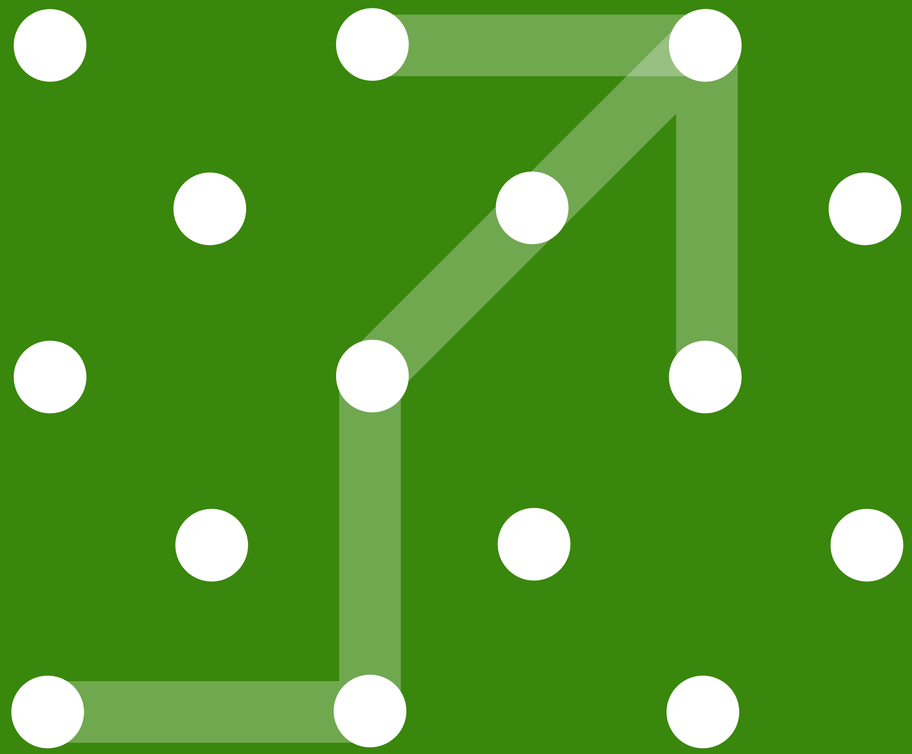
Roadshow overheidspublicaties

Sessie Cyberbeveiligingswet

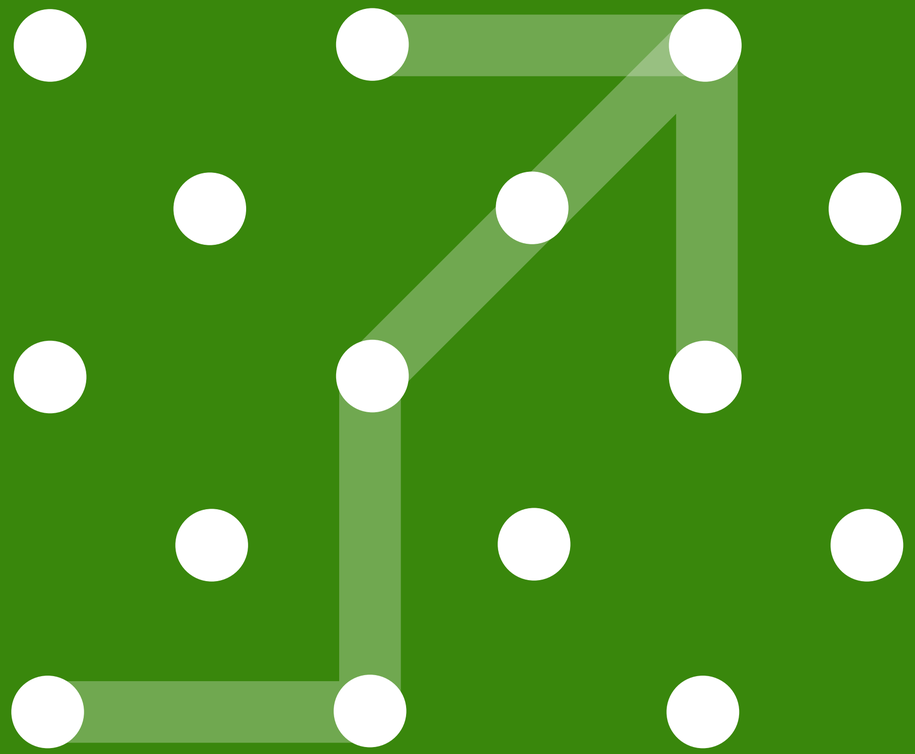
Kim Pfeifer, coördinerend beleidsmedewerker
toezicht informatieveiligheid

