“Om grip te krijgen op cybersecurity moet niet alleen de overheid zich verantwoordelijk voelen, maar alle partijen in de samenleving.” Dat zegt Melanie Peters, directeur van het Rathenau Instituut. “De discussie moet niet alleen gaan over onze veiligheid, maar ook over andere waarden zoals gezondheid, gelijke behandeling, toegang tot noodzakelijke diensten en goederen, eerlijke informatie, een eerlijke prijs en uiteindelijk onze menselijke waardigheid.”

Dr. ir. Melanie Peters
directeur Rathenau Instituut

DEBAT NODIG OVER DE BALANS TUSSEN WAARDEN

CYBERSECURITY? HET GAAT NIET ALLEEN OM VEILIGHEID

In 1993 kreeg ik mijn eerste e-mailaccount. Ik werkte toen aan de universiteit van Texas. Wij waren in Texas een van de eersten met een account. Dat kwam dankzij een van de docenten: dr. Combs. Hij had een bijzondere belangstelling voor digitale zaken. Combs had een handleiding ontwikkeld met de titel "Veilig surfen op het web". Het omslag toonde een plaatje van een man in een gebloemde surfbroek die voor hoge golven stond. De boodschap was: surfen is fun, maar ook gevaarlijk.
Combs vertelde ons dat het web was ontwikkeld door het leger en dat je nooit wist welke route je berichten namen. Dit om ervoor te zorgen dat niet de hele communicatie via het web onmogelijk zou worden als er een route zou uitvallen. "Alles wat je schrijft, wordt gescreend en je weet dus niet waar en door wie", zei hij. "Als je een mail naar een collega stuurt met een doodswens aan de president zul je bezoek krijgen van de autoriteiten."
Nu, 24 jaar later, ben ik me bij elke mail die ik stuur nog steeds ervan bewust dat er iemand meekijkt. Als ik denk aan mijn dochters en hun klasgenoten, dan besef ik dat zij dit idee absoluut niet hebben. Ze zijn opgegroeid met internet en zien het alleen maar als leuk en handig.

Mails naar de halve wereld

Sinds 2015 ben ik directeur van het Rathenau Instituut. Mijn instituut gaat over onderzoek en dialoog over nieuwe ontwikkelingen in wetenschap, technologie en innovatie. Het instituut heeft een speciale taak om de politiek en het publiek te informeren en in staat te stellen zelf betere beslissingen te nemen. Vanaf mijn werk bij het Rathenau Instituut mail ik de spreekwoordelijke halve wereld. Wie staan er niet allemaal in de cc? En hoe makkelijk wordt een mailtje doorgestuurd? Ik krijg ook ’s avonds en in het weekend mail. Een oponthoud van een of twee dagen? Het zou onwerkbaar zijn. Ik merk dat het contact tussen collega’s onderling en tussen organisaties veel minder formeel is geworden. Er worden maar weinig brieven nog officieel ingeboekt.
De wereld is duidelijk veranderd sinds het internet 25 jaar geleden het domein van de liefhebbers verliet en iets werd voor ons allemaal. Kleuters halen spelletjes van het web. Een iPad is speelgoed geworden. Mijn

“Surfen is fun, maar ook gevaarlijk”

tienerdochter en haar klasgenoten appen het liefst tot midden in de nacht en bestellen kleding online (als ze het ID van hun ouders kunnen gebruiken).
Internet en alle applicaties die daar bij horen zijn zo gemakkelijk te gebruiken, dat je niet hoeft na te denken over de wereld die daar achter zit. Dat maakt het juist zo aantrekkelijk. Maar hoe moet dat dan met veiligheid op internet als we er zo onbewust mee om gaan? Of hoeven we ons daar als gebruiker eigenlijk niet mee bezig te houden?

Internet als kritische infrastructuur
Lange tijd was de veiligheid van consumentenproducten misschien niet zo’n probleem. Tenminste, het werd in ieder geval niet in verband gebracht met cybersecurity. Tot zo'n vijf jaar gelden. Toen publiceerde het Rathenau Instituut bijvoorbeeld de uitgave ‘You have been hacked!’, een magazine met als ondertitel ‘cybersecurity can no longer be an afterthought’. Het magazine kwam voort uit een internationaal project en inventariseerde studies van collega-instituten wereldwijd. Het concentreerde zich op risico’s voor kritische infrastructuren. Dat zijn infrastructuren die essentieel zijn voor het functioneren van onze samenleving. Denk daarbij aan het elektriciteitsnet, aan olie en gasbedrijven, aan de waterleiding of het aan verkeerssysteem. Maar denk ook aan ziekenhuizen en alle andere infrastructuur die nodig is voor gezondheid, veiligheid, de openbare orde en economisch welzijn. Bij al deze voorbeelden gold toen al dat ze vaak digitaal aangestuurd werden. Vaak gebeurde dat via netwerken die geleased werden van private partijen en die niet in het zicht waren van overheidsbescherming en controle. Wij waarschuwden toen dat dit de achilleshiel zou worden van deze systemen.

