Microsoft

hypothesis

Databeveiligingsindex

Trends, inzichten en strategieën
om bedrijfsgegevens te beveiligen

Voorwoord

In een tijd die gekenmerkt wordt door een overvloed aan data, wordt het steeds duidelijker dat de gegevens van een organisatie niets minder zijn dan haar levensader. De schat aan data die organisaties creëren en gebruiken, stuurt essentiële bedrijfsactiviteiten aan, is de basis van strategische en mondiale besluitvorming en geeft vorm aan kansen voor de toekomst. Data zijn niet alleen een bron - ze vormen het kloppende hart van de ondernemingen van vandaag.

Maar met deze toegenomen afhankelijkheid van data komt ook de grimmige realiteit dat de kwetsbaarheden in het digitale domein echt zijn en steeds groter worden. Cyberbedreigingen, datalekken en risico-incidenten van binnenuit zijn niet langer zeldzame voorvallen. Ze komen vaak voor, ze escaleren en vormen grote risico's voor organisaties die afhankelijk zijn van data. Van alle besluitvormers die we onlangs hebben ondervraagd, gaf 89% aan dat ze hun databeveiligingsbeleid als cruciaal beschouwen voor hun algehele succes..

In deze whitepaper beginnen we met een verkenning van die fundamentele noodzaak: de bescherming van de data van jouw organisatie. Het is een groot genoegen voor mijn team en mijzelf om onze bevindingen met jullie te delen, en hopelijk een dialoog op gang te brengen over hoe we databeveiliging collectief kunnen blijven verbeteren om uitmuntendheid te bereiken. Onze bevindingen laten zien dat databeveiliging zich op een kritiek punt bevindt. Terwijl besluitvormers op het gebied van beveiliging het er allemaal over eens zijn dat het beveiligen van data essentieel is en de meesten zeggen dat ze vertrouwen hebben in wat ze doen, worden ze tegelijkertijd geconfronteerd met een overvloed aan incidenten en uitdagingen op dit gebied. Daarnaast erkent 80% van de leiders met wie we spraken dat een geïntegreerde aanpak veel beter is dan individuele oplossingen. Desondanks gebruiken de meeste bedrijven nog steeds een gefragmenteerd, multi-toolsysteem om hun data te beschermen - wat vaak leidt tot meer data-incidenten in plaats van minder.

We nodigen je uit om dit laatste rapport te lezen en met anderen delen en het te beschouwen als het begin van nieuwe gesprekken met onze teams over de beste manier om onze gezamenlijke toekomst veilig te stellen.

Rudra Mitra

Corporate Vice President
Microsoft Data Security and Compliance

Kennismaking

Het voorkomen van datalekken en andere beveiligingsincidenten blijft een constante zorg voor besluitvormers op het gebied van beveiliging en risico's - en is een hoeksteen van elk cyberbeveiligingsprogramma. Eén enkele inbreuk kan immers aanzienlijke reputatieschade én financiële schade veroorzaken. Organisaties moeten een breed scala aan gevoelige data beschermen, waaronder gegevens over werknemers en klanten, intellectueel eigendom, financiële prognoses en operationele gegevens.

Om inzicht te krijgen in de huidige praktijken en trends op het gebied van databeveiliging en de kansen voor organisaties vast te stellen om databeveiliging te verbeteren, gaf Microsoft Hypothesis Group, een onafhankelijk onderzoeksbureau, opdracht om een multinationaal onderzoek uit te voeren onder meer dan 800 professionals op het gebied van databeveiliging. Dit rapport presenteert vijf belangrijke bevindingen uit het onderzoek, waaronder trends, inzichten en strategieën om data te beveiligen.

Belangrijkste bevindingen

1

Besluitvormers denken dan wel dat ze beschermd zijn, maar de werkelijkheid blijkt anders te zijn.

Hoewel de meeste besluitvormers zeggen dat ze tevreden zijn en vertrouwen hebben in hun oplossingen voor databeveiliging, worden ze nog steeds geconfronteerd met gemiddeld 59 databeveiligingsincidenten per jaar, met kostbare gevolgen van dien.

2

Het hebben van meer tools betekent niet meer databeveiliging of efficiëntie - integendeel.

80% van de besluitvormers is het erover eens dat veelomvattende, geïntegreerde oplossingen veel beter zijn dan handmatige, zogenaamde best-of-breed systemen. Desondanks blijft de aanpak van tools door organisaties gefragmenteerd en gebruiken ze gemiddeld meer dan tien tools om hun data te beveiligen. Maar degenen met de meeste tools ervaren ook meer incidenten met databeveiliging, wat suggereert dat hoe meer tools er zijn, hoe zwakker de beveiliging.

3

Organisaties worden nog steeds geplaagd door de stress van externe en interne databeveiligingsincidenten, vooral als het om bedrijfsgegevens gaat.

50% van de ondervraagde organisaties heeft het afgelopen jaar te maken gehad met een ransomware- of malware-aanval - en veel besluitvormers zijn er niet van overtuigd dat hun organisatie volledig is voorbereid om toekomstige aanvallen te voorkomen en aan te pakken. Binnen bedrijven zijn opzettelijke datalekken van binnenuit een grote zorg. Daarnaast maken organisaties zich grote zorgen over de kwetsbaarheid van hun bedrijfsgegevens. Dit onderstreept nog maar eens de noodzaak van een beveiligingsplatform dat risico's uitgebreid aanpakt.

Belangrijkste bevindingen

4

Organisaties hebben Cloud en AI nodig om digitale transformatie te stimuleren - maar deze zijn ook de meest kwetsbare datalocaties.

Cloudapplicaties en AI-technologie zijn essentieel geworden voor de samenwerking en productiviteit van organisaties. Deze ontwikkeling brengt echter ook meer dynamische en veelzijdige risico's met zich mee. Hoe meer organisaties AI toepassen, hoe crucialer verantwoord en veilig gebruik van databeveiliging wordt.

5

Automatisering en AI zijn veelbelovende wegen naar een betere bescherming.

Organisaties willen dat hun teams minder tijd besteden aan detectie en meer tijd aan preventie. Dankzij automatisering kunnen teams zich meer richten op proactieve maatregelen, terwijl het gebruik van AI voor databeveiliging organisaties helpt strategischer te handelen en slimmer met toekomstige bedreigingen om te gaan.

1

Besluitvormers denken dan wel dat ze beschermd zijn, maar de werkelijkheid blijkt anders te zijn.

Besluitvormers denken dan wel dat ze beschermd zijn, maar de werkelijkheid blijkt anders te zijn.

In eerste instantie geven besluitvormers aan veel vertrouwen te hebben in en tevreden te zijn over hun oplossingen voor databeveiliging. De meeste organisaties denken dat hun databeveiligingscontroles voldoende zijn om te voorkomen dat gegevens worden gelekt en dat ze weten waar deze zich bevinden, en dat ze de meeste risico's rondom data kunnen detecteren.

