Microsoft Security

Databeveiligingsindex

Trends, inzichten en strategieën om je data veilig te houden en generatieve AI veilig te gebruiken

Rapport voor 2024

Voorwoord

Voor ons tweede jaar aan onderzoek naar het veranderende databeveiligingslandschap kunnen we vaststellen dat de uitdagingen en mogelijkheden nog nooit zo groot zijn geweest. In het afgelopen jaar is de ernst van databeveiligingsincidenten toegenomen. Dit is het tijdperk van data en de strategieën en tools om die data veilig te houden ontwikkelen zich razendsnel.

Dit jaar verkennen we een nieuwe frontlinie: de rol en impact van generatieve AI op databeveiligingsstrategieën.

AI is wereldwijd het gesprek van de dag met zijn ongeëvenaarde mogelijkheden voor meer innovatie en doelmatiger werken. Organisaties zien echter niet alleen dit enorme potentieel, maar ook de bijbehorende databeveiligingsrisico's en hoe deze de verantwoordelijkheden van hun databeveiligingsteams vormgeven. Volgens onze waarnemingen vormt AI voor organisaties een katalysator om hun basispraktijken voor databeveiliging te versterken. Zo kunnen ze zich voorbereiden om de impact van het delen van te veel data en datalekken tot een minimum te beperken, en kunnen ze processen ontwerpen voor veilige AI-implementatie. Anderzijds kunnen organisaties AI ook inzetten om hun databeveiligingspraktijken te verbeteren. Met AI kunnen ze verborgen risico's en lacunes in hun beveiliging vaststellen, AI kan beveiligingsbeleid aanbevelen en kan worden gebruikt voor het sneller onderzoeken en oplossen van beveiligingsincidenten.

Ons onderzoek heeft tot doel om leiders in databeveiliging bruikbare inzichten en advies te bieden, zodat hun teams hun databeveiligingsstrategie vol vertrouwen kunnen aanpassen en het gebruik van AI kunnen beveiligen, maar AI ook kunnen integreren in hun databeveiligingsstrategie. AI mag dan een opmerkelijk bereik en potentieel hebben, maar is slechts de nieuwste transformatiegolf die ondernemingen te verwerken krijgen, zoals voorheen hybride werken, de cloud en mobiliteit. Deze trends hebben in de afgelopen jaren de tijdloze behoefte onderstreept aan inzicht in het gebruik van nieuwe technologieën, het verkleinen van hun risico en maximaliseren van hun impact. Op basis van deze kennis kunnen organisaties de data die voor AI wordt gebruikt beveiligen en AI tevens gebruiken om hun databeveiligingsmaatregelen te versterken. Dat zal leiden tot hogere productiviteit en grotere veerkracht en flexibiliteit bij het aanpakken van de uitdagingen van de toekomst.

We nodigen je uit om kennis te maken met onze nieuwste bevindingen en hopen dat je met behulp van onze inzichten je databeveiligingsstatus kunt versterken en de inspiratie opdoet om AI te omarmen en een complete databeveiligingsstrategie te ontwikkelen, zodat je grotere innovatie kunt ontgrendelen en kunt bijdragen aan een veiligere toekomst voor ons allemaal.

Rudra Mitra
Corporate Vice President
Microsoft Data Security and Compliance

Inleiding

Organisaties krijgen tegenwoordig te maken met gemiddeld 156 databeveiligingsincidenten per jaar en de impact ervan vormt een voortdurende zorg voor beslissers op databeveiligingsgebied. En dat heeft een goede reden: een enkel incident kan leiden tot enorme financiële en reputatieschade, vooral als je rekening houdt met de zich voortdurend ontwikkelende dreigingscontext en aanvallers die alle mogelijke zwakheden uitbuiten. Dit wordt nog eens versterkt door de snelle implementatie van AI, want zonder de juiste beveiligingsmaatregelen kunnen gebruikers per ongeluk of heel bewust gevoelige, kritieke bedrijfsdata (zoals informatie over medewerkers en klanten, intellectueel eigendom, financiële prognoses en operationele data) aan risico's blootstellen. Steeds meer organisaties zijn op zoek naar nieuwe manieren om deze grote hoeveelheden gevoelige data te beschermen en daarom richten veel beslissers hun aandacht op de dramatische opkomst van AI.

De uitdaging op AI-gebied is tweeledig. Twee derde van de organisaties geeft toe dat hun medewerkers niet-goedgekeurde AI-tools gebruiken en dus is het cruciaal dat ze kunnen garanderen dat werknemers AI-tools veilig gebruiken. Tegelijkertijd doet zich een mogelijkheid voor om AI te gebruiken als een effectief wapen in een geavanceerde databeveiligingsstrategie.

Op AI gebaseerde databeveiligingsoplossingen spelen nu al een kritieke rol bij het in realtime identificeren en reageren op bedreigingen, verbeteren de algehele snelheid en nauwkeurigheid van databeveiligingsprogramma's en bieden inzichten waarmee databeveiligingsincidenten in de kiem kunnen worden gesmoord voordat ze plaatsvinden. Organisaties moeten de met AI samenhangende risico's beheren, maar ook gebruikmaken van de kracht ervan om patronen te identificeren die mensen nauwelijks op machinesnelheid zouden kunnen verwerken en analyseren, zodat ze uiteindelijk de steeds geavanceerdere cyberaanvallen kunnen bestrijden.

In 2023 gaf Microsoft een onafhankelijk onderzoeksbureau, Hypothese, de opdracht om een multinationale enquête uit te voeren onder meer dan 800 databeveiligingsprofessionals. Het doel was om een databeveiligingsindex te starten waarvan onze partners en klanten konden profiteren en die bedrijfsmanagers konden gebruiken om hun eigen databeveiligingsstrategie te ontwikkelen.

