Waarom cybersecurity bestuurders aangaat

“De economische en sociale afhankelijkheid van ICT neemt toe. Dat ICT kwetsbaar is, bleek weer door de verspreiding van het I Love You-virus. Cyber-warfare lijkt futuristisch maar kan reële vormen aannemen wanneer systemen platgelegd worden door een e-mailbombardement of doordat sites van bedrijven of overheden gemanipuleerd worden met ongewenste informatie of desinformatie.”

Ter voorbereiding van deze middag heb ik in de archieven van de dienst gezocht naar de termen cybersecurity en cyberdreiging. Ik vond deze passage in het jaarverslag van de BVD over het jaar 2000. 17 jaar geleden dus.

Voor de jongeren onder ons: de Binnenlandse Veiligheidsdienst BVD is de voorloper van de AIVD en het I Love You-virus was een onschuldig ogende mail die zich verspreidde via het adresboek in Outlook.

Probeer maar eens de verleiding te weerstaan een bestand te openen dat je van een bekende krijgt, met als onderwerp I Love You. Door de bijlage te openen overschreef je allerlei bestanden op je computer. De totale schade bedroeg zo'n 5 miljard dollar.

Als je de tekst uit dat jaarverslag nog eens terugleest, dan lijkt er niet zo veel veranderd in de afgelopen 17 jaar. Ook de 'WannaCry'-malware van een week geleden manipuleerde overal ter wereld diverse systemen met grote schade tot gevolg. Het mag voor consumenten misschien aantrekkelijk lijken geheel gratis te parkeren in overdekte garage in het centrum, maar een dergelijke cyberaanval vreet aan de basis van onze maatschappij.

Waar we aan het begin van deze eeuw misschien nog zoekende waren in de digitale ruimte, waar nog sprake was van een zekere onbekendheid met de materie, hebben we tegenwoordig geen enkel excuus meer de digitale dreiging en de urgentie van cybersecurity te onderschatten. Geen enkel excuus!

Ik zou daarom als eerste met nadruk naar voren willen brengen vandaag: de digitale dreiging is vandaag de dag zo groot en divers, dat niemand haar alleen aan kan. Publieke en private sector moeten de handen ineenslaan.

Een platform als iBestuur en het feit dat hier ruim 200 betrokkenen en geïnteresseerden in de zaal zitten, vind ik daarom hoopvol. Goed ook dat lokaal, regionaal en nationaal niveau vertegenwoordigd zijn. Ik zie al vergaande publiek-private samenwerking in de Cyber Security Raad en samenwerkende overheden in Nationaal Cyber Security Centrum. We hebben iets geleerd de afgelopen 17 jaar!

Het is trouwens opmerkelijk dat het dreigingsbeeld in die periode consistent is geweest en zich al aandiende terwijl internet nog in de kinderschoenen stond. Het geeft misschien wel aan dat we een heel bekwame dienst hebben. Ik laat dat natuurlijk aan u!

Let u nog even op de eerste zin:

De economische en sociale afhankelijkheid van ICT neemt toe.

Anno 2017 is de sociale afhankelijkheid inderdaad niet minder geworden.

Een blik op straat, in een winkel of in het openbaar vervoer zegt genoeg. Iedereen is vastgeklonken aan zijn mobiele device. We zitten allemaal op Twitter, Facebook en LinkedIn. We bellen niet, maar we appen. Wie van u schrijft er nog wel eens een brief aan familie of vrienden? Ons privéleven speelt zich grotendeels af in de grote digitale ruimte. “We are all connected”, was het motto van de OneConference vorige week. Het ‘internet of things’ geeft extra dimensies: “All is connected.”

De digitalisering heeft ook een geweldige boost gegeven aan onze economie en aan ons welvaren.

We winkelen online, we boeken onze vakantie online. Stond ons land al in de bovenste regionen van de ranglijstjes van grootste zeehavens en grootste luchthavens in de wereld, nu kunnen we daar de digitale toegangs- en verdeelpoort van de Amsterdamse Internet Exchange aan toevoegen.

We lopen voorop met onze goed ontwikkelde IT infrastructuur. Maar een volwassen connectie met de digitale wereld brengt ook een volwassen digitale dreiging met zich mee. De agrarische technologie, de design sector, de chemische industrie, logistiek of life and health sciences: het zijn allemaal pareltjes van onze economie. Zeer aantrekkelijk voor anderen.

Daarmee kom ik op het tweede element dat ik vandaag onder de aandacht wil brengen.

Spionageaanvallen vormen een reëel risico voor het Nederlandse bedrijfsleven en de overheid.

Het intellectueel eigendom in de genoemde sectoren vertegenwoordigt enorme investeringen in tijd, capaciteit en financiën. We hebben het over miljoenen en miljoenen euro's. Diefstal daarvan brengt het verdienvermogen of zelfs het voortbestaan van bedrijven in gevaar. Met alle gevolgen vandien voor de economie en de maatschappij.

Ik wil dat graag illustreren met een voorbeeld.

Mijn dienst, de AIVD, heeft onlangs een succesvolle digitale aanval onderkend op een grote hightech multinational met diverse vestigingen in Nederland. Het bleek dat een aanvaller ruim twaalf maanden lang toegang heeft gehad tot het wereldwijde netwerk van het getroffen bedrijf. De aanvaller verkreeg toegang tot ruim 250 wachtwoorden van user accounts, waaronder diverse administrator accounts. Dat betekent vrijwel volledige controle over dat netwerk. Volledige controle over het netwerk door een buitenstaander, stelt u zich dat eens voor!