Tegelijkertijd worden organisaties nog steeds geconfronteerd met een aanzienlijk aantal databeveiligingsincidenten, gemiddeld 59 in de afgelopen 12 maanden, waarvan een vijfde als 'ernstig' wordt beschouwd. De impact van deze incidenten is wijdverspreid, want gemiddeld schatten organisaties de totale financiële kosten van hun ernstigste databeveiligingsincident op ongeveer USD 244.000, wat betekent dat jaarlijkse incidenten tot USD 15 mln. kunnen kosten. Bovenop deze kosten zeggen vier op de tien besluitvormers ook de operationele kosten van het herstel van een databeveiligingsincident en de zakelijke verliezen door reputatieschade een grote zorg te vinden.

Daarnaast wordt 92% geconfronteerd met uitdagingen, voornamelijk op het gebied van kosten, integratie en implementatietijd, die hun vermogen om verder te investeren in databeveiliging in de weg staan.

De perceptie van vertrouwen in de gereedheid van databeveiliging verschilt van de realiteit van incidenten die organisaties daadwerkelijk ervaren. Hoewel het belangrijk is voor organisaties om te weten waar gegevens zich bevinden en om risico's op te sporen, zijn deze maatregelen, individueel of afzonderlijk, niet genoeg om organisaties te helpen de incidenten te voorkomen die besluitvormers op het gebied van databeveiliging en risico's 's nachts wakker houden.

Aldus een CISO (Chief Information Security Officer) in de financiële dienstverlening: "Ik kan niet tegen mijn raad van bestuur zeggen 'Ik heb de gegevens wel beveiligd, maar ik heb ze niet beschermd'... het laatste wat we willen is dat onze bank op de voorpagina van de Wall Street Journal komt te staan."

59

Gemiddeld aantal databeveiligingsincidenten in de afgelopen 12 maanden

TOT USD 15 mln.

Jaarlijkse kosten van een ernstig beveiligingsincident

2

Het hebben van meer tools betekent niet meer databeveiliging of efficiëntie - integendeel.

Het hebben van meer tools betekent niet meer databeveiliging of efficiëntie - integendeel.

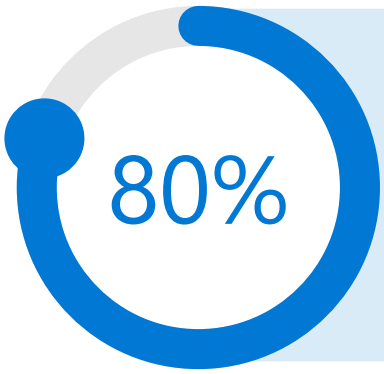
Organisaties realiseren zich steeds meer dat de jarenlange benadering met standaardoplossingen gaten heeft geslagen in de zichtbaarheid en efficiëntie als gevolg van silo's in de tools voor databeveiliging. Die trend maakt nu plaats voor de wens om een geïntegreerde oplossing voor databeveiliging. 80% is het erover eens dat een uitgebreid databeveiligingsplatform met geïntegreerde oplossingen veel beter is dan het gebruik van meerdere best-of-breed oplossingen die handmatig moeten worden geïntegreerd en gemanaged.

Hoewel de overgrote meerderheid geïntegreerde oplossingen superieur vindt, wordt er veel en gefragmenteerd van databeveiligingstools gebruik gemaakt.

Als gevolg hiervan melden organisaties dat ze gemiddeld tien databeveiligingstools gebruiken om de risico's voor databeveiliging aan te pakken, waaronder Data Loss Prevention, Information Protection, Insider Risk Management, Security Information & Event Management (SIEM), Cloud Access Security Broker en meer. Voor organisaties met meer dan 5.000 werknemers is het gemiddelde aantal tools zelfs nog groter.

Het hebben van meer tools kan een misleid gevoel van zekerheid geven, aangezien degenen die meer tools gebruiken (16+) meer vertrouwen hebben in hun aanpak van databeveiliging in vergelijking met degenen die minder tools gebruiken (61% ten opzichte van 56%).

Onderzoek spreekt dat gevoel van zekerheid echter tegen, want organisaties met 16 tools of meer , werden ook met meer databeveiligingsincidenten geconfronteerd in het afgelopen jaar - gemiddeld 133 - vergeleken met 48 incidenten bij organisaties met minder tools.

