cuccibu
Reduce Risk, Create Value

CUCCIBU'S
INSIGHT OF THE MONTH

Een terugblik op het nieuws van de afgelopen weken:

- Canvas datalek raakt Nederlandse universiteiten.
- AP: organisaties nemen geen maatregelen om impact op datalek te beperken.
- Populaire AI-modellen overtreden op grote schaal de wet.

Information Security Privacy

Canvas datalek raakt Nederlandse universiteiten

8 mei 2026 - Studenten en medewerkers van zeven Nederlandse universiteiten zijn getroffen door een datalek bij Instructure, de leverancier van Canvas. Canvas is een webgebaseerd Learning Management System (LMS) waarmee onderwijsinstellingen lesmateriaal, opdrachten en communicatie digitaal aanbieden aan studenten.

Bij het incident zijn basisgegevens van studenten en medewerkers buitgemaakt, waaronder namen, e-mailadressen en mogelijk Canvas-ID's of student- en medewerkersnummers. De aanval wordt gelinkt aan **hackersgroep ShinyHunters**, die eerder dit jaar ook verantwoordelijk werd gehouden voor de grootschalige aanval op telecomprovider Odido waarbij gegevens van miljoenen Nederlandse klanten werden gestolen.

Naar aanleiding van het datalek hebben verschillende universiteiten en hogescholen maatregelen genomen door systemen tijdelijk los te koppelen van Canvas. Hiermee hopen onderwijsinstellingen verdere toegang tot gegevens van studenten en medewerkers te beperken. Daarnaast zijn studenten en medewerkers geïnformeerd over het incident en gewaarschuwd alert te zijn op mogelijke phishingmails die kunnen volgen op het datalek.

Het incident laat opnieuw zien hoe groot de impact kan zijn van cyberaanvallen op leveranciers binnen de keten. Niet alleen de directe organisatie, maar ook aangesloten instellingen en gebruikers kunnen hierdoor worden geraakt.

Bron: Security.nl, NOS

Information Security Privacy

AP: organisaties nemen geen maatregelen om impact datalek te beperken

15 mei 2026 - Cyberincidenten en datalekken zijn aan de orde van de dag. Toch waarschuwt de Autoriteit Persoonsgegevens (AP) dat veel organisaties nog onvoldoende maatregelen nemen om de impact van datalekken te beperken.

In aanloop naar het rondetafelgesprek in de Tweede Kamer over cyberveiligheid en informatiebeveiliging op 21 mei, publiceerde de AP een position paper met drie noodzakelijke verbeterpunten voor de cyberveiligheid van Nederland:

Zorg voor een hoog beveiligingsniveau. Organisaties en ICT-leveranciers moeten hun technische en organisatorische beveiliging verbeteren. Dit begint met het in kaart brengen van risico's en het daarop afstemmen van passende beveiligingsmaatregelen.

Beperk de gevolgen van datalekken. Een datalek is nooit volledig uit te sluiten. Daarom is het niet alleen belangrijk om datalekken te voorkomen, maar ook om de impact ervan te beperken. Denk aan dataminimalisatie, naleving van bewaartermijnen en adequate communicatie richting betrokkenen.

Garanderen van adequaat toezicht. Volgens de AP is sterker preventief toezicht op de AVG en de Cyberbeveiligingswet (NIS2) noodzakelijk. De toezichthouder geeft echter aan dat hiervoor momenteel onvoldoende capaciteit beschikbaar is.

De kernboodschap van de AP is helder: cyberveiligheid draait niet alleen om preventie, maar ook om het beperken van schade wanneer het misgaat. Daarmee onderstreept de AP opnieuw dat gegevensbescherming en digitale veiligheid onlosmakelijk met elkaar verbonden zijn.

Bron: Security.nl, Position Paper (AP)

Information Security Privacy

Populaire AI-modellen overtreden op grote schaal de wet

27 mei 2026 - Uit onderzoek van de Amsterdamse Aithos Research Foundation blijkt dat populaire AI-modellen op grote schaal Europese wetgeving overtreden, waaronder bepalingen uit de AVG en de AI Act. Voor het onderzoek werden twaalf AI-modellen, waaronder Claude, GPT, Gemini, Mistral en DeepSeek, getest aan de hand van drieduizend praktijkscenario's waarin de modellen opdrachten kregen die mogelijk in strijd zijn met Europese regelgeving.

De scenario's varieerden van het analyseren van emoties van medewerkers op basis van e-mails tot het misleiden van kwetsbare gebruikers om duurdere producten te verkopen. Volgens de onderzoekers bleken de AI-modellen regelmatig bereid om:

- kwetsbaarheden te gebruiken voor misbruik van klanten
- misleidende informatie te geven
- zonder toestemming persoonsgegevens te verzamelen

Wanneer dit nodig was om het doel van de gebruiker te behalen.

Zelfs het best presterende model overtrad in bijna de helft van de gevallen de wet. Daarmee laten de resultaten zien dat wet- en regelgeving rondom AI weliswaar in ontwikkeling is, maar dat technische waarborgen en controlemechanismen nog achterblijven.

De onderzoekers waarschuwen dat de snelle uitrol van AI-agents vooruitloopt op de infrastructuur die nodig is om AI verantwoord en compliant in te zetten. Dit vergroot de risico's voor individuen en organisaties, zeker wanneer AI-systemen zelfstandig beslissingen nemen of persoonsgegevens verwerken.

De kernboodschap van het onderzoek: organisaties kunnen niet blind vertrouwen op AI-modellen. Menselijke controle, duidelijke governance en toetsing aan wet- en regelgeving blijven essentieel bij de inzet van AI.

Bron: Security.nl