15 Cyberaanval op de Universiteit Maastricht

Menno van Duin, Vina Wijkhuijs

15.1 Inleiding

In de nacht van 23 december 2019 werd de Universiteit Maastricht getroffen door een cyberaanval. Daarmee kwam de universiteit tijdens de kerstvakantieperiode voor een enorme opgave te staan. Hoe konden het universitair onderwijs, het wetenschappelijk onderzoek en de overige bedrijfsprocessen weer zo spoedig mogelijk worden hervat? Net als voor vele andere organisaties zijn ook voor universiteiten digitale systemen van levensbelang. Vicevoorzitter Bos van het College van Bestuur (CvB) zou na afloop zeggen: 'Je ervaart aan den lijve de afhankelijkheid van systemen op het moment dat je ze niet meer tot je beschikking hebt.'[1] De universiteit moest alle zeilen bijzetten om te kunnen begrijpen wat er was gebeurd en hoe de werkprocessen weer zo spoedig mogelijk te herstellen.

Na een beschrijving van het feitenrelaas gaan we in dit hoofdstuk in op twee dilemma's. Als eerste is dat het dilemma of op de eis van de hackers om losgeld te betalen mag worden ingegaan? Welke afwegingen spelen een rol? Het tweede dilemma betreft het bredere vraagstuk van de ernst van het probleem van cybercriminaliteit. Hoe groot zijn nu de risico's en welke aanpak past daarbij?

Het hoofdstuk is gebaseerd op nieuwsberichten, het openbare rapport van het cybersecuritybedrijf dat onderzoek deed naar de toedracht en omvang van de cyberaanval (Fox-IT, 2020) en de live-registratie van

1 Citaat uit de presentatie die gegeven werd tijdens het Cybersymposium op de Universiteit Maastricht d.d. 5 februari 2020.

het Cybersymposium dat op 5 februari 2020 plaatsvond op de Universiteit Maastricht.[2]

15.2 Feitenrelaas

Het is vlak voor kerst wanneer op dinsdag 24 december 2019 de Universiteit Maastricht een bericht op haar website plaatst met de mededeling dat de universiteit is getroffen door een 'serieuze cyberaanval'. Bijna alle Windows-systemen zijn geraakt, e-mail kan niet meer worden gebruikt en de online bibliotheek en het studentenportaal zijn onbereikbaar.[3] De universiteit heeft het cybersecuritybedrijf Fox-IT ingeschakeld dat die middag vanaf 16.00 uur aanwezig is om de toedracht van de aanval in kaart te brengen en de universiteit van advies te voorzien. Als eerste worden alle ICT-systemen offline gehaald. Met uitzondering van enkele laboratoria worden ook alle universiteitsgebouwen gesloten.

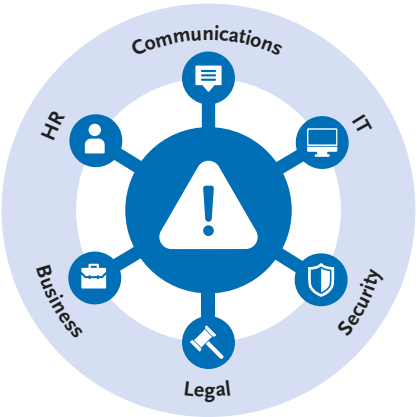
De (voorbereidingen op de) cyberaanval
De cyberaanval op de Universiteit Maastricht vangt in feite aan op 15 oktober, wanneer een medewerker van de universiteit een Excel-document opent via een link uit een ontvangen e-mail. Het blijkt een zogenoemde *phishing-link*. Een dag later opent een andere medewerker een vergelijkbare link. Via deze infecties weten de hackers toegang te verkrijgen tot het digitale netwerk (het zogenoemde UNIMAAS-domein) van de universiteit. Vanaf dat moment worden meerdere servers gecompromitteerd. Op 21 november weten de hackers, via een server met ontbrekende beveiligingsupdates, volledige rechten te verkrijgen binnen de infrastructuur van de universiteit. Zo kan in de avond van 23 december de ransomware-aanval worden uitgevoerd. De aanval treft enkele kritieke systemen voor de bedrijfsvoering van de universiteit, waaronder de e-mailservers, bestandsservers met onderzoeks- en bedrijfsvoeringsgegevens en een aantal back-up servers (Fox-IT, 2020).