Daarmee heeft de aanvaller ruim 100 gigabytes aan voornamelijk ontwerpen en testresultaten van diverse producten, onderdelen en software buitgemaakt.

We hebben het hier over gemaakte investeringen die je nog maar moeilijk terugverdient, als ze in een ander land dezelfde blauwdrukken hebben. Het bedrijf is zijn innovatieve ideeën kwijt. Het zorgt voor toenemende oneerlijke concurrentie, waardoor prijzen onder druk komen te staan. Zoals gesteld, een concrete en directe dreiging voor het verdienvermogen.

Natuurlijk zijn wij in contact getreden met het bewuste bedrijf en hebben hen gewezen op de aanval en op de maatregelen die zij kunnen nemen.

Jaarlijks worden wereldwijd duizenden publieke en private organisaties aangevallen. Ook de Nederlandse overheid ligt dagelijks onder digitaal vuur. En de kosten van herstel bij de getroffen bedrijven en organisaties na een cyberaanval blijken bijna altijd hoger dan de kosten van preventie.

Maar spionage heeft ook een politieke dimensie en dat is mijn derde punt. Mijn dienst ziet ook op het gebied van politieke spionage steeds meer agressiviteit bij verschillende buitenlandse inlichtingendiensten.

Natuurlijk zijn buitenlandse mogendheden van oudsher geïnteresseerd in de werkelijke intenties van ons land: “Wat wil Nederland ten aanzien van de NAVO?”, “In wat voor Defensiematerieel is Nederland geïnteresseerd?”, “Hoe staat de regering tegenover de nieuwe president?” Dat zijn vragen die andere landen zich stellen. Dat doen ze al eeuwen lang.

De digitale ruimte versnelt en vereenvoudigt die klassieke vorm van spionage, maar vergroot ook het bereik. Zonder al te grote risico’s, want attributie (who did it?) is niet eenvoudig.

Ook overheidsinstellingen zijn vrijwel dagelijks doelwit van langdurige en hardnekkige cyberaanvallen. En niet alleen op nationaal niveau.

Ook binnen lagere overheden is voldoende gevoelige en waardevolle informatie beschikbaar waar buitenlandse machten interesse in hebben. Bijvoorbeeld vergaderstukken, notities of beleidsstukken over een vitaal bedrijf dat zich in uw gemeente of provincie bevindt. We mogen daarin niet naïef zijn, onze informatiepositie niet onderschatten en onze veiligheid niet overschatten.

De vraag die u zich daarbij zou kunnen stellen, is: “Heb ik de risico’s wel scherp voor ogen?” Een vraag die wij als AIVD ook aan u stellen. Daarom brengen wij gezamenlijk met onze collega’s van de Militaire Inlichtingen- en Veiligheidsdienst vandaag een brochure uit die organisaties daarbij kan helpen: “Bent u zich bewust van de risico’s van cyberspionage?”

De publicatie geeft inzicht in de manier waarop cyberspionage in zijn werk gaat, reikt basismaatregelen aan en biedt ICT-afdelingen technische handvatten om de weerbaarheid te vergroten.

De publicatie schetst precies waar het hier om gaat vandaag: Waarom gaat het u als bestuurder aan en hoe krijgt u als bestuurder grip op cybersecurity.

De publicatie is vanaf nu terug te vinden op onze website.

Voor de volledigheid, ook wij als AIVD willen inzicht in de verborgen agenda's van bepaalde landen. Ook wij doen daar onderzoek naar en vergaren politieke inlichtingen. Daarmee kan onze regering zijn buitenlandbeleid bepalen. Wij hebben daarvoor een opdracht van de regering en wij hebben een wet die zegt wat wij wel en niet mogen. En wij worden bij de uitvoering nauwlettend gecontroleerd.

Nog even terug naar het jaarverslag 2000, waar we konden lezen:

Cyber-warfare kan reële vormen aannemen doordat sites van bedrijven of overheden gemanipuleerd worden met ongewenste informatie of desinformatie.

Ook dat is nog steeds actueel en brengt me op mijn vierde punt. Desinformatie in het digitale domein is een toenemende dreiging voor politieke besluitvorming.

De verspreiding van desinformatie gebeurt veelal subtieler dan we denken. Via een vervalste site van de Nederlandse ambassade in Moskou, of een ongefundeerd bericht op internet dat een Russisch-Duitse vrouw zou zijn verkracht door Arabische immigranten. Het verspreiden van nepnieuws, als onderdeel van een nieuwe verhevigde vorm van propagandaoorlog.

Ook op het lokale niveau. Probeer maar eens een afgewogen besluit te nemen over de opvanglocatie voor asielzoekers, terwijl zich via sociale media allerlei moeilijk verifieerbare feiten over de risico's van migrantengroepen verspreiden.

Dames en heren,

de inzichten bij onze dienst wijken niet per se af van wat u op basis van open bronnen al dacht. Maar onze

inzichten zijn mede gebaseerd op de informatie die we met inlichtingenoperaties hebben verworven bij de oorsprong van activiteiten in de digitale ruimte, de statelijke actoren. Die inzichten laten een ronduit zorgelijk beeld zien. Het leidt voor mij daarom geen twijfel dat cybersecurity op de bestuurstafel thuis hoort.

Het digitale domein faciliteert en ondersteunt de explosief toenemende omvang en de reikwijdte van economische spionage, de mogelijke indringende gevolgen van politieke spionage en het destabiliserende karakter van politieke desinformatie. Cybersecurity is daarom “chefsache”.