

Bijeenkomst VNG Overijssel

Platform
Informatiesamenleving

26 juni 2025



Van wachtwoord tot wereldorde



ONDERWERPEN

NIEUWS

AGENDA

Waar bent u

[Home](#) / [Nieuws](#) / Gemeenten zijn de kurk waarop de samenleving blijft drijven

Gemeenten zijn de kurk waarop de samenleving blijft drijven

iBestuur

Digitalisering en Democratie

Overheid in Transitie

Markt en Overheid

Data en AI

Digitale

[Digitale weerbaarheid](#) | [Nieuws](#)

Gemeenten stemmen in met gezamenlijke aanpak digitalisering

Programma

1. Opening & introductie
2. Digitale dreigingen in bestuurlijke context
3. Casus & dilemma's
4. Bestuurlijke weerbaarheid en digitale geletterdheid
5. Actieopdracht
6. Afronding



DISCLAIMER

1. Opening & introductie

mr. Ben den Tuinder

*Hoofddocent Recht bij de opleiding Safety & Security Management
en
Onderzoeker bij het lectoraat Weerbare Democratie*



Stellingen

Ja



Nee



Peiling

Hoe digitaal weerbaar voelt u zich als bestuurder?

Op een schaal van 1 tot 10



2. Digitale dreigingen in bestuurlijke context

Dreigingsbeeld Informatiebeveiliging 2025-2026 uit

 Nieuws

Gerelateerde onderwerpen
Informatiesamenleving, Digitale
veiligheid en privacy

donderdag 5 juni 2025

Gemeenten worden geconfronteerd met een complex en structureel dreigingslandschap. Dat blijkt uit het Dreigingsbeeld Informatiebeveiliging 2025–2026 door de Informatiebeveiligingsdienst (IBD). De belangrijkste risico's zijn ransomware-aanvallen, datalekken en verstoringen door incidenten bij leveranciers.



Invoering Europese cyberbeveiligingswetten opnieuw uitgesteld

17 juni 2025

Het omzetten van de NIS2-richtlijn in de Cyberbeveiligingswet (Cbw) en de CER-richtlijn in de Wet weerbaarheid kritieke entiteiten (Wwke) is opnieuw vertraagd. Dat meldt justitieminister David van Weel (VVD) in een Kamerbrief. De wetten zouden in het derde kwartaal van 2025 worden ingevoerd. De minister mikt nu op het tweede kwartaal van 2026. In een brief verzoekt Van Weel de Tweede Kamer om haast te maken met de behandeling van de wetten.

