Basisprincipes voor het beheer van cybersecurityrisico's

In samenwerking met het Centrum voor Cybersecurity België

Dit is een mededeling van de FSMA ter uitvoering van artikel 66 van de wet van 2 augustus 2002.

Dit document is het resultaat van een vruchtbare samenwerking met het Centrum voor Cybersecurity België.

De FSMA heeft de Nationale Bank van België en verschillende gespecialiseerde sectorvertegenwoordigers geraadpleegd en is hun zeer erkentelijk voor hun inbreng.

Voorwoord

Cyberdreigingen vormen een groot operationeel risico voor de bedrijven die actief zijn in de financiële sector. Het is een thema dat onverdeelde aandacht verdient aangezien de meest waardevolle assets van deze bedrijven hun klanten, de gegevens over hun klanten en hun reputatie zijn.

De FSMA wil bedrijven sensibiliseren en inzicht geven in de basisbeginselen om cyberrisico's te beheren. Hiervoor werkt zij nauw samen met het Centrum voor Cybersecurity België (hierna 'CCB'). Met de basisprincipes over informatiesystemen en cybersecurity die de FSMA in dit document aanreikt, wil zij alle bedrijven helpen om organisatorische en technische cybersecuritymaatregelen in te voeren.

Merk op dat samenstellingen met het woord 'cyber' die in dit document worden gebruikt, de betekenis hebben zoals gedefinieerd in het *Cyber Lexicon* van de Financial Stability Board.

De FSMA verwacht van alle bedrijven onder haar toezicht[1] dat zij de noodzakelijke maatregelen treffen om hun informatiebeveiligingsrisico's te beheren, en in het bijzonder het cyberrisico[2], daarbij rekening houdend met de aard, de omvang en de complexiteit van hun bedrijf. Zij moeten die maatregelen regelmatig herzien en bijwerken, gebruikmakend van de meest recente technieken en best practices.

De financiële sector is een diverse sector wat de omvang en juridische structuur van de bedrijven betreft, variërend van grote ondernemingen tot eenmanszaken. De FSMA erkent dat het belang van de cyberrisicoproblematiek varieert afhankelijk van het bedrijfsmodel, de omvang en de technische complexiteit van een bedrijf. De diepgang en reikwijdte van de onderwerpen die in dit document aan bod komen zijn dan ook niet exhaustief.

---

1 ***Dit document richt zich niet op de cyberweerbaarheid van de handels- of afwikkelingsplatforms van systemisch belang (waarvoor stengere richtlijnen en vereisten gelden), zoals EURONEXT en genoteerde bedrijven die voor hun informatieverstrekking onder toezicht van de FSMA staan.***

2 De meeste definities in dit document zijn ontleend aan het *Cyber Lexicon* dat door de Financial Stability Board is gepubliceerd (12 november 2018) (hierna het 'Cyber Lexicon'). Samenstellingen met 'cyber' hebben de betekenis zoals gedefinieerd in het Cyber Lexicon. Bij twijfel verwijzen wij naar de Engelse begrippen en definities in het Cyber Lexicon. In dit document hanteren wij een officieuze vertaling van die begrippen en definities.

Cyberrisico wordt gedefinieerd als de combinatie van de waarschijnlijkheid van het optreden van cyberincidenten en de gevolgen daarvan.

Cyberincident wordt gedefinieerd als een cybergebeurtenis die i) de Cybersecurity van een informatiesysteem of de informatie die het systeem verwerkt, opslaat of verzendt in gevaar brengt of ii) een inbreuk vormt op het beveiligingsbeleid, de beveiligingsprocedures of het beleid voor aanvaardbaar gebruik, al dan niet ten gevolge van malafide activiteiten.

Dit document richt zich niet op de gevolgen van eventuele niet-naleving van de gegevensbescherming vanuit het perspectief van de Algemene Verordening Gegevensbescherming (AVG of GDPR)[3]. Alle bedrijven moeten voor elk afzonderlijk geval een eigen analyse uitvoeren.

Cybersecurity is niet slechts een IT-probleem maar vormt een uitdaging voor de gehele organisatie.

Cybersecurity[4] betreft de gehele organisatie. Hiervan moet iedere bedrijfsleider doordrongen zijn. Het is een cruciaal onderdeel van elke organisatiestrategie voor de beveiliging van de belangrijkste resources (assets) van het bedrijf. Cyberincidenten vinden hun oorsprong zowel binnen als buiten het bedrijf. De oorzaak kan een onvoorziene gebeurtenis zijn, menselijk falen of kwaad opzet (van binnenuit het bedrijf of van buitenaf).