We bouwen het rapport voor 2024 op de bevindingen van dit eerdere onderzoek met nieuwe inzichten dankzij een nog grotere multinationale enquête onder meer dan 1300 databeveiligingsprofessionals. Uit onze data worden eerdere inzichten en trends bevestigd in de markten die we hebben onderzocht, maar we hebben ook nieuwe kennis opgedaan over de meest recente databeveiligings- en AI-praktijken en -trends wereldwijd.

hypothesis Microsoft Security

Belangrijkste bevindingen

1

De databeveiligingscontext is en blijft gefragmenteerd, waardoor er een sterkere behoefte bestaat aan een samenhangende databeveiligingsstrategie die zowel de traditionele als nieuwe risico's van het gebruik van AI kan aanpakken

Organisaties melden grote tevredenheid over en vertrouwen in hun databeveiligingsmaatregelen. Databeveiligingsincidenten hebben echter steeds ernstigere gevolgen, met name vanwege de gaten die organisaties vaststellen tussen hun huidige databeveiligingsbeleid en het toegenomen gebruik/de introductie van een toenemend aantal AI-applicaties. Veel organisaties vertrouwen echter nog op meerdere databeveiligingstools, die hun algehele kwetsbaarheid en de risico's waarmee ze te maken krijgen kunnen vergroten, om de noodzakelijke beveiliging te waarborgen.

2

Naarmate eindgebruikers steeds meer AI-apps gaan gebruiken, loopt de integriteit van de gevoeligste data van organisaties een groter risico, waardoor groter inzicht en een nieuwe beveiliging zijn vereist

AI-tools worden een onmisbaar onderdeel van het dagelijkse werk en dus maken organisaties zich grotere zorgen over het databeveiligingsrisico. Ze onderkennen dat ze hun beveiliging moeten versterken en streven ernaar om databeveiligingsincidenten als gevolg van AI te voorkomen, maar het onbevoegde gebruik van deze tools benadrukt nog eens de noodzaak van robuustere zichtbaarheid.

3

Beslissers zijn optimistisch over het potentieel van AI om het streven naar databeveiliging te versterken

Organisaties investeren actief in databeveiligingstools met AI om detectie- en responsmogelijkheden te verbeteren. Met behulp van AI kunnen ze onbeschermde data detecteren, aanbevelingen ontvangen voor beschermingsbeleid en databeveiligingsincidenten sneller onderzoeken en verhelpen. Dankzij al deze mogelijkheden kunnen databeveiligingsteams meer tijd en aandacht besteden aan strategische werkzaamheden. Met het gebruik van AI worden ook het vertrouwen in en de tevredenheid over de algehele databeveiligingsstrategie van organisaties verbeterd, met name dankzij het vermogen om zowel snel als nauwkeurig te reageren op incidenten.

1

De databeveiligingscontext is en blijft gefragmenteerd, waardoor er een sterkere behoefte bestaat aan een samenhangende databeveiligingsstrategie die zowel de traditionele als nieuwe risico's van het gebruik van AI kan aanpakken

Er bestaat een kloof tussen het vertrouwen van beslissers in hun databeveiligingspraktijken en het werkelijke beschermingsniveau van hun data

Zoals we in ons rapport van 2023 vermeldden, heeft de meerderheid van beslissers vertrouwen in hun databeveiligingsstrategie, terwijl 74% in 2024 zegt tevreden te zijn met de huidige oplossingen. Ze hebben vertrouwen in hun vermogen om gevoelige data bij te houden en te beheren: 88% zegt te weten waar de meeste van hun kritieke informatie zich bevindt en 85% zegt dat hun data correct is geclassificeerd en gelabeld. De meeste beslissers spreken ook vertrouwen uit in hun verdedigingsmechanismen, waarbij 79% zegt erop te vertrouwen dat ze ontvreemding van hun data kunnen voorkomen en 76% de aanpak als proactief in plaats van reactief omschrijft.

Hun vertrouwen wordt echter op de proef gesteld naarmate de ernst van incidenten blijft toenemen. **Het gemiddelde aantal jaarlijkse databeveiligingsincidenten is hoog gebleven: met 166 in 2023 en 156 in 2024. De ernst van deze incidenten is toegenomen: waar 20% van de incidenten in 2023 als ernstig werd omschreven, is dat 27% in 2024.**

156

databeveiligingsincidenten

27%

van de incidenten wordt als ernstig beschouwd (tegen 20% in 2023)

63%

van de waarschuwingen wordt dagelijks beoordeeld

"De locatie voor het opzetten van een softwareplatform, de vraag waar de data moet worden opgeslagen en wie er toegang tot die data krijgt, bemoeilijkt de databeveiliging en het beheer van onze AI-tools en -leveranciers. We hebben meer dan 100 jaar aan data die we moeten beschermen en beheren in overeenstemming met de wettelijke vereisten in elk rechtsgebied waarin we actief zijn", aldus een Senior Manager voor Information Governance bij een fabrikant van zware apparatuur.

Het feit dat de ernst van databeveiligingsincidenten toeneemt, heeft ook geleid tot een veel groter aantal waarschuwingen. **Organisaties krijgen nu dagelijks te maken met gemiddeld 66 waarschuwingen, vergeleken met 52 in 2023.** Dat aantal hangt sterk af van de grootte van een organisatie, waarbij middelgrote ondernemingen (500-999 werknemers) en grote ondernemingen (1000-4999 werknemers) gemiddeld 56 waarschuwingen ontvangen en zeer grote ondernemingen (meer dan 5000 werknemers) gemiddeld 80 waarschuwingen per dag ontvangen.

