cuccibu
Reduce Risk, Create Value

CUCCIBU'S
INSIGHT OF THE WEEK

Een terugblik op het nieuws van de afgelopen week:

- Algoritmes Dienst Toeslagen en Belastingdienst voldoen niet aan AVG
- UWV meldde vorig jaar 900 datalekken bij Autoriteit Persoonsgegevens
- Een op de vijf bedrijven had vorig jaar schade door Cybercriminaliteit
- Celstraf voor boa die adressen gaf aan criminelen

Data Privacy

Algoritmes Dienst Toeslagen en Belastingdienst voldoen niet aan AVG

21 mei 2025 - De Algemene Rekenkamer heeft onderzoek gedaan naar drie algoritmes die door overheidsinstellingen worden gebruikt. Algoritmes dragen bij aan een effectievere uitvoering van overheidsbeleid, maar dit onderzoek bracht aan het licht dat de algoritmes van de Dienst Toeslagen en de Belastingdienst niet voldoen aan de eisen van de Algemene Verordening Gegevensbescherming (AVG), wat leidt tot privacyrisico's voor burgers.

Tekortkomingen bij beide algoritmes
De Dienst Toeslagen gebruikt een algoritme om ouders met financiële problemen door terugbetalingen van de kinderopvangtoeslag snel op te sporen, en de Belastingdienst zet een algoritme in om carrouselfraude te detecteren. Ondanks de toegevoegde waarde, voldoen beide algoritmes niet aan de AVG. Persoonsgegevens worden onvoldoende beschermd en het ontbreekt aan een Data Protection Impact Assessment (DPIA) en adequate IT-beheersmaatregelen.

Algoritme UWV
Het UWV gebruikt een algoritme om te bepalen of een uitkeringsaanvragen verwijtbaar werkloos is. De Rekenkamer concludeert dat het UWV veruit de meeste risico's goed beheerst. Hoewel er nog werk te doen is op het gebied van het IT-beheer van de risicoscan, is de toegevoegde waarde van dit model duidelijk. Het UWV heeft veel maatregelen getroffen om de privacyrisico's te beperken.

Betere controle nodig
Dit onderzoek benadrukt het belang van strengere eisen vanuit de Rijksoverheid voor het gebruik van complexe algoritmes en AI binnen overheidsinstellingen. Het is essentieel dat de overheid verantwoord gebruik maakt van de kansen die AI biedt, met inachtneming van privacybescherming, adequaat IT-beheer en het voorkomen van discriminatie.

Bron: Security.nl en Algemene Rekenkamer

Data Security

Een op de vijf bedrijven had vorig jaar schade door cybercriminaliteit

21 mei 2025 - Een recent onderzoek van ABN Amro laat zien dat in 2024 één op de vijf Nederlandse bedrijven schade ondervond door cybercriminaliteit. Bij grote bedrijven is dit zelfs het geval voor drie op de tien ondernemingen. Het vaakst ging het om financiële verliezen, gevolgd door verlies van gegevens en operationele verstoringen.

Onvoldoende beveiliging in het MKB

Hoewel veel bedrijven denken dat hun beveiliging op orde is, onderschatten ze vaak de cyberrisico's, vooral in het midden- en kleinbedrijf (mkb). Veel mkb'ers hebben geïnvesteerd in basisbeveiliging, zoals firewalls en antivirusprogramma's, maar richten zich te weinig op de detectie van inbraken en het herstel na een aanval.

Zo sterk als de zwakste schakel

Cybercriminelen richten zich steeds vaker op het mkb, omdat grotere bedrijven hun beveiliging beter op orde hebben. Ze vallen specifieke doelwitten aan, zoals kritieke infrastructuur en de zorgsector, via zwakkere schakels in de keten. Veel mkb’ers zijn zich echter onvoldoende bewust van de cyberrisico’s waarmee zij te maken hebben. Een cyberaanval kan niet alleen de getroffen bedrijven schaden, maar ook hun toeleveranciers en de gehele keten.

NIS2 wetgeving: onvoldoende bekend

De NIS2-richtlijn verplicht bedrijven om hun cyberveiligheid te verbeteren, met eisen op het gebied van risicobeheersing, het melden van incidenten en ketenverantwoordelijkheid. Toch blijkt uit onderzoek dat veel bedrijven onvoldoende op de hoogte zijn van de nieuwe regelgeving. Slechts twee op de drie grote bedrijven en minder dan de helft van het mkb is bekend met de NIS2-verplichtingen. Hoewel het mkb niet direct aan NIS2 hoeft te voldoen, kunnen klanten of leveranciers die wel onder de wet vallen, eisen stellen aan hun cybersecurity.

