Interview door Pieter Peerlings

‘Het is een geweldige tijd om technologische antwoorden te vinden’

Ab van der Touw

“Het is een geweldige tijd om technologische antwoorden te vinden op allerlei vraagstukken.” Als ceo van Siemens is Ab van der Touw zeer goed op de hoogte van de kansen die digitale ontwikkelingen bieden. Maar hij is ook zeer gespitst op de risico’s. Cybersecurity is van fundamenteel belang bij de activiteiten van bedrijven. Niet iedereen is van dat belang doordrongen. Raden van bestuur en commissarissen houden zich meer bezig met finance dan met IT. “Men heeft gewoon te weinig ervaring op dat gebied.”

Dat de meeste mensen nauwelijks oog hebben voor digitale veiligheid illustreert Van der Touw met een voorbeeld. "De ceo van een telecombedrijf praat regelmatig met collega's over het belang van cybersecurity. Na zo'n gesprek geeft hij dan een usb-stick aan de secretaresse, met de vraag of ze dat even kan openen. En vrijwel iedereen doet dat zonder nadenken. Men is zich er niet van bewust hoe gevaarlijk dat is." Van der Touw gaat bij Siemens over de kritieke infrastructuur, en die is naar zijn zeggen 'vergeven van embedded software'. Die software verhoogt de gebruiksvriendelijkheid, maar biedt ook openingen voor misbruik.

Spionage

"Bij Siemens doen 30.000 man aan research and development, waarvan er 20.000 software ontwikkelen, voornamelijk voor hogesnelheidstreinen en energiecentrales. Voor ons is het dus een core competence om ons bewust te zijn van de gevaren voor kritieke infrastructuur. Ook al omdat niet alle landen waar we opereren even stabiel zijn als Nederland. Veel software die nu gebruikt wordt is al wat ouder en ongedocumenteerd, en is daarmee extra kwetsbaar. In de begintijd maakte niemand zich zorgen om cybersecurity, dus er zijn nogal wat systemen waar je vrij gemakkelijk in kunt." Bedrijfsspionage is aan de orde van de dag, zegt Van der Touw. "Wij krijgen wereldwijd training in tegenmaatregelen. Want dat is feitelijk het grootste gevaar: dat kritieke kennis wordt gestolen, of dat ermee gemanipuleerd wordt."

Er wordt veel meer gespioneerd dan we denken, weet Van der Touw. "Nederland is open en netjes, en denkt dat de rest van de wereld dat ook is. Maar in andere landen hebben ze minder scrupules. Er zijn bedrijven en staten die heel bewust spioneren. Stel je een land voor dat de ambitie heeft om superieure auto's te maken, en dat heel graag even wil inloggen bij bijvoorbeeld BMW of Audi om toegang te krijgen tot de broncodes van de software van die auto's. Alles zit in software, vanaf het ontwerpproces tot aan de productie en het onderhoud. Dat is kennis van honderdduizenden manjaren, en die kun je soms gratis en voor niets krijgen. Als je weet hoe het werkt is dat niet zo moeilijk."

Cybergerelateerde kansen en risico's

Een goede manier om het thema meer onder de aandacht te brengen van het bestuur is om aan te haken bij risicomanagement, denkt Van der Touw. "Bij de bestaande enterprise risk management systems zet je kansen en risico's op een rijtje. Dat framework is heel geschikt om de cybergerelateerde kansen en bedreigingen te bespreken. Het staat namelijk toch al op de agenda van de raad van bestuur en van de raad van commissarissen."
Naarmate de kennis van de risico's toeneemt, neemt de naïviteit af, al verwacht Van der Touw dat er eerst een paar incidenten moeten plaatsvinden voor er echt actie wordt ondernomen. Terwijl het gevaar toch heus reëel is. En het beperkt zich niet tot het bedrijfsleven. "Toen het Nederlandse leger afscheid nam van zijn tanks vroegen sommigen zich af hoe dat nou moest met onze verdediging. Maar die tanks spelen daar geen enkele rol bij, dat is nostalgie. Het gevaar komt nu uit de stekkerdoos."