Gezien de enorme hoeveelheid databeveiligingswaarschuwingen mag het geen verrassing heten dat de meeste organisaties ze gewoon niet kunnen bijbenen. Gemiddeld evalueren databeveiligingsteams 63% van hun dagelijkse waarschuwingen. Van deze waarschuwingen blijkt 35% een fout-positieve waarschuwing te zijn. Deze discrepantie tussen het gevoel van controle dat heerst en de realiteit van de dagelijkse ervaring is overweldigend voor beveiligingsteams. Ze proberen te beoordelen of ze wel de juiste bescherming hebben geïmplementeerd of hoe ze hun maatregelen fijn kunnen afstemmen, maar maken zich ook zorgen dat een mogelijk zeer ernstig incident onopgemerkt zou kunnen blijven.

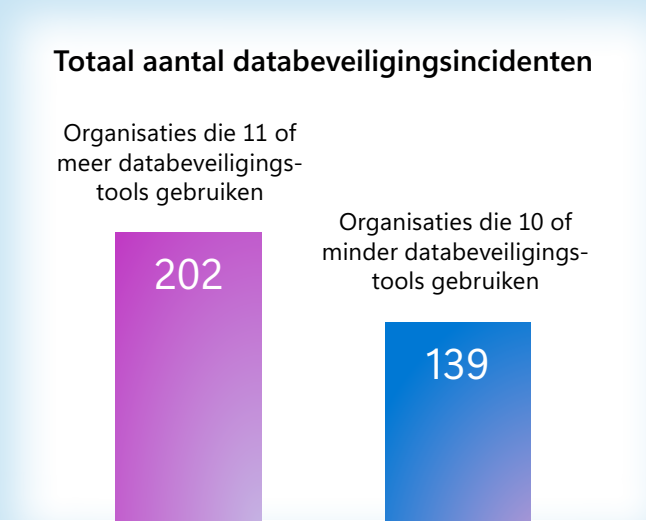
Om traditionele en opkomende datarisico's in verband met het gebruik van AI-tools te bestrijden, is er een groeiende behoefte aan robuustere en beter samenhangende databeveiligingsstrategieën

Ondanks het groeiende aantal tools waarover beslissers kunnen beschikken, erkent een groot deel van hen dat meer niet altijd beter is. Sterker nog, 21% noemt het gebrek aan geconsolideerde en uitgebreide zichtbaarheid (en gedeeld inzicht in risico's) als gevolg van uiteenlopende tools als hun grootste uitdaging/risico.[1]

De meeste beslissers (82%) zijn van mening dat een compleet en volledig geïntegreerd platform beter is dan meerdere geïsoleerde tools te moeten beheren. **Ze moeten gemiddeld 12 verschillende databeveiligingsoplossingen zien te coördineren, en die complexiteit vergroot hun kwetsbaarheid.** Dit geldt met name voor de grootste organisaties: middelgrote ondernemingen gebruiken gemiddeld 9 tools, grote ondernemingen 11 en zeer grote ondernemingen 14.

Uit de data blijkt een sterke correlatie tussen het aantal gebruikte databeveiligingstools en de frequentie van databeveiligingsincidenten. Middelgrote en grote ondernemingen melden gemiddeld 89 incidenten per jaar, terwijl zeer grote ondernemingen jaarlijks te maken krijgen met maar liefst 248 incidenten. Dit grote verschil benadrukt nog eens de grote risico's waarmee grote organisaties te maken hebben, ook al zeggen ze dan veel vertrouwen in hun databeveiligingsmaatregelen te hebben.

In 2024 kregen organisaties die meer databeveiligingstools (11 of meer) gebruikten gemiddeld met 202 databeveiligingsincidenten te maken, vergeleken met 139 voor bedrijven die 10 of minder tools gebruikten.



Vanwege gefragmenteerde oplossingen is het lastig om inzicht te krijgen in de databeveiligingsstatus omdat data is geïsoleerd en onsamenhangende workflows een uitgebreid inzicht in potentiële risico's kunnen beperken. Wanneer databeveiligingsteams met niet-geïntegreerde tools moeten werken, moeten ze processen ontwikkelen om data te correleren en samenhangend inzicht in risico's te krijgen, wat kan leiden tot blinde vlekken en het moeilijk kan maken om risico's te detecteren en bestrijden.

Een groeiend punt van zorg is de toename van het aantal beveiligingsincidenten als gevolg van het gebruik van AI-applicaties; dit werd bijna twee keer groter, met 40% in vergelijking met 27% in 2023. De toename van het aantal incidenten wordt gevoed door een sterke stijging in het aantal malware- en ransomwareaanvallen, met 59% vergeleken met 50% in 2023. Aanvallen als gevolg van het gebruik van AI stellen niet alleen gevoelige data bloot aan risico's, maar brengen ook het functioneren van AI-systemen zelf in gevaar, waardoor de toch al zo gefragmenteerde databeveiliging alleen nog maar complexer wordt. Kortom, er is een steeds dringendere behoefte aan sterkere, meer samenhangende databeveiligingsstrategieën die zowel traditionele als opkomende risico's als gevolg van het gebruik van AI-tools aankunnen.

1. Enquête gehouden in september 2024 onder beslissers op het gebied van databeveiliging, -beheer, -compliance en -privacy uitgevoerd in opdracht van Microsoft door het bureau MDC Research

De weg voorwaarts

De toename van de ernst van databeveiligingsincidenten brengt ook de mogelijkheden van AI om daarbij te helpen voor het voetlicht. De meest toonaangevende organisaties implementeren databeveiliging op basis van AI om prioritering van incidenten af te handelen, dataclassificatie te automatiseren en manieren aan te duiden om het bestaande beveiligingsbeleid fijn af te stemmen. AI kan automatisch de potentiële ernst van incidentwaarschuwingen afleiden, waardoor databeveiligingsteams bruikbare inzichten krijgen om snel te reageren en de tijd die wordt besteed aan fout-positieven te verminderen. Dit stroomlijnt workflows en biedt databeveiligingsteams de mogelijkheid om te focussen op meer strategische verbeteringen in de databeveiliging en op proactieve maatregelen.

