Microsoft Security

Datasikkerhedsindeks

Tendenser, indsigter og strategier til at beskytte dine data og navigere i generativ AI

2024-rapport

Forord

Når vi begiver os ud på vores andet år inden for forskning i det foranderlige datasikkerhedslandskab, oplever vi udfordringer og muligheder, som aldrig har været større. I det forløbne år er alvorsgraden af datasikkerhedshændelser steget. I denne datacentrerede ære udvikles strategierne og værktøjerne, der bruges til at beskytte data, i et hastigt tempo.

I år udforsker vi en ny frontlinje: betydningen og virkningen af generativ AI på datasikkerhedsstrategier.

AI skaber bølger rundt omkring i verden med hidtil usete muligheder for at opnå mere innovation og større effektivitet. Men med dette enorme potentiale følger også datasikkerhedsrisici, og organisationer er bekymrede for datasikkerhedsrisici, og hvordan det kan forme ansvarsområderne for datasikkerhedsteams. Vi ser AI som en accelerator for organisationer, der kan styrke de grundlæggende datasikkerhedspraksisser, så organisationerne kan forberede sig på at minimere konsekvenserne af overdeling og datalækager og skabe processer til sikker implementering af AI. På den anden side kan AI også hjælpe organisationer med at forbedre deres datasikkerhedspraksisser ved at identificere skjulte risici og mangler i beskyttelsen, anbefale beskyttelsespolitikker samt hjælpe med hurtigere at undersøge og afhjælpe sikkerhedshændelser.

Målet med vores forskning er at give datasikkerhedsledere handlingsrettede indsigter og vejledning, der kan hjælpe deres teams med trygt at tilpasse deres datasikkerhedsstrategi til effektivt at beskytte brugen af AI og integrere AI i deres datasikkerhedsstrategier. Selvom AI er bemærkelsesværdig i både rækkevidde og potentiale, er det kun den seneste transformationsbølge, der går på tværs af virksomheder, f.eks. hybridarbejde, cloud og mobilitet, som i de seneste år har understreget det tidløse behov for synlighed i deres brug for at afbøde risici og maksimere indflydelse. Med denne viden vil korrekt sikring af de data, der anvendes i AI, samt brug af AI til at forbedre datasikkerhedsforanstaltningerne give mulighed for større produktivitet, robusthed og fleksibilitet, når teams navigerer i fremtidige udfordringer.

Vi inviterer dig til at udforske de seneste resultater og håber, at indsigten vil hjælpe dig med at styrke din datasikkerhed samt inspirere dig til at tage AI til dig og opbygge en omfattende datasikkerhedsstrategi, der giver plads til mere innovation og skaber en mere sikker fremtid for os alle.

Rudra Mitra
Corporate Vice President
Microsoft Data Security and Compliance

Introduktion

Organisationer oplever i gennemsnit 156 datasikkerhedshændelser om året, og derfor er konsekvenserne af disse hændelser et konstant problem for beslutningstagerne inden for datasikkerhed. Der er en god grund til, at: en enkelt hændelse kan medføre enorme økonomiske og omdømmerelaterede skader, især i et trusselslandskab i konstant udvikling, hvor hackere udnytter alle tilgængelige sårbarheder. Dette forstærkes kun af den hurtige implementering af AI, hvor brugere uden tilstrækkelige beskyttelses- og sikkerhedsforanstaltninger ved et uheld eller med skadelig hensigt kan bringe følsomme forretningskritiske data (herunder medarbejder- og kundeoplysninger, immaterielle rettigheder, finansielle prognoser og driftsdata) i fare. I takt med, at organisationer søger nye metoder til at beskytte denne store vifte af følsomme data, har mange beslutningstagere vendt deres opmærksomhed mod den dramatiske stigning i AI.

AI-udfordringen er todelt. Da to tredjedele af organisationerne indrømmer, at deres medarbejdere bruger uautoriserede AI-værktøjer, er det vigtigt at sørge for, at medarbejderne bruger AI-værktøjer på en sikker måde. Samtidig er det muligt at bruge AI som et effektivt værktøj i en sofistikeret datasikkerhedsstrategi.

