BW
BANK|WERELD

GASTCOLUMN

SAMEN WERKEN AAN CYBERVEILIGHEID

WIM HAFKAMP OVER HET VERHOGEN VAN DE CYBERWEERBAARHEID

De opkomst van de informatietechnologie (ICT) betekende ook de opkomst van 'de cybercrimineel'. Bij veel ondernemingen in de financiële sector gingen ICT en informatiebeveiliging vanaf het begin hand in hand. Hoe kun je informatie het best beschermen? Welke risico's en trends zijn er en hoe speel je daarop in? De komst van internetbankieren bracht weer nieuwe risico's en technieken met zich mee, zoals phishing, malware en computervirussen. Banken werkten al snel onderling samen om kennis over cyberveiligheid te delen. Banken zijn een goed georganiseerde sector als het gaat om cyberveiligheid en data-uitwisseling om *cybercrime* tegen te gaan. De strijd tegen *cybercrime* is voor elke bank dezelfde. Dat is denk ik echt een voorbeeld voor andere sectoren."

"Publiek-private samenwerkingen waarbij gegevens met overheidsorganisaties worden gedeeld om *cybercrime* tegen te gaan, zijn wat jonger maar zeker succesvol. Bij het vrij jonge Z-CERT ben ik verantwoordelijk voor het verhogen van de cyberweerbaarheid in de Nederlandse zorgsector. Een sector die formeel niet als 'vitaal' is verklaard en daarom nu geen beroep kan doen op het *Nationaal Cyber Security Centrum*. Maar natuurlijk moet je er niet aan denken dat een IC-afdeling van een ziekenhuis plat komt te liggen omdat het systeem wordt gehackt. Dus de sector is wel van cruciaal belang voor de samenleving. Z-CERT helpt op dit moment ziekenhuizen en GGZ-instellingen bij het voorkomen en oplossen van cyberincidenten. Ons werk gebeurt vooral 'onder de motorkap': welke actuele dreigingen en kwetsbaarheden zijn er in de informatiesystemen van deelnemers? Zien wij iets, dan sluizen we dat zo snel mogelijk door naar de betreffende instellingen. Daarbij geven we ook aan hoe ze die kwetsbaarheden kunnen verhelpen. Soms moeten hele systemen uitgezet worden, omdat de risico's op bijvoorbeeld een DDoS-aanval of gegevenslek te groot worden."

"Wat de zorg en de financiële sector van elkaar zouden kunnen leren? Ik ben blij verrast over de enorme samenwerkingsbereidheid binnen de zorg. Binnen de financiële sector is er weliswaar een Financial-CERT, maar die kent nog weinig deelnemers en het samenwerkingsverband staat ook (nog) niet op eigen benen. Aan de andere kant zijn de middelen in de zorgsector schaarser. Dat zie je terug in de capaciteit voor maatregelen tegen complexe cyberdreigingen. Banken zijn vanaf het begin van de digitalisering doelwit geweest van cybercrime, daar leer je van en daar pas je je maatregelen op aan. Ik stond zelf aan de basis van het programma *Threat Intelligence Based Ethical Red Teaming* (TIBER). Daarbij worden onder leiding van De Nederlandsche Bank aanvallen op financiële systemen nagebootst om te kijken of die gedetecteerd worden. Dat is iets waarvan ik zeg: ik wou dat we als zorgsector zo ver waren. Misschien dat de banken de zorg daar ook in zouden kunnen helpen? Dan zou de zorg op haar beurt ervaringen kunnen delen met het inrichten van een sectorale CERT voor de hele financiële sector in het kader van de goede samenwerking." —

Dr. Wim Hafkamp, managing director Z-CERT (Computer Emergency Respons Team)