Cybercrime 2022

Cybercrime is een van de grootste uitdagingen van deze tijd. Het afgelopen jaar nam het aantal cyberaanvallen met 31% toe. Uit het alarmerende rapport van de Onderzoeksraad voor Veiligheid van eind 2021 blijkt dat de Nederlandse aanpak van digitale veiligheid niet voldoet. Deze moet snel en fundamenteel veranderen. Alle reden dus om aandacht te besteden aan cyber. Wij zullen dat doen in een reeks artikelen. In dit eerste deel schetsen Robert Pessers en Annevi Etienne het feitelijke kader en gaan zij onder meer in op bekende cyberrisico's en wat er bekend is over de hackers achter de cyberaanvallen.

1. Inleiding

De omvang en de ernst van cyberrisico's zijn het afgelopen jaar sterk toegenomen. Dit blijkt onder meer uit een door de Onderzoeksraad voor Veiligheid (OVV) op 16 december 2021 gepubliceerd rapport met aanbevelingen om de digitale veiligheid van Nederland te bevorderen, getiteld 'Kwetsbaar door software'.[1]

Wij zullen de komende tijd in een reeks van artikelen ingaan op verschillende aspecten van cyberrisico's. Daarin zal onder meer worden ingegaan op datalekken, aansprakelijkheden en cyberverzekeringen.

In dit artikel zullen we uitleggen wat cyberrisico's zijn. We zullen allereerst een beknopte introductie geven over de invloed van digitalisering op de maatschappij (paragraaf 2). Vervolgens zal worden ingegaan op cyberaanvallen en komen verschillende cyberrisico's aan bod (paragraaf 3). Daarna zal aandacht worden besteed aan de mensen en organisaties achter deze aanvallen, de hackers (paragraaf 4).

2. Digitalisering

De steeds verder voortschrijdende digitalisering draagt bij aan de economische groei en welvaart. Dat is algemeen bekend. De keerzijde van deze ontwikkeling is dat niet alleen individuele personen, ondernemingen en organisaties, maar ook de maatschappij en economie als geheel, afhankelijker worden van ICT-systemen. Daardoor is een kwetsbaarheid ontstaan voor al dan niet moedwillig veroorzaakte verstoringen van ICT-systemen.[2] Het risico dat verbonden is aan deze kwetsbaarheid groeit.

In 2021 werden gemiddeld 270 aanvallen (ongeoorloofde toegang tot gegevens, applicaties, diensten, netwerken of apparaten) per onderneming gerapporteerd, hetgeen een stijging van 31% is ten opzichte van 2020.[3] Daarbij dient opgemerkt te worden dat de indruk bestaat dat veel ondernemingen er in de praktijk voor kiezen om niet naar buiten te treden als ze zijn aangevallen, onder meer vanwege angst voor claims en reputatieschade. Daardoor mag worden aangenomen dat het werkelijke aantal aangevallen ondernemingen nog groter is.[4]

> *In 2021 werden gemiddeld 270 aanvallen per onderneming gerapporteerd, hetgeen een stijging van 31% is ten opzichte van 2020*

Enkele bekende cyberincidenten in de afgelopen tijd zijn deze: in januari 2021 kwam naar buiten dat al maanden op grote schaal zou zijn gehandeld in privégegevens van Nederlanders, afkomstig uit de coronasystemen van de GGD.[5] In november 2021 werd de Raad voor de rechtspraak door een *DDoS*-aanval getroffen.[6] De aanval zorgde ervoor dat verschillende websites van de Raad voor de rechtspraak slecht bereikbaar waren en was het niet mogelijk om online zittingen bij te wonen. In juli 2021 moest Coop bijna 800 winkels in Zweden sluiten na een cyberaanval.[7] Begin oktober maakte de VDL Groep, bestaande uit 105 ondernemingen met ruim 15.000 medewerkers, bekend slachtoffer te zijn van een cyberaanval.[8] VDL besloot daarop alle IT-systemen te ontkoppelen en van de buitenwereld te isoleren. Daarmee viel de VDL-groep min of meer stil. In november 2021 werd de

