# DNB 2025 | Cyberstrategie

DeNederlandscheBank

EUROSYSTEEM

# Inleiding

DNB werkt aan vertrouwen. We maken ons sterk voor financiële stabiliteit en dragen daarmee bij aan duurzame welvaart in Nederland. We doen dit in een omgeving die dynamischer is dan ooit. Ontwikkelingen zoals digitalisering en toenemende geopolitieke spanningen vergroten de cyberrisico's waaraan de financiële sector blootstaat. Daarom zetten we ons in op het verhogen van de cyberweerbaarheid van de financiële sector.

## Een weerbare financiële sector

Toenemende digitalisering van de samenleving, werken op afstand en oplopende geopolitieke spanningen leiden tot een complexer en dynamischer risicolandschap waarin cyberrisico's voor de maatschappij, de financiële sector verder toenemen. Financiële instellingen zijn, vanwege hun hoogwaardige bezittingen, gevoelige klantinformatie en hun centrale rol binnen de economie, een aantrekkelijk doelwit. Ook DNB zelf staat aan deze cyberrisico's bloot.

Cyberrisico's kunnen tot een forse schadelast leiden en zelfs de veiligheid en continuïteit van betalingsverkeer in gevaar brengen. Cyberaanvallen vinden niet alleen plaats op financiële instellingen zelf, maar in toenemende mate ook op ICT-dienstverleners waarvan instellingen steeds intensiever gebruik maken. Wanneer verschillende instellingen van dezelfde partij ICT-diensten afnemen, kunnen ook concentratierisico's ontstaan. Een groot cyber-incident schaadt niet alleen de instelling, maar potentieel ook het vertrouwen in de sector en kan zo gevolgen hebben voor de financiële stabiliteit. Zo kan een operationele verstoring in het digitale betalingsverkeer steeds grotere gevolgen hebben naarmate chartaal geld minder wordt gebruikt. Het cyberrisico moet dan ook beschouwd worden als een systeemrisico.

In deze cyberstrategie geeft DNB duidelijkheid over hoe we vanuit onze taken als centrale bank, toezichthouder en resolutieautoriteit, bijdragen aan het versterken van de cyberweerbaarheid van de financiële sector. Deze cyberstrategie is een nadere uitwerking van de DNB2025 visie en strategie.

> Welke externe ontwikkelingen DNB om zich heen ziet?

> Hoe DNB de cyberweerbaarheid versterkt?

> Wat DNB zelf doet

# Veranderend cyberlandschap

## Belangrijkste cyberrisico's anno 2023

1. **Ransomware**
   Een type cyberaanval waarbij systemen en data worden versleuteld door middel van malware. Deze versleuteling kan ongedaan worden gemaakt door losgeld (ransom) aan de daders te betalen. Naast de versleuteling wordt data ook vaak gestolen. Publicatie daarvan kan dan worden voorkomen door het betalen van losgeld.
2. **Aanval op derde partijen**
   Een cyberaanval op derde partijen die vitale diensten leveren. Uitval van systemen of diefstal van data bij die derde partij kan verstrekkende gevolgen hebben voor de afnemende financiële instelling.
3. **Aanval via derde partijen**
   Een cyberaanval waarbij de crimineel zich toegang verschaft tot de systemen van de financiële instelling via een leverancier.
4. **Geavanceerde phishing door middel van Artificiële Intelligentie**
   Nederlandse financiële instellingen zijn regelmatig het doelwit van geavanceerde phishing richting directies en (kritieke) medewerkers. Deze vormen van phishing kunnen de komende tijd nog geavanceerder en gerichter worden met de opkomst van (gemakkelijk te verkrijgen) AI-tools zoals face cloning en voice cloning.
5. **Insiders**
   Een kwaadwillende medewerker binnen een organisatie die daar geplaatst is of gerekruteerd wordt door criminelen en zodoende een bedreiging vormt voor de organisatie.

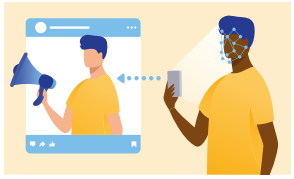
Door verdergaande digitalisering en sterke onderlinge verbondenheid staan financiële instellingen meer dan ooit bloot aan cyberrisico's. Bovendien zijn deze risico's aan continue verandering onderhevig.

Belangrijke trends die de risico's waaraan instellingen blootstaan beïnvloeden zijn bijvoorbeeld voortschrijdende technologische ontwikkeling, oplopende geopolitieke spanningen en uitbesteding van digitale bedrijfsprocessen aan IT-dienstverleners.

