prof. dr. Peter Werkhoven,
directeur Kennis, TNO Defensie en Veiligheid

Cybersecurity – introductie

Het thema van deze special is Cybersecurity, een thema dat steeds belangrijker wordt in onze samenleving. Als de informatie- en communicatietechnologie (ICT) uitvalt, trekken bij veel bedrijven en overheden de medewerkers al binnen een uur gefrustreerd hun jas aan. Langdurige e-mailuitval lijkt voor enkelen zelfs traumatischer te zijn dan een echtscheiding. Ook de vitale infrastructuur is grotendeels afhankelijk van het goed functioneren van ICT. Bij grootschalige ICT-uitval vallen vitale functies weg, kunnen domino-effecten ontstaan en bestaat een substantieel risico op systeemfalen. Bij veel burgers komt dan de vraag op of Nederland voorbereid is op een grootschalige ICT-uitval of -verstoring. Hebben de private partijen en de overheid daar een crisisplan voor?

Reeds bij de vroegere voorlopers van het internet, het Arpanet van Defensie, was men zich bewust van veiligheidsproblemen. Begin jaren tachtig vond er drie keer maal per jaar overleg plaats tussen zes NAVO-landen (waaronder Nederland) over het internationaal synchroon upgraden van de Arpanet-routers. Recent werkten honderden Internet Service Providers in de hele wereld in onderling vertrouwen samen om een ernstige fout in de kern van het internet weg te nemen en zo misbruik te voorkomen. Toch kan een volgende keer niet worden uitgesloten dat een medewerker vroegtijdig kritische informatie lekt en de weg vrij maakt voor criminelen. Naast technologische beveiliging zijn ook gedrag en organisatie essentieel.

Cybersecurity strekt zich echter verder uit dan alleen het internet. Ook andere vormen van telecommunicatie zijn vitaal voor de samenleving. Zij kunnen, mede door de toenemende convergentie van tele-communicatiediensten, net zo goed getroffen worden door uitval en (on) opzettelijke verstoring. Cybersecurity nu vergt meer dan het oude achterkamertjes-overleg van enkele mensen die elkaar vertrouwen. Aanpak van cyber-onheil vereist nu internationaal samenwerken op grote schaal, overigens wel op basis van vertrouwen. Een sterke positie daarin als land, als private ICT-partijen, en als overheid is gewenst. Onze samenleving verwacht namelijk dat Nederland als innovatieve ICT-trendsetter voorbereid is om iedere vorm van onopzettelijke en opzettelijke ICT-verstoring het hoofd te kunnen bieden, ongeacht of deze nu veroorzaakt wordt door technisch falen, een menselijke fout, activisten (denk aan de aanvallen op Estland en aan Fitna) of door kwaadwillige staten (*cyberwar*). Nederland moet op ICT-gebied de continuïteit van haar samenleving en economie nu en in de toekomst kunnen waarborgen zonder voor die kennis afhankelijk te zijn van andere landen.

Daarnaast zal de ICT-veiligheidsbeleving van de burger en bedrijven hersteld moeten worden.

Dit themanummer gaat in op de vele proactie-, preventie-, preparatie-, incidentrespons- en incidentopvolgings-activiteiten op cybersecuritygebied die Nederland nationaal en in internationale dialoog uitvoert. Uit de bijdragen komt desondanks naar voren dat er nog zeer grote uitdagingen zijn op technisch vlak, op organisatorisch vlak, en op het vlak van bewustwording en ICT-veilig gedrag. Het Verenigd Koninkrijk heeft uit oogpunt van de bescherming van hun nationale veiligheid deze uitdagingen opgepakt met hun 'Cyber Security Strategy'. Voorbeeld doet volgen. Een soortgelijke krachtige Nederlandse kabinetsvisie op de aanpak van het gehele cybersecurity spectrum van spam en virussen tot en met cyberwar is nodig om onze cybersecurity ook in de toekomst te waarborgen. Hierbij moet al onze publieke en private kennis en kunde samengebracht en in stelling gebracht worden.