AI-baserede datasikkerhedsløsninger spiller allerede en afgørende rolle i identificering og reaktion på trusler i realtid. Dette forbedrer den overordnede hastighed og nøjagtighed af datasikkerhedsprogrammer og giver indsigt, der hjælper med at forhindre datasikkerhedshændelser, før de opstår. Organisationer skal håndtere de risici, som AI introducerer. Derudover skal de udnytte dens funktioner til at identificere mønstre, der kan være udfordrende for mennesker at behandle og analysere, med maskinhastighed, og i sidste ende bekæmpe stadig mere sofistikerede cyberangreb.

I 2023 bestilte Microsoft et uafhængigt forskningsagentur, Hypotese, til at foretage en multinational undersøgelse blandt mere end 800 datasikkerhedseksperter og påbegynde initiativet for et datasikkerhedsindeks for bedre at kunne betjene vores partnere og kunder og hjælpe virksomhedsledere med at udvikle deres egne datasikkerhedsstrategier.

I 2024 bygger denne rapport videre på den forudgående forskning med nye indsigter fra en udvidet multinational undersøgelse med mere end 1.300 eksperter inden for datasikkerhed. Selvom dataene giver ensartede indsigter og tendenser på tværs af de markeder, vi undersøgte, afdækker vi ny viden om de nyeste praksisser og tendenser inden for datasikkerhed og AI over hele verden.

hypothesis Microsoft Security

Vigtige resultater

1

Datasikkerhedslandskabet er stadig splittet, og det øger behovet for sammenhængende datasikkerhedsstrategier på tværs af både traditionelle og nye risici i forbindelse med brugen af AI

Organisationer rapporterer om høje niveauer af tilfredshed og tillid til deres datasikkerheds-foranstaltninger. Men alvorsgraden af datasikkerheds-hændelser stiger fortsat, især på grund af de mangler, som organisationer oplever mellem deres nuværende datasikkerhedspolitikker og den øgede brug/introduktion af AI-applikationer. Stillet over for disse udfordringer oplever mange organisationer, at de stadig er afhængige af flere datasikkerhedsværktøjer, og dette kan øge deres overordnede sårbarhed og risiko.

2

Efterhånden som flere og flere af slutbrugerne implementerer AI-apps, udsættes integriteten af organisationernes mest følsomme data for en større risiko, hvilket kræver mere synlighed og nye beskyttelseskontroller

I takt med at AI-værktøjer bliver en stadig større del af det daglige arbejde, stiger organisationernes bekymring over datasikkerhedsrisici. Organisationerne anerkender behovet for at styrke deres forsvar og er indstillet på at forhindre datasikkerhedshændelser forårsaget af AI – men den uautoriserede brug af disse værktøjer understreger behovet for en mere robust synlighed.

3

Beslutningstagerne er optimistiske med hensyn til AI's potentiale til at fremme deres datasikkerhedsindsats

Organisationer investerer aktivt i datasikkerheds værktøjer, der inkorporerer AI til at forbedre registrerings- og reaktionsfunktionerne. AI kan hjælpe med at registrere ubeskyttede data, anbefale beskyttelsespolitikker og hjælpe med at undersøge og afhjælpe datasikkerheds-hændelser hurtigere. Dette giver i sidste ende datasikker-hedsteams mere tid og opmærksomhed til at fokusere på strategisk arbejde. Brugen af AI fremmer også tilliden til og tilfredsheden over organisationernes samlede datasikkerhedsstrategi – især evnen til at reagere hurtigt og præcist på hændelser.

1

Datasikkerhedslandskabet er stadig splittet, og det øger behovet for sammenhængende datasikkerhedsstrategier på tværs af både traditionelle og nye risici i forbindelse med brugen af AI

Der er en uoverens-stemmelse mellem beslutningstagerens tillid til deres datasikkerhedsprak-sis og det reelle beskyttelsesniveau for deres data

Som rapporteret i 2023 er langt de fleste beslutningstagere trygge ved deres datasikkerhedsstrategier, og 74 % rapporterer, at de er tilfredse med deres nuværende løsninger i 2024. De føler sig trygge ved deres muligheder for at spore og administrere følsomme data: 88 % mener, at de ved, hvor de fleste af deres kritiske oplysninger findes, og 85 % udtaler, at deres data er korrekt klassificeret og mærket. De fleste har også tillid til deres forsvarskontroller. 79 % har tillid til, at de kan forhindre dataudfiltrering, og 76 % beskriver deres tilgang som proaktiv i stedet for reaktiv.