[1] OVV, *Kwetsbaarheid door software – Lessen naar aanleiding van beveiligingslekken door software van Citrix*, 16 december 2021, Den Haag: OVV. Te raadplegen op https://www.onderzoeksraad.nl/nl/page/17171/kwetsbaar-door-software---lessen-naar-aanleiding-van.
[2] A.W. Hagdorn, 'De Wet beveiliging netwerk- en informatiesystemen. Betekenis voor de vervoersector in het licht van cybersecurity', *Tijdschrift Vervoer & Recht* 2021, afl. 5, p. 110.
[3] Accenture, *State of Cybersecurity Resilience 2021. How aligning security and the business creates cyber resilience*, 2021. Te raadplegen op https://securityinsight.nl/report/state-of-cybersecurity-resilience-2021.
[4] A.W. Hagdorn, 'De Wet beveiliging netwerk- en informatiesystemen. Betekenis voor de vervoersector in het licht van cybersecurity', *Tijdschrift Vervoer & Recht* 2021, afl. 5, p. 111.
[5] 'Datadiefstal: "Goed dat OM tot vervolging overgaat"', ggdghor.nl.
[6] 'DDoS-aanval zorgt voor problemen bij websites van de Rechtspraak', rechtspraak.nl.
[7] 'Supermarktketen Coop moet bijna 800 Zweedse winkels sluiten na cyberaanval', nu.nl.
[8] 'VDL Groep weer in bedrijf na cyberaanval', vdlgroep.com.

MediaMarkt in de gehele Benelux getroffen door een cyberaanval waardoor de computers in al haar winkels niet meer gebruikt konden worden.[9] Recentelijk is ook het Internationale Comité van het Rode Kruis doelwit geworden van een omvangrijke cyberaanval. Bij die aanval zijn de persoonsgegevens van mogelijk 515.000 kwetsbare mensen buitgemaakt.[10]

Op micro niveau kunnen deze cyberaanvallen tot aanzienlijke schade lijden. Coop moest bijvoorbeeld haar winkels tijdelijk sluiten, VDL ging geheel 'offline' en MediaMarkt kon haar klanten maar beperkt bedienen. In de visie van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) gaan de risico's echter veel verder en vormen die een bedreiging voor de gehele Nederlandse samenleving omdat de gehele digitale infrastructuur bedreigd wordt. Hij concludeert dat uit de cyberincidenten die Nederland hebben geraakt, blijkt dat de weerbaarheid niet voldoende is.[11] Ook in een recent verschenen advies van de Cyber Security Raad (CSR) wordt dit bevestigd.[12]

Dit brengt ons bij de vraag wat nou eigenlijk verstaan wordt onder de begrippen 'cyberrisico's' en 'cyberaanval'.

3. Cyberrisico's en cyberaanvallen

Het begrip 'cyberrisico's' is vrij abstract.[13] In de literatuur wordt geen eenduidige definitie van dit begrip gegeven. Het Verbond van Verzekeraars heeft cyberrisico's in 2013 als gedefinieerd als "*het financiële nadeel dat een verzekerde oploopt door of via computer- en/of ICT-systemen, zonder dat er sprake is van materiele schade*".[14] Brouwer hanteert in haar proefschrift de volgende definitie: "*De risico's die voortvloeien uit het gebruik van IT en computernetwerken*".[15] De drie voornaamste manieren waarop cyberrisico's ontstaan, zijn door moedwillig handelen van buitenaf, menselijke fouten en technisch falen van eigen of externe IT-systemen.[16]

> *De drie voornaamste manieren waarop cyberrisico's ontstaan, zijn door moedwillig handelen van buitenaf, menselijke fouten en technisch falen van eigen of externe IT-systemen*

3.1 Moedwillig handelen buitenaf

Bij moedwillig handelen kan gedacht worden aan cybercriminaliteit, zoals cyberaanvallen. Met een 'cyberaanval' wordt gedoeld op (samenhangende) gebeurtenissen of activiteiten die leiden tot verstoring van één of meer digitale processen.[17] Bekende voorbeelden hiervan zijn het verspreiden van kwaadaardige software (*malware*), identiteitsfraude en hacking.