2 Liveregistratie van het Cybersymposium te raadplegen via www.maastrichtuniversity.nl/nl/cybersymposium-um-lessons-learnt.

3 Maastricht University, 24 december 2019. Nieuws: 'UM getroffen door cyberaanval'. Op 4 september 2020 ontleend aan www.maastrichtuniversity.nl/nl/nieuws/um-getroffen-door-cyberaanval.

Op de universiteit wordt een crisismanagementteam gevormd dat onder meer bestaat uit de vicevoorzitter van het CvB, de directeur van het ICT Service Centre, de directeur bestuurlijk-juridische zaken, een communicatieadviseur en leden van het *quick-reponse team* van Fox-IT (zie figuur 15.1).

Figuur 15.1 Samenstelling multidisciplinair crisismanagementteam



Bron: Fox-IT, 2020

Voor het crisismanagementteam zijn van meet af aan de belangen van de studenten, onderzoekers en medewerkers leidend. Het onderwijs komt daarbij op de eerste plaats.

> 'Hoe kunnen we ervoor zorgen dat we op 6 januari 19.000 studenten hun onderwijs kunnen laten volgen? Hoe kunnen we 6000 studenten vanaf diezelfde datum de voorziene toetsen laten doen?', aldus vicevoorzitter Bos van het CvB.[4]

Alle acties zijn erop gericht om het onderwijs weer op het normale moment na de kerstvakantie te laten starten en om onderzoekers zo snel mogelijk toegang te verschaffen tot wetenschappelijke data. Speciale aandacht is er ook voor zaken als scripties, aanmeldingen voor

4 Citaat uit de presentatie die gegeven werd tijdens het Cybersymposium op de Universiteit Maastricht d.d. 5 februari 2020.

numerus fixus-opleidingen, subsidieaanvragen en sollicitaties. Vanaf 27 december (tot en met 24 januari 2020) volgen op de website van de universiteit in totaal 22 updates over de maatregelen die zijn of worden genomen. Voor studenten en medewerkers van de universiteit wordt een lijst met FAQ's opgesteld en zijn vanaf 30 december speciale hulplijnen beschikbaar.[5] Tientallen 'en later misschien wel tweehonderd' medewerkers van de universiteit brengen hun kerstvakantie deels door op de universiteit (Maastricht University, 2020, p. 7):

> 'Behalve de IT-medewerkers zijn na verloop van de eerste dagen ook heel veel stafleden uit faculteiten en ondersteunende diensten bij het oplossen van de gevolgen van de hack betrokken geraakt vanwege hun kennis van onderwijsprocessen en studentenwelzijn; uiteenlopend van docenten en medewerkers bureaus onderwijs tot studieadviseurs, studentendecanen, studentenpsychologen, roosteraars, help-desk-medewerkers, beleidsadviseurs met juridische, financiële, HR- en academische expertise, medewerkers van de universiteitsbibliotheek en medewerkers van facility services (...). We hebben op heel veel van onze medewerkers en hun leidinggevenden een beroep mogen doen.'

De universiteit besluit op 29 december het losgeld te betalen dat door de hackers wordt geëist (Fox-IT, p. 4). Het zou gaan om in totaal 30 bitcoins die op het moment van betaling een waarde van 197.000 euro vertegenwoordigen. Met deze betaling wordt de zogenoemde *decryptor* verkregen om stukje bij beetje de gegijzelde data weer te ontsleutelen en systemen te ontsmetten.[6] Zodoende komen vanaf 2 januari de belangrijkste onderwijsgerelateerde computersystemen weer beschikbaar, zij het nog in beperkte vorm.[7] Vanaf die datum zijn ook alle universiteitsgebouwen weer open.

5 Maastricht University, 30 december 2019. Nieuws: 'Update #5: cyberaanval UM'. Op 4 september 2020 ontleend aan www.maastrichtuniversity.nl/nl/nieuws/update-5-cyberaanval-um.

6 *De Limburger*, 5 februari 2020. Regio Noord-Limburg: 'Universiteit Maastricht betaalde 197.000 euro aan Russische hackgroep'. Op 4 september 2020 ontleend aan www.limburger.nl/cnt/dmf20200205_00146231/universiteit-maastricht-betaalde-197-000-euro-aan-russische-hackers.