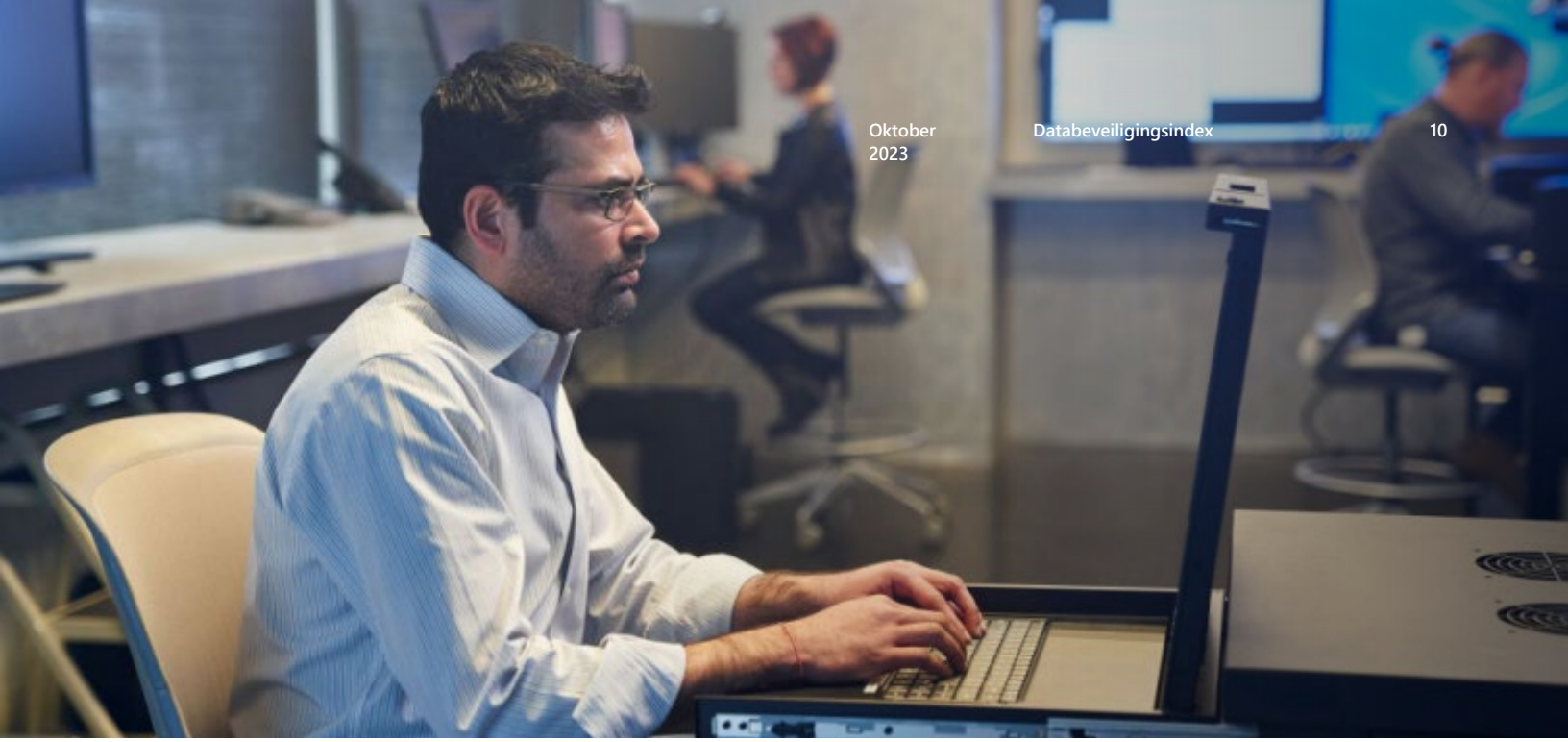


Mee eens dat een uitgebreid beveiligingsplatform met geïntegreerde oplossingen beter is dan het gebruik van meerdere best of-breed oplossingen die handmatig moeten worden geïntegreerd en gemanaged.

2,8x

Meer databeveiligingsincidenten in het afgelopen jaar

Voor organisaties met 16 of meer tools (vergeleken met organisaties met minder tools)



Het pleidooi voor een betere databeveiliging door middel van meer geïntegreerde oplossingen en minder tools wordt nog sterker als we kijken naar de gevoelens en praktijken van degenen die de voorkeur geven aan best-of-breed oplossingen of meer tools.

"Hoe worden data uit een groot aantal systemen verzameld, samengevoegd en gebruikt? Er moeten veel verschillende datapunten worden samengevoegd in één ecosysteem om het echt te laten werken. Anders heb je een gatenkaas aan databeveiliging."

VP IT
Manufacturing/Production

Ten eerste kunnen meerdere verschillende tools voor databeveiliging leiden tot hiaten in de zichtbaarheid en tot meer schaduwdata. In feite geven degenen die zich zorgen maken over schaduwdata, eerder de voorkeur aan best-of-breed oplossingen. Dit komt waarschijnlijk doordat organisaties met een best-of-breed aanpak meer moeite moeten doen om een uitgebreid overzicht te krijgen van hun databeveiligingsstatus.

Ten tweede brengt het beheren van silo-oplossingen meer complexiteit met zich mee voor databeveiligingsteams, omdat elke ongelijksoortige oplossing speciale mensen, installatie en onderhoud van eindpuntbeheerders en verschillende nieuwe processen vereist. Neem bijvoorbeeld de controle en triage van waarschuwingen, een van de taken waarvoor mensen en middelen nodig zijn. Een toenemend aantal waarschuwingen betekent dat databeveiligingsteams zich extra moeten inspannen bij het beheren van geïsoleerde oplossingen. Organisaties met meer tools ontvangen gemiddeld 96 waarschuwingen voor databeveiliging per dag, terwijl teams met minder tools 44, dus minder dan de helft van dat aantal, ontvangen. Bovendien zijn ze niet in staat om dezelfde hoeveelheid waarschuwingen te bekijken als teams met minder tools (61%, tegenover 68%). Dit leidt er vaak ook toe dat organisaties met meer tools meer reactief zijn in vergelijking met organisaties die minder tools gebruiken.

Tot slot geven meer tools ook aan dat organisaties veel moeite moeten doen om inzichten en herstelplannen te integreren, en dat tijdens dat proces informatie verloren kan gaan. Gevraagd naar de belangrijkste uitdagingen op het gebied van databeveiliging, worden de kosten van het implementeren of onderhouden van databeveiligingsoplossingen en de uitdagingen bij het integreren van deze oplossingen als de belangrijkste twee gerangschikt.

Dit vertaalt zich in langere, langzamere processen, waarbij 37% van degenen die 16 of meer tools gebruiken, melden dat ze een maand of langer nodig hebben om een onderzoek naar databeveiliging te voltooien, vergeleken met slechts 21% van degenen die minder tools hebben.

"Op dit moment bewegen we in een slakkengang. Alle systemen die we hebben, hebben hun eigen portals, hun eigen tools en hun eigen manieren om met dingen om te gaan. Elk gaat zijn eigen weg, waarbij diegene de expert is. Dan komen ze allemaal weer bij elkaar om te beslissen wat er aan de hand is en van daaruit worden de dingen aangepakt. Op dit moment is het dus een beetje handen- en voetenwerk", aldus een directeur infrastructuur en operaties in fabricage en productie.

Door ervoor te kiezen door te gaan met meerdere oplossingen, negeren organisaties uiteindelijk hun eigen woorden van inzicht dat geïntegreerde oplossingen veel beter zijn en lopen ze in de tegenovergestelde richting. En dat kost tijd en geld.

UITKOMSTEN VAN DEGENEN DIE MINDER TOOLS (<16) TEN OPZICHTE VAN MEER (16+) TOOLS VOOR DATABEVEILIGING GEBRUIKEN	Weinig tools	Veel tools
Aantal **databeveiligingsincidenten** in de afgelopen 12 maanden	48	133
Percentage **ernstige** databeveiligingsincidenten	19%	26%
Onze huidige databeveiligingsstrategie is meer **reactief**	31%	40%
Uitdagingen met **het integreren van** oplossingen	24%	39%
Databeveiligingsteam is de meeste tijd kwijt aan **reageren**	19%	26%
We hebben **vertrouwen** in onze aanpak van databeveiliging	56%	61%
Aantal waarschuwingen **ontvangen** gemiddeld per dag	44	96
Percentage waarschuwingen die we **kunnen onderzoeken** per dag	68%	61%
We hebben minstens een maand nodig om een databeveiligingsonderzoek te doen	21%	37%

3

Organisaties worden nog steeds geplaagd door de stress van externe en interne databeveiligingsincidenten, vooral als het om bedrijfsgegevens gaat.

Organisaties worden nog steeds geplaagd door de stress van externe en interne incidenten op het gebied van databeveiliging, vooral met betrekking tot bedrijfsgegevens.

Omdat de factoren rondom gegevens - waaronder de mensen die met data omgaan, activiteiten rondom data, apparaten en apps die worden gebruikt om ze te verwerken - voortdurend veranderen, kunnen incidenten met betrekking tot databeveiliging en datalekken altijd en overal plaatsvinden. En deze bedreigingen zijn afkomstig van zowel externe aanvallers als vertrouwde medewerkers, zoals werknemers, onderaannemers en partners. Of ze nu kwaadwillig of onopzettelijk zijn, alle betrokkenen kunnen databeveiligingsincidenten veroorzaken. Dit betekent dat er een constante behoefte is aan bescherming op een groot aantal gebieden.