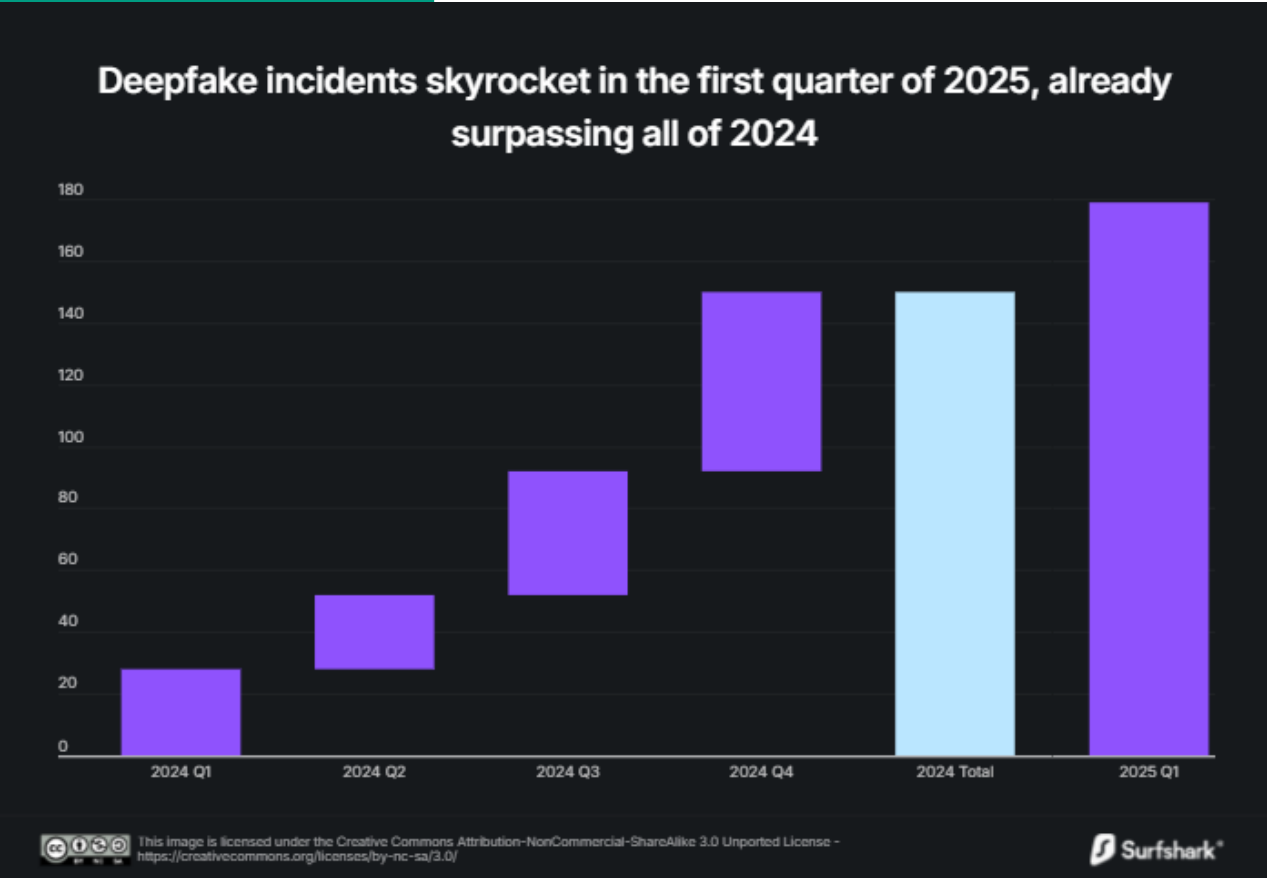


Reflectievraag

Wat is het grootste digitale risico voor uw gemeente?



3. Casus & dilemma's



Deepfake burgemeester

Een deepfake-video van een burgemeester waarin hij/zij discriminerende uitspraken doet, gaat viraal op sociale media. De video lijkt authentiek, maar is volledig nep. Binnen enkele uren staat de lokale media op de stoep en vragen inwoners om opheldering.

Wat doe je als bestuurder? En hoe communiceer je?

1. Herken en erken het incident snel
2. Communiceer transparant en proactief
3. Bescherm de burgemeester én het ambt
4. Onderzoek en aangifte
5. Gebruik het incident als leerpunt

Hof van Twente mag schade van hack niet verhalen op IT-leverancier

Gelderse gemeenten doelwit van ransomware-aanval

Dreigingsbeeld Informatiebeveiliging 2025-2026 uit

 Nieuws

Gerelateerde onderwerpen
Informatiesamenleving, Digitale
veiligheid en privacy

donderdag 5 juni 2025

Gemeenten worden geconfronteerd met een complex en structureel dreigingslandschap. Dat blijkt uit het Dreigingsbeeld Informatiebeveiliging 2025–2026 door de Informatiebeveiligingsdienst (IBD). De belangrijkste risico's zijn ransomware-aanvallen, datalekken en verstoringen door incidenten bij leveranciers.

Op de afgelopen twee jaar zijn meer dan 150 Nederlandse gemeenten direct of indirect getroffen door ransomware-incidenten. Dat blijkt uit het *Dreigingsbeeld informatiebeveiliging Nederlandse gemeenten 2025/2026* van de Informatiebeveiligingsdienst (IBD) van de Vereniging van Nederlandse Gemeenten (VNG). Ransomware blijft daarmee de grootste digitale dreiging voor lokale overheden.

Ransomware- aanval op gemeente

De gemeente wordt getroffen door een ransomware-aanval. Alle systemen zijn versleuteld: burgerzaken, uitkeringen, e-mailverkeer. De aanvallers eisen losgeld in cryptovaluta. De dienstverlening ligt stil.

Wat doe je als bestuurder? En hoe communiceer je?

1. Niet betalen/wel betalen
2. Wees open en feitelijk
3. Bied perspectief
4. Toon leiderschap
5. Voorkom paniek of speculatie

4. Bestuurlijke weerbaarheid en digitale geletterdheid

Persoonlijke Digitale Hygiëne

- Gebruik sterke, unieke wachtwoorden en een wachtwoordmanager
- Activeer tweefactorauthenticatie (2FA) op alle accounts
- Herken phishingmails en verdachte links
- Wees terughoudend met het delen van persoonlijke informatie online
- Laat je regelmatig bijscholen in digitale veiligheid

Organisatorische Maatregelen

- Stel een Chief Information Security Officer (CISO) aan
- Zorg voor een actueel crisiscommunicatieplan
- Voer regelmatig cybercrisisoefeningen uit
- Houd toezicht op leveranciers en ketenpartners
- Zorg dat digitale veiligheid structureel op de agenda staat

Politiek-bestuurlijke Rol

- Geef het goede voorbeeld in digitaal gedrag
- Agendeer digitale veiligheid in raadsvergaderingen
- Stimuleer digitale geletterdheid bij ambtenaren én inwoners
- Maak digitale weerbaarheid onderdeel van integrale veiligheidsbeleid
- Werk samen met andere gemeenten, VNG, IBD en NCSC

5. Actieopdracht

Wat kunt u morgen doen om de digitale weerbaarheid van uw gemeente te versterken?



6. Afronding



- Digitale dreigingen zijn reëel, actueel en raken ook het lokaal bestuur.
- Bestuurlijke weerbaarheid vraagt om actie op drie niveaus: persoonlijk, organisatorisch en politiek-bestuurlijk.
- Casus zoals deepfakes en ransomware zijn geen fictie, maar realistische scenario's waarvoor voorbereiding nodig is.

6. Afronding



TAKE ACTION

- Agendeer het onderwerp structureel in het college en de raad.
- Laat een risicoanalyse uitvoeren op digitale kwetsbaarheden.
- Stimuleer bewustwording en training binnen de organisatie.
- Benoem een bestuurlijk aanspreekpunt voor digitale veiligheid.

6. Afronding



- Raadpleeg de handreiking “**Digitale Weerbaarheid voor Gemeentebestuurders**” van de IBD/VNG.
- Overweeg deelname aan een regionale cybercrisisoefening.
- Sluit aan bij het netwerk van bestuurlijke ambassadeurs digitale veiligheid.



Neem gerust contact op:

b.c.dentuinder@saxion.nl

[Ben den Tuinder | LinkedIn](#)