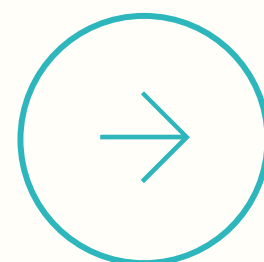




CUCCIBU'S INSIGHT OF THE WEEK

Een terugblik op het nieuws van de afgelopen week:

- AP: Politie kan gegevens niet langer bewaren dan wettelijk toegestaan
- DDoS-aanvallen op Nederlandse organisaties rondom NAVO-top
- CO2 heffing verdwijnt: industrie opgelucht, klimaatdoelen onder druk
- Hogescholen starten grootschalig onderzoek: 'Weerbaar tegen online criminaliteit'



AP: Politie kan gegevens niet langer bewaren dan wettelijk toegestaan

19 juni 2025 - De Autoriteit Persoonsgegevens (AP) waarschuwt de Tweede Kamer dat het overschrijden van de wettelijke bewaartermijnen van politiegegevens niet is toegestaan. De politie bewaart structureel persoonsgegevens langer dan wettelijk mag. Het gaat om miljoenen gegevens van onschuldige burgers, zoals meldingen over buurtruzies of verkeersovertredingen – zonder aantoonbare meerwaarde en niet relevant voor cold cases.

Wettelijke kader: Wet politiegegevens (Wpg)

Volgens de Wet politiegegevens (Wpg) moeten deze gegevens:

- Na 5 jaar uit actieve systemen worden verwijderd
- En na 10 jaar volledig vernietigd worden

Toch overtreedt de politie deze regels sinds 2019, onder het mom van een aangekondigde wetswijziging die er nog steeds niet is. Dit leidt tot een voortdurende schending van de wet én van de grondrechten van betrokkenen, met verhoogde risico's op misbruik en datalekken.

Advies: houd je aan de geldige bewaartermijnen

De AP stelt duidelijk: als de Kamer wil dat politiegegevens langer worden bewaard dan wettelijk is vastgelegd, dan moet eerst de wet worden aangepast. Tot die tijd geldt: óók de politie moet zich houden aan de privacy wetgeving.

Deze situatie onderstreept het belang van:

- Strikte naleving van wet- en regelgeving (zoals vastgestelde bewaartermijnen)
- Transparante en doelgerichte verwerking van persoonsgegevens
- Beperken van risico's op privacyschending en datalekken



DDoS-aanvallen op Nederlandse organisaties rondom NAVO-top

23 juni 2025 - Rondom de NAVO-top zijn meerdere Nederlandse organisaties – waaronder gemeenten en vervoersbedrijven – het doelwit geweest van opeenvolgende DDoS-aanvallen. De aanvallen zijn grotendeels geclaimd door de pro-Russische groepering NoName057(16) en lijken symbolisch van aard: websites werden tijdelijk traag of onbereikbaar, maar er was geen inbraak of dataverlies.

Geen verrassing voor het NCSC

Deze aanvallen kwamen niet onverwacht. Het Nationaal Cyber Security Centrum (NCSC) had vooraf al gewaarschuwd voor een verhoogd risico tijdens de NAVO-top. De aanvallen zijn gericht op publieke organisaties die direct of indirect betrokken zijn bij het evenement. De activiteiten van NoName057(16) worden al langere tijd gevolgd door het NCSC en passen binnen een bekend patroon van digitale verstoringen rondom geopolitieke gebeurtenissen.

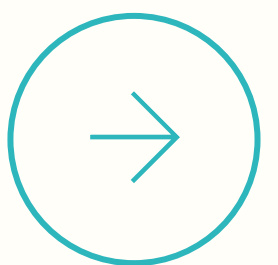
Wat is een DDoS-aanval?

Een Distributed Denial-of-Service (DDoS)-aanval is bedoeld om websites, servers of netwerken onbereikbaar te maken. Door het versturen van extreem veel dataverkeer tegelijk raken systemen overbelast, wat leidt tot vertragingen of uitval. Belangrijk om te weten: Bij een DDoS-aanval is er geen sprake van datadiefstal of systeeminbraak. De integriteit en vertrouwelijkheid van gegevens blijft intact. Wel kan de dienstverlening tijdelijk worden verstoord, wat met name organisaties die afhankelijk zijn van digitale bereikbaarheid kan raken.