Aldus een VP van IT in de financiële dienstverlening, “Waar je je tegen probeert te beschermen, verandert continu. Het is een bewegend doelwit. Het zal zich altijd ontwikkelen, veranderen en flexibel zijn. Wat je beschermt en waar het zich bevindt, wordt alleen maar gevarieerder.”

Terwijl databeveiligingsincidenten uit verschillende bronnen kunnen komen, is de externe dreiging van malware of ransomware - gevallen waarin kwaadaardige software een systeem infiltreert en aanvallers ongeautoriseerde toegang tot systemen of netwerken verschaft - verreweg het meest voorkomend: 50% van de ondervraagde organisaties heeft er het afgelopen jaar minstens één meegemaakt.

Bovendien voelen organisaties zich het meest kwetsbaar voor deze aanvallen: 41% zegt zich het minst voorbereid te voelen om toekomstige malware- of ransomware-aanvallen in het komende jaar het hoofd te bieden. Dit gevoel van kwetsbaarheid is nog groter bij degenen die de voorkeur geven aan een best-of-breed aanpak - 44% voelt zich onvoorbereid op een aanval van deze aard, tegenover slechts 36% die de voorkeur geeft aan een geïntegreerde oplossing.

Het beveiligen tegen en voorkomen van risico's bij intern lekken van data is ook een topprioriteit voor besluitvormers. 35% zegt dat ze hun verdediging moeten versterken tegen kwaadwillende datalekken van binnenuit en gecompromitteerde accounts, en een derde maakt zich zorgen over onopzettelijke incidenten met datalekken van binnenuit. Hoewel incidenten met kwaadwillende datalekken van binnenuit misschien niet de belangrijkste oorzaak zijn van inbreuken op de databeveiliging, zijn ze wel het op één na meest voorkomende type incident waarop besluitvormers zich het minst voorbereid voelen.

"Minstens één keer per maand word ik gebeld door een directeur in paniek... ´We hebben een incident gehad, ik heb een incident ontdekt of het bedreigingsteam heeft een incident ontdekt. Sommige zijn onopzettelijk, andere komen door mensen die niet weten of begrijpen wat hun privileges toestaan."

CISO bij de Amerikaanse overheid

Insiders zijn vertrouwde personen die toegang hebben gekregen tot, of kennis hebben van, bedrijfsbronnen, gegevens of systemen die niet beschikbaar zijn voor het algemene publiek. Daarom zijn de risico's voor databeveiliging die te maken hebben met insiders vaak ongrijpbaarder en moeilijker te detecteren. Bret Arsenault, de CISO van Microsoft: "Uiteindelijk maakt het niet uit of het lek opzettelijk of per ongeluk heeft plaatsgevonden. Risicoprogramma's voor insiders moeten deel uitmaken van de beveiligingsstrategie van elk bedrijf."

SAMENVATTING DATABEVEILIGINGSINCIDENTEN

Oorzaken van databeveiligingsincidenten	Meest voorkomende incidenten in afgelopen 12 maanden	Minst voorbereid op het voorkomen in komende 12 maanden
Malware of ransomware	**50%**	**41%**
Gecompromitteerde accounts	**38%**	**35%**
Denial-of-service (DoS) aanvallen	**35%**	**33%**
Onachtzame insiders	**32%**	**29%**
Niet-kwaadwillende insiders	**31%**	**32%**
Kwaadwillende insiders	**31%**	**35%**
Fysieke eigendommen	**29%**	**29%**

De databeveiligingsoplossingen die organisaties kiezen, moeten ook geschikt zijn voor meerdere verschillende gevoelige data, waaronder bedrijfsgegevens van hoge waarde, operationele gegevens en persoonsgegevens. Tijdens databeveiligingsincidenten in de afgelopen 12 maanden werden bij 74% van de organisaties bedrijfsgegevens blootgelegd, 65% zag operationele gegevens gecompromitteerd en 58% ondervond dat persoonsgegevens kwetsbaar werden gemaakt. Van de verschillende soorten data zijn intellectueel eigendom, IT- en netwerkdesigns en PII het vaakst gecompromitteerd of blootgesteld aan risico.

Vooruitkijkend ziet 77% van de organisaties bedrijfsgegevens, zoals intellectuele eigendommen en broncodes, als het meest kwetsbaar. Dit komt vooral omdat bedrijfsgegevens een cruciale rol spelen bij het vaststellen van concurrentievoordelen en het genereren van inkomsten. Het identificeren en classificeren van dergelijke data kan echter een uitdaging zijn, omdat traditionele patroonherkenning, reguliere expressie of functiematchtechnologie content zonder specifieke tekenindelingen of trefwoorden mogelijk niet optimaal identificeert. Organisaties hebben op hun beurt meer geavanceerde technologieën nodig om die kwetsbare gevoelige data te ontdekken en te beschermen.

DATASOORTEN DIE DE KOMENDE 12 MAANDEN HET GROOTSTE RISICO LOPEN

77% **Bedrijfsgegevens**		64% **Operationele gegevens**		63% **Persoonsgegevens**	
Intellectuele eigendom	**30%**	IT- en netwerkdesigns	**29%**	Persoonlijk Identificeerbare Informatie (PII)c	**31%**
Broncode	**28%**	Financiële overzichten	**18%**	Personeelsinformatie (salarisadministratie, cv´s enz)	**21%**
Bedrijfsplannen	**27%**	Verkoop- en omzetrapporten	**15%**	Gegevens betaalkaartindustrie (PCI)	**18%**
Handelsgeheimen	**24%**	Inkoop en facturering	**12%**	Beschermde gezondheids informatie (PHI)	**18%**
Fusie- en overnamedossiers	**20%**	Juridische documenten/ contracten	**12%**	Referenties	**17%**
Bouwplannen	**18%**	Productieprocessen/ batchbestanden	**11%**		

4

Organisaties hebben Cloud en AI nodig om digitale transformatie te stimuleren - maar deze zijn ook de meest kwetsbare datalocaties.

Organisaties hebben Cloud en AI nodig om digitale transformatie te stimuleren - maar deze zijn ook de meest kwetsbare datalocaties.

Samenwerking via cloudapplicaties en -platforms, gecombineerd met nieuwe AI-technologie, verbetert de productiviteit van werknemers aanzienlijk en maakt flexibele werkafspraken mogelijk, waardoor cloudapplicaties en AI-technologie onmisbaar worden voor organisaties. Gemiddeld maken organisaties nu gebruik van 147 openbare cloudservices, zoals SaaS, PaaS en IaaS.[1] En 66% van de organisaties heeft een AI-strategie ontwikkeld en 36% heeft deze al geïmplementeerd.[2] Deze ontwikkeling brengt echter meer dynamische en veelzijdige risico's met zich mee, omdat het moeilijk is om de grenzen van data in verschillende omgevingen duidelijk af te bakenen.