Bron: NOS en ABN AMBRO

Data Privacy

Celstraf voor boa die adressen gaf aan criminelen

22 mei 2025 - De 60-jarige Amsterdamse buitengewoon opsporingsambtenaar (boa), Christina H., is veroordeeld tot een gevangenisstraf van twee jaar, waarvan zes maanden voorwaardelijk. Daarnaast krijgt ze een beroepsverbod van vijf jaar.

Misbruik van toegang tot gemeentelijke systemen

De boa maakte misbruik van haar toegang tot gemeentelijke systemen en keek tientallen keren naar gegevens die niets met haar werk te maken hadden, waaronder tijdens de nachtelijke uren. Tussen november 2023 en oktober 2024 gebruikte ze deze toegang om persoonsgegevens, zoals adressen gekoppeld aan kentekens, te achterhalen en door te geven aan criminelen. Deze gegevens werden vervolgens ingezet bij misdrijven waarbij ook geweld werd toegepast.

H. verklaarde dat zij geen financiële vergoeding ontving, maar wel een lening terugkreeg van een persoon die zij 'Ronaldo' noemde. Daarnaast ontving ze een horloge als tegenprestatie. De rechter oordeelde dat H. mensen in groot gevaar heeft gebracht en veroordeelde haar voor computervredebreuk, schending van haar ambtsgeheim en omkoping.

Verantwoordelijkheid onder de Wet politiegegevens

De Wet politiegegevens (Wpg) regelt de verwerking van persoonsgegevens door opsporingsinstanties en boa’s. Deze wet stelt strikte eisen aan het verzamelen, gebruiken en delen van politiegegevens om de privacy van burgers te waarborgen. In dit geval heeft de boa misbruik gemaakt van haar toegang tot gemeentelijke systemen, die mogelijk onder de reikwijdte van de Wpg vallen, door persoonsgegevens zonder rechtmatige grond te delen met derden.

Dit incident benadrukt het belang van strikte naleving van privacy wetgeving en de noodzaak voor organisaties om passende technische en organisatorische maatregelen te treffen om onbevoegde toegang tot en verwerking van persoonsgegevens te voorkomen.

Bron: NOS

Data Privacy

UWV meldde vorig jaar 900 datalekken bij Autoriteit Persoonsgegevens

22 mei 2025 - In 2024 meldde het UWV maar liefst 919 datalekken bij de Autoriteit Persoonsgegevens (AP), waarvan 334 meldingsplichtig waren. Bijna 65% van deze meldingen werd binnen de wettelijk vereiste termijn van 72 uur gedaan. Een opvallend incident betrof de online werkzoeksite Werk.nl, waarbij via één werkgeversaccount maar liefst 150.000 cv's werden bekeken en mogelijk gedownload. Dit incident leidde ertoe dat het UWV besloot persoonsgegevens in cv's volledig af te schermen en voortaan alleen de noodzakelijke gegevens zoals naam, woonplaats, telefoonnummer en e-mailadres zichtbaar te maken.

Het aantal datalekken bij het UWV benadrukt dat bijna elke organisatie vroeg of laat te maken krijgt met een datalek. Het is dan ook essentieel om een goed ingericht proces te hebben voor het melden van datalekken. Het is van groot belang dat organisaties snel en effectief kunnen handelen om de (privacy)schade te beperken. Dit voorkomt juridische en reputatieschade en helpt om de gevolgen voor betrokkenen te minimaliseren.

Welke stappen nemen je bij een datalek?

- Breng het datalak in kaart: wat is de oorzaak en welke persoonsgegevens zijn gelekt?
- Tref maatregelen om het datalek te stoppen en schade te beperken.
- Beoordeel of je het datalek moet melden bij de AP.
- Bepaal of slachtoffers geïnformeerd moeten worden.
- Registreer het datalek in het datalekregister (verplicht volgens de AVG).

Melden aan Autoriteit Persoonsgegevens

Niet elk datalek hoeft gemeld te worden bij de AP. Dit hangt af van de risico-inschatting die een organisatie maakt en de mogelijke impact van het datalek op de betrokkenen. De AVG bepaalt:

- Een datalek moet worden gemeld bij de AP, tenzij het niet waarschijnlijk is dat het datalek een risico oplevert voor 'de rechten en vrijheden van betrokkenen'.
- De slachtoffers moet worden geïnformeerd als een datalek waarschijnlijk een hoog risico voor hen oplevert.

Bron: Security.nl en Autoriteit Persoonsgegevens