> Technologische ontwikkeling
> Geopolitieke spanningen
> Uitbesteding

# Technologische ontwikkeling leidt tot snel evoluerende cyberrisico's

Technologische ontwikkelingen in de financiële sector volgen elkaar snel op en bieden mogelijkheden tot onder andere kostenbesparing en het vergroten van het gebruiksgemak voor de consument. Tegelijkertijd stellen nieuwe technologieën kwaadwillenden ook in staat om steeds geavanceerdere cyberaanvallen uit te voeren en bieden zij toegang tot nieuwe modus operandi.



Zo kunnen met behulp van artificiële intelligentie *deep fakes* gecreëerd worden voor desinformatiecampagnes, die zich via social media razend snel kunnen verspreiden.

In de toekomst kan *quantum* computing mogelijk de encryptie waarmee instellingen werken doorbreken. Dit heeft gevolgen voor vertrouwelijke klantdata, vitale systemen, authenticatie processen en de versleuteling en ontsleuteling van betalingen.

Tot slot wordt geavanceerde technologie ook voor een steeds breder publiek toegankelijk, al dan niet doordat deze tegen betaling wordt aangeboden door criminelen *(crime as a service)*.

> Technologische ontwikkeling
> Geopolitieke spanningen
> Uitbesteding

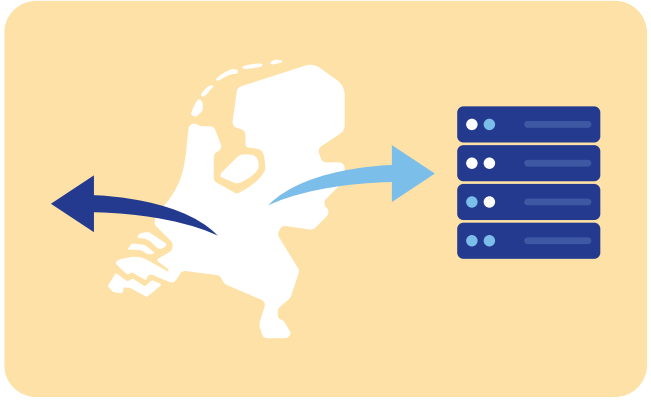
# Oplopende geopolitieke spanningen versterken cyberdreiging

De huidige politieke spanningen (zoals situatie in Oekraïne) hebben het wereldbeeld veranderd. Gebeurtenissen die plaatsvinden, belichten ontwikkelingen die al langere tijd gaande zijn: de verschuiving van een unipolaire wereldorde, met daarin een centrale rol voor de VS, naar een multipolaire wereldorde, waarbij door invloedrijke landen en regio's wordt ingezet op fundamentele veranderingen in de wereldorde. De spanningen op het wereldtoneel waarmee dit gepaard gaat, vertalen zich door naar potentiële dreigingen voor instellingen in het digitale domein. Denk aan dreigingen zoals disruptieve cyberaanvallen door statelijke actoren, cyberspionage en insider threats.

> Technologische ontwikkeling
**> Geopolitieke spanningen**
> Uitbesteding

# Uitbesteding creëert ketenafhankelijkheden en potentiële concentratierisico's

Financiële instellingen maken in toenemende mate gebruik van derde partijen voor hun digitale bedrijfsprocessen, zoals IT-bedrijven en clouddienstverleners. Hoewel deze partijen vaak veel expertise hebben en hoge normen voor cyberveiligheid en informatiebeveiliging kennen, introduceert deze uitbesteding ook ketenafhankelijkheid en complexiteit. Mede als gevolg van deze uitbesteding verschuiven cyberaanvallen zich dan ook naar derde partijen. Uitbesteding kan ook tot concentratie risico's leiden, wanneer meerdere instellingen gebruik maken dezelfde partij. Het uitvallen van één cruciale partij, kan de dienstverlening bij een groot deel van de financiële sector stilleggen. Inzicht en beheersing van cyberweerbaarheid betreffende de gehele keten is hierbij evident.



> Technologische ontwikkeling
> Geopolitieke spanningen
> **Uitbesteding**

# Versterken cyberweerbaarheid financiële sector

Cyberrisico's evolueren snel. Dat vergt dat financiële instellingen onder andere actief monitoren wat voor hen de relevante cyberrisico's zijn, de beveiliging van hun IT-systemen up to date houden en periodiek hun cyberweerbaarheid testen. Een cyberweerbare financiële sector vergt daarom een blijvende inspanning.