1. Risico's en risicogovernance meten, Cloud Security Alliance (CSA), 2022
2. Microsoft databeveiliging AI-onderzoek, Hypothesis, maart 2023

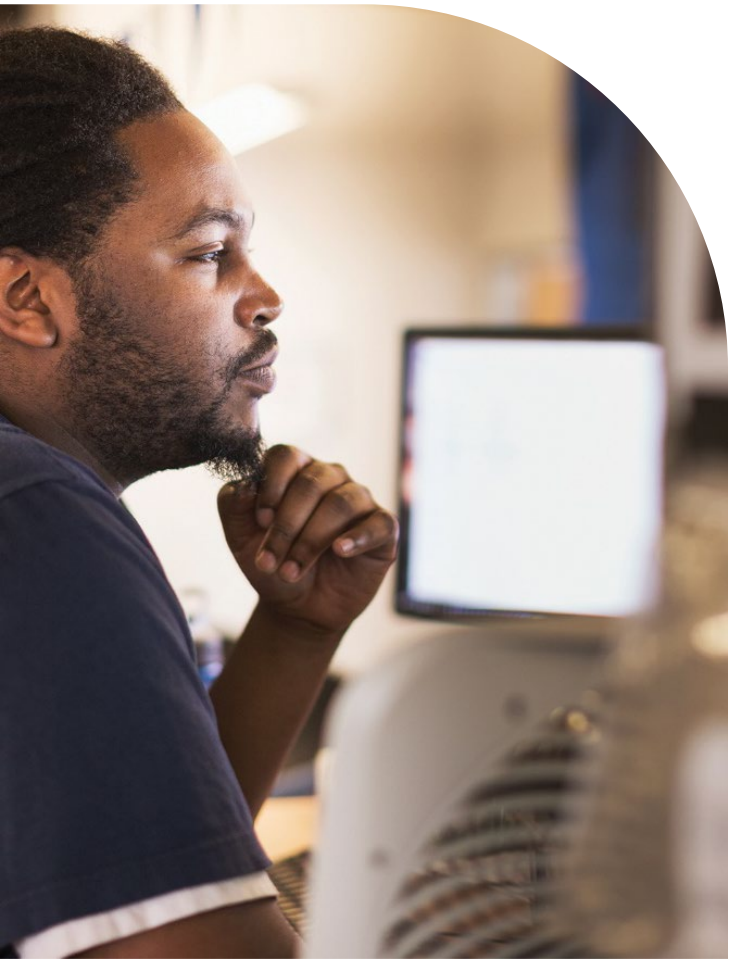
Het is nu nog belangrijker om voor deze zeer productieve datalocaties de juiste oplossing voor databeveiliging te hebben. In de afgelopen 12 maanden meldde 42% van de organisaties beveiligingsincidenten bij cloudopslag en 31% bij e-mails, instant messaging of tools voor online vergaderingen. Incidenten lijken het meest voor te komen waar de meeste productiviteit en samenwerking plaatsvindt.

Voor het beheren van dit soort incidenten zijn resources nodig en 79% van de organisaties geeft aan dat hun databeveiligingsteam meer mensen nodig heeft om de meest belangrijke verantwoordelijkheden op het gebied van databeveiliging effectief te managen. Van de organisaties die zeggen meer mensen nodig te hebben, geeft de meerderheid (57%) echter de voorkeur aan een best-in-breed-aanpak. Deze voorkeur laat zien dat organisaties die meer oplossingen gebruiken, meer moeite hebben om de echte risico's te identificeren tussen de talloze gebruikersactiviteiten.

SAMENVATTING DATALOCATIES

Datalocaties	Gecompromitteerd in de afgelopen 12 maanden	Grootste risico
Cloudopslag (bijv. Box, OneDrive, Google Drive)	42%	54%
E-mails/Instant messaging/Online vergaderen	31%	39%
Platform-as-a-service (PaaS)	29%	34%
Infrastructure-as-a-service (IaaS)	28%	36%
AI (bijv. ChatGPT, Bard enz.)	27%	38%
SaaS-gebaseerde databases/data lakes	27%	41%
Eindpunten/apparaten	25%	36%
Opslagplaatsen/bestandsdeling/databases op locatie	24%	28%
Schaduwdata	21%	23%
Branchespecifieke applicaties	17%	25%
Ontwikkeltools	16%	23%

Nu meer dan een derde van de organisaties een AI-strategie heeft geïmplementeerd en er nog meer op komst zijn, wordt AI in een ongekend tempo overgenomen, veel sneller dan het invoeren van cloud en e-mail in het verleden. Nu meer organisaties AI toepassen, wordt het steeds crucialer databeveiliging te verbeteren, verantwoord gebruik mogelijk te maken en risico's te voorkomen. AI wordt beschouwd als een risicolocatie voor databeveiligingsincidenten, vergeleken met andere locaties, en 27% van de organisaties heeft te maken gehad met een AI-inbreuk op de databeveiliging. De zorgen van organisaties over de risico's van het gebruik van AI richten zich op een gebrek aan controle over data die wordt gedeeld met AI, een gebrek aan controle om riskant gebruik van AI te detecteren en te beperken, een gebrek aan transparantie over hoe generatieve AI-modellen worden getraind en het lekken van vertrouwelijke informatie via AI.



"AI is goed voor de productiviteit en efficiëntie, maar het heeft potentiële beveiligings- en datarisico's", aldus een besluitvormer op het gebied van beveiliging.

Hoewel er bezorgdheid bestaat over AI, zien besluitvormers ook het potentieel, vooral omdat leveranciers op de markt innovaties ontwikkelen om bedrijven de mogelijkheid te bieden op een verantwoorde manier gebruik te maken van AI. Om AI verder te benutten, geven organisaties echter aan dat de belangrijkste controles die ze nodig hebben, kwaadaardige of risicovolle content in AI moeten kunnen detecteren, data moeten versleutelen, maskeren of anonimiseren, voordat ze naar AI kunnen worden geüpload en gevoelige data die door AI wordt gegenereerd, moeten kunnen identificeren.

BELANGRIJKSTE 5 DATABEVEILIGINGSCONTROLES DIE NODIG ZIJN VOOR AI

1. **Detectie van kwaadwillende of risicovolle content** in AI
2. **Data versleutelen, maskeren of anonimiseren,** voordat ze kunnen worden geüpload naar AI
3. **Gevoelige data identificeren** die door AI worden gegenereerd
4. **Voorkomen dat gevoelige data worden geüpload** naar AI
5. **Model- of datamanipulatie detecteren** in AI

5

Automatisering en AI zijn veelbelovende wegen naar een betere bescherming.

Automatisering en AI zijn veelbelovende wegen naar een betere bescherming.