Als een computer niet goed beschermd is, kan dit leiden tot infectie met zogenaamde *malware*. Dit is een kwaadaardige software, die een cybercrimineel (ook wel hacker genaamd) de mogelijkheid geeft de computer te besturen. De twee belangrijkste vormen van *malware* die digitale processen doelbewust ontoegankelijk maken, zijn een *DDoS*-aanval of de inzet van *ransomware*.

Bij een *Distributed Denial of Service* (*DDoS*-aanval) wordt de computer door middel van *malware* (als één van vele) bestuurd door een hacker. Die verzameling van computers heet een 'botnet'. Met een dergelijk botnet kan een *DDoS*-aanval worden uitgevoerd. Dat is een soort verstikkingsaanval

[9] 'Grote cyberaanval op MediaMarkt: '43 miljoen euro losgeld geëist', ad.nl.
[10] 'Internationale Rode Kruis getroffen door cyberaanval', rodekruis.nl.
[11] NCTV, *Cybersecuritybeeld Nederland 2021*, 28 juni 2021, Den Haag: NCTV, p. 10. Te raadplegen op https://www.nctv.nl/documenten/publicaties/2021/06/28/cybersecuritybeeld-nederland-2021.
[12] CSR, *Nederlandse Digitale Autonomie en Cybersecurity*, 14 mei 2021. Te raadplegen op https://www.cybersecurityraad.nl/documenten/adviezen/2021/05/14/csr-advies-nederlandse-digitale-autonomie-en-cybersecurity---csr-advies-2021-nr.-3.
[13] A.J. Nagtegaal, J.A. Kruit en F.L. Stevens, 'IMO Cyber Risk Management Resolution – óók relevant voor ladingbelanghebbenden', *Tijdschrift Vervoer & Recht* 2021, afl. 4, p. 87.
[14] Verbond van Verzekeraars, *Virtuele risico's, echte schade. Over het verzekeren van cyberrisico's*, Position paper 2013, p. 4. Te raadplegen op https://www.mkb-bedrijfsverzekeringen.nl/pdf/hiscox/cyber/cyber-risks-informatie.pdf.pdf.
[15] N.M. Brouwer, *De cyberverzekering vanuit civielrechtelijk perspectief*, Deventer: Wolters Kluwer 2021, p. 35.
[16] Zie *Virtuele risico's, echte schade. Over het verzekeren van cyberrisico's*, Verbond van Verzekeraars 2013, p. 4.
[17] Zie Cybersecuritybeeld Nederland 2021, NCTV 28 juni 2021, p. 13.

waarbij de capaciteit van onlinediensten of de ondersteunende servers en netwerkapparatuur wordt aangevallen. Hierbij wordt een website overladen met communicatieverzoeken waardoor deze onbereikbaar wordt voor gebruikers.[18]

Daarnaast kan *malware* worden gebruikt om slachtoffers af te persen. Dan is sprake van *ransomware*. Door middel van *ransomware* worden de systemen en data van de slachtoffers 'gegijzeld' door hackers. De systemen of data worden versleuteld en slechts tegen betaling van losgeld wordt de sleutel vrijgegeven. Daarbij komt het steeds vaker voor dat gedreigd wordt met publicatie of doorverkoop van de versleutelde data als niet aan de losgeldeis wordt voldaan.

Gemiddeld zou voor het uitvoeren van een cyberaanval tussen de 66 en 500 dollar worden gevraagd

In dit verband wijzen wij ook op *phishing*. Vaak is *phishing* de eerste stap voor een cyberaanval. Kort gezegd houdt *phishing* het verkrijgen van belangrijke gegevens in, bijvoorbeeld inloggegevens en betalingsgegevens, vaak door middel van e-mails, of via WhatsApp-berichten. Iemand ontvangt een bericht dat betrouwbaar overkomt, met name omdat het gestuurd lijkt te zijn door een vertrouwd contact (bijvoorbeeld de directeur) of een bekende organisatie. In het bericht wordt gevraagd om gegevens te sturen of achter te laten op een ogenschijnlijk betrouwbare website, of om een betaling te doen die dan terechtkomt bij de hacker.[19]

