

Security & Privacy Awarenessmeting 2026: AI-gebruik blijkt grootste kwetsbaarheid

7.9.2026 - | SURF

De kennis over cyberveilig en privacybewust werken is relatief sterk bij medewerkers in het onderwijs en onderzoek, maar leidt nog niet tot consistent veilig gedrag. Ook groeit het gebruik van AI-toepassingen sneller dan het beleid kan bijhouden. Dat blijkt uit de sectorrapportage security- en privacy-awareness 2026 van SURF en BDO.

In opdracht van SURF voerde BDO voor de 5e keer de security- en privacy-awarenessmeting uit, dit jaar bij 30 onderwijs- en onderzoeksinstituten in het mbo, hbo en wo. Nieuw in deze rapportage is een onderzoek van de Haagse Hogeschool naar de ervaringen van medewerkers met cyberincidenten en de impact daarvan op hun werk.

AI-gebruik: het grootste spanningsveld

Een belangrijke bevinding van de meting is dat medewerkers steeds vaker AI-tools gebruiken in hun dagelijkse werk, terwijl beleid en richtlijnen daar onvoldoende houvast voor bieden. Het gebrek aan goedgekeurde, veilige AI-alternatieven zorgt ervoor dat medewerkers teruggrijpen op openbare AI-tools, wat de kwetsbaarheid van de organisatie vergroot.

Cyberincident raakt 4 op de 10 medewerkers

Uit het aanvullende onderzoek van de Haagse Hogeschool blijkt dat 40,1 procent van de medewerkers de afgelopen 2 jaar een cyberincident bij hun instelling heeft meegemaakt. In de meeste gevallen ging het om een datalek. Medewerkers ervaren hiervan vooral hinder in hun dagelijkse werkzaamheden; het kost hen veel tijd om het incident op te lossen of betrokkenen te informeren. Ook blijkt dat de benodigde richtlijnen en meldroutes soms moeilijk te vinden zijn, of zelfs ontbreken. Van de medewerkers die een incident meemaakten, zegt 17 procent sindsdien voorzichtiger te zijn op internet.

Aanbevelingen voor instellingen

Met de volgende adviezen uit de rapportage kun je binnen je instelling direct aan de slag om het bewustzijn over cybersecurity te vergroten:

- **Maak informatieveilig werken concreet per werksituatie**
Zorg voor awareness- en communicatiestrategieën die aansluiten bij concrete werksituaties en helder beschrijven wat medewerkers precies moeten doen.
- **Verlaag de drempel voor veilig gedrag**
Laat maatregelen zoveel mogelijk aansluiten op hoe mensen al werken, bijvoorbeeld bij het veilig delen van gegevens of bij autorisatiebeheer.
- **Stel een AI-richtlijn op en bied veilige alternatieven**
Maak waar mogelijk sectorbrede afspraken over AI-gebruik en bied medewerkers toegankelijke, veilige tools als alternatief voor schaduw-IT.

Daarnaast blijven een aantal fundamentele aandachtspunten relevant die ook uit eerdere metingen

naar voren kwamen: blijf investeren in cultuur en voorbeeldgedrag van leidinggevenden, maak cyberveilig werken onderdeel van het onboardingsprogramma, herhaal trainingen met oog voor rolspecifieke risico's, en zorg voor een centrale, goed vindbare plek voor richtlijnen en meldroutes.

Volledige rapportage lezen?

Lees meer over de bevindingen en adviezen in de Sectorrapportage security- en privacy-awareness 2026.

Het originele artikel staat op de website van het Security Expertise Centrum.

<https://www.surf.nl/nieuws/security-privacy-awarenessmeting-2026-ai-gebruik-blijkt-grootste-kwetsbaarheid>