2

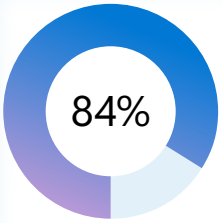
Naarmate eindgebruikers steeds meer AI-apps gaan gebruiken, loopt de integriteit van de gevoeligste data van organisaties een groter risico, waardoor groter inzicht en een nieuwe beveiliging zijn vereist

AI wordt snel onmisbaar voor dagelijkse werkzaamheden, en organisaties moeten deze nieuwe realiteit omarmen en zich hieraan aanpassen

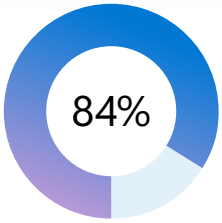
De snelle invoering van AI-tools door medewerkers heeft geleid tot grote veranderingen in de manier waarop organisaties databeveiliging aanpakken. AI transformeert productiviteit en workflows, maar kan net als elke andere opkomende technologie ook bestaande risico's versterken en nieuwe risico's introduceren waarvoor een heel andere beveiligingsaanpak voor gevoelige data is vereist. Bedrijven proberen dan ook nog steeds hun houding te bepalen in deze snel veranderende omgeving. Een Director of Engineering and Analytics bij een transportbedrijf zeg het volgende: "we bewaken data die door AI wordt gebruikt zorgvuldiger. Er is een bepaalde spanning geweest tussen productiviteit en veiligheid, nauwkeurigheid en privacy."

Het vertrouwen in de beveiliging van AI-gebruik door medewerkers is niet overal even groot. Een meerderheid (84%) zou graag meer vertrouwen hebben in het beheren en detecteren van data-invoer. Waar 22% van de organisaties het volste vertrouwen heeft in hun vermogen om data veilig te houden, verklaart slechts 59% "veel vertrouwen" te hebben, wat er duidelijk op wijst dat het een stuk beter kan. De meeste bedrijven (86%) erkennen dat ze meer vertrouwen zouden willen in het beheren en detecteren van de data die door AI-tools wordt gegenereerd.

Naarmate AI belangrijker wordt voor de dagelijkse productiviteit, heeft het gebruik van AI-apps ook geleid tot grotere zorgen over incidenten met databeveiliging. **Bijna een derde (31%) van de organisaties verwacht een toename in databeveiligingsincidenten als gevolg van het gebruik van AI door medewerkers, en 84% geeft toe meer te moeten doen om zich tegen deze risico's te beschermen.** Dit soort zorgen leeft met name sterk bij de grootste organisaties: slechts 26% van de middelgrote ondernemingen verwacht een toename van databeveiligingsincidenten als gevolg van het gebruik van AI en 29% van de grote ondernemingen verwacht hierin een stijging; als we echter naar de zeer grote ondernemingen kijken, hebben we met 36% met een veel grotere groep te maken die een stijging verwacht.



wil graag meer vertrouwen hebben in het beheren en detecteren van data-invoer in AI-apps en -tools



is van mening dat ze meer moeten doen om bescherming te bieden tegen risicovol gebruik van AI-apps en -tools door medewerkers

Ongeautoriseerd gebruik van AI is wijdverbreid

Veertig procent meldt dat hun AI-apps al zijn gehackt bij een databeveiligingsincident. Dit cijfer ligt opnieuw hoger bij grotere organisaties: het percentage voor middelgrote ondernemingen ligt op 36%, voor grote ondernemingen op 38% en zeer grote ondernemingen hebben met 44% met de meeste incidenten te maken.

Ongeautoriseerd gebruik van AI komt vaak voor wanneer medewerkers zich aanmelden met persoonlijke referenties of persoonlijke apparaten gebruiken voor werktaken. **Gemiddeld verklaart 65% van de organisaties dat hun medewerkers niet-geautoriseerde AI-tools gebruiken.** Manieren waarop medewerkers ongeautoriseerde AI-tools gebruiken zijn onder andere:

- 53% van de medewerkers meldt zich aan met persoonlijke referenties voor werkdoeleinden
- 48% van de medewerkers gebruikt een persoonlijk apparaat wanneer ze AI voor hun werk gebruiken
- 47% van de medewerkers gebruikt werkreferenties om AI voor persoonlijke doeleinden te gebruiken