7 Maastricht University, 2 januari 2020. Nieuws: 'Update #9: cyberaanval UM'. Op 4 september 2020 ontleend aan www.maastrichtuniversity.nl/nl/nieuws/update-9-cyberaanval-um.

Op 6 januari kan het onderwijs weer worden hervat. De circa 4000 herkansingen die in die week gepland staan, kunnen gewoon doorgaan. Er komt daarnaast een extra herkansingsmogelijkheid en er zal een coulanceregeling gelden voor studenten die aantoonbaar zijn benadeeld door de cyberaanval. Studenten kunnen zich hiervoor wenden tot een speciaal daartoe in het leven geroepen commissie.[8]

In de loop van de dagen worden steeds meer systemen vrijgegeven, maar het zal nog enkele weken duren voordat dit voor alle systemen geldt.[9] Onderwijl is het Openbaar Ministerie op basis van de aangifte die de universiteit heeft gedaan, een strafrechtelijk onderzoek gestart. Op 5 februari 2020 vindt op de Universiteit Maastricht een Cybersymposium plaats om de geleerde lessen uit deze casus te delen met de buitenwereld.[10]

15.3 Losgeld betalen?

Een dilemma dat in deze casus feitelijk heeft gespeeld, was de vraag of er al dan niet losgeld zou moeten worden betaald. Het betalen van losgeld wordt vaak om uiteenlopende redenen zeer onwenselijk geacht, of het nu gaat om een gijzeling van personen of – zoals in deze casus – om een cyberaanval op digitale communicatiesystemen en databeheer. In het verleden zijn verschillende keren Nederlanders slachtoffer van een gijzeling geweest en is in veel gevallen losgeld betaald om hen weer vrij te krijgen, al bleef na afloop soms onduidelijk of er daadwerkelijk losgeld was betaald. Bekende voorbeelden zijn de ontvoeringen van Freddy Heineken (1983), Gerrit Jan Heijn (1986, die al enkele uren na zijn ontvoering bleek te zijn doodgeschoten) en Arjan Erkel (2002). Tegenwoordig lijken criminelen vooral met cyberaanvallen losgeld te willen afdwingen, waarvan de aanvallen op Maersk (2017), de gemeente

8 Maastricht University, 31 december 2019. Nieuws: 'Update #6 en 7: cyberaanval UM'. Op 4 september 2020 ontleend aan www.maastrichtuniversity.nl/nl/nieuws/update-6-en-7-cyberaanval-um.

9 Maastricht University, 13 januari 2020. Nieuws: 'Update #18: cyberaanval UM'. Op 4 september 2020 ontleend aan www.maastrichtuniversity.nl/nl/nieuws/update-18-cyberaanval-um.

10 Liveregistratie van het Cybersymposium te raadplegen via www.maastrichtuniversity.nl/nl/cybersymposium-um-lessons-learnt.

Lochem (2019), het ziekenhuis van Aruba (2019) en het Medisch Centrum Leeuwarden (2020) enkele voorbeelden zijn. In elk van die gevallen speelde min of meer eenzelfde afweging van belangen.

Afweging van belangen

De belangrijkste reden om geen losgeld te betalen is van principiële aard: met criminelen wordt niet onderhandeld, zeker niet door overheidsinstanties. Met het betalen van losgeld worden immers dergelijke criminele activiteiten in leven gehouden. De minister van Justitie en Veiligheid verwoordde het in zijn reactie op de berichtgeving dat de Universiteit Maastricht losgeld had betaald als volgt:[11]

> 'Door losgeld te betalen worden criminele activiteiten beloond en gestimuleerd. Daarnaast is de verwachting van de politie dat het betalen van losgeld leidt tot meer aanvallen van ransomware.'

Als nooit en te nimmer op een dergelijk verzoek zou worden ingaan, zou deze vorm van afpersing niet bestaan. Er horen daarom geen deals te worden afgesloten met criminelen of criminele organisaties. Daarnaast blijft onzeker of na betaling de problemen daadwerkelijk zijn of kunnen worden opgelost. Ook blijft er vaak onzekerheid bestaan of de betreffende criminelen niet opnieuw zullen proberen om toe te slaan. Met het betalen van losgeld geven zij zich niet over, maar kunnen zij nog steeds hun gang blijven gaan.

