DOOR GLENN HARWOOD, XANDER SALARI
EN JAN-WILLEM ZEIJEN

Cyberdreigingen, risico's en weerbaarheid

Trefwoorden als 'cyberaanval' op Google leveren direct een lijst aan hits op met recente voorbeelden van organisaties die het slachtoffer zijn geworden van een hack door cybercriminelen. Ook financiële instellingen zijn slachtoffer van cyberaanvallen. Dat cyberrisk niet onderschat moet worden blijkt ook uit bijvoorbeeld het EIOPA Financial Stability Report van december 2022[1]: cyberrisico's zijn met afstand de grootste drivers van het risico, gerelateerd aan digitalisering en worden als een belangrijk 'emerging risk' gezien. 'DNB ziet dat cyberdreigingen in de maatschappij toenemen'[2] en constateert tegelijkertijd dat 'niet alle basismaatregelen bij instellingen effectief zijn ingericht en functioneren'[3]. In 2023 voert DNB een Themaonderzoek uit naar cybersecurity[4].

Ing. G. Harwood CISSP CISM CISA CRISC CEH (links), Bba. X. Salari EMIA RO CRISC (midden) en J.W. Zeijen MSc AAG zijn alle drie werkzaam als Principal bij Triple A – Risk Finance.



WELKE ROL KAN DE ACTUARIS SPELEN OP DIT ACTUELE EN BELANGRIJKE THEMA?

Een logische link is het definiëren, parametriseren en doorrekenen van een cyberrisicoscenario in de Own Risk and Solvency Assessment (ORSA) voor verzekeraars. Hierbij is het zaak om business-continuityrisico, reputatierisico en de financiële schade adequaat in te schatten. Zie hiervoor ook een eerdere blog van Jan-Willem Zeijen, waarin hij de rol van de actuaris op het gebied van cyberrisico bespreekt[5].

Onlangs verscheen, gezien de toenemende zorgen vanuit de toezichthouders, ook een discussion paper vanuit EIOPA[6], waarin wordt ingegaan op methodieken voor stresstesten met de focus op cyberrisico. EIOPA onderscheidt hierbij twee hoofdzaken.

1) Enerzijds wordt 'cyber underwriting risk' benoemd, aangeduid als de mate waarin de verzekeraar vanuit kapitaals- en solvabiliteitsperspectief de gevolgen kan dragen die zijn ontstaan door het effect van het cyber-event op de dekkingen vanuit de polissen van de verzekeraar. Dit is breder dan specifiek op cyberrisico gerichte polissen; ook zogenaamd 'silent cyber risk' speelt hierin een rol. Denk bijvoorbeeld aan mogelijke dekking van gevolgen van cyberrisico vanuit een aansprakelijkheidsverzekering.

2) Anderzijds gaat het over 'cyber resilience', aangeduid als de mate waarin de verzekeraar de financiële gevolgen van een cyberevent kan dragen. Deze gevolgen kunnen bestaan uit directe verliezen, verliezen door beschikbaarheid en herstel van systemen, verliezen door juridische gevolgen (boetes bijvoorbeeld) en reputatieschade.

In het vervolg van het paper werkt EIOPA scenario's uit, waarbij wordt gekeken naar de waarschijnlijkheid en mogelijke impact vanuit underwriting en resilience perspectief. De impact is tweeledig: operationeel (afhankelijk van de benodigde hersteltijd tot 'business as usual' en het aantal geraakte business processen) en financieel (via kasstromen en / of voorzieningen). Eén van de scenario's is 'cloud outage' (verlies van verbinding met cruciale systemen), door bijvoorbeeld brand of sabotage. Wanneer dit een verzekeraar treft, is de duur van de 'outage' relevant. Deze duur hangt ervan af of het datacentrum intern of extern is en of het in handen is van een gespecialiseerde aanbieder. EIOPA reikt externe bronnen aan waarmee de duur kan worden ingeschat. Op het operationele vlak is de impact gerelateerd aan het aantal stilgevallen processen en applicaties en de tijd die ervoor nodig is om deze weer operationeel te krijgen. Qua financiële impact kan in dit scenario worden gedacht aan de kosten van 'downtime' en het opnieuw opstarten en inrichtingen van systemen.