Men deres tillid sættes på prøve, da alvorsgraden af hændelser fortsætter med at vokse. **Det gennemsnitlige antal årlige datasikkerhedshændelser er stadig højt. Det har ændret sig fra 166 i 2023 til 156 i 2024, og alvorsgraden af disse hændelser er steget fra 20 % alvorlige hændelser i 2023 til 27 % i 2024.**

156

datasikkerhedshændelser

27 %

af hændelserne betragtes som alvorlige (stigning fra 20 % i 2023)

63 %

advarsler gennemgås pr. dag

"Placeringen af en softwareplatform, hvor dens data er lagret, og hvem der får adgang til disse data, har gjort datasikkerheden og administrationen af vores AI-værktøjer og -leverandører mere kompliceret. Vi har mere end 100 års data, som vi skal beskytte og holde styr på i overensstemmelse med lovkrav i alle de jurisdiktioner, vi opererer i", siger en Senior Manager for Information Governance hos en stor producent af tungt udstyr.

Stigningen i alvorsgraden af datasikkerhedshændelser har derfor ført til en stigning i mængden af advarsler. **Organisationer får i gennemsnit 66 advarsler om dagen, en stigning fra 52 i 2023.** Dette antal varierer betydeligt efter organisationsstørrelse, hvor mellemstore virksomheder (500-999-medarbejdere) og store virksomheder (1.000-4.999 medarbejdere) i gennemsnit får 56 advarsler, og ekstra store virksomheder (5.000+ medarbejdere) i gennemsnit får 80 advarsler om dagen.

I betragtning af den store mængde af datasikkerhedsadvarsler er det ikke nogen overraskelse, at de fleste organisationer ganske enkelt ikke kan følge med. Datasikkerhedsteams gennemgår i gennemsnit 63 % af de daglige advarsler. 35 procent af disse advarsler viser sig at være falske positiver. Denne uoverensstemmelse mellem den opfattede kontrol og den operationelle virkelighed medfører, at datasikkerhedsteams overvældes – de forsøger at vurdere, om de har den rette beskyttelse, eller hvordan den skal finjusteres, samtidig med at de er bekymrede for, at potentielt alvorlige hændelser kan glide gennem sprækkerne.

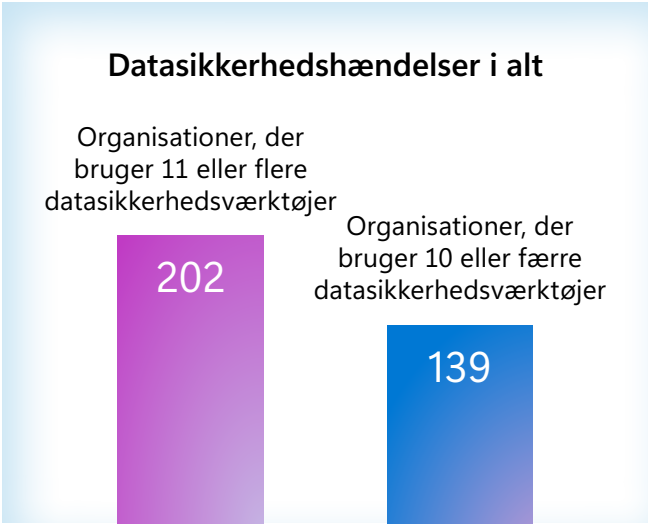
For at bekæmpe traditionelle og nye datarisici i forbindelse med brugen af AI-værktøjer er der et stigende behov for mere robuste og sammenhængende datasikkerhedsstrategier

På trods af det stigende antal tilgængelige værktøjer anerkender mange beslutningstagere fortsat, at flere ikke altid er bedre. Faktisk nævner 21 % manglen på konsolideret og omfattende synlighed (og fælles forståelse af risici) forårsaget af forskellige værktøjer som deres største udfordring/risiko.[1]

De fleste beslutningstagere (82 %) er enige om, at en omfattende, fuldt integreret platform er bedre end at skulle administrere flere isolerede værktøjer. **I gennemsnit jonglerer de med 12 forskellige datasikkerhedsløsninger, og det skaber en kompleksitet, der øger deres sårbarhed.** Dette gælder især for de største organisationer: I gennemsnit bruger mellemstore virksomheder 9 værktøjer, store virksomheder bruger 11, og ekstra store virksomheder bruger 14 værktøjer.