In de afweging die de Universiteit Maastricht maakte, speelden zonder meer deze principiële bezwaren; toch ging de universiteit over tot betaling van het losgeld. 'In dit duivelse dilemma moest de universiteit een afweging maken tussen twee zwaarwegende maatschappelijke belangen', zo vertelde vicevoorzitter Bos van het CvB tijdens zijn presentatie op het Cybersymposium. Aan de ene kant was dat het belang om criminelen niet te betalen. Hoewel dit niet bij wet verboden is, kleven daaraan – zoals gezegd – morele bezwaren. Aan de andere kant had de universiteit rekening te houden met de belangen van de studenten, de wetenschappelijk onderzoekers en de continuïteit van de universiteit. Een analyse van de inbraak in de computersystemen maakte dui-

11 Brief van de minister van Justitie en Veiligheid aan de Tweede Kamer d.d. 20 mei 2020; TK 2019-2020, 26243/28684, nr. 678.

delijk dat er niet al binnen enkele dagen een oplossing voorhanden zou zijn en dat volledig herstel, zonder betaling van het losgeld, niet alleen de nodige kosten met zich mee zou brengen maar ook weken tot misschien wel enkele maanden zou kunnen duren. De universiteit vond ook dit onaanvaardbaar.

Uiteindelijk waren de mate en de duur van de verstoring van het onderwijs- en onderzoeksproces leidend in de keuze die de universiteit maakte. Voordat tot betaling werd overgegaan, is de keuze aan verschillende personen voorgelegd, zowel binnen de universiteit, als daarbuiten. Ook het ministerie van Onderwijs en de Onderwijsinspectie werden op de hoogte gesteld. Minister Van Engelshoven van Onderwijs had uiteraard haar bedenkingen. Zij stelde zich op het standpunt 'dat er geen geld naar criminelen toe moet vloeien'.[12] De Onderwijsinspectie toonde echter na afloop begrip voor de betaling van het losgeld. Medio 2020 kwam de inspectie op basis van haar onderzoek naar de crisisafhandeling door de universiteit tot de volgende conclusie (Onderwijsinspectie, 2020, p. 4):

> 'De inspectie heeft geen aanwijzingen gevonden dat de Universiteit Maastricht na het ontdekken van de ransomware aanval andere, meer passende, maatregelen had kunnen nemen. (...) We concluderen dat door het adequaat ingrijpen tijdens de cyberaanval, de goede voortgang van het onderwijs en onderzoek (...) slechts beperkt in gevaar is geweest. Er is slechts voor een korte periode sprake geweest van een continuïteitsprobleem (...).'

Met de betaling op 29 december van de geëiste 30 bitcoins werd de sleutel verworven om de computersystemen weer te kunnen herstellen. Op 6 januari was de universiteit weer 'up-and-running'. De meeste systemen werkten weer, zij het niet volledig, maar aan het einde van de maand konden de salarissen aan het personeel gewoon worden uitbetaald.

12 Brief van de minister van Onderwijs aan de Tweede Kamer d.d. 14 februari 2020; TK 2019-2020, 26643, nr. 832.

Stilzwijgen of transparantie?

Over de vraag of de universiteit losgeld had betaald en wat de hoogte van het losgeld was, werd veel gespeculeerd. Op 2 januari meldde de universiteitskrant *Observant* dat de universiteit aan de hackers losgeld zou hebben betaald.[13] Het nieuws werd door verschillende media overgenomen. De universiteit zelf wilde hierover echter niks zeggen, omdat het onderzoek naar de cyberaanval nog in volle gang was.

> 'In het licht van het lopende onderzoek wil de universiteit op geen enkele wijze iets doen of communiceren wat de digitale veiligheid van de instelling, en daarmee de belangen van onze studenten, wetenschappers, medewerkers en de universiteit zelf, op enigerlei wijze schade kan berokkenen', aldus de woordvoerder van de Universiteit Maastricht.[14]

Volgens *de Volkskrant* zou de universiteit de hackers 'een kwart miljoen' oftewel een bedrag tussen de 200.000 en 300.000 euro hebben betaald.[15] Het bedrag dat feitelijk is betaald, was echter iets lager. Op het moment van betaling stonden 30 bitcoins gelijk aan 197.000 euro. Tijdens het symposium van 5 februari werd het exacte bedrag bekendgemaakt, om verdere speculaties en geruchtvorming te voorkomen. De vicevoorzitter van het CvB gaf daarbij vooraf aan dat het noemen van het bedrag, het risico met zich meebrengt dat een soort van norm wordt gezet, waarmee criminelen in het vervolg rekening zouden kunnen houden. Ook zouden reacties in de media op de hoogte van het bedrag ('dat valt alleszins mee') mogelijk effect kunnen hebben. Hoewel transparantie waardevol is en daarmee speculaties worden voorkomen, is dus het wel of niet noemen van het feitelijk betaalde losgeldbedrag op zichzelf ook weer een dilemma.