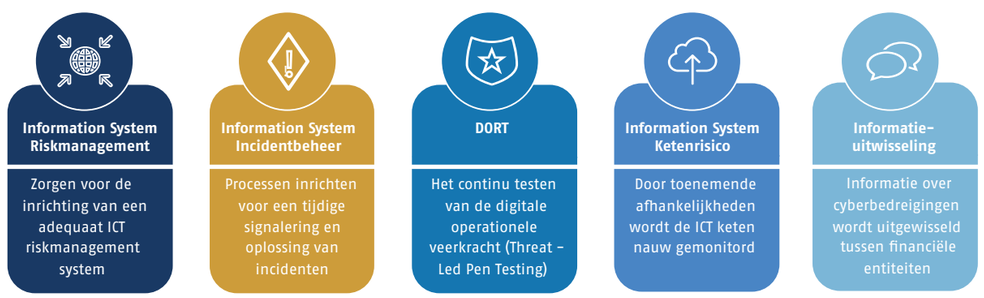
CYBER RESILIENCE IN DE PRAKTIJK

Dat cyber resilience niet 'slechts' een item is dat terugkomt in de ORSA of (potentieel) in stresstesting, blijkt wel uit twee recente, belangrijke wetten om cyber resilience te waarborgen: DORA (Digital Operational Resilience Act)[7] en NIS-2 (Network & Information Systems regulations 2018)[8].

Wat zijn de DORA en NIS-2?

De NIS-2 stelt vereisten aan de beveiliging van netwerk- en informatiesystemen van essentiële (digitale) dienstverleners. De wet heeft tot doel de cyberveiligheid en digitale weerbaarheid van deze dienstverleners te versterken en de impact van cyberaanvallen te minimaliseren. DORA stelt stringentere regels vast voor ICT-risicobeheer, incidentrapportage, operationele veerkrachttests en risicomonitoring op derde partijen. Het uiteindelijke doel van DORA, in combinatie met NIS-2, is ervoor te zorgen dat de financiële sector in Europa veerkrachtig kan blijven ondanks een ernstige operationele verstoring.

In onderstaande Figuur 1 zijn de vijf relevante DORA pijlers weergegeven. Het uitwerken van deze pijlers vergt goed inzicht in de ICT-processen, -systemen en -risico's in de gehele keten van de verzekeraar. De actuaris en het bestuur kunnen deze kennis goed gebruiken in de definitie en parametrisatie van een cyberrisico scenario in de ORSA. Zo kan een scenario met een significante impact dat tevens realistisch is gegeven de kwetsbaarheden van de verzekeraar worden bepaald. Vervolgens kunnen de managementacties in de ORSA worden gekoppeld aan de detectieve maatregelen die vanuit DORA/NIS-2 zijn vastgesteld.



Figuur 1

Wij geven een korte toelichting op de pijler 'Information System Ketenrisico'.

Ketenverantwoordelijkheid
Steeds meer financiële instellingen zijn voor een groot deel afhankelijk van derde partijen door het voeren van een IT strategie met CSP's, ofwel Critical Service Providers. Ketens worden langer, complexer en zijn veelal met elkaar verbonden. Tezamen neemt daarmee het cyberrisico voor de organisatie in potentie toe. Deze ketenwerking wordt steeds meer pijnlijk duidelijk gemaakt door cyberaanvallen van de afgelopen tijd[9]. Daarom zijn NIS-2 en DORA ook van toepassing op CSP's die ICT (gerelateerde) diensten leveren. Alle partijen in de keten moeten bestand zijn tegen, reageren op en werken aan herstel van alle soorten ICT(-gerelateerde) verstoringen en bedreigingen. De vergunninghoudende entiteit draagt, als opdrachtgever, eindverantwoordelijkheid en committeert zich aan een beheerste bedrijfsvoering in de gehele (uitbestede) keten.

FACTS & FIGURES
Dat NIS-2 en DORA nodig zijn, komt tot z'n recht als er naar historische data wordt gekeken. Onderstaande grafieken zijn gecreëerd op basis van een dataset van **datalekt**[10]. Deze pagina geeft een overzicht van gerapporteerde cyberaanvallen die in Nederland het nieuws hebben gehaald tussen 2016 en april 2023.