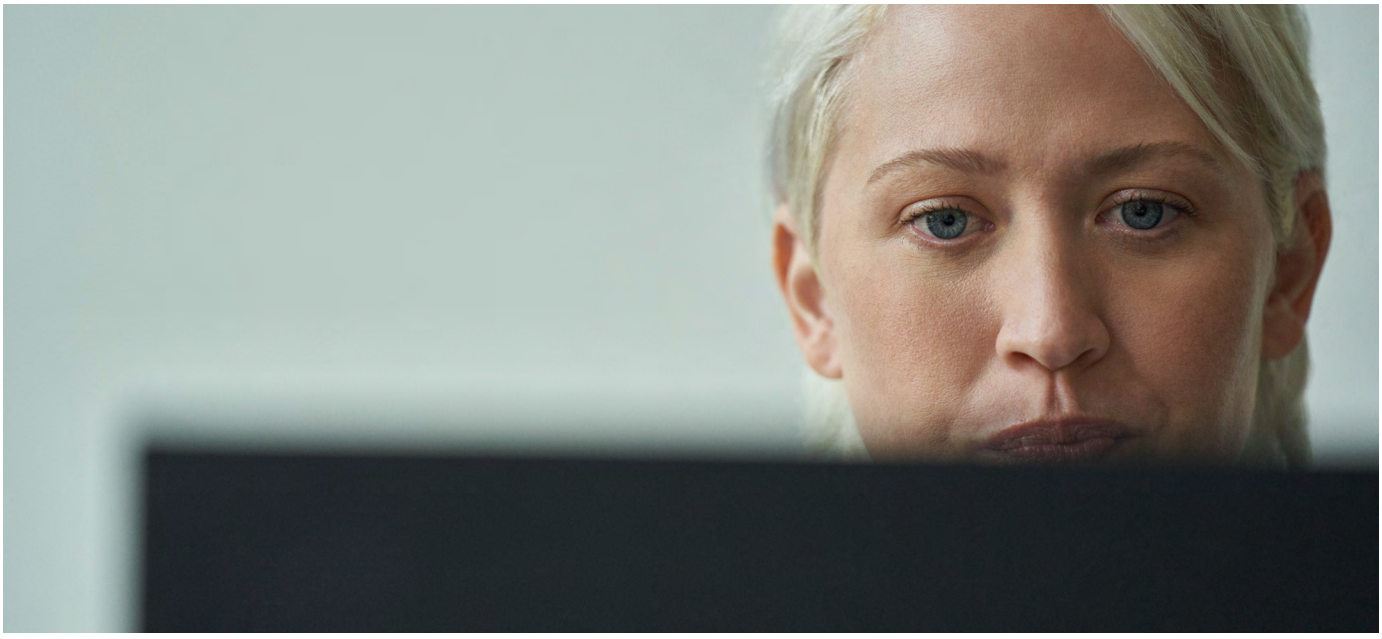
De helft van alle organisaties zegt zich zorgen te maken over een gebrek aan controles om risico's te detecteren en te beperken wanneer medewerkers AI-apps op onveilige manieren gebruiken. Deze cijfers variëren afhankelijk van de bedrijfsgrootte, waarbij 43% van de middelgrote ondernemingen, 50% van de grote ondernemingen en 54% van de zeer grote ondernemingen hun bezorgdheid uiten over hun vermogen om deze risico's te beheersen.

Gezien het toenemende gebruik van AI zijn meer databeveiligingsmaatregelen nodig

Naarmate AI meer ingebed raakt in de dagelijkse activiteiten, erkennen organisaties de behoefte aan sterkere bescherming. **Terwijl 96% van de bedrijven zich zorgen maakt over het gebruik van deze tools door medewerkers, zijn bijna evenveel bedrijven bereid om te investeren in oplossingen om deze zorgen het hoofd te bieden.**

"De focus moet liggen op hoe je AI kunt beheersen. Bij de beveiliging gaat het om het beperken van de grootte van data en hoe je deze zorgvuldiger kunt bewaken. Maar voor AI heb je juist meer data nodig om modellen representatiever te maken en vooroordelen aan te duiden. Hoe breng je die factoren in overeenstemming?", vraagt een Director of Engineering, Architecture and Analytics bij een transportbedrijf zich af. De overgrote meerderheid van de beslissers (87%) is bereid om zowel tijd als geld te besteden aan het trainen van medewerkers in veilige praktijken voor AI-tools. **De reden hiervoor is dat 85% van mening is dat het gebruik van deze tools door hun medewerkers van cruciaal belang is om concurrerend te blijven.**

Bijna alle organisaties (93%) bevinden zich in een ontwikkelings- of implementatiefase voor controles op AI-gebruik, maar in veel gevallen gaat het hier om een zeer vroeg stadium. Slechts 39% heeft databeveiligingsmaatregelen voor AI volledig geïmplementeerd, terwijl 24% beleid heeft ontwikkeld, maar dit nog niet uitvoert. Een VP voor Data Security in de horeca zegt: "we moeten het nog eens worden over controles voor AI, maar omarmen het gebruik van AI in de tussentijd. Het maakt het leven gemakkelijker en helpt ons efficiënter te werken."



Hoewel organisaties stappen ondernemen om gevoelige data te beschermen tegen misbruik in AI-apps, bestaat er een duidelijke behoefte aan uitgebreidere controles. Momenteel richt 43% van de bedrijven zich op het voorkomen van het uploaden van gevoelige data naar AI-apps, terwijl nog eens 42% alle activiteiten en content in deze apps registreert voor potentieel onderzoek of mogelijke incidentrespons. Ook blokkeert 42% de toegang van gebruikers tot ongeautoriseerde tools en een gelijk percentage investeert in training van medewerkers in veilig gebruik van AI.

Bedrijven met medewerkers die AI onbevoegd gebruiken, hebben een grotere behoefte aan bepaalde soorten controles. **Van de bedrijven waarin AI op onbevoegde wijze wordt gebruikt, heeft 42% controles nodig om risicovolle gebruikers te identificeren op basis van AI-query's; voor bedrijven waarin AI niet op onbevoegde wijze wordt gebruikt, ligt dat percentage bij 30%. Bovendien heeft 40% van de organisaties die te maken hebben met onbevoegd gebruik van AI controles nodig om de levenscyclus van data (zoals bewaar- en verwijderingsprotocollen) te beheren, vergeleken met 27% van de bedrijven waarin dit probleem niet optreedt.**

Vijf belangrijkste AI-controles die nodig zijn

Voorkomen dat gevoelige data wordt geüpload naar AI	43%
Alle activiteiten en content in AI-tools registreren voor potentieel onderzoek of incidentrespons	42%
Toegang van gebruikers tot niet-geautoriseerde AI-tools blokkeren	42%
Medewerkers trainen in het veilige gebruik van AI-tools	42%
Risicovolle gebruikers op basis van query's in AI identificeren	41%

De weg voorwaarts

Teams kunnen alleen een krachtige databeveiligingsstatus behouden met een complete set controles voor het detecteren, beschermen en beheren van hun data in AI-apps. Dit zijn drie belangrijke strategieën die teams kunnen gebruiken:

De zichtbaarheid van het gebruik van AI-apps en de data die door de app stroomt, vergroten: zet databeveiligingstools in die het gebruik van AI-apps kunnen detecteren. Deze tools bieden inzicht in een uitgebreide lijst van AI-apps die worden gebruikt, samen met hun risicoprofiel, waaronder details zoals ondersteunde databeveiligingscontroles en compliance van regelgeving. Gebruik tools met mogelijkheden voor consistente classificatie van gevoelige data in AI-interacties en die trends laten zien in de manier waarop data door AI-apps stroomt.