13 *Observant*, 2 januari 2020. Nieuws: 'Cyberhack: Universiteit Maastricht betaalt losgeld'. Op 4 september 2020 ontleend aan www.observantonline.nl/Home/Artikelen/articleType/ArticleView/articleId/17789/Cyberhack-Universiteit-Maastricht-betaalt-losgeld.

14 NU.nl, 2 januari 2020. Tech: 'Universiteitsblad: Universiteit Maastricht betaalde losgeld na cyberaanval'. Op 4 september 2020 ontleend aan www.nu.nl/tech/6021315/universiteitsblad-universiteit-maastricht-betaalde-losgeld-na-cyberaanval.html.

15 *de Volkskrant*, 24 januari. Nieuws & Achtergrond: 'Universiteit Maastricht betaalde hackers kwart miljoen euro'. Op 4 september 2020 ontleend aan www.volkskrant.nl/nieuws-achtergrond/universiteit-maastricht-betaalde-hackers-kwart-miljoen-euro~b0a1707b.

15.4 Cybercriminaliteit: het probleem en de aanpak

Digitale verstoringen kunnen een maatschappij behoorlijk ontwrichten, zo is de veronderstelling. Tegenwoordig gaat immers vrijwel alles via internet. Verstoringen van digitale systemen worden deels veroorzaakt door verkeerd menselijk handelen: het kopje koffie dat omvalt, net verkeerd terechtkomt en een systeem verstoort, of een verkeerde handeling die forse gevolgen heeft. Ook kunnen ze het gevolg zijn van verstoringen elders (bijvoorbeeld elektriciteitsuitval). Daarnaast zijn er verschillende vormen van cybercriminaliteit (hacking, DDos-aanvallen en dergelijke) waarmee doelbewust geprobeerd wordt om computersystemen plat te leggen.

Het zal geen verbazing wekken dat vooral cybercriminaliteit als een van de grootste risico's en bedreigingen wordt gezien en het thema geniet tegenwoordig dan ook grote belangstelling. Sinds een aantal jaren is er bij het ministerie van Justitie en Veiligheid het Nationaal Cyber Security Centrum (NCSC). De taken van het NCSC zijn onder meer:

- reageren op incidenten die vrijwillig of volgens de Wet beveiliging netwerk- en informatiesystemen verplicht bij het NCSC (moeten) worden gemeld;
- incidenten op nationaal niveau monitoren en informatie over risico's en incidenten verspreiden;
- optreden als *Computer Security Incident Response Team* (CSIRT) en deelnemen aan het internationale netwerk van CSIRT's.

Daarnaast wordt door de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) jaarlijks een *Cybersecurity beeld Nederland* uitgebracht, waarin wordt ingegaan op digitale dreigingen, de belangen die daarmee gemoeid zijn en de weerbaarheid van de samenleving tegen deze dreigingen. In het jaarbeeld van 2020 – dat vooral terugblikt op ervaringen uit 2019 – wordt aangegeven dat de digitale risico's van met name spionage en sabotage door andere landen onverminderd groot zijn. Ook is er het risico van cyberaanvallen door criminelen. In het jaarbeeld van 2020 worden de ransomware aanvallen op de gemeente Lochem (zie onderstaand kader) en de Universiteit Maastricht als voorbeeld genoemd. Verder waren er problemen met Citrix en aanvallen op

het software-updateprogramma Asus Live Update en het antivirussoftwarebedrijf Avast (NCTV, 2020).