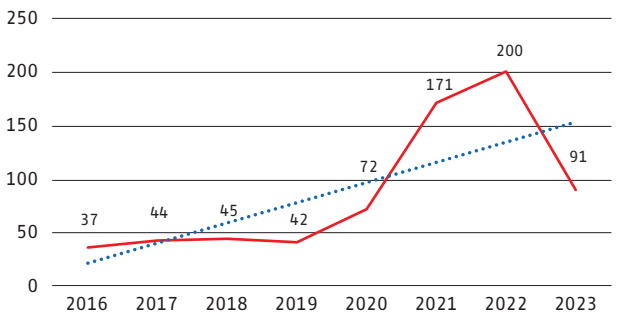
1. Totaal gerapporteerde cyberaanvallen

2. In de eerste 4 maanden van elk jaar gerapporteerde cyberaanvallen: een sterke stijging in 2023

3. Totaal gerapporteerde cyberaanvallen in financiële sector.

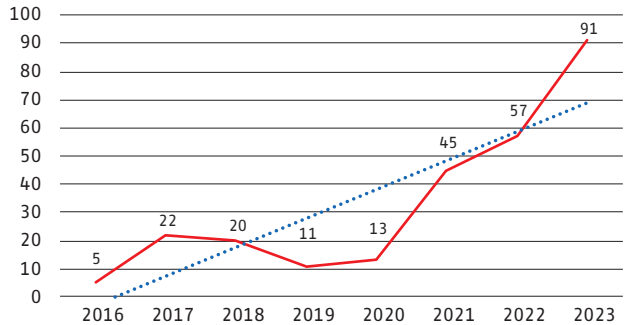
Aan de hand van de bovenstaande data worden onderstaande voorbeelden behandeld om de noodzaak voor inregeling van DORA en de NIS-2 voor de financiële wereld te illustreren:

Gerapporteerde cyberaanvallen in Nederland (alle data)



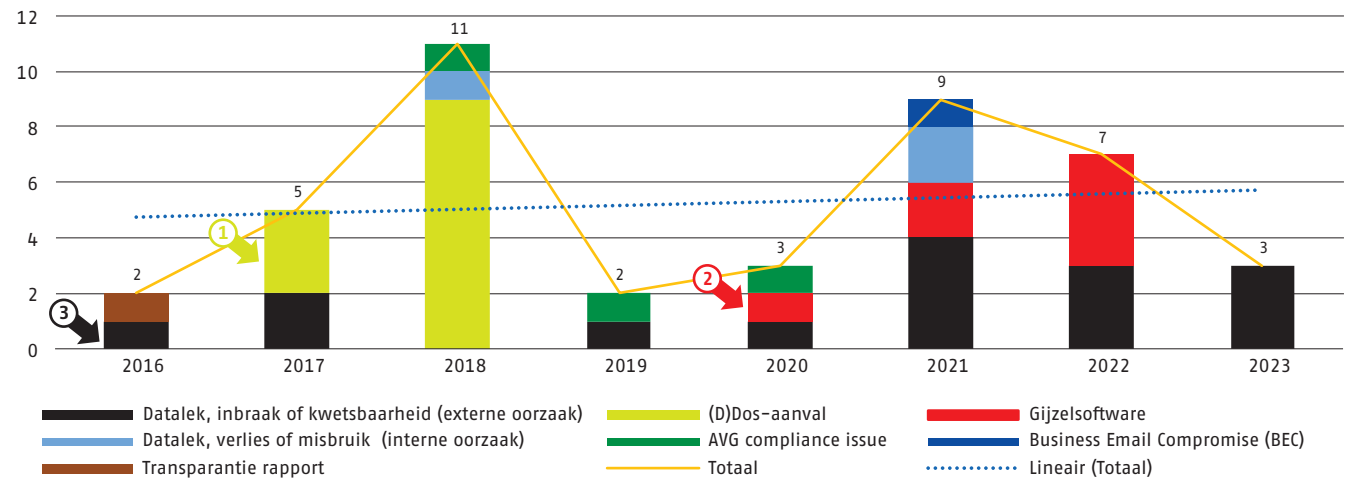
Grafiek 1

Gerapporteerde cyberaanvallen in Nederland (alleen data van eerste 4 maanden van elk jaar)



Grafiek 2

Overzicht per type gebeurtenis in financiële branche



Grafiek 3

1. **Distributed Denial of Service (DDoS) aanvallen** (GEEL): In grafiek 3 zien we twaalf DDoS aanvallen in 2017/2018, vaak gericht op dezelfde financiële instellingen. Na 2018 zijn DDoS aanvallen afgenomen, waarschijnlijk doordat de instellingen voldoende maatregelen hebben getroffen om zich ertegen te beschermen. DDoS-aanvallen kunnen de servers van een financiële instelling overbelasten, waardoor o.a. online diensten niet beschikbaar zijn voor klanten. Dit kan leiden tot financiële verliezen en reputatieschade.