In een ideale wereld, zonder beperkingen als het gaat om organisatorische prioriteiten of budgetten, zou de helft van de organisaties proactiever willen zijn op het gebied van databeveiligingsbeheer en meer tijd willen besteden aan zaken zoals het ontdekken van gevoelige data en de bijbehorende risico's en het voorkomen van databeveiligingsincidenten. Op dit moment besteedt echter meer dan de helft van de organisaties de meeste tijd aan reactieve maatregelen, zoals detectie van incidenten, reactie en onderzoek. En het opsporen van en reageren op databeveiligingsincidenten is tijdrovend - de meeste organisaties doen er ongeveer een maand over om een databeveiligingsincident op te lossen en bij sommige kan dat zelfs zes maanden duren.

Het voordeel van een meer proactieve strategie is duidelijk, aangezien de ondervraagde en meer proactieve organisaties al minder kostbare incidenten met databeveiliging ervaren, vaker in staat zijn om die incidenten in minder dan een maand te onderzoeken en vaker menen dat hun verdedigingscontroles afdoende zijn in het voorkomen van datalekken.

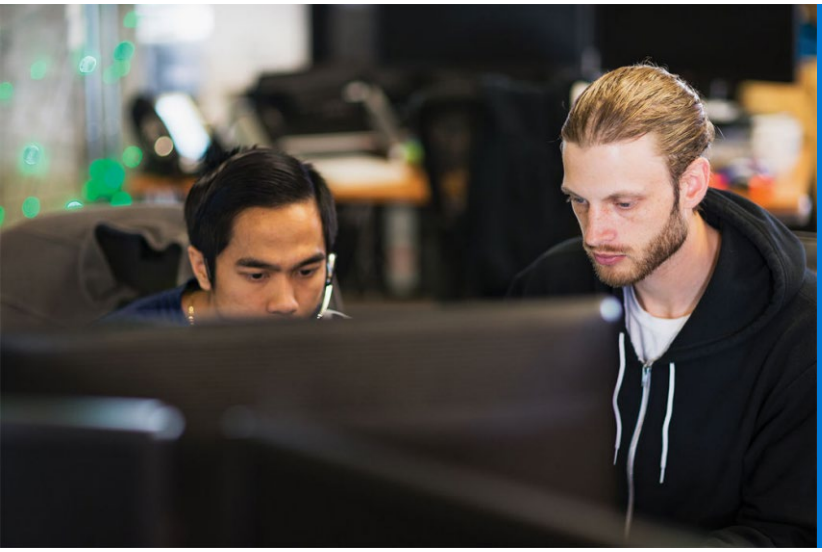
Hoewel organisaties zich ervan bewust zijn dat proactieve maatregelen voor databeveiliging de risico's bij databeveiliging kunnen verkleinen, boeken ze geen vooruitgang bij het implementeren van deze maatregelen. Wie bijvoorbeeld proactiever wil zijn door meer tijd aan preventie te besteden, zal eerder kiezen voor best-of-breed oplossingen, die in feite meer inspanningen vereisen bij het aanpakken van reactieve maatregelen wanneer detectiesignalen en responscontroles worden samengebracht.

RESULTATEN VAN ORGANISATIES DIE MEER PROACTIEF ZIJN IN PLAATS VAN REACTIEF	Proactiever	Reactiever
Gemiddelde kostenimpact van een databeveiligings incident in de afgelopen 12 maanden	**USD 207.000**	**USD 330.000**
Rondt een onderzoek naar databeveiliging in gemiddeld minder dan een maand af	**80%**	**68%**
Onze verdedigingscontroles zijn toereikend om datalekken te voorkomen	**77%**	**68%**

Omdat middelen en mensen beperkt zijn en de verdeling van inspanningen tussen activiteiten misschien niet ideaal is, zoeken organisaties technologieën die hen kunnen helpen meer tijd vrij te maken voor proactieve activiteiten. Automatisering is één manier waarop organisaties tijd kunnen vrijmaken voor een meer proactieve aanpak van databeveiliging. 74% van de ondervraagde organisaties geeft de voorkeur aan semi- of volledig geautomatiseerde risicobeperking, waardoor beveiligingsteams de impact van potentiële databeveiligingsincidenten op voorhand kunnen minimaliseren, in plaats van handmatige controles uit te voeren. Bovendien erkennen organisaties veel andere taken die baat zouden kunnen hebben bij automatisering, zoals het maken van rapporten over databeveiliging, automatisering van de workflow voor incidentbeheer en het reageren op en onderzoeken van incidenten. De meeste taken die beveiligingsteams willen automatiseren zijn reactieve maatregelen. Door deze taken te automatiseren, kunnen organisaties de last van hun databeveiligingsteams verlichten, zodat ze een meer proactieve aanpak kunnen uitvoeren.

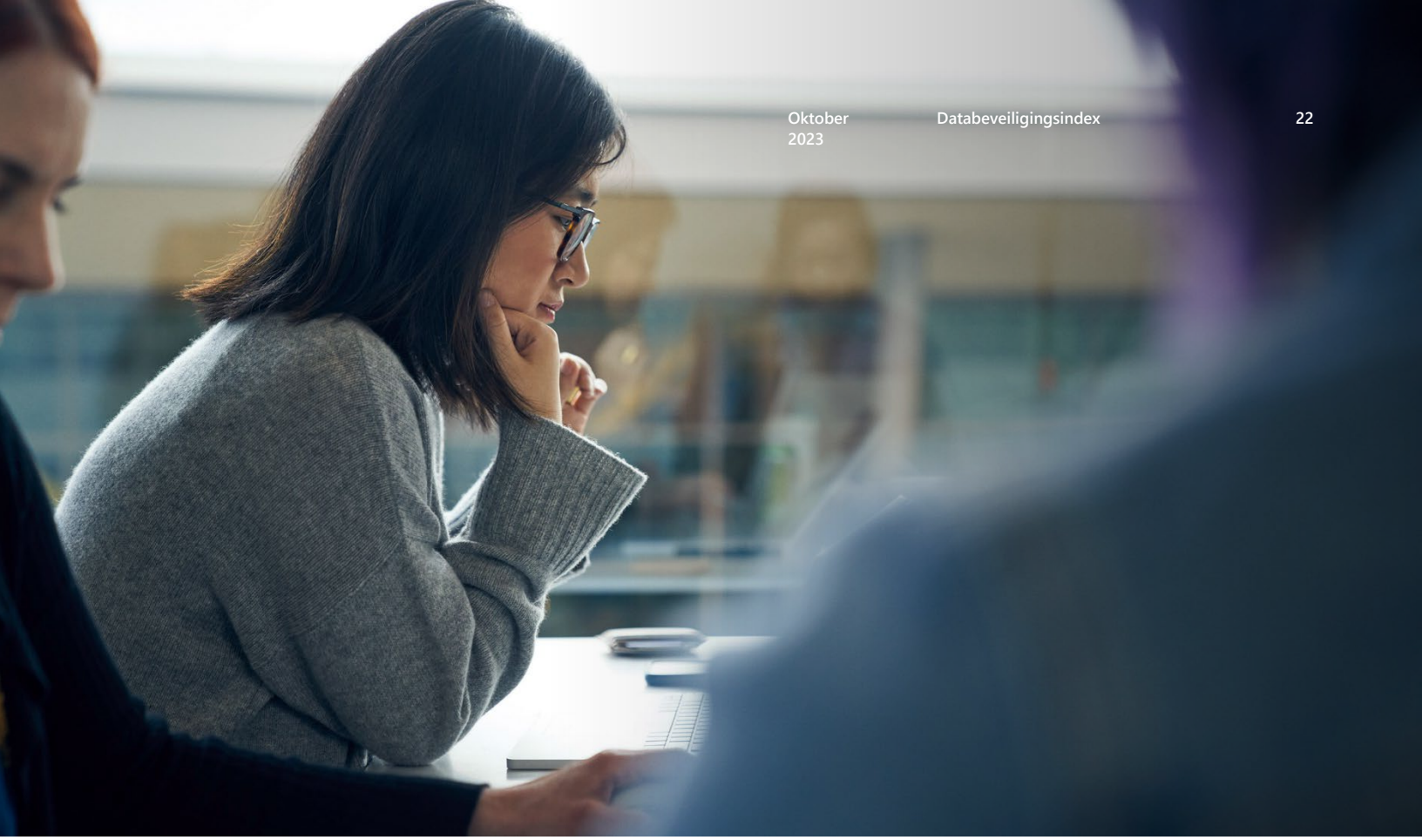
5 BELANGRIJKSTE GEBIEDEN DIE DATABEVEILIGINGSTEAMS HET LIEFST AUTOMATISEREN/VERLICHTEN