Cyberaanval gemeente Lochem
Bij een cyberaanval op de gemeente Lochem begin juni 2019 is misbruik gemaakt van een kwetsbaarheid in het Remote Desktop Protocol (RDP) dat wordt gebruikt om computers op afstand te beheren. Bij het incident werd via 'brute force aanvallen' op de RDP-poort toegang tot een thuiswerkserver verkregen. Na het inloggen op de server installeerde(n) de hacker(s) verschillende applicaties. Hiermee werd inzicht verkregen in het netwerk en de gebruikers. Ook werd ransomware ingezet, waardoor een aantal bestanden werd versleuteld. Na de aanval is besloten om de computersystemen opnieuw in te richten. Zaken als het aanvragen van paspoorten, het registreren van een verhuizing en het aangeven van een geboorte waren tijdelijk niet mogelijk. De aanval resulteerde in een schadepost van 200.000 euro (NCTV, 2020, p. 18).

In 2019 verscheen van de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) het rapport *Voorbereiden op digitale ontwrichting*. Daarin wordt gesteld dat Nederland onvoldoende is voorbereid op de 'digitaliserende samenleving'. Zorgelijk is vooral dat digitale incidenten de vitale processen in onze samenleving kunnen aantasten: het betalingsverkeer, de elektriciteitsvoorziening, toegang tot overheidsdiensten. Digitale verstoringen kunnen zo ons land ernstig verstoren en zelfs ontwrichten. De voorbereiding op digitale verstoringen zal daarom nadrukkelijk onderdeel moeten zijn van het veiligheidsbeleid, gericht op de continuïteit van de samenleving. De WRR gebruikt daarbij de vergelijking met de brandweer: er is behoefte aan een 'digitale brandweer'. Daarmee geeft het WRR-rapport vooral aan dat meer aandacht nodig is voor de problematiek van de (dreigende) digitale ontwrichting.

De vraag is echter hoe problematisch de situatie van onze digitaliserende samenleving nu is. Uit informatie over de cyberaanval op de Universiteit Maastricht blijkt hoe de criminelen te werk gingen. Ook wordt uit de Maastrichtse casus duidelijk hoeveel kansen er feitelijk voor criminelen zijn om een computernetwerk binnen te komen. Enkele cijfers ter illustratie. Het computernetwerk van de Universiteit Maastricht bestond uit 1647 servers en 7307 (ook virtuele) werkplekken. Jaarlijks zijn zo'n honderdduizend updates nodig om 'onveilige achterdeurtjes' in software dicht te houden. Per seconde worden zo'n

30.000 inbraakpogingen tegengehouden en zo'n 1400 keer per dag worden malware aanvallen geblokkeerd. De cyberaanval in december 2019 raakte 267 servers van het Windows-domein. Deze enorme getallen geven een indicatie dat een computersysteem van enige omvang veel kenmerken heeft die Perrow beschrijft in zijn theorie over *normal accidents* (Perrow, 1999). Volgens Perrow zijn systemen die zeer complex en tegelijkertijd strak gekoppeld zijn, zeer gevoelig voor een verstoring: als daarin wat misgaat – en zeker als daarbij opzet in het spel is – is de kans op snel herstel gering, wat kan leiden tot ontwrichting.

De Delftse hoogleraar Bestuurskunde Van Eeten acht de gevolgen van digitale verstoringen echter niet zo extreem als wel wordt verondersteld. In zijn boeiende Van Slingelandt-lezing voor de Vereniging voor Bestuurskunde stelt hij – in reactie op het WRR-rapport – dat de overheid geen digitale brandweer in het leven hoeft te roepen, omdat digitalisering ons over het geheel genomen niet kwetsbaarder maakt (Van Eeten, 2019). Daarbij maakt hij de vergelijking met elektriciteit. De levering daarvan werd in de loop van een aantal decennia zo betrouwbaar, dat wij ons er meer afhankelijk van maakten. Toch zijn er geen voorbeelden dat heel Nederland langdurig zonder stroom zat. De betrouwbaarheid van de energielevering is kennelijk – parallel aan de groei van het netwerk – steeds meer verbeterd.

Ook bij digitalisering is sprake van een dergelijk 'duet van afhankelijkheid en betrouwbaarheid' (Van Eeten, 2019). Waarschijnlijk is dat de reden dat het aantal voorbeelden van grootschalige uitval door bijvoorbeeld een cyberaanval gering is en eigenlijk steeds dezelfde voorbeelden worden genoemd: DigiNotar, Maersk (zie hierover Van Duin & Maan, 2018) en nu ook de Universiteit Maastricht. Ondanks de vele grote computernetwerken en de feitelijk oneindige aantallen mogelijkheden van criminelen om systemen binnen te komen, blijft het aantal grootschalige uitvallen beperkt. We zijn dan ook feitelijk niet kwetsbaarder geworden. Natuurlijk zijn er risico's en bezorgen incidenten overlast, maar dat is tegelijk ook de reden dat er zoveel wordt geïnvesteerd om de systemen betrouwbaarder te maken.

