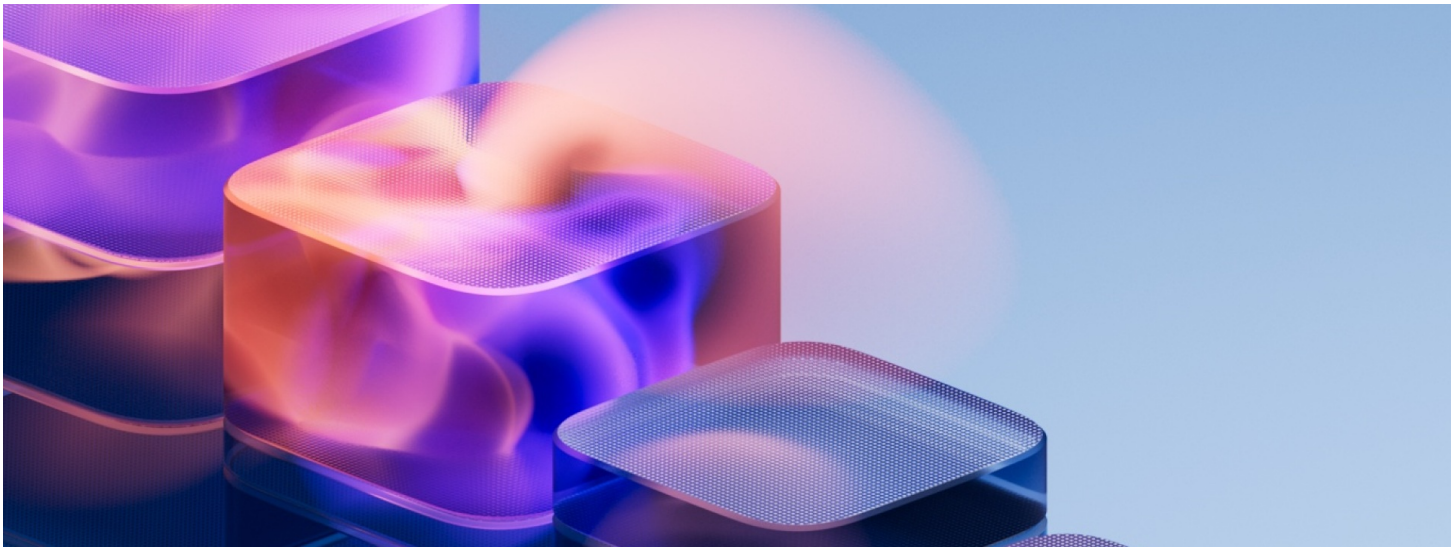
IBM NCEE News Room

Kosten van een datalek in de Benelux stijgen naar gemiddeld 6,35 miljoen euro

Eén op de vier kwaadwillige datalekken nu mogelijk gemaakt door AI



Amsterdam, 30 juli 2026 — De gemiddelde kosten van een datalek in de Benelux zijn gestegen naar 6,35 miljoen euro, blijkt uit het IBM Cost of a Data Breach Report 2026. De gemiddelde totale kosten van een datalek in de Benelux zijn hiermee gestegen ten opzichte van de 6 miljoen euro in 2025 en 5,45 miljoen euro in 2024. Ter vergelijking, dit ligt fors hoger dan het wereldwijde gemiddelde voor datalekken van 4,99 miljoen dollar.

Eén op de vier kwaadwillige datalekken in de Benelux (26%) werden mogelijk gemaakt door AI. Deze aanvallen, die voornamelijk bestaan uit deepfake-imitatie en door AI ondersteunde malware, veranderen de economische impact van datalekken. Cyberaanvallen worden sneller en goedkoper om uit te voeren, terwijl het steeds duurder wordt om datalekken op te sporen en te herstellen. Organisaties in de Benelux die AI en automatisering uitgebreid inzetten binnen hun securityoperaties verlagen de kosten van datalekken gemiddeld met 1,64 miljoen euro (kosten van 5,45 miljoen euro bij uitgebreid gebruik versus 7,09 miljoen euro bij organisaties die geen AI/automatisering inzetten). Toch heeft ruim één op de vier Benelux-organisaties (26%) deze technologieën nog altijd niet geïntegreerd in hun beveiligingsactiviteiten.

Geavanceerde AI-dreigingen zetten organisaties aan tot eerder handelen Organisaties beginnen actie te ondernemen op basis van toekomstige risico's, in plaats van pas te reageren na een incident. Uit aanvullend wereldwijd vervolgonderzoek van het Ponemon Institute blijkt dat wereldwijd 85% van de organisaties van plan is de securityuitgaven te verhogen nadat zij inzicht hebben gekregen in de geavanceerde cybermogelijkheden van frontier AI. Ter vergelijking gaf in het reguliere Benelux-onderzoek 68% van de organisaties aan de securityuitgaven te willen verhogen nadat zij daadwerkelijk met een datalek te maken hadden gehad.