Een ander risico is de gevoeligheid van digitale systemen voor storingen. "Dat is een directe bedreiging van je bedrijfszekerheid. Als het netwerk uitvalt, kun je iedereen naar huis sturen. En juist wij zijn daar erg afhankelijk van. In India is er zo vaak geen stroom, dat ze wel zorgen voor analoge of digitale alternatieven om door te kunnen gaan. Op dit moment lopen wij dat risico niet, maar vergis je niet: de veranderingen in de energiehuishouding en de opwekking van energie leiden tot een enorme druk op het transmissie- en transportnetwerk. Het gevolg zijn meer storingen met mogelijk fatale gevolgen. Er moeten enorme inhaalslagen worden gemaakt."

Business ontwikkelen

Kansen zijn er natuurlijk ook. Meer dan genoeg zelfs, volgens Van der Touw. "Nederland is een van de meest technologisch vooraanstaande landen, met een grote welvaart en een open cultuur. Nederland is daarmee heel goed gepositioneerd om die kennis toe te passen en wereldwijd te exploiteren. We kunnen dus echt business ontwikkelen op dit gebied. Ik ben zelf betrokken bij een samenwerking onder de naam Hague Security Delta, tussen een aantal marktpartijen, de overheid en het European Network of Cyber Security. De bedoeling is om in Den Haag een campus te ontwikkelen waar overheid,

‘Als het netwerk uitvalt, kun je iedereen naar huis sturen.’

bedrijfsleven en onderwijs samenwerken. Dat is zowel voor Nederland als voor Den Haag een kans.”

Samenwerken

Van der Touw gelooft sterk in de voordelen van een transparante samenwerking tussen bedrijfsleven en overheid. “Siemens werkt aan een opleiding tot medisch technoloog, samen met de universiteiten van Groningen en Twente en tientallen mkb-bedrijven. Uit de apparatuur die daarvoor wordt ontwikkeld komen toepassingen die zelfs de bedenkers niet hadden voorspeld, en die alleen maar kunnen ontstaan omdat de deelnemende partijen beseffen dat ze samen meer kunnen dan alleen. Of neem een spoortraject. Dat kun je alleen efficiënt aanleggen als overheid en bedrijfsleven nauw samenwerken. Treinen zelf kunnen ook het beste worden ontworpen als bekend is waar ze moeten worden ingezet, en aan welke eisen ze moeten voldoen. Die samenwerking moet innig zijn, zodat potentiële problemen in een vroeg stadium worden herkend. Dan kun je er iets aan doen voor het probleem werkelijkheid wordt.”

De toekomst ligt bij de smart networks, denkt Van der Touw. “In de energiesector heet dat overigens smart grids, wat ook de naam is van onze eigen wereldwijde divisie op dat gebied. Zowel daar als bij de verkeersinfrastructuur moet je de netwerken intelligenter maken om de energieconsumptie en de kosten naar beneden te brengen. Dat geldt bijvoorbeeld ook voor dijken. Nederland is van dijken afhankelijk. We werken met TNO aan een project waarbij we slimme sensoren gebruiken om te meten wanneer een dijk gebreken gaat vertonen en je hem dus zou moeten verstevigen. Nu weet je dat niet, en dus versterken we dijken onnodig, om maar zeker te weten dat ze niet doorbreken. We stoppen er voor miljoenen euro’s aan zand en puin in, maar eigenlijk is dat geld weggooien. Door sensoren te plaatsen kun je veel gerichter zeggen waar de risico’s zitten. Iets dergelijks geldt ook voor het verkeer. Door meer informatie te verzamelen over verkeersstromen kun je ingrijpen voor er problemen ontstaan.”