28 mei 2026



Mededelingen

- Alle sessies worden opgenomen (deelnemers niet in beeld)
- Opnames zijn na afloop terug te kijken op YouTube (mits toestemming van spreker(s))
- PowerPoint na afloop op website KOOP te vinden
- Stel uw vragen via de chat
- Geen antwoord? U kunt uw vraag altijd stellen via implementatie.op@logius.nl
- Evaluatie aan einde sessie



Doel van het webinar

1: Informeren op hoofdlijnen over de Cyberbeveiligingswet

2:Praktisch

Doel Cyberbeveiligingswet (artikel 2)

Deze wet is gericht op het verhogen van de cyberbeveiliging door regels te stellen ten aanzien van:

a. het beheersen van risico’s voor de beveiliging van netwerk- en informatiesystemen;

b. het voorkomen van incidenten;

c. het beperken van gevolgen van incidenten;

d. het verkrijgen en verstrekken van informatie over incidenten, bijna-incidenten, cyberdreigingen en kwetsbaarheden.

Nodig omdat….

RTL Nieuws

Alle gestolen data Odido-hack gepubliceerd, dit is wat je kan doen als je ertussen zit

RTL Nieuws / RTL Z · 2 maart 2026 · Aangepast: 2 maart 2026

Het zat al in de lijn der verwachting, en sinds afgelopen weekend is het een feit: alle gestolen Odido-klantdata is door de cybercriminele groep Shinyhunters gepubliceerd. Het gaat om namen, adressen, bankrekeningnummers en documentnummers van identiteitsbewijzen van zo'n 6 miljoen mensen. Zitten jouw gegevens erbij? En wat kun je doen? Vijf vragen en antwoorden.

security.nl Certified Secure

Nieuws Achtergrond Community

Nieuws

Autoriteit Persoonsgegevens en Raad voor de rechtspraak gehackt via Ivanti-lek

vrijdag 6 februari 2026, 16:28 door **Redactie**, 28 **reacties**

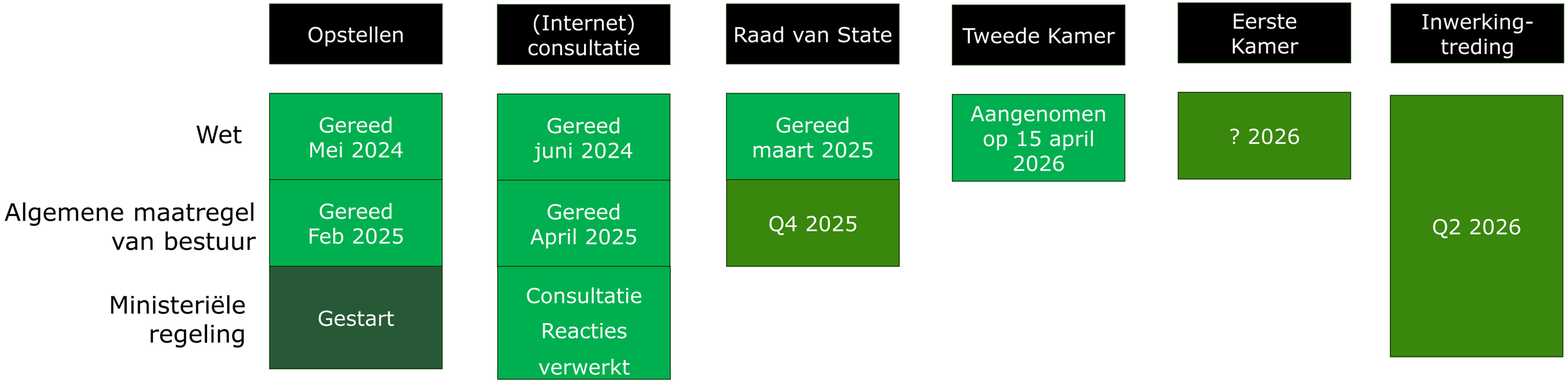
Aanvallers zijn erin geslaagd de Ivanti EPMM-server van de Autoriteit Persoonsgegevens (AP) en Raad voor de rechtspraak te hacken. In het geval van de AP hebben de aanvallers toegang gekregen tot werkgerelateerde gegevens van medewerkers van de AP, zoals naam, zakelijk e-mailadres en telefoonnummer. Dat schrijft demissionair staatssecretaris Rutte van Justitie en Veiligheid in een **brief** aan de Tweede Kamer.

NOS Nieuws • Donderdag 23 april, 10:58

Persoonsgegevens van vrijwel alle inwoners Epe gestolen bij cyberaanval

Bij een cyberaanval op de server van de gemeente Epe zijn vorige maand van vrijwel alle inwoners persoonsgegevens buitgemaakt. Dat meldt de gemeente na uitvoerig onderzoek.