Dataene viser en stærk korrelation mellem antallet af brugte datasikkerhedsværktøjer og hyppigheden af datasikkerhedshændelser. Mellemstore og store virksomheder rapporterer i gennemsnit 89 hændelser om året, mens ekstra store virksomheder står over for svimlende 248 hændelser hvert år. Denne forskel fremhæver den store risiko, som større organisationer står over for, selvom de udtrykker stor tillid til deres datasikkerhedsforanstaltninger.

I 2024 oplevede organisationer, der bruger flere datasikkerhedsværktøjer (11 eller flere), i gennemsnit 202 datasikkerhedshændelser, sammenlignet med 139 hændelser for dem, der bruger 10 eller færre værktøjer.



Fragmenterede løsninger gør det vanskeligt at forstå datasikkerhedsniveauet, da data er isolerede, og uensartede arbejdsprocesser kan begrænse omfattende indsigt i potentielle risici. Når værktøjerne ikke integreres, skal datasikkerhedsteams bygge processer for at korrelere data og skabe et sammenhængende overblik over risici. Dette kan føre til blinde vinkler og gøre det udfordrende at opdage og afbøde risici på en effektiv måde.

En voksende bekymring er stigningen i antallet af datasikkerhedshændelser fra brugen af AI-applikationer, som næsten er fordoblet fra 27 % i 2023 til 40 % i 2024. Denne stigning i antallet af hændelser skyldes en kraftigere stigning i antallet af malware- og ransomware-angreb – en stigning til 59 % fra 50 % i 2023. Angreb fra brugen af AI-apps eksponerer ikke kun følsomme data, men kompromitterer også selve AI-systemerne, hvilket yderligere komplicerer et allerede fragmenteret datasikkerhedslandskab. Kort sagt er der et stadig mere presserende behov for stærkere og mere sammenhængende datasikkerhedsstrategier, der kan håndtere både de traditionelle og nye risici, der er forbundet med brugen af AI-værktøjer.

1. Undersøgelse fra september 2024 blandt beslutningstagere inden for styring, overensstemmelse og beskyttelse af personlige oplysninger, bestilt af Microsoft fra MDC Research

Vejen frem

Stigningen i alvorsgraden af datasikkerhedshændelser belyser en mulighed for, at AI kan være en hjælp. Organisationer, der er på forkant, implementerer AI-drevet datasikkerhed til at hjælpe med at prioritere hændelser, automatisere dataklassificering og identificere metoder til at finjustere de nuværende beskyttelsespolitikker. AI kan automatisk syntetisere den potentielle alvorsgrad af hændelsesadvarsler, og det giver datasikkerhedsteams handlingsrettet indsigt, så de kan reagere hurtigt og reducere den tid, der bruges på falske positiver. Dette strømliner arbejdsprocesser og gør det muligt for datasikkerhedsteams at fokusere på mere strategiske forbedringer af datasikkerheden og proaktive foranstaltninger.

2

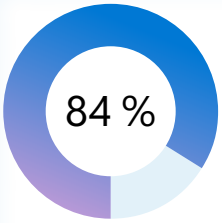
Efterhånden som flere og flere af slutbrugerne implementerer AI-apps, udsættes integriteten af organisationernes mest følsomme data for en større risiko, hvilket kræver mere synlighed og nye beskyttelseskontroller

AI er hurtigt ved at blive vigtigt i det daglige arbejde – og organisationer skal byde denne ny virkelighed velkommen og aktivt tilpasse sig

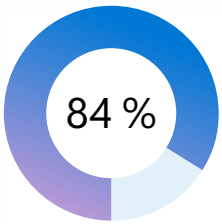
Medarbejdernes hurtige implementering af AI-værktøjer har skabt store ændringer i organisationernes tilgang til datasikkerhed. Samtidig med at AI transformerer produktiviteten og arbejdsprocesserne, kan det ligesom enhver anden ny teknologi også forstærke eksisterende risici eller introducere nye risici, der kræver en anden tilgang til at beskytte følsomme oplysninger. Som følge heraf søger virksomheder stadig efter fodfæste i et hurtigt skiftende landskab. En Director of Engineering and Analytics inden for transport udtaler, "vi overvåger data mere omhyggeligt på AI-siden. Det har været vanskeligt at skabe balance mellem produktivitet og sikkerhed, præcision og beskyttelse af personlige oplysninger."