Reactief	1	Geautomatiseerde workflows maken voor incidentbeheer en reactie
	2	Databeveiligingsrapporten maken
Reactief	3	Reageren op en beheersen van databeveiligingsincidenten
	4	Incidenten tijdens onderzoeken doorsturen naar de juiste teams (bijv. SOC, juridische zaken, HR)
	5	Databeveiligingsincidenten onderzoeken



"Er zijn zoveel riskante gegevens om handmatig te evalueren. AI kan helpen om de reactietijden van ons team te versnellen en data te beschermen, aangezien we over te weinig mensen beschikken."

Besluitvormer veiligheid in het VK



Het gebruik van AI voor databeveiliging kan organisaties ook helpen strategischer te werk te gaan en slimmer om te gaan met toekomstige bedreigingen. Dankzij technologie kan sneller op gedetecteerde incidenten worden gereageerd, waardoor databeveiligingsprofessionals meer tijd hebben om verder onderzoek te doen. Net als bij automatisering noemen organisaties veel scenario's waarbij AI kan helpen om een betere beveiliging te bieden, **dus besparen ze hun team tijd.** Tot de beste scenario's voor het gebruik van AI behoren het automatisch blokkeren van ongepast delen van gegevens, het detecteren van kritieke risico's voor databeveiliging/afwijkende data-activiteiten en het onderzoeken van potentiële databeveiligings-incidenten.

Door gebruik te maken van de voordelen van AI en automatisering en over te stappen op meer geïntegreerde oplossingen, kunnen organisaties een proactievere databeveiligingsstrategie toepassen en zich voorbereiden op een veiligere toekomst.

DE SCENARIO'S WAARIN HET MEEST AI WORDT GEBRUIKT

Automatisch blokkeren van ongepast delen van data

Detecteren van kritieke databeveiligingsrisico's/ afwijkende data-activiteiten

Aanbevelingen om je data-omgeving beter te beveiligen

Onderzoeken van potentiële databeveiligingsincidenten

Afstemmen van databeveiligingsregels

Laatste aanbevelingen

- Gebruik een geïntegreerd platform om de databeveiliging te verbeteren
- Bescherm jezelf tegen databeveiligingsincidenten van buitenaf en van binnenuit met een defense-in-depth aanpak
- Verbeter je databeveiligingsstrategieën met AI en automatisering

Gebruik een geïntegreerd platform om de databeveiliging te verbeteren

Volgens de bevindingen in dit onderzoek kunnen minder oplossingen voor meer veiligheid zorgen. Het lijkt misschien contra-intuïtief, maar organisaties moeten het valse gevoel van vertrouwen bestrijden dat door een veelheid aan geïsoleerde oplossingen ontstaat. Het consolideren van leveranciers zorgt voor een strategische aanpak die niet alleen de kosten verlaagt, maar ook de beveiliging verbetert.

Besluitvormers op het gebied van databeveiliging kunnen deze transformatie in gang zetten door hun teams meer tijd te laten besteden aan strategisch werk, zoals het onderzoeken en plannen van nieuwe beveiligingscontroles en het optimaliseren van het beveiligingsbeleid - iets waar 84% van de besluitvormers het over eens is dat ze dit willen doen. Dit proces omvat het vervangen van oude silo-oplossingen, die vaak als best-of-breed worden beschouwd, maar niet effectief met andere tools samenwerken.

Besluitvormers kunnen nauw samenwerken met hun teams om doelen voor het databeveiligingsprogramma en belangrijke prestatie-indicatoren (KPI's) vast te stellen. Ze kunnen dan verder gaan met het definiëren van oplossingseisen en het identificeren van niet-onderhandelbare kenmerken. Dankzij deze aanpak kunnen ze leveranciers vinden die tools kunnen leveren die bij hun overkoepelende doelstellingen aansluiten. Het bevordert vooral een vooruitdenkende mindset en helpt teams te voorkomen dat ze te veel gefixeerd raken op bestaande handelingen of geïsoleerde gebruiksgevallen. Op deze manier kunnen ze de noodzakelijke veranderingen doorvoeren om een meer geïntegreerde aanpak tot stand te brengen.

Een geïntegreerd databeveiligingsplatform moet beveiligingsteams in staat stellen al deze belangrijke taken naadloos uit te voeren:

1. Gevoelige data ontdekken en beschermen in hun digitale landschap.
2. Kritieke risico's met betrekking tot deze data opsporen.
3. Ongeoorloofd gebruik van gevoelige data voorkomen zonder de legitieme bedrijfsactiviteiten te beïnvloeden.

Door een geïntegreerde databeveiligingsstrategie in te voeren, kunnen organisaties een hoger beschermingsniveau bereiken en tegelijkertijd hun beveiligingsinfrastructuur vereenvoudigen.