Volgens Belgische verzekeringsmakelaars die gespecialiseerd zijn in dit domein zou 60 tot 70 procent van de veiligheidsincidenten te wijten zijn aan interne gebeurtenissen zoals menselijk falen (bijvoorbeeld ongewenst tonen van data aan onbevoegden, verzenden van e-mails met verkeerde bijlagen, onbedoeld publiceren van vertrouwelijke databases)[5].

De IT-infrastructuur kan ook worden bedreigd door alledaagse gevaren, zoals brand, overstroming of blikseminslag, of doordat het bedrijf delen van de IT heeft uitbesteed aan externe leveranciers die de gevraagde diensten niet kunnen leveren of zelf slachtoffer zijn van beveiligings- of cyberincidenten.

Bovendien worden externe cyberdreigingen steeds complexer. De financiële sector behoort tot de sectoren die het vaakst het doelwit zijn van cyberaanvallen[6]. Zelfs verregaande cybersecuritymaatregelen kunnen tevergeefs zijn, bijvoorbeeld wanneer een medewerker een e-mailbijlage opent die malware bevat of via welke malware naar de bedrijfssystemen wordt gedownload. Gangbare aanvallen zijn onder meer phishing en spear phishing[7],

---

[3] Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG.

[4] **Cybersecurity** is het behoud van vertrouwelijkheid, integriteit en beschikbaarheid van informatie en/of informatiesystemen via het cybermedium. Daarnaast kunnen er andere eigenschappen een rol spelen, zoals authenticiteit, verantwoordelijkheid, onweerlegbaarheid en betrouwbaarheid.

[5] Bevindingen van een rondetafelconferentie met gespecialiseerde verzekeringsmakelaars die de FSMA in mei 2019 in haar kantoren heeft georganiseerd.

[6] Volgens de data-analyse 2018 van IBM X-factor is de financiële en verzekeringssector al drie jaar op rij de sector die de meeste aanvallen te verduren krijgt. Menselijk falen, zoals onjuist geconfigureerde servers, onbeveiligde clouddatabases en slecht beveiligde back-ups, waren goed voor 43% van de incidenten met betrekking tot publiekelijk vrijgegeven informatie. Dat is een toename van 20% sinds het jaar voordien.

[7] **Phishing- en spear phishing-aanvallen**: phishing is een ruimere term voor pogingen om slachtoffers gevoelige informatie te laten delen, zoals wachtwoorden, gebruikersnamen en creditcardgegevens, voor kwaadwillige doeleinden. Anders dan bij spear-phishingaanvallen zijn phishingaanvallen niet gepersonaliseerd en worden

malware/ransomware[8] en frauduleuze berichten van derden waarbij vaak gebruik gemaakt wordt van e-mails of gestolen gegevens van klanten of financieel adviseurs.

Cyberincidenten kunnen, ongeacht de oorzaak, uiterst schadelijk zijn en er zelfs toe leiden dat bedrijven hun deuren moeten sluiten.

Als er omwille van een cyberincident geen financiële diensten kunnen worden verleend, is dat in de eerste plaats schadelijk voor het publiek. Het is echter ook schadelijk voor de reputatie en de activiteiten van het bedrijf en mogelijk ook voor de reputatie van de financiële sector als geheel.

Zijn bedrijven verplicht om actie te ondernemen?

Alle bedrijven zijn wettelijk verplicht om gegevens over klanten en transacties te bewaren.

Als een bedrijf persoonsgegevens kwijtraakt, kan het aansprakelijk worden gesteld voor inbreuk op de privacywetgeving (GDPR)[9].

In het ergste geval kan ernstige nalatigheid bij het beheer van klantgegevens worden beschouwd als een criminele daad. De bedrijfsleider of het hoofd bedrijfsvoering kan aansprakelijk worden gesteld en dat kan leiden tot aanzienlijke financiële claims en aansprakelijkheden.

De FSMA herinnert de bedrijven onder haar toezicht eraan dat zij alle voor hen geldende wettelijke en reglementaire vereisten inzake cybersecurity en het beheer van cyberrisico's moeten naleven, alsook alle relevante Europese en internationale vereisten of richtsnoeren, zoals die van de Europese toezichthoudende autoriteiten (ESMA, EIOPA, EBA) of de International Organisation of Securities Commissions (IOSCO).

Dit is vooral het geval voor **bedrijven die wettelijk verplicht zijn om te allen tijde over een passende organisatie te beschikken**. Dat houdt onder meer het volgende in: een passende strategie hanteren en een passend kader opzetten voor het beheer van cyberrisico's om aldus essentiële data en functies te behouden, diensten en activiteiten te handhaven of, als dat niet mogelijk is, die data en functies zo snel mogelijk te herstellen en de diensten en activiteiten zo snel mogelijk te hervatten.