Beleid ontwikkelen en handhaven: creëer beleid op basis van de inzichten die zijn verkregen uit de analyse. Dit beleid kan richtlijnen omvatten voor goedgekeurde AI-apps, evenals procedures voor het blokkeren of beperken van het gebruik van niet-goedgekeurde apps door medewerkers. Zelfs voor goedgekeurde AI-apps kun je gedetailleerd beleid samenstellen om niet-gevoelige data door de app te laten stromen en tegelijkertijd het gebruik van gevoelige en bedrijfskritische data te beperken. Dit kan blokkeren van bepaalde acties omvatten, zoals gevoelige data in browsergebaseerde AI-tools plakken, om databeveiliging te waarborgen.

Regelmatig risico's beoordelen en beleid verfijnen: genereer regelmatig rapporten met het risiconiveau van de AI-apps die worden gebruikt, trends in de manier waarop gevoelige data door deze apps stroomt, evenals de gebruikersactiviteiten voor deze apps. Hiermee kun je het algehele risiconiveau beoordelen en onderbouwde beslissingen nemen over het relevantste databeveiligingsbeleid.

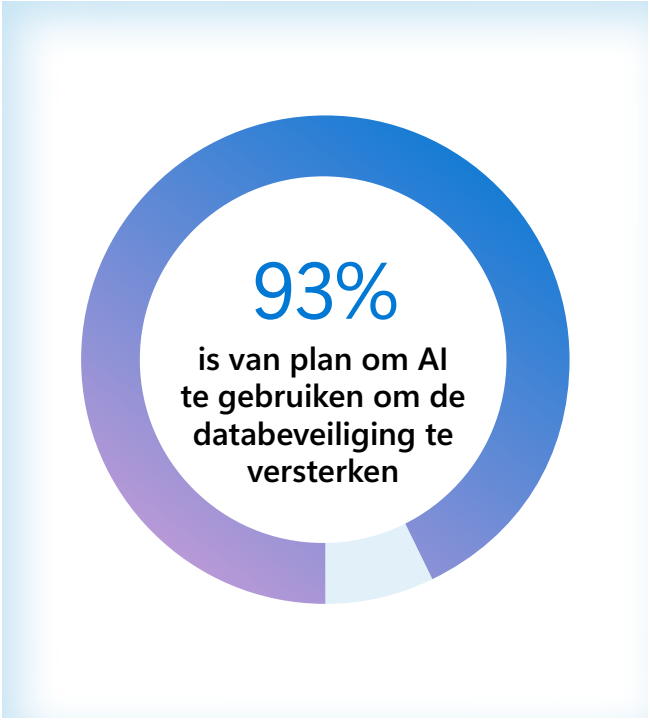
3

Beslissers zijn optimistisch over het potentieel van AI om het streven naar databeveiliging te versterken

Databeveiligingsonderzoek is sterk afhankelijk van AI

De overgrote meerderheid (88%) van de organisaties investeert al in AI om de detectie- en responsinzet te verbeteren: gevoelige data detecteren, afwijkende activiteiten vaststellen en data die een risico loopt automatisch beschermen. **Zevenenzeventig procent van de organisaties is ervan overtuigd dat AI deze processen zal versnellen, en 76% is van mening dat het de nauwkeurigheid van hun detectie- en responsstrategie zal verbeteren.**

Hoewel 73% van de beslissers zorgen uit over het gebruik van AI om de databeveiliging te versterken, zegt 50% dat dit hun gebruik van AI om de databeveiliging te versterken niet heeft belemmerd en verklaart slechts 23% hierdoor terughoudend te zijn. In totaal is een overweldigende 93% ten minste van plan om AI te gebruiken om de databeveiliging te versterken, ondanks genoemde zorgen.

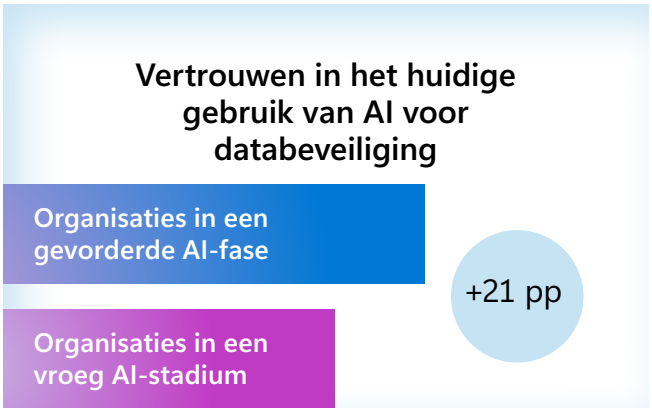


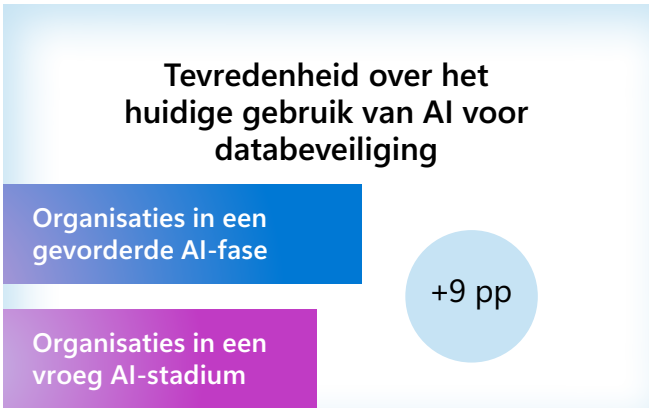
AI gebruiken om de databeveiliging te versterken, vergroot de zichtbaarheid, het vertrouwen en de tevredenheid

