Schrijftalent gezocht!
In deze Militaire Spectator is plaats gemaakt voor een gastcolumn. Daarin gaat R. van Doorn in op het debat rond cybersecurity.
De redactie van de Militaire Spectator daagt ook andere lezers uit om een gastcolumn te schrijven. Het thema is vrij, maar moet passen binnen de formule van het tijdschrift. De boodschap moet relevant zijn voor de lezers.
Het moet gaan om een gefundeerde eigen mening, om een logisch opgebouwd betoog en de feiten moeten kloppen en verifieerbaar zijn. Een bijdrage mag maximaal duizend woorden tellen. U kunt uw gastcolumn sturen naar de bureauredactie (zie colofon). De redactie wacht reacties met belangstelling af.

De hoofdredacteur

Cybersecurity is een illusie

Maj. (R) R. van Doorn

Om maar met de computer in huis te vallen: computersystemen zijn niet adequaat te beveiligen. Een gemiddelde gatenkaas is beter beschermd. Een computersysteem is een *black box*. Er is niemand in de hele wereld die exact weet hoe de hardware en software van een computersysteem precies in elkaar zitten en werken, welke bewuste en onbewuste fouten er in zitten. Het gevolg is dat software continu geüpdatet moet worden, wat overigens in de praktijk niet altijd gebeurt. Na een update is een systeem niet veilig, want het betekent slechts dat bekende kwetsbaarheden verholpen zijn. Er zijn bedrijven en individuen die actief zoeken naar *zero-day* (onbekende) kwetsbaarheden, hier geen melding van maken en deze doorverkopen aan derden. Die klanten krijgen de garantie dat beveiligingssoftware die zero-day-aanval niet detecteert.

De grootste dreiging gaat niet uit van technische gebreken of ondoorzichtigheid, maar van de mens. De Amerikaanse cryptografiedeskundige Bruce Schneier schreef jaren geleden al: 'Alleen amateurs vallen machines aan, professionals richten zich op mensen en die professionals worden steeds beter'. Via zeer geraffineerde *social engineering* vallen de professionele hackers systemen aan via de mens, met de precisie van een laser. De kans van slagen van dergelijke aanvallen is zeer groot.

Dat computersystemen niet adequaat te beveiligen zijn zou het uitgangspunt moeten zijn van het Nederlandse cyber- en veiligheidsbeleid. De overheid heeft een begin gemaakt om Nederland weerbaarder te maken tegen de cyberdreiging, maar van een integraal, nationaal cyberbeleid is echter nog lang geen sprake. Een probleem is dat de politiek zich onvoldoende bewust is van de kwetsbaarheid van de elektronische systemen en dat de samenleving afhankelijk is van het goed functioneren van deze systemen. Met stijgende verbazing volg ik de politieke discussie over onder meer het elektronisch stemmen en het Elektronisch Patiënten Dossier. Vanuit beveiligingsoogpunt is de situatie niet veel anders dan bij de eerste, mislukte pogingen. Het is dan ook niet moeilijk om nu al vast te stellen dat beide initiatieven vanuit beveiligingsoogpunt gedoemd zijn te mislukken.

In het cyberdomein heerst een offensieve dominantie, want het is goedkoper, sneller en gemakkelijker om elektronische systemen aan te vallen dan te beschermen. Over de hele linie groeit het aantal cyberincidenten exponentieel en hier zitten ook aanvallen bij die gericht zijn op de vitale infrastructuur. In 2012 was er bijvoorbeeld Shamoon, een aanval op het Saudische oliebedrijf Aramco, met dertigduizend

geïnfecteerde computers. Er waren ook aanvallen op diverse water- en energiebedrijven in de VS en recentelijk nog een aanval op twee grote Zuid-Koreaanse banken en verschillende televisiemaatschappijen. Tot nu toe is er geen grote schade geweest. Maar de technieken om ernstige schade aan de vitale infrastructuur toe te brengen zijn ruim voorhanden. Veel van deze systemen zijn namelijk zeer kwetsbaar en nooit ontwikkeld om aan het internet te hangen. Het is dan ook een kwestie van tijd voordat het eerste grote incident, met een grote impact, zich zal voordoen in Nederland. Vaak wordt de kwestie-Diginotar genoemd als groot incident, maar deze aanval was niet op Nederland gericht en het ging slechts om *collateral damage*. Ik maak mij vooral zorgen over de kwetsbare, vitale infrastructuur. Een succesvolle aanval kan immers een enorme, ontwrichtende impact hebben op de Nederlandse samenleving.