De FSMA verwacht dat de directies en hogere leidinggevenden van deze bedrijven onder haar toezicht hun verantwoordelijkheid nemen voor het cybersecurityrisico en dit hoog op de

---

deze meestal in één keer naar een groot aantal personen gestuurd (https://digitalguardian.com/blog/what-is-spear-phishing-defining-and-differentiating-spear-phishing-and-phishing).

[8] **Malware**: software die voor kwaadwillige doeleinden wordt ontwikkeld en die functies of mogelijkheden bevat die direct of indirect schade kunnen aanrichten bij entiteiten of hun informatiesystemen.

Ransomware is malware die wordt gebruikt om een gebruiker af te persen door zijn IT-systeem te blokkeren, om het vervolgens tegen betaling van losgeld (vaak in cryptovaluta) te deblokkeren.

[9] Voor alle duidelijkheid wordt vermeld dat dit document de inbreuken op de GDPR-regels NIET behandelt.

agenda plaatsen. Zij moeten de juiste en meest geavanceerde maatregelen nemen om hun cyberweerbaarheid (*cyber resilience*)[10] te verbeteren en daadkrachtig belangrijke zaken ter hand nemen, zoals het op elkaar afstemmen van de IT- en bedrijfsstrategie, het uitbesteden van risicobeheer, 'change management' en cybersecuritybeheer.

Bedrijven die bij wet verplicht zijn om een 'passende organisatie' te hebben, moeten over afdoende organisatorische en technische maatregelen, beleidsregels en procedures beschikken zodat hun cybersecurity en cyberweerbaarheid gewaarborgd zijn. Bedrijven die cyberrisicogevoelige activiteiten uitbesteden, moeten erop toezien dat de dienstverlener op wie zij een beroep doen, beschikt over passende organisatorische en technische maatregelen, beleidsregels en procedures om de cybersecurity en cyberweerbaarheid van de gegevens, diensten en activiteiten te waarborgen.

Maar strategieën, kaders en beleidsregels voor de aanpak van cyberincidenten, computervirussen of cyberaanvallen hebben natuurlijk weinig zin als ze niet in praktijk worden gebracht. De bedrijven moeten dan ook procedures uitwerken om te reageren op cyberdreigingen en om ervan te herstellen. Zij moeten ook afdoende testen uitvoeren op basis van scenario's over hun corebusiness. Hoewel het document dat de FSMA aanreikt daarbij nuttig zijn, mag het niet worden beschouwd als een allesomvattende bron van inspiratie.

Ook de **overige bedrijven** (die niet wettelijk verplicht zijn om te beschikken over een passende organisatie, bv. de meeste financiële tussenpersonen) zouden maatregelen moeten treffen om de financiële data van hun klanten te beschermen en zodoende bij te dragen aan een solide en gezond financieel systeem en aan een degelijke en betrouwbare financiële dienstverlening.

De FSMA moedigt **alle bedrijven** aan om zowel hun informatiebeveiligingsbewustzijn als hun organisatorische en technische cybersecuritymaatregelen naar een hoger niveau te tillen en als prioritair aandachtspunt te behandelen. Zij moeten ten volle beseffen wat deze risico's inhouden en ze doeltreffend beheersen.

Dat betekent dat zij zich een aantal vragen moeten stellen en daar daadwerkelijke oplossingen voor moeten zoeken. Die oplossingen moeten zij uitvoerig testen. Een voorbeeld: koop geen back-upsysteem voor de data van uw bedrijf zonder eerst grondig te testen of dat systeem de data in de praktijk wel kan bewaren.

Het is ook zaak deze problematiek duidelijk te maken aan de medewerkers. Cybersecurity belangt alle medewerkers aan. Het is niet uitsluitend een aangelegenheid voor IT-specialisten.

---

[10] **Cyberweerbaarheid** is het vermogen van een organisatie om de uitvoering van haar missie voort te zetten door te anticiperen op, en zich aan te passen aan cyberdreigingen en andere relevante veranderingen in de omgeving en door cyberincidenten het hoofd te bieden, onder controle te brengen en snel te boven te komen.