Tegelijkertijd blijft er een kloof bestaan op het gebied waar cybercriminelen zich het snelst ontwikkelen. Hoewel meer dan de helft van de Benelux-organisaties (52%) AI-agents inzet in hun Security Operations Center (SOC), gebruikt wereldwijd slechts 18% deze agents voor vulnerability management. Hierdoor blijven bekende kwetsbaarheden bestaan, terwijl AI de tijd die cybercriminelen nodig hebben om misbruik te maken van zwakke plekken verkort. Bijna drie kwart van de organisaties wereldwijd geeft aan dat dreigingen vanuit frontier AI hen ertoe aanzetten opnieuw te kijken naar de manier waarop agents binnen hun securityactiviteiten worden ingezet.

“De bevindingen uit het rapport laten zien dat cybersecurity niet langer alleen een technologievraagstuk is, maar een essentieel onderdeel van bedrijfsweerbaarheid. Nu de gemiddelde kosten van een datalek in de Benelux zijn opgelopen tot €6,35 miljoen, moeten organisaties de overstap maken van reactieve beveiliging naar proactief risicomanagement," aldus Marcell Schmidt, Country General Manager and Technology leader bij IBM. *“De prioriteit ligt nu bij het verkorten van de tijd tussen het ontdekken en oplossen van een inbreuk. Organisaties moeten daarom herstelmaatregelen integreren in ontwikkelingsprocessen, identiteiten tijdens runtime beter beveiligen en risico’s sneller aanpakken, in hetzelfde tempo waarin aanvallers nieuwe technieken ontwikkelen.”*

Kritieke infrastructuur loopt groter risico door AI-gedreven aanvallen De meeste AI-gedreven aanvallen wereldwijd waren gericht op sectoren met kritieke infrastructuur (62%). Vooral organisaties in de financiële dienstverlening en de energiesector kregen wereldwijd relatief vaak met deze aanvallen te maken, waardoor het risico op bredere verstoring van essentiële systemen toeneemt. Datalekken in de Benelux financiële sector kosten inmiddels gemiddeld 7,90 miljoen euro, terwijl dat voor de Benelux-communicatiesector (7,03 miljoen euro) en de Benelux-industriële sector (7,02 miljoen euro) eveneens fors boven het gemiddelde ligt. De concentratie van aanvallen op deze sectoren vergroot de kans op keteneffecten die gevolgen kunnen hebben voor economieën, toeleveringsketens en essentiële dienstverlening.

Andere bevindingen:

- **De zwakste schakel van AI.**
  Meer dan 20% van de organisaties wereldwijd kreeg te maken met een datalek waarbij AI-modellen of AI-toepassingen het doelwit waren. De meest voorkomende oorzaken wereldwijd lagen in kwetsbaarheden rondom deze systemen, zoals gecompromitteerde API’s, applicaties of plug-ins (27%) en foutief geconfigureerde cloudomgevingen die invloed hadden op AI-workloads (27%).
- **Tekortkomingen in encryptie blijven bestaan terwijl quantumrisico’s toenemen.**
  Fundamentele zwakheden in encryptie en cryptografisch beheer blijven organisaties blootstellen aan risico’s, ondanks toenemende investeringen in quantumveilige beveiliging. Slechts 36% van de Benelux-organisaties die met een datalek te maken kregen, geeft aan gevoelige data zowel tijdens opslag als tijdens transport te versleutelen. Echter, 61% van de Benelux-organisaties heeft formele controles ingevoerd om veilige cryptografie en cryptografische objecten te bewaken.
- **Cybercriminelen zetten reputatie steeds vaker in als drukmiddel.**
  Het aantal ransomware-incidenten wereldwijd is gestegen ten opzichte van vorig jaar (39% tegenover 34%), waarbij cybercriminelen AI steeds vaker gebruiken om aanvallen te automatiseren en op te schalen. Hoewel operationele verstoring nog steeds een rol speelt, richten cybercriminelen zich wereldwijd steeds vaker op impactvolle drukmiddelen. Het meest gebruikte middel wereldwijd is het beschadigen van de merkreputatie (41%), gevolgd door het buitmaken van werknemersgegevens (35%) en intellectueel eigendom (31%).

Het Cost of a Data Breach Report van 2026 bevat voor de Benelux een specifieke steekproef van 34 organisaties. Het overkoepelende, wereldwijde onderzoek is uitgevoerd door het Ponemon Institute en gebaseerd op datalekken die bij 602 organisaties wereldwijd plaatsvonden tussen maart 2025 en februari 2026. Als aanvulling op dit onderzoek voerde het Ponemon Institute in mei 2026 een vervolgonderzoek uit onder deze organisaties. In totaal reageerden 456 organisaties uit het oorspronkelijke onderzoek. Daarvan was 78%, oftewel 356 organisaties, bekend met recente ontwikkelingen rondom zeer geavanceerde frontier AI-modellen, zoals Mythos.

Download hier het volledige onderzoek.

Media Contact
Jasmina Premrl

jasmina.premrl@si.ibm.com

---

https://ncee.newsroom.ibm.com/CODB