2. **Ransomware-aanvallen** (ROOD): In 2020 zien we de eerste ransomware-aanval in de financiële sector. Per jaar zien we een verdubbeling ten opzichte van voorgaande jaren. Ransomware-aanvallen kunnen de gegevens van een financiële instelling ongewild versleutelen en daardoor ontoegankelijk maken totdat er losgeld wordt betaald voor het vrijgeven van een sleutelcode. Dergelijke aanvallen kunnen leiden tot aanzienlijke financiële verliezen en onderbreking van de bedrijfsvoering.

3. **Datalekken** (ZWART): De laatst opvallende observatie is dat de categorie 'Datalek, inbraak of kwetsbaarheid (externe oorzaak)' bijna jaarlijks terugkeert. Er vindt dus regelmatig een datalek plaats via een externe partij. Dit benadrukt de noodzaak voor ketenverantwoordelijkheid. Financiële instellingen slaan grote hoeveelheden gevoelige persoonlijke gegevens op, waaronder financiële en gezondheidsinformatie, wat hen tot een belangrijk doelwit maakt voor cybercriminelen. Datalekken kunnen resulteren in diefstal van deze informatie, wat kan leiden tot identiteitsdiefstal en andere vormen van fraude.

DUS: CYBERDREIGING IS DICHTERBIJ DAN WE DENKEN
In het nieuws zien we zeer regelmatig cyberaanvallen voorbij komen. Cyberaanvallen kunnen leiden tot financiële verliezen, operationele gevolgen en reputatieschade. Daarbij is de verzekeraar voor de gehele keten eindverantwoordelijk! Implementatie van DORA en NIS-2 door de verzekeraar en haar kritische leveranciers is daarom essentieel. Daarnaast kan de actuaris helpen bij het inzichtelijk maken van de impact van cybergerelateerde scenario's, door middel van de ORSA. Zware, maar realistische scenario's, die in een breed gremium binnen de organisatie zijn afgestemd (denk ook bijvoorbeeld aan de IT Security Risk functionaris) helpen hierbij. Ondertussen moet de organisatie door met het implementeren van preventieve, detectieve en correctieve risicoreacties. Denk aan het grondig uitvoeren van due dilligence en third party risicoanalyse voorafgaand aan het contracteren van een derde partij of periodieke monitoring van kritische leveranciers op de effectiviteit van vereiste prestatie en control indicatoren of het periodiek onderhouden van een Cyber Incident Response plan, waarin duidelijk vastgelegd is wie verantwoordelijk is voor het afweren van een aanval. Want... liever voorkomen dan genezen! ■

1 – https://www.eiopa.europa.eu/system/files/2022-12/eiopa_financial_stability_report_december_2022.pdf

2 – https://www.dnb.nl/nieuws-voor-de-sector/toezicht-2022/dnb-ziet-cyberdreiging-toenemen-terwijl-basismaatregelen-niet-altijd-op-orde-zijn/

3 – https://www.dnb.nl/nieuws-voor-de-sector/toezicht-2022/dnb-ziet-cyberdreiging-toenemen-terwijl-basismaatregelen-niet-altijd-op-orde-zijn/

4 – https://www.dnb.nl/media/wwjh3kik/toezichtkalender-verzekeraars-2023-versie-website-dnb.pdf

5 – https://www.actuarieelgenootschap.nl/actueel/cyberrisico-wat-is-de-rol-van-de-actuaris.htm

6 – https://www.eiopa.europa.eu/system/files/2022-11/discussion_paper_on_methodological_principles_in_insurance_stress_testing_-_cyber_competent.pdf

7 – https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0595

8 – https://www.legislation.gov.uk/uksi/2018/506

9 – https://www.channelconnect.nl/security-en-privacy/cyber-aanvallen-op-msp-in-2023-veelvuldiger/

10 – https://www.datalekt.nl/home/overzicht-cyberincidenten/