Door middel van *phishing* kan ook *malware* op computersystemen worden geïnstalleerd, hetgeen weer kan leiden tot de *ransomware*-aanvallen. Zo begon de Maastrichtse cybercrisis met een simpele *phishing*-mail, wat uiteindelijk leidde tot betaling van een *ransomware*-som van € 197.000,- door de universiteit.[20]

Het weren tegen dit soort aanvallen wordt steeds lastiger nu tegenwoordig vaker via gestandaardiseerde ICT-systemen wordt binnengedrongen. Uit het OVV-rapport blijkt dat er meerdere voorvallen zijn waarbij kwetsbaarheden in software tot beveiligingslekken bij organisaties hebben geleid.[21] Voorbeelden hiervan zijn SolarWinds/SUNBURST, Microsoft Exchange en Kaseya VSA-software.

3.2 Menselijke fout

Cyberrisico's blijven zoals hiervoor vermeld echter niet beperkt tot gerichte aanvallen. Ook kunnen medewerkers de ICT-infrastructuur niet goed beheren, gebruiken of beveiligen. Dit kan variëren van te eenvoudige wachtwoorden tot onbeveiligde usb-sticks met vertrouwelijke informatie.[22] In dit verband kan echter ook worden gedacht aan mobiele telefoons en laptops die per abuis in de trein of elders worden achtergelaten.

3.3 Technisch falen

Ten slotte bestaat de mogelijkheid van technisch falen van ICT-systemen, servers en hard- en software.[23] Dit kan leiden tot storingen of uitval, hetgeen cyberincidenten tot gevolg kan hebben.

Deze cyberrisico's doen zich overal voor. Wij verwijzen in dit verband naar de bijdrage van Aaron Nagtegaal en Jolien Kruit, waarin zij ingaan op de cyberrisico's waaraan een schip zoal kan worden blootgesteld.[24]

4. Cybercriminelen

Hierboven zijn wij betrekkelijk uitvoerig ingegaan op cyberaanvallen. Direct daaraan gekoppeld is natuurlijk de vraag wie de hackers zijn die die cyberaanvallen uitvoeren. Ook daarover is inmiddels het een en ander bekend.

De hackers kunnen worden onderscheiden in statelijke actoren en cybercriminelen. De eerste groep richt zich op spionage, verspreiding van desinformatie en beïnvloeding.[25] De tweede groep blijkt inmiddels een goed ontwikkelde illegale bedrijfstak te zijn die wereldwijd opereert. Volgens

[18] 'DDoS', ncsc.nl.
[19] M.J. Bonthuis, *50 misverstanden over de AVG*, Deventer: Wolters Kluwer 2020, p. 120.
[20] 'Universiteit Maastricht betaalde ransomware-aanvallers losgeld', nos.nl.

[21] OVV, *Kwetsbaarheid door software – Lessen naar aanleiding van beveiligingslekken door software van Citrix*, 16 december 2021, Den Haag: OVV, p. 44-118. Te raadplegen op https://www.onderzoeksraad.nl/nl/page/17171/kwetsbaar-door-software---lessen-naar-aanleiding-van.
[22] P.J. Hartman, 'Cyberrisico's bieden ongekende kansen!', *Tijdschrift Aansprakelijkheids- en Verzekeringsrecht in de praktijk* 2017, afl. 6.
[23] Verbond van Verzekeraars, *Virtuele risico's, echte schade. Over het verzekeren van cyberrisico's*, Position paper 2013, p. 4. Te raadplegen op https://www.mkb-bedrijfsverzekeringen.nl/pdf/hiscox/cyber/cyber-risks-informatie.pdf.pdf.
[24] A.J. Nagtegaal, J.A. Kruit en F.L. Stevens, 'IMO Cyber Risk Management Resolution – óók relevant voor ladingbelanghebbenden', *Tijdschrift Vervoer & Recht* 2021, afl. 4, p. 87-92.
[25] NCTV, *Cybersecuritybeeld Nederland 2021*, 28 juni 2021, Den Haag: NCTV, p. 24-25. Te raadplegen op https://www.nctv.nl/documenten/publicaties/2021/06/28/cybersecuritybeeld-nederland-2021.