Vanuit haar taken als centrale bank, toezichthouder en resolutieautoriteit draagt DNB bij aan het versterken van de cyberweerbaarheid door:

**Toezicht te houden op de beheersing van cyberrisico's door instellingen**

- Gerichte inzet van toezichtsinstrumenten
- Monitoren van ketenafhankelijkheden en concentratierisico's

**Samen te testen en oefenen om cyberweerbaarheid te verhogen**

- TIBER-testen & sector informatiedeling
- Cyber-crisisoefeningen & parate crisis-structuur voor de financiele kern infrastructuur

**Onderlinge kennisdeling met de sector en andere stakeholders**

- Delen van kennis en expertise met de financiële sector, overheid, vitale infrastructuur en EU

> Toezicht op beheersing cyberrisico's

> Oefenen en testen

> Kennisdeling

# Toezicht op de beheersing van cyberrisico's

Voor een beheerste en integere bedrijfsvoering is het essentieel dat financiële instellingen risico's op het gebied van informatiebeveiliging en cybersecurity beheersen, ook wanneer sprake is van uitbesteding. DNB ziet er op toe dat instellingen hun cyberweerbaarheid op orde hebben en houden. Met de inwerkingtreding van de Digital Operational Resilience Act (DORA) in januari 2025 krijgt DNB additionele instrumenten in handen om de cyberweerbaarheid van de financiële sector, inclusief derde partijen, verder te borgen.

## Gerichte inzet van toezichtinstrumenten

Terwijl de cyberdreiging toeneemt, blijkt dat instellingen basismaatregelen niet altijd op orde hebben. Met uitvragen en gerichte onderzoeken bij meerdere instellingen ziet DNB erop toe dat instellingen voldoen aan wet- en regelgeving. Bredere lessen uit deze onderzoeken worden ook aan de sector teruggegeven. Het waarborgen van voldoende aandacht en kennis van cyberrisico's aan de bestuurstafel en bij leden van raden van commissarissen en raden van toezicht is belangrijk. In de geactualiseerde corporate governance code is dit nadrukkelijker opgenomen. In ons toezicht besteden we expliciet aandacht aan dit kennisniveau. Daarnaast voert DNB in het kader van het Single Supervisory Mechanism (SSM) cyberstresstesten uit. Zo worden kwetsbaarheden inzichtelijk gemaakt en achterblijvende instellingen geactiveerd om hun cyberweerbaarheid te verhogen.

## Monitoren van ketenafhankelijkheden en concentratierisico's

DNB ziet dat financiële instellingen in toenemende mate diensten uitbesteden. Het is belangrijk dat instellingen de hieruit voortvloeiende uitbestedingsrisico's en aansprakelijkheden adequaat beheersen. Inzicht en beheersing van cyberweerbaarheid in de gehele uitbestedingsketen is belangrijk en vormt mede door de komst van DORA een belangrijk onderdeel van ons toezicht. Dit omvat ook het ontvangen van toereikende assurance-rapportages over de gehele uitbestedingsketen, waarbij naast ex-post ook ex-ante informatie wordt gerapporteerd. Met DORA worden hiervoor belangrijke stappen gezet. Onder andere doordat kritieke derde aanbieders van ICT-diensten onder rechtstreeks oversight worden geplaatst, ondanks dat zij geen financiële instelling zijn. Door instellingen te laten rapporteren over hun afhankelijkheid van ICT-dienstverleners, kunnen daarnaast potentiële concentratierisico's inzichtelijk gemaakt worden.

**> Toezicht op beheersing cyberrisico's**

> Oefenen en testen

> Kennisdeling

# Oefenen en testen om cyberweerbaarheid te verhogen

Om de cyberweerbaarheid te verhogen is het belangrijk de weerbaarheid van instellingen tegen geavanceerde cyberaanvallen te testen en om cybercrisisoefeningen uit te voeren. Zowel om sterke en zwakke punten te identificeren, als om te leren hoe na een aanval snel hersteld kan worden.

## TIBER-testen & sector informatiedeling

In het TIBER-NL programma coördineert DNB het dreigingsgebaseerd testen van de digitale weerbaarheid van (kritieke) financiële instellingen. Aan het TIBER-NL programma nemen onder andere grote banken, pensioenuitvoerders en verzekeraars deel. Het doel is om de cyberweerbaarheid van de Nederlandse financiële sector tegen geavanceerde cyberaanvallen te verhogen. Hiertoe wisselen deelnemende instellingen ook onderling ervaringen uit. Het TIBER programma wordt uitgevoerd in een groeiend aantal Europese landen. DNB deelt kennis en ervaring met Europese landen die een eigen TIBER programma willen opstarten. Door DORA kan voor financiële instellingen Threat Lead Penetration Testing verplicht worden.

