kun je dat tegengaan? Hoeveel schade lijdt de maatschappij erdoor?

Die bredere insteek van beveiliging is belangrijk, maar natuurlijk is de informatica nog steeds cruciaal, aldus Bos. 'Voor een scala aan zaken zoeken we oplossingen. Hoe ontwerp je nieuwe programmatuur inherent veilig? Hoe ga je om met oude, embedded software die overal in liften, stoplichten en allerlei andere zaken zit? Hoe ga je om met het forensische onderzoek na een incident, hoe bewijs je wat er is gedaan? Ook is het interessant om te analyseren hoe malware is opgezet, maar uiteraard maken de cybercriminelen die analyse zo moeilijk mogelijk.'

Verder ligt er het punt van het identity management – waarin een balans tussen transparantie en privacy nodig is. Steeds vaker wordt de digitale identiteit gestolen om 'vermomd' cybermisdaad te plegen. Dat vraagt om oplossingen en dus om onderzoek. Het ontwerpen van zeer goede digitale veiligheidsvoorzieningen is belangrijk. Toch bepaalt de gebruiksvriendelijkheid ervan uiteindelijk mede de effectiviteit. Daarom krijgt ook dit onderwerp de nodige onderzoeksaandacht in het onderzoeksprogramma.

Knelpunten

Er is nu een goede organisatorische inbedding van cyber security gecreëerd en er vindt goed onderzoek plaats. Dat wil niet zeggen dat alle knelpunten zijn opgelost, maakt Bos duidelijk: 'Onze kritische infrastructuur, gas, water, elektra is allemaal bereikbaar via het net. Je kunt dat niet zomaar even offline gaan doen, dan kun je niet concurreren. De bouwers van de systemen zijn goede engineers, maar ze zijn traditioneel altijd gericht geweest op "safety" en niet op "security". Dat maakt deze veelal oudere systemen kwetsbaar, want security laat zich moeilijk invoegen. Het is essentieel dat die diensten ononderbroken doorgaan, dus je kunt niet zomaar even security updates doorvoeren, omdat je niet zeker weet of het daarna nog wel werkt. Om die reden beperken de organisaties dit tot één keer per jaar. Wat je ook doet, je doet het hier nooit helemaal goed.'

Een tweede probleem is de kenniscapaciteit: 'Er is een schreeuwend tekort aan mensen met verstand van cyber security. Defensie heeft 50 miljoen euro uitgetrokken voor cyber security, maar de vraag is waar de specialisten vandaan moeten komen die het werk moeten uitvoeren. De universitaire infrastructuur is sterk uitgebreid, maar het kost tijd voordat er voldoende afgestudeerden de arbeidsmarkt opkomen om kennis aan bedrijven en overheid te leveren.'

Het onderwerp cyber security zal, zowel vanwege deze knelpunten als vanwege de toenemende actualiteit, voorlopig nog op voldoende prioriteit mogen rekenen. I/O

Bart Jacobs: 'In het NCSC zitten als het ware de stoot- en verbindingstroepen in de digitale loopgraven'

Workshop Cyber Security Verenigde Staten

Eind februari namen Bos en Jacobs deel aan een bijeenkomst over Cyber Security in Washington, geïnitieerd door NWO en het Department of Homeland Security (DHS). Deskundigen uit de Nederlandse Cyber Security-onderzoeksgemeenschap en specialisten van het Nationaal Cyber Security Centrum en het Nederlands Forensisch Instituut spraken met specialisten van DHS over de onderzoeksagenda's van beide landen. Deze bijeenkomst was georganiseerd in het kader van het bezoek aan de VS door Minister Opstelten van Veiligheid en Justitie. De Minister en de Amerikaanse Minister Janet Napolitano van het Department of Homeland Security tekenden een intentieverklaring over de samenwerking tussen Nederland en de VS voor het creëren van een veilige en veerkrachtige cyberomgeving. De komende maanden werken de Nederlandse en Amerikaanse overheid aan een Wetenschaps- en Technologieovereenkomst. NWO en DHS zullen het subsidieproces ontwikkelen, terwijl onderzoekers in beide landen gezamenlijke onderzoeksvoorstellen uitwerken. Het is de intentie om nog dit jaar de eerste projecten te laten starten.

'Wetenschappelijke kennis kan sterk bijdrage aan de oplossing van actuele uitdagingen in Cyber Security. Gezien het wereldwijde karakter van cybercrime is internationale samenwerking essentieel. Het is dan ook goed om te zien dat beide landen concrete mogelijkheden zien voor samenwerkingsprojecten', aldus Louis Vertegaal, directeur NWO/EW. Vooraf zei Bos: 'Het is belangrijk om contacten te leggen en mogelijkheden voor gezamenlijke projecten met gedeelde financiering te onderzoeken. Wat er uitkomt weten we niet, maar ik zou calls voor onderzoeksprojecten toejuichen.' Jacobs: 'De bijeenkomst is een internationaal signaal dat het onderwerp op de agenda staat.'