Beheer van cybersecurity – vier belangrijke principes

Een doeltreffend beheer van cybersecurity is gebaseerd op vier belangrijke principes:

1. **Beveiligingsstrategie en -ondersteuning – Governance**
   - Het management betrekken en aandringen op ondersteuning;
   - Een strategie uitstippelen voor informatiebeveiliging (veiligheidsbeleid), afgestemd op de bedrijfsstrategie;
   - Een meerjarenplan opstellen voor regelmatige training en sensibilisering van alle medewerkers;
   - Voor alle nieuwe projecten een cultuur van informatiebeveiliging en risicoanalyse creëren;
   - Een plan opstellen om grote/ernstige beveiligingsincidenten en -crisissen te beheren;
   - Een register bijhouden van belangrijke veranderingen in de omgeving;
   - Een plan uitwerken om te reageren op cyberincidenten (Cyber Incident Response Plan).
2. **Inventarisatie van de resources (assets) en risicoanalyse – Inventarisatie**
   - De belangrijkste informatiesystemen en data inventariseren;
   - Een beleid hanteren om gevoelige informatiesystemen en data te categoriseren;
   - De risico's voor informatiebeveiliging beheren om prioriteiten te stellen.
3. **Implementatie van maatregelen – beschermen / detecteren / reageren en herstellen**
   - Specifieke (technische/organisatorische/procesgerelateerde) maatregelen treffen om de informatie te beveiligen;
   - Middelen die zijn toegewezen aan informatiebeveiliging en -infrastructuur effectief en efficiënt beheren, inclusief medewerkers aanstellen voor informatiebeveiliging.
4. **Evaluatie van beveiligingsmaatregelen**
   - Minstens eenmaal per jaar de beveiligingsmaatregelen evalueren om de status van het beveiligingsplan te beoordelen;
   - Geregeld nagaan welk resultaat de ondernomen acties opleveren en eveneens hoe dreigingen en kwetsbaarheden evolueren om ervoor te zorgen dat de doelstellingen worden bereikt (een proces van voortdurende verbetering);
   - Nagaan of de risicoanalyse en controlemaatregelen kunnen worden verfijnd uitgaande van evaluaties, audits, incidenten en grote veranderingen die een impact hebben of hebben gehad op de bedrijfsactiviteiten.

1. Beveiligingsstrategie en -ondersteuning – Governance

Het cyberrisico op een adequate manier beheren is eerder een bedrijfsprobleem dan een technisch IT-probleem. Doeltreffend bestuur begint bij een helder en allesomvattend kader voor informatiebeveiliging en cyberweerbaarheid. Daarom moet het bedrijf regels opstellen om zijn aanpak van het cyberrisicobeheer uit te werken, te implementeren en te herzien.

De FSMA spoort **alle bedrijven** aan om een **Cyber Incident Response Plan**[11] op te stellen met een uitgebreid schema van de maatregelen die moeten worden getroffen om de data te beschermen en de bedrijfsactiviteiten te hervatten als een incident plaatsvindt.

Volgens de FSMA is een dergelijk plan onmisbaar voor de bedrijven die ingevolge de wet te allen tijde moeten kunnen aantonen dat zij over een passende organisatie beschikken.

Het Cyber Incident Response Plan moet voorrang geven aan de dienstverlening aan klanten en alle noodzakelijke maatregelen bevatten opdat het bedrijf zijn activiteiten snel, veilig en met accurate data zou kunnen hervatten. Idealiter is dit plan opgebouwd rond de meest gangbare rampscenario's en de aspecten die de meeste bescherming behoeven. Daarnaast moet het zorgen voor adequate en snelle communicatie met alle betrokken partijen zoals, maar niet beperkt tot, de juridische instanties, de **Cyber Incident Response Teams**[12] en - als en zo mogelijk - de Gegevensbeschermingsautoriteit, de klanten, enz. Het plan kan ook ondersteuning door externe partners inhouden.

Bedrijven met doeltreffende cybersecurityprogramma's eisen doorgaans dat hun medewerkers geregeld deelnemen aan zowel algemene als specifiek op hun functie afgestemde cybersecuritytrainingen en -testen, zoals oefeningen met phishing e-mails.

Ook al heeft een bedrijf goede methoden van aanpak, het moet ook aandacht besteden aan zijn bijkantoren of verkooppunten die elders zijn gevestigd omdat die wellicht, meer nog dan het hoofdkantoor, worstelen met wachtwoordbeheer, de implementatie van patches[13] en software-updates, het updaten van antivirussoftware, het beheren van verwisselbare opslagapparaten (zoals USB-sticks), dataversleuteling en rapportage van incidenten.

Alle verkooppunten moeten worden getraind in het omgaan met cyberincidenten die een weerslag kunnen hebben op het bedrijf: klanten gaan immers vragen stellen aan de

---

[11] **Cyber Incident Response Plan (reactieplan voor cyberincidenten)**: de documentatie van vooraf opgestelde instructies of procedures om te reageren op een cyberincident en de gevolgen van het incident te beperken.

[12] **Cyber Incident Response Team**: team van goed toegeruste en betrouwbare leden van de organisatie die incidenten aanpakken gedurende de levenscyclus daarvan.

[13] **Patchbeheer (*Patch Management*)**: de systematische kennisgeving, identificatie, inzet, installatie en verificatie van revisies van softwarecode van besturingssystemen en applicaties. Deze revisies worden uitgevoerd in de vorm van patches, *hot fixes* en *service packs*.

verkoopmedewerkers, niet aan de IT-medewerkers (die op dat moment druk in de weer zijn met het technische probleem).