Bescherm jezelf tegen databeveiligingsincidenten van buitenaf en van binnenuit met een defense-in-depth aanpak

Databeveiligingsncidenten zijn vaak het gevolg van externe aanvallers en kwaadwillende of onopzettelijke lekken van binnenuit. Organisaties moeten maatregelen nemen om hun data te beschermen, zowel door ongeautoriseerde toegang van externe bedreigingen te voorkomen als door het risico van datadiefstal van binnenuit of onbedoelde blootstelling van data te beperken.

Om deze uitdagingen aan te gaan, kunnen organisaties kiezen voor een defense-in-depth aanpak van databeveiliging. Deze strategie is vergelijkbaar met de bescherming van onbetaalbare kunstwerken door een museum: geavanceerde beveiligingscamera's met informatie over bedreigingen houden toezicht op bezoekers, kaartverkoopsystemen beheren de identiteit en toegang tot het museum en strenge beveiligingsmaatregelen rond de kunstwerken werken op dezelfde manier als beveiligingscontroles die je waardevolle data beschermen. Deze maatregelen ontmoedigen potentiële incidenten, of ze nu afkomstig zijn van externe slechte actoren of personen die zich al binnen de omgeving van de organisatie bevinden.

Het bestrijden van veranderende risico's op het gebied van databeveiliging vereist een gezamenlijke inspanning van de hele organisatie om deze defense-in-depth strategie te implementeren. De samenwerking van het databeveiligingsteam met andere afdelingen, zoals het Security Operations Center (SOC), kan de investering in databeveiliging optimaliseren. Met name 66% van de organisaties die zichzelf als proactief beschouwen, werken samen met hun SOC-team, vergeleken met 54% die dat niet doen.

Net als teamwork tussen beveiligingsteams moeten oplossingen voor databeveiliging ook naadloos met andere systemen integreren, zoals Extended Detection and Response (XDR) of Identity and Access Management (IAM), om databeveiligingsincidenten van zowel externe als interne bronnen effectief te voorkomen. Dankzij deze integraties kunnen organisaties uitgebreide onderzoeken uitvoeren en reageren op beveiligingsincidenten, een grondig begrip krijgen van de getroffen data, actoren en activiteiten, en reageren met meerdere risicobeperkende maatregelen. Hierdoor kunnen ze weloverwogen, nauwkeurige en snelle reacties geven om de impact van potentiële beveiligingsincidenten te minimaliseren.

Verbeter je databeveiligingsstrategieën met AI en automatisering

Automatisering en AI kunnen organisaties helpen om data proactiever te beveiligen. Hier zijn enkele aanbevelingen voor je organisatie om de reis naar automatisering en AI te beginnen:

- Ontdek gevoelige data: gebruik AI om te helpen bij het identificeren van gevoelige data en het toepassen van een beschermingsbeleid, waaronder versleuteling en rechtenbeheer. Dit is vooral waardevol voor bedrijfsgegevens die moeilijk te detecteren zijn met traditionele patroonherkenningstechnologieën. Organisaties kunnen classificatietechnologie gebruiken, zoals machine-learning of AI-ondersteunde classificeerders, die bekend staan om hun intelligentie en vermogen om snel gevoelige content te lokaliseren op basis van de gegevenscontext of bedrijfscategorie. Als alternatief kunnen organisaties gebruik maken van technologie voor het exact matchen van data om operationele of persoonlijke gegevens te ontdekken.

  Naarmate de regelgeving in de sector zich verder ontwikkelt (bijv. AVG, HIPAA of PCI DSS) en het datalandschap steeds dynamischer wordt, is het bovendien essentieel om over geavanceerde classificatietechnologie te beschikken die gemakkelijk aanpasbaar is om nieuwe categorieën gevoelige data te identificeren.

- Kritieke risico's bij databeveiliging detecteren: gebruik de kracht van AI om kritieke risico's met betrekking tot je gevoelige gegevens vast te stellen en resources strategisch toe te wijzen om potentiële incidenten met hoog risico aan te pakken. AI-technologieën kunnen waarheidsgetrouwe waarschuwingen genereren, waardoor beveiligingsteams kostbare tijd kunnen besparen die anders zou worden besteed aan het doorzoeken van een overvloed aan fout-positieve waarschuwingen. Bovendien kan AI organisaties helpen bij het identificeren van ongrijpbare risico's, met name wanneer kwaadwillende actoren detectie proberen te omzeilen. Het is essentieel om de snelheid van computers te gebruiken om deze bedreigingsactoren voor te blijven.

- Databeveiligingsincidenten dynamisch voorkomen: gebruik AI en automatisering om je preventie- en risicobeperkende maatregelen automatisch aan te passen op basis van beoordeelde risico's, waardoor een meer aanpasbare en proactieve databeveiligingsstrategie mogelijk wordt. Wanneer AI-ondersteunde oplossingen risico's detecteren en beoordelen, kunnen geautomatiseerde preventieve controles snel worden ingeschakeld om de data te beschermen, waarbij risicobeperkende controles exact worden toegepast op de gebieden met een hoog risico. In gevallen waarin vroegtijdige indicatoren van de intentie tot data-exfiltratie worden gedetecteerd door gebruikers met een hoog risico, kunnen organisaties bijvoorbeeld strengere beleidsregels voor Data Loss Prevention (DLP) toepassen en potentiële beveiligingsincidenten proactief voorblijven.

We hopen dat je de inzichten en aanbevelingen in dit rapport nuttig vindt om je databeveiliging te verbeteren en je organisatie sterker te maken tegen veranderende risico's.

Ga voor meer informatie over Microsoft Data Security naar https://aka.ms/DataSecurityNews

Gedetailleerde onderzoeksdoelstellingen, methodologie en werving van publiek

De doelstellingen van het onderzoek waren onder andere:

1. Het databeveiligingslandschap begrijpen, inclusief prioriteiten, mindsets en uitdagingen
2. De oorzaak en het gevolg van databeveiligingsincidenten in kaart brengen en acties identificeren die databeveiligingsteams kunnen nemen om de databeveiligingsstatus te verbeteren
3. De toekomst van databeveiliging verkennen, waaronder opkomende strategieën en innovaties rond het gebruik van AI voor databeveiliging

De methode was:

Van 28 juli tot 9 augustus 2023 werd een 15 minuten durende multinationale online-enquête gehouden onder 822 besluitvormers op het gebied van databeveiliging.

De vragen concentreerden zich op het landschap van databeveiliging, hoe teams voor databeveiliging hun middelen, incidenten met databeveiliging en de houding ten opzichte van en het gebruik van kunstmatige intelligentie (AI) voor databeveiliging toewijzen.

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

CISO en aangrenzende besluitvormers (C-2 en hoger) met bevoegdheid over databeveiliging

Werken bij Enterprise-organisaties (500+ werknemers; verschillende groottes)

Mix van gereguleerde en niet-gereguleerde sectoren (geen onderwijs, overheid of non-profit)

Van de 822 ondervraagde besluitvormers op het gebied van databeveiliging die het onderzoek afrondden per land:

VS	329
Verenigd Koninkrijk	322
Australië	171