Blijvende transparantie

Smart networks hebben ook een nadeel, en dat is dat ze inbreuk kunnen maken op de privacy. “Met een slim gebouwensysteem of een smart grid kun je tot op huisadres en persoonsniveau in de gaten houden wat er gebeurt. Ik ben in Texas bij bepaalde power grid companies geweest. Die zijn zeer vooruitstrevend in die smart grids, want als er een probleem is in het net moet je snel kunnen zien waar dat is. In Texas moet je immers grote afstanden overbruggen, en je wilt niet voor niets 80 kilometer naar een boerderij rijden. In die grids hangen camera’s, tot op huisniveau aan toe. In de controlekamer van dat bedrijf zie je dus dat meneer X van die en die gemeente op dit moment zoveel energie gebruikt, en dat zijn vrouw weg is. Dat zou in Nederland niet zijn toegestaan. Maar die mogelijkheden zijn er wel. We zijn zo transparant geworden als de pest.”

Die openheid is blijvend, zegt Van der Touw, omdat de voordelen ervan te groot zijn. “Kijk eens naar de geestelijke gezondheidszorg of de ouderenzorg. Er gaat onvermijdelijk veel meer digitale bewaking plaatsvinden. Dat brengt allerlei risico’s met zich mee voor de privacy en de bescherming van de persoonlijke integriteit. Er zal dus ook nieuwe regelgeving komen om slimme netten af te schermen, en om die wetten te handhaven is blauw op straat minder relevant. Je moet eerder meer blauw in het stopcontact hebben. Ik denk dat de Belastingdienst, de milieuautoriteiten en het Openbaar Ministerie extreem achterlopen op dat vlak.”

Privacy

Het opgeven van privacy kan ook vrijwillig gebeuren. “In Groningen nemen we deel aan een project waarbij we mensen op individuele basis volgen. We brengen alles in kaart, van hun eet- en sportgedrag tot hun werk, hun medicijngebruik, hun ziekten en genen. Je kunt dan bepalen waar mensen met bepaalde genen en een bepaald leefpatroon wel of geen baat bij hebben als het om hun gezondheid gaat. We ontwikkelen dus personalised medicine. De bedoeling is om ervoor te zorgen dat mensen als ze ouder worden twee jaar langer gezond blijven. Dat betekent dat de gezondheidszorg enkele miljarden goedkoper kan, en dat de kwaliteit van leven stijgt. Dat is iets wat heel veel mensen willen. De prijs die je daarvoor betaalt is dat je hele hebben en houden gevolgd wordt, maar er zijn genoeg mensen die er vrijwillig aan meewerken. Het is namelijk ook in hun persoonlijk belang.”

Van der Touw heeft duidelijk plezier in zijn werk. “Het is een geweldige tijd om technologische antwoorden te vinden op allerlei vraagstukken. Je moet je voorstellen dat je degene bent die de technologie ontwikkelt die de fileproblematiek min of meer oplost, zonder het asfalt aan te passen. Er zijn miljarden te winnen in de gezondheidszorg en in de energievoorziening. Er zijn slimme oplossingen mogelijk om het net efficiënter te laten functioneren. Er wordt ontzettend veel verspild in deze samenleving. Het is toch prachtig om dat op een slimme manier tegen te gaan?”

Drs. **Ab van der Touw** (1955) studeerde geschiedenis en klassieke talen aan de Universiteit van Leiden en heeft een MBA in supply chain management. Sinds 1985 was hij werkzaam in diverse bestuursfuncties, waaronder divisie directeur Engineering & Services, Industrial Solutions, Water & Technologies en Oil & Gas bij Siemens. Sinds 2010 is hij bestuursvoorzitter van Siemens Nederland.
Daarnaast is hij lid van de commissie Nationale Veiligheid (NIVD), voorzitter van het Dutch Ambassadors Diversity Network, commissaris bij Deloitte, Jet-Net en Rabobank Vlietstreek-Zoetermeer, lid van de raad van advies Defensie en Veiligheid van TNO en lid van het dagelijks bestuur van VNO-NCW.

‘Er wordt ontzettend veel verspild in deze samenleving. Het is toch prachtig om dat op een slimme manier tegen te gaan?’