2. Inventarisatie van de resources (assets) en risicoanalyse – Inventarisatie

Bedrijven inventariseren, op volgorde van prioriteit, hun kritieke operaties en ondersteunende informatiemiddelen (*critical operations and supporting information assets*) die moeten worden beschermd om niet in het gedrang te komen. Deze inventarisatie is een eerste noodzakelijke en belangrijke stap: welke zijn de meest vitale assets of processen die moeten worden beschermd? Welke gegevens zijn het meest gevoelig?

Bedrijven met doeltreffende programma's voor informaticabeveiliging of cybersecurity hebben meestal sterke 'governance'-structuren en -processen (aangepast aan het bedrijf) om binnen een context van risicomanagement invulling te geven aan cybersecurity. Beslissingen en problemen rond risicoacceptatie worden doorgegeven aan de juiste niveaus om er een oplossing voor te vinden, en er wordt informatie gegeven over de toekomstige ontwikkeling van programma's.

Tot de maatregelen die deze bedrijven implementeren, behoren onder meer regelmatige risicobeoordelingen met gedetailleerde, tijdsgebonden plannen voor vervolgacties om problemen met een hoger risico op te lossen. Bedrijven met doeltreffende programma's voor cybersecurity ondersteunen hun risicobeoordeling met regelmatige kwetsbaarheids- en IT-penetratietesten[14].

Alle bedrijven moeten in gedachte houden dat proportionaliteit essentieel is bij de implementatie van cybersecurityprocessen en -procedures. Zij moeten uitgaan van hun eigen risicoprofiel, waarbij het aantal medewerkers niet de enige of belangrijkste risicoprofielindicator is.

3. Implementatie van maatregelen – beschermen, detecteren, reageren en herstellen

Alle bedrijven moeten afdoende maatregelen treffen om hun klanten en transactiedata te beschermen tegen externe en interne inbreuken. Daarbij helpt een duidelijke toewijzing van verantwoordelijkheden binnen het bedrijf de kloof tussen theorie en praktijk te overbruggen. Een vroege detectie van inbreuken stelt bedrijven in staat snel te reageren en tegenmaatregelen te nemen om verdere potentiële inbreuken en de gevolgen van daadwerkelijke inbreuken te beperken.

Naargelang hun omvang implementeren sommige bedrijven een SIEM-oplossing (Security Information and Event Management), een instrument voor het analyseren van gedrag met

[14] **Penetratietest**: een testmethodologie waarbij beoordelaars met behulp van alle beschikbare documentatie (bijvoorbeeld systeemontwerp, broncode, handleidingen) en op basis van specifieke beperkingen proberen de beveiligingsfuncties van een informatiesysteem te omzeilen.

betrekking tot systeemgebruik en tools ter voorkoming van dataverlies om mogelijk afwijkende of verdachte activiteiten op hun netwerken te detecteren, op te volgen en aan te pakken.

Bedrijven zijn voor hardware en software grotendeels afhankelijk van IT-serviceproviders. Het is verstandig om te beschikken over een formeel proces waarmee kan worden beoordeeld hoe een potentiële leverancier zich op het gebied van cybersecurity heeft voorbereid of ervoor gezorgd kan worden dat nieuwe leveranciers over de juiste bescherming beschikken.

Zo zou een contract met een externe leverancier belangrijke aspecten moeten regelen, waaronder de verantwoordelijkheid van de leverancier om aan het bedrijf een inbreuk op de bescherming van klantgegevens of bedrijfsgegevens te melden. Als er cybersecuritydiensten worden verleend aan verschillende onderling verbonden bedrijven, moet de verantwoordelijkheid voor cybersecurity voldoende zijn gedocumenteerd ten behoeve van alle bedrijven, bijvoorbeeld in een *service level agreement*.

4. Evaluatie van beveiligingsmaatregelen

Alle bedrijven moeten hun beveiligingsmaatregelen ten minste eenmaal per jaar opnieuw evalueren. Daarbij gaan zij na of de acties die zij hebben ondernomen doeltreffend zijn. Dreigingen en kwetsbaarheden moeten nauwgezet worden opgevolgd.

Zij moeten op hun hoede blijven voor snel evoluerende bedreigingen en kwetsbaarheden. Ze moeten zich voortdurend afvragen of de geïmplementeerde maatregelen nog actueel en afdoende zijn om te beantwoorden aan het doel en de risicobereidheid van het bedrijf.