Een van de belangrijkste voordelen van het gebruik van AI om de databeveiliging te versterken, is dat het de zichtbaarheid van systemen vergroot, wat een belangrijke zorg wegneemt die beslissers hebben, omdat ze niet weten waar data wordt opgeslagen en hoe deze wordt geclassificeerd (20%).[1] Achtentachtig procent van de beslissers op databeveiligingsgebied is ervan overtuigd dat de integratie van AI in databeveiligingsoplossingen teams meer zichtbaarheid zal geven, waardoor organisaties veel meer data kunnen verwerken en analyseren dan anders mogelijk zou zijn. Middelgrote organisaties richten zich voornamelijk op het verminderen van risico op de korte termijn, zoals het minimaliseren van menselijke fouten in hun databeveiligingsprocessen. Sterker nog, 43% van de middelgrote ondernemingen verleent prioriteit aan het terugdringen van het risico als gevolg van menselijke fouten, vergeleken met slechts 37% van de zeer grote ondernemingen.

Grotere ondernemingen zijn daarentegen geavanceerder in hun aanpak, waarbij de nadruk wordt gelegd op risico's op de langere termijn en de noodzaak van aanpassingsvermogen. Dankzij deze geavanceerdere aanpak kunnen databeveiligingsteams zich beter aanpassen aan veranderende risico's, en dat is een topprioriteit voor 49% van de zeer grote ondernemingen, vergeleken met 43% van de middelgrote organisaties.

Over het algemeen verklaren organisaties die verder zijn in het gebruik van AI om databeveiliging te versterken veel meer vertrouwen in hun databeveiligingsstrategie te hebben en hierover veel tevredener te zijn. **Van de bedrijven die zich al in een vergevorderd stadium van AI-implementatie bevinden, heeft 90% zeer veel of veel vertrouwen in het gebruik van AI om de databeveiliging te versterken, vergeleken met 69% van de bedrijven die zich in een eerdere fase bevinden. Hetzelfde patroon zien we bij organisaties die geavanceerder zijn in het gebruik van AI: 76% van de organisaties is tevreden over hun oplossingen voor databeveiliging, terwijl slechts 67% van de organisaties in een eerdere fase deze mening is toegedaan.**





1. Enquête gehouden in september 2024 onder beslissers op het gebied van databeveiliging, -beheer, -compliance en –privacy uitgevoerd in opdracht van Microsoft door het bureau MDC Research

Organisaties slagen erin het aantal databeveiligingsincidenten te verminderen en het beheer van waarschuwingen met AI te verbeteren

Organisaties die AI gebruiken om hun databeveiligingsactiviteiten te versterken, melden aanzienlijk minder waarschuwingen. **Gemiddeld ontvangen organisaties die tools voor databeveiliging op basis van AI hebben geïmplementeerd 47 waarschuwingen per dag, vergeleken met 79 waarschuwingen voor de organisaties die dit niet hebben gedaan. En de organisaties die AI gebruiken kunnen 66% van hun dagelijkse waarschuwingen beoordelen, terwijl organisaties die geen AI gebruiken slechts aan 60% toekomen.**

Bovendien is de kans groter dat organisaties die AI gebruiken om de databeveiliging te versterken, AI ook inzetten om risico's te beperken (56% versus 26%). De afname van het aantal waarschuwingen, samen met de toename van de mogelijkheden om de bijbehorende risico's te beperken met behulp van AI, lijkt een dramatische impact te hebben gehad op het totale aantal databeveiligingsincidenten. Organisaties die AI hebben geïmplementeerd om de databeveiliging te versterken, zien een vermindering van 65% in databeveiligingsincidenten vergeleken met organisaties die AI hiervoor niet gebruiken.

AI zal naar verwachting de grootste impact hebben op de respons

Voor wat betreft detectie verwacht 33% van de beslissers dat AI zal bijdragen aan het detecteren van afwijkende activiteiten, terwijl 23% van mening is dat het zal helpen bij het onderzoeken van potentiële databeveiligingsincidenten. Nog eens 22% onderkent het potentieel van AI om aanbevelingen te doen voor een betere beveiliging van hun dataomgeving.

Op het gebied van de respons verwachten beslissers echter dat AI de diepste impact zal hebben. Vierendertig procent is ervan overtuigd dat AI het ongewenst delen van gevoelige data automatisch kan blokkeren, en 32% verklaart dat het data die een risico loopt, beschermt. Nog eens 26% verwacht dat AI zal helpen om de databeveiligingsrisico's te beperken en passende controles toe te passen, terwijl hetzelfde aantal verwacht dat AI risicovol gebruikersgedrag automatisch zal markeren.