Stand van zaken wetgevingstraject



Scope Cyberbeveiligingswet voor de overheid

-Ministeries en hun agentschappen

-Provincies

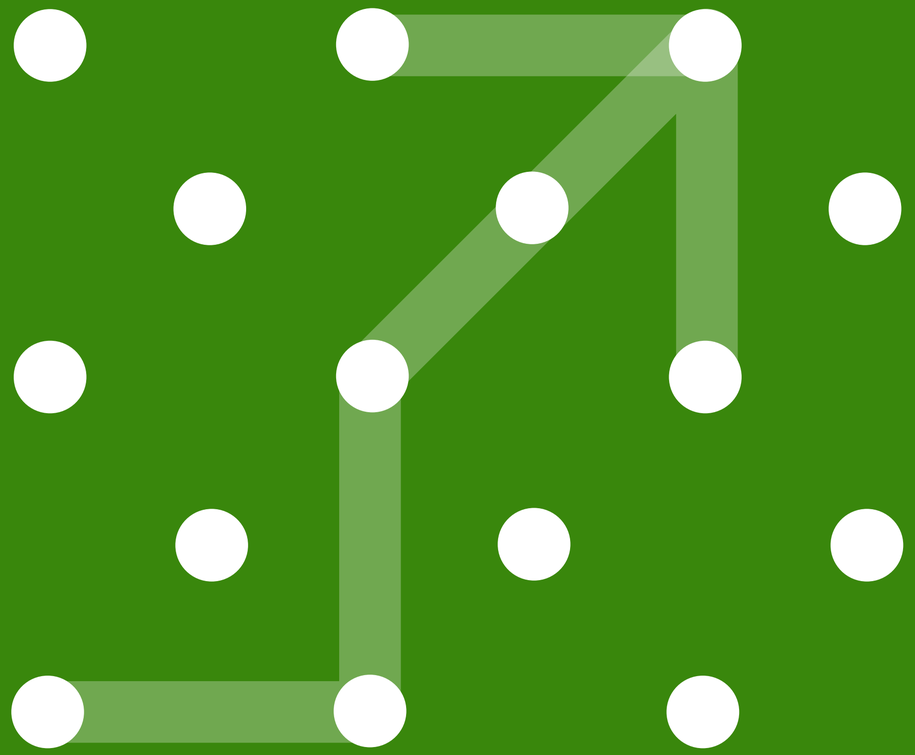
-Gemeenten

-Gemeenschappelijke regelingen

-Zbo’s

-Uitzonderingen: organisaties die een taak hebben op terrein nationale veiligheid

-Waterschappen horen bij de sector water van het ministerie van Infrastructuur en Waterstaat



Verplichtingen Cyberbeveiligingswet

- Registratieplicht
- Zorgplicht
- Meldplicht
- Toezicht

Registratieplicht

- Koppeling met het Register van Overheidsorganisaties (ROO)

- Voorbereiden van registratie:

- Zorgen dat eHerkenning beschikbaar is

- Overzicht van domeinlevel namen (zie ook digitoegankelijkheid dashboard)

- Afgesproken in organisatie wie registreert

- Afgesproken in organisatie wie contactpersonen zijn

- Bereikbaarheid organiseren buiten kantooruren

Meldplicht (1)

- Significante cyberincidenten moeten worden gemeld bij het Computer Security Incident Response Team (CSIRT) en toezichthouder

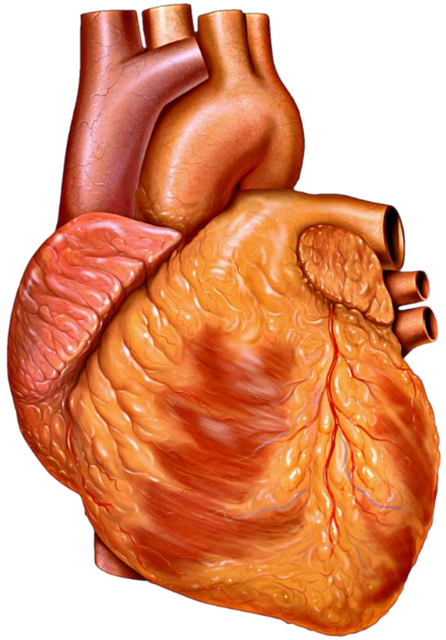
- Voor gemeenten: Informatiebeveiligingsdienst (IBD) en de Rijksinspectie Digitale Infrastructuur (RDI)

- In de ministeriele regeling overheid uitgewerkt wat wordt bedoeld met ‘significant incident’ > hierover is veel afstemming geweest met alle bestuurslagen