In lijn met de publicatie *Versterken van veerkracht* (Boin et al., 2020) geeft Van Eeten aan dat het zeer onwaarschijnlijk is dat een digitale verstoring zal leiden tot grote maatschappelijke ontwrichting. Ontwrichting is zeer uitzonderlijk. Veelal blijven de consequenties beperkt

tot enkel fysieke gevolgen, waarop hulpdiensten moeten acteren en dat ook gewend zijn te doen. De aanval op Maersk bijvoorbeeld, waardoor de containeroverslag in de Rotterdamse haven stil kwam te liggen, leidde vooral tot fileproblemen in het Rijnmondgebied, omdat vrachtauto's niet konden worden geladen of gelost. Aan het verhelpen van dergelijke problemen kunnen hulpdiensten een bijdrage leveren, maar dat de overheid een digitale brandweer zou moeten oprichten, waarvoor de WRR pleit, acht Van Eeten vrij zinloos. Als zich een gebeurtenis voordoet zoals bij Maersk of de Universiteit Maastricht, zijn er gespecialiseerde bedrijven waar een beroep op kan worden gedaan. De grote angst voor vergaande ontwrichting is volgens Van Eeten dus onterecht: de kans op grote verstoringen is beperkt en als het misgaat, is de reactie vaak behoorlijk adequaat.

15.5 Afronding

Onze samenleving wordt elke dag meer afhankelijk van informatietechnologie en digitale systemen. De groeiende complexiteit en de strakke koppelingen tussen de interactieve systemen zijn te beschouwen als risicofactoren voor het plaatsvinden van wat Perrow *normal accidents* noemt. De kans dat informatiesystemen worden verstoord, is in theorie vrijwel onbeperkt. Voor criminelen zijn ze een doelwit om geld te verdienen en voor buitenlandse mogendheden bieden ze toegang om tweedracht te zaaien of de positie van bepaalde partijen te verzwakken. De komende jaren zal blijken of cyberincidenten daadwerkelijk zo maatschappelijk ontwrichtend zijn als momenteel wel wordt verondersteld. Er zijn argumenten aan te dragen waarom het niet zo'n vaart zal lopen, die Van Eeten overtuigend heeft geschetst. Wetende dat criminelen en vreemde mogendheden trachten informatiesystemen te verstoren, worden deze systemen steeds robuuster gemaakt. Tegenover de bedreigingen die van cyberaanvallen uitgaan, staat ook een veerkrachtige samenleving die wel tegen een stootje kan. De welvaart die alle ontwikkelingen op het gebied van informatietechnologie ons brengt, vormt tegelijk de basis om veerkrachtig op verstoringen te (kunnen) reageren.

Verschillende sectoren – waaronder inmiddels ook de veiligheidsregio's – hebben een *Information Sharing and Analysis Centre* opgericht

om met organisaties uit dezelfde sector informatie over dreigingen, incidenten en maatregelen te delen. Zo ook werden na de cyberaanval op de Universiteit Maastricht ervaringen met de sector gedeeld. Volgens de Onderwijsinspectie heeft de universiteit, door onder meer met het eerdergenoemde symposium openheid van zaken te geven, bijgedragen aan het lerend vermogen van het stelsel van hoger onderwijs.

Om in de toekomst cyberaanvallen te voorkomen en vroegtijdig te signaleren, deed cybersecurity-expert Fox-IT de universiteit een aantal aanbevelingen, waaronder de volgende (Onderwijsinspectie, 2020):

- Hou bij gebruikers van de informatiesystemen het veiligheidsbewustzijn op niveau door periodiek hieraan aandacht te schenken. Het gaat dan niet alleen om campagnes, maar ook om bijvoorbeeld het binnen de organisatie uitvoeren van phishing-tests.
- Stimuleer dat gebruikers (onbedoelde) incidenten melden én zorg ervoor dat de meldingen vervolgens opvolging en adequate adressering krijgen.

Aangezien wij allemaal gebruikers van informatiesystemen zijn, kunnen dit ook voor ons relevante tips zijn.