Bedrijven met een doeltreffend Cyber Incident Response Plan hanteren een **proces van voortdurende verbetering** (*continuous improvement cycle*). Dat houdt in dat zij hun risicoanalyses en controlemaatregelen tenminste eenmaal per jaar verder uitdiepen en verfijnen, met het oog op evaluaties, audits, incidenten en grote veranderingen die een impact hebben of hebben gehad op hun activiteiten.

Wat als een bedrijf klein is?

Kleine bedrijven die moeite hebben om een strategie en een kader te ontwikkelen voor het beheer van cybersecurityrisico's kunnen wellicht hun voordeel doen met de **Cyber Security Reference Guide** die gepubliceerd is door het Centrum voor Cybersecurity België (https://cyberguide.ccb.belgium.be).

Als een klein bedrijf wil weten waar het staat op het vlak van cybersecurity, kan het zich eerst de '**Belangrijke Vragen'** stellen die als bijlage bij dit document zijn gevoegd[15].

[15] Deze vragen komen uit het eindrapport van de Cyber Task Force OICV – IOSCO (FR09/2019, juni 2019). (https://www.iosco.org/library/pubdocs/pdf/IOSCOPD633.pdf).

Is het moeilijk om deze problematiek in kaart te brengen, dan roept een bedrijf best de hulp in van externe consultantes of gespecialiseerde ondernemingen, en wacht het vooral niet tot het onheil is geschied.

Ook verzekeringsondernemingen die bedrijven verzekeringsdekking bieden, kunnen helpen met een preventieve screening van de cyberweerbaarheid om het cybersecurityrisico dat het bedrijf loopt te beoordelen.

Informatie delen

De FSMA spoort alle bedrijven aan om hun ervaring te delen met collega-bedrijven, bijvoorbeeld via de contactpagina op de website van de **Cyber Security Coalition**[16] of via hun beroepsverenigingen. Zo dragen zij immers bij aan een betere bescherming van de financiële sector en een groter maatschappelijk vertrouwen dat deze sector in staat is de financiële belangen van het publiek te waarborgen.

Ingevolge de **wet van 7 april 2019**[17] moeten exploitanten van handelsplatforms die worden aangemerkt als exploitanten van essentiële diensten, belangrijke incidenten melden aan het nationale Computer Security Incident Response Team (CSIRT)[18] en aan de FSMA. Financiële instellingen die zijn aangemerkt als exploitanten van essentiële diensten zonder exploitant van een handelsplatform te zijn, moeten belangrijke incidenten melden aan de Nationale Bank van België, die op haar beurt het CSIRT op de hoogte brengt.[19]

Enkele nuttige referenties:

Het Centrum voor Cybersecurity België heeft een **Cyber Security Reference Guide** gepubliceerd die online staat (https://cyberguide.ccb.belgium.be). Hierin vinden bedrijven praktische adviezen die zijn onderverdeeld in basismaatregelen en geavanceerde maatregelen.

In de onderstaande documenten vinden bedrijven uitgebreider advies dat geregeld wordt bijgewerkt. Zij moeten evenwel altijd rekening houden met het proportionaliteitsbeginsel en met hun wettelijke statuut, alsook met de invloed van de bedrijfsactiviteiten op afnemers van financiële diensten of op de financiële stabiliteit:

1. de rapporten, richtsnoeren, aanbevelingen e.d.m. die worden gepubliceerd door internationale instanties (zoals IOSCO of de OESO), door de Europese toezichthoudende autoriteiten (ESMA, EIOPA, EBA), door de centrale banken, door nationale bevoegde autoriteiten (zoals de Nationale Bank van België) of door instellingen die ervaring hebben met cybersecurity (zoals het Swift Institute).

---

16 www.cybersecuritycoalition.be

17 Wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid.

18 Op het ogenblik dat dit document wordt gepubliceerd, moet het nationale CSIRT nog bij KB worden opgericht.

19 Zie artikel 26 van de wet van 7 april 2019.

Zie bijvoorbeeld de CPMI-IOSCO Guidance on Cyber Resilience for Financial Market Infrastructures (www.bis.org/cpmi/publ/d146.pdf), evenals het eindrapport van de IOSCO Cyber Task Force (juni 2019) (https://www.iosco.org/library/pubdocs/pdf/IOSCOPD633.pdf), het NIST (National Institute of Standards and Technology) Framework for Improving Critical Infrastructure Cybersecurity (https://www.nist.gov/cyberframework) en de toolkit die in juli 2019 gepubliceerd is door het Swift Institute (***Cyber Resilience and Financial Organizations: A Capacity-building Tool Box*** - https://swiftinstitute.org/research/securing-the-long-tail-of-financial-services-toolkit/).

2. de **wet van 7 april 2019** tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid zet de Europese NIS-richtlijn (over de beveiliging van netwerk- en informatiesystemen) om in Belgische wetgeving[20], wat het delen van informatie en melden van incidenten betreft[21].