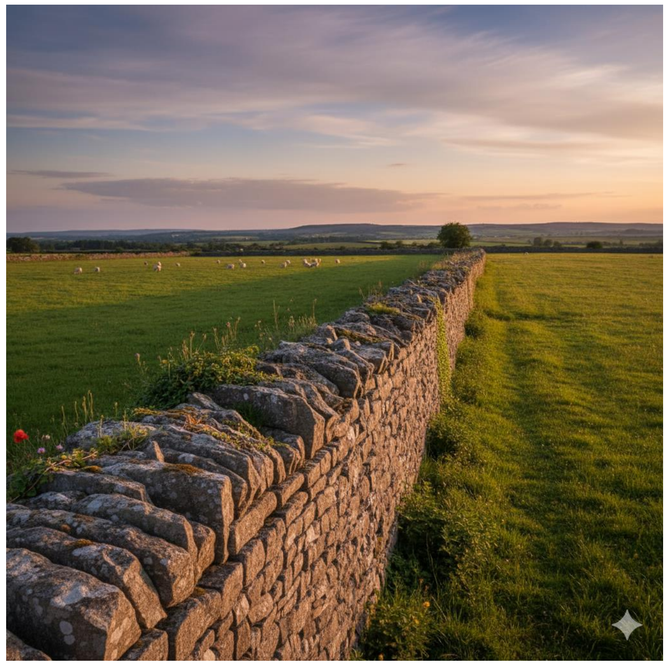
- Let op: persoonsgegevens? Dan óók melden bij Autoriteit Persoonsgegevens

Meldplicht (2) Welke incidenten melden?

Bij een essentiële dienst: ieder incident



Bij een niet essentiële dienst: drempelwaarden



Meldplicht (3): melden van een incident

Meldplicht (4) Aanwijzing CSIRT

Ministeries, agentschappen en ZBO’s	NCSC
Provincies	NCSC
Gemeenten	IBD
Gemeenschappelijke regelingen met een gemeente	IBD
Gemeenschappelijke regelingen zonder een gemeente	NCSC

Toezicht (1)

- Een onafhankelijke toezichthouder toetst de naleving van de verplichtingen uit de richtlijn, zoals de zorg- en meldplicht

- Rijksinspectie Digitale Infrastructuur (RDI) wordt de toezichthouder voor sector overheid

- Waterschappen uitgezonderd, zij vallen onder toezicht Inspectie Leefomgeving en Transport (ILT)

Toezicht (2)

- Toezicht heeft een doel: gewenst gedrag > maatschappelijke waarde!
- Toezicht Rijksinspectie Digitale Infrastructuur is systeemgericht
- Verzamelen informatie op basis van bestaande verantwoording
- Bevindingen opvolgen in beleid

Praktisch

- Organisaties willen instructie voor implementatie van de Cyberbeveiligingswet
- Alleen: de Cyberbeveiligingswet kan niet worden nageleefd aan de hand van een algemeen stappenplan/vinkenlijstje
- Entiteiten die onder de Cyberbeveiligingswet vallen, moeten zelf nadenken wat voor hun eigen organisatie nodig is
- Wel zijn hulpmiddelen beschikbaar om de invulling van de verplichtingen te realiseren. Bijvoorbeeld: Cbw (NIS2) Control Framework | Auditdienst Rijk

Wie moet dit allemaal gaan doen?! En wat als ik de capaciteit niet heb….

- Iedereen in een organisatie moet mee helpen, van inkoop tot archivering

  Bijvoorbeeld: gezamenlijk maken van risicoanalyse

- Bestuurder: is verantwoordelijk (zie art 24 Cyberbeveiligingswet)

  Moet risico’s kennen en maatregelen goedkeuren

- Bestuurders bij gemeenten: college B&W > op advies internetconsultatie

- Chief Information Security Officer (CISO): adviserend aan de organisatie

Communicatie door het ministerie van Binnenlandse Zaken

- 17 juni Symposium Cyberbeveiligingswet bij de overheid > ook online te volgen
- Brief aan alle overheidsorganisaties die onder de Cyberbeveiligingswet vallen
- Overzicht tooling: https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/cyberbeveiligingswet/tooling-cyberbeveiligingswet/
- Ondersteuningsprogramma Baseline Informatiebeveiliging Overheid (BIO): https://www.bio-overheid.nl/

Communicatie door Nationaal Cybersecurity Centre en Rijksinspectie Digitale infrastructuur

- https://www.ncsc.nl/cyberbeveiligingswet-nis2
- Cyberbeveiligingswet | Rijksinspectie Digitale Infrastructuur (RDI)
- https://www.rdi.nl/onderwerpen/digitale-weerbaarheid/cyberbeveiligingswet/risicomanagement/operationele-technologie

Tip: volg deze organisaties op LinkedIn voor de berichtgeving over de Cyberbeveiligingswet