Belangrijke takeaways

Deze incidenten maken opnieuw duidelijk hoe kwetsbaar onze digitale infrastructuur is tijdens belangrijke internationale bijeenkomsten, zoals de NAVO-top. Daarom is het essentieel om:

- Alert te blijven op dreigingen
- Preventieve maatregelen toe te passen
- En te zorgen dat kritieke processen goed beschermd zijn



CO2 heffing verdwijnt: industrie opgelucht, klimaatdoelen onder druk

25 juni 2025 - De Tweede Kamer heeft besloten de nationale CO₂-heffing voor de industrie af te schaffen. Deze maatregel – ingevoerd om bedrijven extra te stimuleren hun uitstoot terug te dringen – kwam bovenop het bestaande Europese emissiehandelssysteem (ETS).

Opluchting bij de industrie

VNO-NCW en andere werkgeversorganisaties zijn positief: zij zien het besluit als het wegnemen van dubbele belastingdruk en een stap richting een gelijk speelveld binnen Europa.

Hoewel de industrie verduurzaming belangrijk vindt, wijzen zij op praktische belemmeringen die investeringen momenteel moeilijk maken: overvolle stroomnetten, stikstofproblematiek, vastgelopen bouw en een gebrek aan infrastructuur voor waterstof en CO₂-afvang. Volgens bedrijven werkte de heffing daardoor niet als effectieve prikkel.

Klimaatdoelen onder druk

Milieuorganisaties en klimaatexperts uiten forse kritiek en waarschuwen dat het klimaatbeleid door de afschaffing van de CO₂ heffing aan kracht verliest. Tegenstanders noemen het een “cadeautje voor de vervuiler” dat het behalen van de klimaatdoelen in 2030 verder in gevaar brengt.

Het Planbureau voor de Leefomgeving (PBL) verwacht dat de uitstoot zonder de heffing ongeveer 1 procentpunt hoger ligt in 2030. Het PBL concludeerde vorig jaar al dat de kans kleiner dan 1 op 20 is dat Nederland zijn klimaatdoel – 55% minder uitstoot dan in 1990 – in 2030 haalt.

Minister Hermans kwam met aanvullende maatregelen, maar een eerste analyse in opdracht van milieuorganisaties toont aan dat dit pakket onvoldoende is, zelfs als de CO₂-heffing nog zou blijven bestaan.



Hogescholen starten grootschalig onderzoek: 'Weerbaar tegen online criminaliteit'

25 juni 2025 - De Haagse Hogeschool en Hogeschool Saxion starten een vierjarig onderzoek onder de naam 'Weerbaar tegen online criminaliteit'. Dit grootschalige onderzoek richt zich op de preventie van cybercrime en de nazorg van slachtoffers. Met het onderzoek willen ze onder andere praktische ondersteuning voor slachtoffers ontwikkelen, effectieve preventiecampagnes ontwerpen en hulpmiddelen voor kwetsbare groepen creëren.

Het onderzoek dient twee centrale doelen:

- **Preventie:** het versterken van digitale weerbaarheid om slachtofferschap van cybercriminaliteit te voorkomen.
- **Nazorg:** het bieden van emotionele, psychologische en praktische hulp aan slachtoffers, om hun veerkracht en herstellervermogen te vergroten.

Samenwerking met Fonds Slachtofferhulp

Het project wordt uitgevoerd in samenwerking met Fonds Slachtofferhulp, dat jaarlijks €550.000 investeert in het onderzoek. Hiervan is €250.000 afkomstig van het Ministerie van Justitie en Veiligheid. Naast financiële steun levert het fonds ook inhoudelijke expertise op het gebied van slachtofferzorg en preventie.

De noodzaak is groot

Cybercriminaliteit treft jaarlijks bijna 2 miljoen Nederlanders. De impact gaat verder dan alleen financiële schade. Slachtoffers ervaren vaak angst, schaamte en een verminderd gevoel van veiligheid. De emotionele en psychologische schade is aanzienlijk.

Ondanks de toenemende aandacht voor het probleem, blijven veel vragen nog onbeantwoord als het gaat om impact, preventie en passende hulpverlening bij online slachtofferschap. Met dit onderzoek zetten de betrokken partijen een belangrijke stap richting betere hulp voor slachtoffers én een effectievere aanpak van online criminaliteit in de toekomst.