Tillid til sikring af medarbejdernes brug af AI er stadig blandet. Et flertal (84 %) vil gerne have større tillid til administration og registrering af datainput. Selvom 22 % af organisationerne føler sig ekstremt trygge ved deres evne til at beskytte data, er de fleste (59 %) kun "meget sikre", og det indikerer, at der er plads til forbedringer. De fleste virksomheder (86 %) anerkender, at de gerne vil føle sig mere trygge ved administration og registrering af data, der er genereret af AI-værktøjer.

Efterhånden som AI bliver mere afgørende for daglig produktivitet, har brugen af AI-apps også øget bekymringerne omkring datasikkerhedshændelser. **Næsten en tredjedel (31 %) af organisationerne forudser en stigning i mængden af datasikkerhedshændelser på grund af medarbejdernes brug af AI, og 84 % indrømmer, at de er nødt til at gøre mere for at beskytte mod disse risici.** Sådanne bekymringer er især store i de største organisationer: Mens 26 % mellemstore virksomheder forventer at opleve en stigning i antallet af AI-relaterede datasikkerhedshændelser, og 29 % store virksomheder forventer en stigning, forudser en betydeligt større gruppe, der repræsenterer 36 % af de ekstra store virksomheder, en stigning.



ønsker at føle sig mere trygge ved at administrere og registrere datainput i AI-apps og -værktøjer



er enige i, at de skal gøre mere for at beskytte mod risikabel brug af AI-apps og -værktøjer blandt medarbejdere

Uautoriseret brug af AI er udbredt

40 % rapporterer, at deres AI-apps allerede har været udsat for sikkerhedsbrud eller er blevet kompromitteret i en datasikkerhedshændelse. Igen er dette tal højere blandt større organisationer: mellemstore virksomheder melder om en hændelsesfrekvens på 36 %, store virksomheder 38 %, og ekstra store virksomheder har oplevet flest hændelser med 44 %.

Uautoriseret brug af AI forekommer ofte, når medarbejderne logger på med personlige legitimationsoplysninger eller bruger personlige enheder til arbejdsrelaterede opgaver. **I gennemsnit indrømmer 65 % af organisationerne, at deres medarbejdere bruger uautoriserede AI-værktøjer.** Måder, som medarbejdere bruger uautoriserede AI-værktøjer på, omfatter:

- 53 %, der logger på med personlige legitimationsoplysninger i arbejdsøjemed
- 48 %, der bruger deres personlige enhed, når de bruger AI til arbejde
- 47 %, der bruger deres arbejdslegitimationsoplysninger for at bruge AI til personlige formål