Met alleen technische beveiligingshulpmiddelen is de cyberdreiging niet af te wenden. Zijn verdragen dan een oplossing? Regelmatig verschijnen er berichten dat er internationale verdragen dienen te komen om de cyberdreiging in te dammen. Het probleem is echter dat attributie (wie zit er achter?) bij een goed uitgevoerde aanval zo goed als onmogelijk is. Dat maakt de handhaving van eventuele verdragen onmogelijk. De nadruk moet komen te liggen op de *situational awareness*. We dienen onszelf onder andere vragen te stellen, zoals: hoe maken we de gebruiker minder kwetsbaar? Welke risico's zijn er bij een hack en/of bij sabotage van het systeem en hoe kunnen die worden beperkt? Welke informatie kan door cyberspionage worden ontvreemd en wat zijn daar de gevolgen van? Op welke manier gaan we met die gevolgen om? En hoe ziet de *manual override* eruit? Die handmatige (nood)bediening en organisatorische (nood)procedures van systemen zijn door efficiencyslagen op de achtergrond geraakt en moeten dus weer opnieuw ontwikkeld worden.

Nederland mist een pure, operationele cybereenheid die 24 uur per dag actief is, een Dienst Cyber Interventie (DCI). De koude fase zou onder meer moeten bestaan uit het monitoren van internet en openbare, sociale mediaberichten en het uitvoeren van gecontroleerde *pen/red team testing* van overheids- en vitale infrastructuursystemen om te kijken waar de kwetsbaarheden liggen. In de warme fase zou de nadruk moeten liggen op schadebeperking, het opsporen van daders en het coördineren van de acties van betrokken partijen. In de DCI zouden Defensie, politie en inlichtingendiensten moeten samenwerken. Naast fulltime medewerkers dient er ook een grote reservistencomponent te zijn. Deze reservisten zouden niet uit beveiligingsexperts moeten bestaan, maar vooral uit goedwillende *white hat hackers* en studenten. Hackers denken niet in ISO-normen en best *practise*, maar zijn gestructureerd en creatief op zoek naar kwetsbare plekken. Ze denken *out of the box*.

Hack-kennis en vaardigheden zijn zo schaars dat je er niet aan ontkomt om hackers te rekruteren. In een aantal landen, zoals bijvoorbeeld Zuid-Korea, Israël en de VS, zet de overheid al hackers in. Werving vindt plaats via onder meer *challenges* en het aanbieden van opleidingen. Het gros van de hackers is geen doorgewinterde crimineel, het is velen van hen vooral te doen om de spanning en sensatie. Als een overheid dat kan bieden in een gecontroleerde omgeving kunnen beide partijen daar hun voordeel meedoen.

Tijdens de Digital Forensics Challenge 2012 eindigde de 26-jarige Brit Chris Doman als nummer twee, achter het team van het defensiebedrijf Northrop Grumman, uit een veld van 1209 deelnemers. Het Amerikaanse legerteam eindigde op de elfde plaats. Saillant detail: de amateur Doman werkte niet in de digitale beveiligingsindustrie, inmiddels overigens wel. Het illustreert hoe groot de dreiging is die van een eenling kan uitgaan, maar ook hoe waardevol ze als white hat hacker kunnen zijn voor een overheid. Het is goed te realiseren dat kwaadwillende *black hat hackers* zich maar aan één regel hoeven te houden, namelijk dat er geen regels zijn. En dat doen ze dan ook braaf. ■