3. de ISO **27000-familie van normen voor beheersystemen voor informatiebeveiliging**, die wordt gepubliceerd door de Internationale Organisatie voor Standaardisatie (ISO) en de International Electrotechnical Commission (IEC) (zie bijvoorbeeld ISO, 'ISO/IEC 27000:2018', februari 2018, https://www.iso.org/standard/73906.html).

4. de regelmatig bijgewerkte informatie over cybercriminaliteit van het **Computer Emergency Response Team van de EU** (CERT-EU) (https://cert.europa.eu/cert/filteredition/en/CERT-LatestNews.html).

---

[20] Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie (de 'NIS'-richtlijn): https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive. De NIS-Richtlijn biedt wettelijke maatregelen om het algehele niveau van cybersecurity in de EU te bevorderen door het volgende te waarborgen:

- Voorbereiding van de lidstaten door van hen te verlangen dat zij naar behoren zijn toegerust, bijvoorbeeld door middel van een Computer Security Incident Response Team (CSIRT) en een bevoegde nationale NIS-autoriteit;
- Samenwerking tussen alle lidstaten door middel van een samenwerkingsgroep om strategische samenwerking en de informatie-uitwisseling tussen lidstaten te ondersteunen en te faciliteren. Ze zullen ook een CSIRT-netwerk moeten opzetten om vlotte en effectieve operationele samenwerking bij specifieke cybersecurity-incidenten en het delen van informatie over risico's te bevorderen;
- Een cultuur van beveiliging van de sectoren onderling die voor onze economie en samenleving vitaal zijn en die bovendien sterk afhankelijk zijn van ICT, zoals energie, transport, water, het bankwezen, infrastructuren van financiële markten, de zorg en de digitale infrastructuur. Bedrijven die door de lidstaten als exploitanten van essentiële diensten worden aangemerkt, moeten afdoende beveiligingsmaatregelen treffen en ernstige incidenten melden bij de desbetreffende nationale autoriteit. Ook belangrijke aanbieders van digitale diensten (zoekmachines, cloudcomputingdiensten en sites voor online winkelen) moeten aan de beveiligings- en kennisgevingsvereisten ingevolge de nieuwe Richtlijn voldoen.

[21] Zie artikel 4, § 3 van de wet van 7 april 2019.

5. de informatie en documenten die worden gepubliceerd door het **Centrum voor Cybersecurity België** (https://www.ccb.belgium.be/nl) en de **Belgische Cyber Security Coalition** (https://www.cybersecuritycoalition.be).

6. de **G7 fundamental elements of cybersecurity for the financial sector** (fundamentele elementen van cybersecurity voor de financiële sector, opgesteld door de G7) (https://fin.gc.ca/activty/G7/pdf/G7-cyber-risk-management-gestion-risques-cybernetiques-eng.pdf) en de **G7 Fundamental Elements for Threat-Led Penetration Testing** (fundamentele elementen voor penetratietesten op basis van dreiging, opgesteld door de G7) (https://www.fin.gc.ca/activty/G7/pdf/G7-penetration-testing-tests-penetration-eng.pdf).

Terminologie

Omdat de standaardisatie beperkt is in verband met het woord 'cyber', kan u in andere bronnen andere definities aantreffen.

De meeste definities die in dit document worden gehanteerd, zijn ontleend aan het **Cyber Lexicon** dat door de **Financial Stability Board** is gepubliceerd (op 12 november 2018). Alle samenstellingen met het woord 'cyber' die in dit document worden gebruikt, hebben de betekenis zoals gedefinieerd in het Cyber Lexicon, tenzij uitdrukkelijk anders vermeld (https://www.fsb.org/2018/11/cyber-lexicon).

De belangrijkste termen die in dit document worden gebruikt:

Cyberrisico (*Cyber Risk*)	De combinatie van de waarschijnlijkheid van het optreden van cyberincidenten en de gevolgen daarvan.
Cyberincident (*Cyber Incident*)	Een cybergebeurtenis die i) de cybersecurity van een informatiesysteem of de informatie die het systeem verwerkt, opslaat of verzendt in gevaar brengt, of ii) een inbreuk vormt op het beveiligingsbeleid, de beveiligingsprocedures of het beleid voor aanvaardbaar gebruik, al dan niet ten gevolge van malafide activiteiten.
Cyber Incident Response Plan	De documentatie van vooraf opgestelde instructies of procedures om te reageren op een cyberincident en de gevolgen van het incident te beperken.
Incident Response Team	Een team van goed toegeruste en betrouwbare leden van de organisatie die incidenten aanpakken gedurende de levenscyclus daarvan.
Cyberweerbaarheid (*Cyber Resilience*)	Het vermogen van een organisatie om de uitvoering van haar missie voort te zetten door te anticiperen op, en zich aan te passen aan cyberdreigingen en andere relevante veranderingen in de omgeving en door cyberincidenten het

