FINNIUS

Cyberincident bij uw financiële instelling

Vier concrete tips vanuit het financieel toezicht

Cyberaanvallen zijn aan de orde van de dag

Cyberaanvallen zijn één van de **meest acute systeemrisico's** voor de financiële sector. Dat zegt ook de AFM in Trendzicht 2027. Het komt voortdurend in het nieuws: hacks bij cryptoplatformen, ddos-aanvallen op betaaldienstverleners en datalekken bij partners van grootbanken. Een hack of storing kan leiden tot **gestolen klantgegevens**, **financiële schade**, **reputatieschade** en **kritische vragen van toezichthouders**.

Finnius begeleidt regelmatig financiële instellingen die te maken hebben met cyberincidenten. Graag delen wij **vier concrete tips** voor het correct en adequaat omspringen met cyberincidenten, om toezichtrechtelijke gevolgen te voorkomen.

DORA: eerste melding binnen 4 uur

Onder de Digital Operational Resilience Act (DORA), moeten **ICT-incidenten direct** worden **vastgelegd en geclassificeerd**. Ernstige ICT-incidenten moeten zo snel mogelijk bij de toezichthouder worden gemeld en regelmatig gerapporteerd:

4 uur	**24 uur**	**72 uur**	**1 maand**
eerste kennisgeving na classificatie	uiterlijk na detectie	tussentijds rapport	eindverslag

Raakt een ernstig ICT-incident de **financiële belangen van klanten?** Dan moet u de klanten zonder onnodige vertraging informeren.

Aparte incidentenmeldplicht

Een cyberincident kan ook een meldingsplichtig incident zijn in de zin van het Bpr/BGfo: een gedraging of gebeurtenis die een ernstig gevaar vormt voor de integere uitoefening van het bedrijf. Een incident moet zonder onnodige vertraging bij de toezichthouder worden gemeld. Ten onrechte niet of te laat melden is op zichzelf al een overtreding.

Heeft het meldingsplichtig incident inhoudelijk 'volledige overlap' met een ernstig ICT-incident onder DORA? Dan hoeft u alleen te melden onder DORA.

Vervalt de overlap? Bijvoorbeeld omdat er meer speelt dan enkel een cyberaanval of omdat de naleving van toezichtregels in het geding komt? Beoordeel dan opnieuw of de aparte Bpr/BGfo-meldplicht is ontstaan.

Bedrijfscontinuïteit

Een cyberaanval kan leiden tot forse **schade voor uw financiële instelling**, bijvoorbeeld doordat onderzoeks- en herstelkosten moeten worden gemaakt, klanten weglopen of de dagelijkse business wordt beperkt of zelfs tijdelijk tot stilstand komt.

Monitor daarom de **bedrijfscontinuïteits-thresholds** en eventuele aanvullende thresholds die passen bij het cyberincident, zoals vastgelegd in het bedrijfscontinuïteits-beleid van uw financiële instelling.

Neem gepaste maatregelen wanneer thresholds dreigen te worden overschreden, om de continuïteit te waarborgen.

Klachten en claims van klanten

Na een datalek volgen vaak **klachten of (claim)brieven** van klanten of haar belangenbehartigers.

Uw eerste reactie bepaalt vaak de verdere positie van de financiële instelling. Reageer daarom niet overhaast. Betrek tijdig een adviseur om aansprakelijkheidsrisico's in kaart te brengen en stem de communicatie met klanten af op de meldingen aan de AFM/DNB en, bij gestolen persoonsgegevens, de Autoriteit Persoonsgegevens.

Wij helpen u verder. Bij Finnius adviseren wij financiële instellingen over cyberincidenten en bijbehorende meldplichten, contact met de AFM en DNB en de reactie op klachten en/of claims van klanten. Neem gerust contact op met Laurens Hillen, Rick Sanders of Joris Viellevoije.



Laurens Hillen
laurens.hillen@finnius.com
M: +31 (0)6 216 637 76



Rick Sanders
rick.sanders@finnius.com
M: +31 (0)6 226 307 63



Joris Viellevoije
joris.viellevoije@finnius.com
M: +31 (0)6 151 160 35

Deze factsheet bevat algemene informatie en is geen juridisch advies. | © Finnius advocaten | finnius.com