## Cyber-crisisoefeningen

Ook het oefenen van crisiscoördinatie, communicatie en herstel na een cyberaanval heeft aandacht. Snel herstel en duidelijke communicatie na een cyberaanval helpen bij het behoud van vertrouwen in de financiële sector. DNB initieert en neemt daarom deel aan cybercrisis-oefeningen om zo samen beter voorbereid te zijn. De scenario's die in deze oefeningen worden gesimuleerd zijn gebaseerd op actuele dreigingen en ontwikkelingen zoals het afnemende gebruik van chartaal geld en de gevolgen als alternatief voor digitaal betalingsverkeer. Ervaringen die daarmee opgedaan worden, geven richting aan het verhogen van de cyberweerbaarheid.

DNB coördineert het Tripartiete Crisismanagement Operationeel (TCO) voor de financiële sector en richt zich op sector crisismanagement in het geval van operationele verstoringen in het betalings- en effectenverkeer. Hiervoor organiseert DNB, samen met AFM en het Ministerie van Financiën, oefeningen en coördineert zij deelname aan (inter)nationale oefeningen, zoals ISIDOOR.

> Toezicht op beheersing cyberrisico's

**> Oefenen en testen**

> Kennisdeling

# Kennisdeling met de sector en andere stakeholders

De toenemende complexiteit van cyberaanvallen maakt het delen van kennis en ervaring tussen instellingen in de financiële sector belangrijker. DNB deelt kennis en inzichten over cyberdreigingen en hoe de cyberweerbaarheid verhoogd kan worden. Dit doet DNB onder andere met de overheid, andere toezichthouders en beroepsorganisaties.

## Brede deling van kennis en expertise

DNB deelt inzichten en kennis en haalt deze op door onder meer:

- In samenwerking met de sector periodiek een dreigingslandschap, het One Financial Threat Landscape, op te stellen. Dat geeft inzicht in de meest actuele cyberdreigingen waarop instellingen kunnen acteren. Ook deelt DNB informatie over IT-security en cybercrime-gerelateerde incidenten in trusted communities, zoals FI-ISAC.
- Periodiek nieuwsberichten over haar waarnemingen over IT- en cyberrisico's te publiceren. Ook deelt DNB benchmarkinformatie en resultaten van onderzoeken met de sector, zoals de Good Practice informatiebeveiliging. Dit doet DNB naast de individuele terugkoppeling aan de instelling zelf.
- Actief te participeren in conferenties en deel te nemen aan werkgroepen binnen de overheid, beroepsorganisaties en Europese toezichthouders en centrale banken. Daarnaast adviseert DNB over nieuwe wet- en regelgeving (bijv. Digital Operational Resilience Act, DORA).

DNB richt zich primair op de financiële sector. Waar er afhankelijkheden met de financiële sector zijn én dit passend is binnen haar mandaat, ondersteunt DNB ook de vitale sectoren die het meest kritiek zijn voor de financiële sector, zoals de energiesector en telecomsector. DNB doet dat ook richting de overheid en het Nationale Cyber Security Centrum (NCSC), onder andere door advies te geven over het opzetten van een TIBER framework bij het Rijk. Tenslotte werkt DNB samen met de ECB en andere Europese centrale banken en toezichthouders, investeert ze in TIBER-EU (DORA TLPT) en begeleidt Europese cybertesten op de meest vitale systemen voor de EU. Ook zet DNB zich actief in als liason tussen Nederlandse financiële instellingen en ESCB/EU instellingen.

> Toezicht op beheersing cyberrisico's

> Oefenen en testen

**> Kennisdeling**

# Wat doet DNB om zelf cyberweerbaar te zijn en blijven?

DNB heeft, als onderdeel van de Nederlandse financiële sector, ook te maken met de snel veranderende omgeving en bijbehorende risico's. Dit vraagt om een voortdurende inspanning om de cyberweerbaarheid op orde te houden. We leggen onszelf dan ook dezelfde normen op als die we voor de financiële sector hanteren. Ook nemen we hiervoor diverse maatregelen. Zo beoordelen we op basis van de Good Practice Informatiebeveiliging hoe DNB scoort in de benchmark ten opzichte van andere financiële instellingen. Ook heeft DNB zitting in de FI-ISAC en werken we met inlichtingen- en veiligheidsdiensten om de fysieke- en digitale dreigingen het hoofd te bieden. Daarnaast nemen we deel aan het TIBER programma waarbij wij onszelf intensief laten testen. Ten slotte bekijken we hoe DNB op basis van internationale standaarden scoort en wisselen wij kennis uit, zoals best practices, met andere centrale banken.

De Nederlandsche Bank N.V.
Postbus 98, 1000 AB Amsterdam
020 524 91 11
dnb.nl

Volg ons op:

DeNederlandscheBank
EUROSYSTEEM