	hoofd te bieden, onder controle te brengen en snel te boven te komen.
Cyber Incident Response Team	Een team van goed toegeruste en betrouwbare leden van de organisatie die incidenten aanpakken tijdens gedurende de levenscyclus daarvan.
Ransomware of malware	Software die voor kwaadwillige doeleinden wordt ontwikkeld en die functies of mogelijkheden bevat die direct of indirect schade kunnen aanrichten bij entiteiten of hun informatiesystemen.
Patchbeheer (*Patch Management*)	De systematische kennisgeving, identificatie, inzet, installatie en verificatie van revisies van softwarecode van besturingssystemen en applicaties. Deze revisies worden uitgevoerd in de vorm van patches, hot fixes en service packs.
Penetratietest (*Penetration Testing*)	Een testmethodologie waarbij beoordelaars met behulp van alle beschikbare documentatie (bijvoorbeeld systeemontwerp, broncode, handleidingen) en op basis van specifieke beperkingen proberen de beveiligingsfuncties van een informatiesysteem te omzeilen.

BELANGRIJKE VRAGEN

Bron: Eindverslag Cyber Task Force OICV-IOSCO, juni 2019
(https://www.iosco.org/library/pubdocs/pdf/IOSCOPD633.pdf)[22]

Om uw situatie op het vlak van cybersecurity te analyseren, kan u uitgaan van de volgende vragen:

A. KADER CONFORM DE INDUSTRIENORM

1. *Hanteert uw bedrijf een industrienorm om een strategie en een kader uit te werken voor het beheer van cyberrisico's (bijvoorbeeld ISO, NIST Cyber Security Framework)? Zo ja, welke norm?*

B. IDENTIFICEREN EN BESCHERMEN

2. *Houdt uw bedrijf een overzicht bij van zijn software, hardware, applicaties en leveranciers?*

[22] Officieuze vertaling.

3. *Gaat uw bedrijf na welke cyberrisico's en kwetsbaarheden een invloed kunnen hebben op de bedrijfsvoering?*
4. *Beschikt uw bedrijf over een programma voor identificatie- en toegangsbeheer waarmee het de toegang kan beperken en gebruikers tijdig de toegang kan ontzeggen?*
5. *Heeft uw bedrijf een programma voor bewustwording van cybersecurity en cybersecuritytraining zodat medewerkers hun rol daarin kennen en meer leren over nieuwe dreigingen?*
6. *Hanteert uw bedrijf een programma voor patchbeheer om de gekende kwetsbaarheden in de software aan te pakken? Gebruikt uw bedrijf hardware (bijvoorbeeld firewalls, systemen om binnendringing in het netwerk te detecteren) en software (bijvoorbeeld antimalware, systemen om binnendringing van de host te detecteren) om zijn informatiesystemen te beschermen?*
7. *Heeft uw bedrijf schriftelijke procedures om ervoor te zorgen dat er regelmatig informatieback-ups worden uitgevoerd, onderhouden en getest?*

C. DETECTEREN

8. *Spoort uw bedrijf potentiële cyberincidenten op en analyseert het die om inzicht te krijgen in de aard en reikwijdte van dreigingen en in de methoden die cybercriminelen gebruiken?*
9. *Gebruikt uw bedrijf mechanismen om e-mails te beschermen zodat malware of kwaadwillige links in e-mails automatisch worden gescand, gedetecteerd en geblokkeerd?*
10. *Heeft uw bedrijf een testprogramma om de doeltreffendheid van zijn processen en controlemechanismen voor de detectie van incidenten te beoordelen?*

D. REAGEREN/HERSTELLEN

11. *Heeft uw bedrijf een 'Incident Response Plan' om de gevolgen van cyberincidenten te beperken? Heeft het applicaties en processen om dit plan te activeren?*
12. *Behandelt het 'Incident Response Plan' het delen van informatie, waaronder het kenbaar maken van kwetsbaarheden en andere communicatie, en het melden van cyberincidenten aan interne en externe belanghebbenden, derden, toezichthouders of wetshandhavers?*
13. *Test uw bedrijf zijn 'Incident Response Plan' regelmatig en werkt het dit zo nodig bij op basis van dreigingsinformatie en cyberincidenten die zich hebben voorgedaan?*
14. *Beschikt uw bedrijf over een herstelplan om na een cyberincident zo snel mogelijk weer operationeel te zijn?*
15. *Beoordeelt uw bedrijf zijn herstelplan geregeld en werkt het dit geregeld bij?*