De weg voorwaarts

Het integreren van AI in databeveiligingsoplossingen kan ook een positieve bijdrage leveren door teams realtime advies te bieden, informatie samen te vatten en support in natuurlijke taal te bieden om gebieden te benadrukken die anders mogelijk over het hoofd worden gezien. Dit kan ook het onderzoek versnellen en de expertise voor alle databeveiligingsteams versterken. Deze mogelijkheden kunnen op de volgende manier impact hebben:

Samenvatting van waarschuwingen: onderzoek kan ontmoedigend zijn vanwege de hoeveelheid bronnen die moeten worden geanalyseerd en de uiteenlopende beleidsregels die gelden. Door AI in te sluiten in preventie van dataverlies (DLP of Data Loss Prevention) en intern risicobeheer (IRM of Insider Risk Management), kunnen teams snel een samenvatting van waarschuwingen ontvangen, inclusief de bron, beleidsregels en inzichten in gebruikersrisico's om te begrijpen welke gevoelige data gevaar loopt en wat het bijbehorende gebruikersrisico is.

Contextuele berichten: organisaties moeten zich houden aan de wettelijke vereisten voor zakelijke communicatie, wat vaak een uitgebreide beoordeling van schendingen vereist. AI kan databeveiligingsteams helpen bij het beoordelen van content door deze te controleren op het naleven van de regelgeving en het bedrijfsbeleid, om berichten met een hoog risico te markeren die zouden kunnen leiden tot een databeveiligingsincident.

Natuurlijke taal voor sleutelwoordquery's: zoeken kan een complexe en tijdrovende workflow zijn tijdens onderzoeken, waarbij meestal de sleutelwoordquerytaal wordt gebruikt. Met AI kunnen databeveiligingsteams zoekprompts in natuurlijke taal invoeren om de start van de zoekactie te stroomlijnen en geavanceerdere onderzoeken mogelijk te maken.

Laatste aanbevelingen

1 Bescherm jezelf tegen databeveiligingsincidenten door een geïntegreerd platform te implementeren

Met een volledig geïntegreerd platform voor databeveiliging beschik je over een veiligere, meer gestroomlijnde strategie in een voortdurend veranderend landschap, waarbij de complexiteit wordt verminderd en de zichtbaarheid en bescherming worden verbeterd. Met een geïntegreerde aanpak kunnen organisaties hun databeveiligingsstatusbeheer verbeteren door databeveiligingscontroles centraal uit te voeren en geïntegreerde zichtbaarheid te bieden van data, gebruikers en activiteiten. Hierdoor versterken en stroomlijnen ze detectie en bescherming tegen datarisico's. Tweeëntachtig procent van de organisaties van mening is dat een geïntegreerd platform superieur is en derhalve biedt de stap naar consolidatie niet alleen een aantal voordelen; deze is volkomen onmisbaar.

2 Vergroot de zichtbaarheid van intern gebruik van AI om de noodzakelijke controles voor AI-gebruik door medewerkers te beoordelen die niet van invloed zijn op de productiviteit

Naarmate AI vaker op de werkplek wordt gebruikt, kan AI bestaande risico's versterken en nieuwe risico's introduceren. Organisaties geven toe dat ze meer moeten doen om bescherming te bieden tegen onveilig AI-gebruik. Het gebruik van ingebouwde controles en zichtbaarheid in AI-apps is van cruciaal belang om de databeveiliging te handhaven zonder de productiviteit te verstoren. Door medewerkers te trainen in veilig gebruik van AI kunnen organisaties risicovol gedrag tot een minimum beperken en kunnen teams profiteren van deze krachtige tools.

3 Verbeter je databeveiligingsstrategie met behulp van AI

Met AI kunnen databeveiligingsteams zich richten op meer strategische initiatieven. Ze hoeven dan niet te reageren op de voortdurende bedreigingen of een grote aantallen waarschuwingen te verwerken. Bedrijven die zich in een vergevorderd stadium van AI-implementatie bevinden, hebben meer vertrouwen in en zijn tevredener met hun databeveiligingsoplossingen dan bedrijven die net beginnen. Door AI te implementeren als onderdeel van een uitgebreide databeveiligingsstrategie kunnen organisaties hun zichtbaarheid vergroten, waardoor ze beter in staat zijn om risico's te detecteren en erop te reageren. Uiteindelijk versterkt dat hun algehele databeveiligingsstatus.

Onderzoeksdoelstellingen

De doelstellingen van het onderzoek waren onder andere:

1. Inzicht krijgen in het databeveiligingslandschap, waaronder prioriteiten en mindsets, uitdagingen en oorzaak en gevolg van databeveiligingsincidenten.
2. De toekomst van databeveiliging verkennen, waaronder welke strategieën en innovaties in opkomst zijn en hoe organisaties van plan zijn te investeren in de toekomst.
3. De rol van AI bij het verbeteren van databeveiliging en de rol die AI speelt in het beschermen van data blootleggen.

Onderzoeksmethode

Van 5 tot 23 augustus 2024 werd een 20 minuten durende multinationale online-enquête gehouden onder 1376 beslissers op het gebied van databeveiliging.

Vragen richtten zich op het databeveiligingslandschap en databeveiligingsincidenten in vergelijking met 2023. Daarnaast werden in de enquête van dit jaar vragen gesteld over het beveiligen van AI-gebruik door medewerkers en het gebruik van AI om de databeveiliging te versterken.

Doelgroepwerving

Om aan de screeningcriteria te voldoen, moesten beslissers op het gebied van databeveiliging aan het volgende voldoen:

- CISO en vergelijkbare beslissers (C-2 en hoger) met bevoegdheid voor databeveiliging
- Werken bij ondernemingsorganisaties (500+ medewerkers; verschillende grootten)
- Een mix van gereguleerde en niet-gereguleerde bedrijfstakken (geen onderwijs, overheid, of non-profit)

Van de 1376 ondervraagde beslissers op het gebied van databeveiliging die het onderzoek afrondden per land:

- VS: 302
- Verenigd Koninkrijk: 305
- India: 301
- Brazilië: 158
- Frankrijk: 156
- Australië: 154

hypothesis Microsoft Security