Oorlogen in cyberspace
Een van de voorbeelden uit het Rathenaurapport kan ik me nog goed herinneren. Het ging over een Iraanse kerncentrale. In 2010 werd Stuxnet gevonden in een uraniumfabriek in Iran. Stuxnet is software die spioneert of sabotage pleegt op het type computers dat gebruikt wordt in industriële processen. Stuxnet werd ontwikkeld om software van Siemens-systemen aan te vallen en kon onopgemerkt pompen, centrifuges en andere onderdelen ontregelen. De capaciteit van de uraniumfabriek daalde tot 30%. Aangenomen werd dat alleen een andere staat een dergelijk complexe en gerichte software kon schrijven en dus achter de aanval zou zitten.
Het is niet verwonderlijk dat alle rapporten in die tijd wezen op nationale actie en internationale afspraken tegen wat toen al ‘oorlogen in cyberspace’ heette. Als je een opwerkingsfabriek kon stilleggen, dan kon ook de olietoevoer of de samenstelling van drinkwater veranderd worden en dan kon je ook een heel land schaden.

Kleine speler, grote schade
Het World Economic Forum zette het onderwerp op de agenda, de NAVO werd wakker en nationale overheden lieten onderzoek doen. Ook de Verenigde Naties werden opgeroepen om met acties te komen. Er moest nieuwe internationale wetgeving komen en afspraken in WTO-achtige setting. Het gaat namelijk om vergrijpen die over de grenzen heen gaan en die opsporing en handhaving bemoeilijken. Toch werd toen al duidelijk dat deze kritische infrastructuur niet alleen door staten kon worden aangevallen, maar ook door individuen of in groepen opererende hackers. De groep Anonymus sprak tot de verbeelding. Kleine spelers zijn ook al snel in staat om grote schade aan te richten. Om dit aan te tonen hackten tv-journalisten bijvoorbeeld een pompstation dat ervoor zorgt dat Nederland niet onder water loopt.

Internet of everything
Wat als deze kritische infrastructuur ook nog eens verweven wordt met consumentensoftware? Dat is op dit moment gaande. Alles wordt met alles verbonden. Neem het voorbeeld van een decentrale elektriciteitsvoorziening. Energie van zonnepanelen wordt teruggeleverd aan het net op het moment dat een huishouden te veel energie heeft opgewekt. Bewoners kunnen dit volgen via een slimme meter, die zo gebruiksvriendelijk mogelijk is vormgegeven. Hoe beveilig je alle schakels in dat netwerk? Is het dan nog voldoende om het internet en apps alleen te zien als behulpzaam en als gadget? Nog een voorbeeld van kritische infrastructuur is wat mij betreft valse Facebookberichten. De berichten zijn heel makkelijk in omloop te brengen en beïnvloeden de publieke opinie en de democratie. Vroeger kon je de gedrukte krant niet zomaar veranderen.
En het gaat verder. Wij gebruiken niet alleen het internet, het internet gebruikt ons ook. Wij lezen niet alleen Facebook, Facebook leest ons ook. De elektronische infrastructuur verzamelt data over ons en combineert die zonder dat wij als gebruikers daar zicht op hebben.

Balans tussen waarden
Al met al kunnen we concluderen dat niet alleen het internet kwetsbaar is en daarmee onze kritische infrastructuur en collectieve voorzieningen. Ook wij als personen zijn kwetsbaar. Ook onze waardigheid is kwetsbaar. Want cybersecurity gaat inmiddels ook over

het hacken of misbruiken van persoonsdata. Nou staan privacy en veiligheid wel aardig hoog op de agenda, maar andere waarden zoals onze gezondheid, onze autonomie, gelijke behandeling en eerlijke informatie nog niet. Wat mij betreft zou het debat moeten gaan over de balans tussen deze waarden.
Als het gaat om de ontwikkelingen rondom nieuwe technologieën en de impact daarvan op de Nederlandse samenleving, dan hebben weinig partijen het totaalbeeld op het netvlies. Daarmee is er ook te weinig zicht op de negatieve en positieve mogelijkheden voor de samenleving.
Ik vind het overigens niet vreemd dat we geen goed overzicht hebben over alle ontwikkelingen. Aan de ene kant diende internet het gemak en de mens en hoefden we ons er ook niet mee bezig te houden. Aan de andere kant hebben we de grote discussies over ‘cyber’, waar internationale afspraken voor nodig zijn. Nu komen die twee werelden bij elkaar. Het cybersecurityprobleem is in elk geval niet opgelost als burgers hun privacy opgeven en denken dat alleen de overheid ons zal beschermen.

Vormgeven van samenleving

Nederland bevindt zich op een mooie positie. We lopen op veel terreinen voor in de ICT-ontwikkeling. Maar dat kan alleen zo blijven als gebruikers alerter worden en als maatschappelijke spelers een grotere rol gaan spelen. Dan denk ik aan het onderwijs, aan de werkgevers, aan softwareontwerpers en aan de bedrijven die apps in de markt zetten en die slimme apparaten ontwikkelen. Cybersecurity gaat niet alleen over veiligheid. Het gaat om de samenleving die we met hulp van digitale technologie met elkaar willen vormgeven.

Meer informatie

- You have been hacked! Magazine van het Rathenau Instituut (2012) https://www.rathenau.nl/en/publication/volta02
- Big data en slimme algoritmen - projecten van het Rathenau Instituut die gaan over cybersecurity https://www.rathenau.nl/nl/page/big-data-en-slimme-algoritmen