NCTV is sprake van een 'volwassen cybercriminele economie'.[26]

In het hiervoor genoemde Cybersecuritybeeld Nederland van NCTV wordt onder meer ingegaan op de verschillende cybercriminelen.[27] Er blijken drie dadercategorieën te bestaan: cybercriminele dienstverleners, afhankelijke plegers en autonome groepen.[28]

Cybercriminele dienstverleners bieden als variant op het in de 'bovenwereld' bekende *Software-as-a-Service (SaaS)* concept in de 'onderwereld' inmiddels *Cybercrime-as-a-Service (CaaS)* aan. Dit gebeurt veelal op ondergrondse, online platformen zoals gesloten cybercriminele fora. Gemiddeld zou voor het uitvoeren van een cyberaanval tussen de 66 en 500 dollar worden gevraagd.[29] Deze dienstverleners zijn tot zeer veel in staat. Een door justitie opgespoorde aanbieder van *DDos-as-a-Service* voerde bijvoorbeeld in een half jaar tijd circa 4 miljoen *DDoS*-aanvallen uit voor ruim 150.000 gebruikers.

Daarnaast zijn er de zogenaamde afhankelijke plegers, die de voornaamste groep afnemers van cybercriminele diensten vormen. Deze dadercategorie is zeer divers, groot van omvang en opereert zowel individueel als in groepen. Hoewel zij diverse vormen van cybercriminaliteit plegen, beschikken zij niet zelf over hoogwaardige technische capaciteiten. Om cyberaanvallen te kunnen plegen en zichzelf daarbij voor opsporingsdiensten te beschermen, zijn zij grotendeels afhankelijk van producten en diensten van voormelde cybercriminele dienstverleners.

Ten slotte zijn er autonome groepen, die vaak verantwoordelijk zijn voor geavanceerde aanvallen met een hoge organisatiegraad en een wereldwijde impact. Hoewel deze dadercategorie kleiner is qua omvang, zijn zij in staat om langdurige cybercriminele aanvalscampagnes uit te voeren. Veelal zijn het losse, niet-hiërarchische samenwerkingsverbanden die al langer actief zijn en daardoor veel kapitaal en expertise hebben. Deze groepen zijn autonoom, omdat ze hun cybercriminele proces hoofdzakelijk in eigen beheer ontwikkelen en uitvoeren.

Zoals hiervoor vermeld, bestaat er geen goed beeld van de bedragen die deze cybercriminelen jaarlijks met hun activiteiten verdienen. Duidelijk is echter dat het om aanzienlijke bedragen gaat.

Over de hoogte van het losgeld dat in de praktijk wordt betaald is weinig bekend. Volgens sommige schattingen zou in circa 70 procent van de gevallen losgeld worden betaald en de gemiddelde losgeldeis in het derde kwartaal van 2020 zou circa € 200.000 hebben bedragen. Het Russische *ransomware*-collectief REvii beweert € 100 miljoen per jaar te verdienen.[30] Dat verklaart wellicht in elk geval ten dele de verwachting dat de cybercriminaliteit de komende jaren alleen maar verder zal toenemen.

5. Meer informatie en contact

Wilt u meer weten over cyber, dan kunt u contact opnemen met Robert Pessers of Annevi Etienne.

In onze volgende bijdrage zullen de publiekrechtelijke regelgeving en initiatieven centraal staan.

Robert Pessers

pessers@vantraa.nl
+31 6 50 51 26 62
+31 10 22 45 502

Annevi Etienne

etienne@vantraa.nl
+31 6 82 06 69 96
+31 10 22 45 520

[26] Zie Cybersecuritybeeld Nederland 2021, NCTV 28 juni 2021, p. 27.
[27] Zie Cybersecuritybeeld Nederland 2021, NCTV 28 juni 2021, p. 28.
[28] Deze ruwe indeling neemt niet weg dat deze categorieën overlap kunnen vertonen.
[29] 'Most damaging cybercrime services cost less than $500 on the dark web', atlasvpn.com.
[30] 'Russische hackers laten bedrijven miljoenen aan losgeld betalen: 'Je kunt criminelen niet vertrouwen", ad.nl.