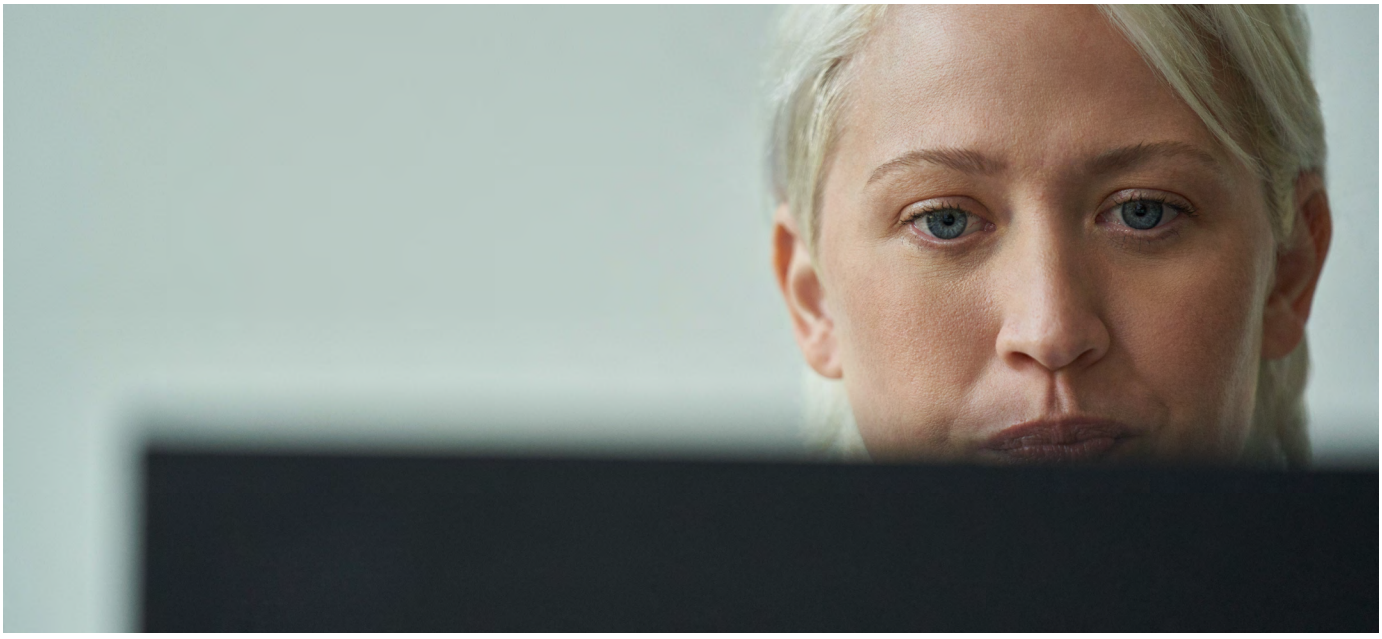
Halvdelen af alle organisationerne siger, at de er bekymrede over den manglende kontrol til at opdage og afbøde risici, når medarbejderne bruger AI-apps på usikre måder. Dette tal varierer efter virksomhedens størrelse, og 43 % af mellemstore virksomheder, 50 % af store virksomheder og 54 % af de ekstra store virksomheder udtrykker bekymring over deres evne til at håndtere disse risici.

I betragtning af den øgede brug af AI er det nødvendigt med flere datasikkerhedskontroller

Organisationerne anerkender, at i takt med at AI bliver mere og mere integreret i den daglige drift, stiger behovet for stærkere beskyttelse. **Mens 96 % af virksomhederne har bekymringer om medarbejdernes brug af disse værktøjer, er næsten lige så mange villige til at investere i løsninger for at overvinde deres bekymringer.**

"Det store fokus er, hvordan man kan holde sig på forkant med AI. Fokus på sikkerheden handler om at reducere størrelsen af data og overvåge data mere omhyggeligt. På AI-siden er der brug for flere data for at gøre modellerne mere repræsentative til at identificere bias. Så hvordan afstemmer vi dette?", siger en Director of Engineering, Architecture, and Analytics inden for transport. Langt de fleste beslutningstagere (87 %) er villige til at bruge både tid og penge på at undervise medarbejdere i sikre fremgangsmåder for brug af AI-værktøjer. **Dette skyldes, at det i henhold til 85 % er afgørende for konkurrenceevnen, at medarbejderne bruger disse værktøjer.**

Næsten alle organisationer (93 %) er i gang med at udvikle eller implementere kontroller omkring AI-brug, men mange er stadig i de tidlige faser. Kun 39 % har implementeret datasikkerhedskontroller for AI fuldt ud, mens 24 % har udviklet politikker, men er endnu ikke begyndt at anvende dem. En vicedirektør inden for hotel- og restaurationsbranchen udtaler, "Vi er nødt til at tilpasse kontrollerne til AI, men i mellemtiden tager vi brugen af AI til os. Det gør livet nemmere og hjælper os med at være mere effektive."



Mens organisationer tager skridt til at beskytte følsomme data mod misbrug i AI-apps, er der et tydeligt behov for mere omfattende kontroller. I øjeblikket fokuserer 43 % af virksomhederne på at forhindre, at følsomme data uploades til AI-apps, mens yderligere 42 % registrerer alle aktiviteter og alt indhold i disse apps med henblik på potentielle undersøgelser eller hændelsesrespons. Tilsvarende blokerer 42 % brugeradgang til uautoriserede værktøjer, og en tilsvarende procentdel investerer i undervisning af medarbejdere i sikker brug af AI.

Virksomheder med medarbejdere, der er involveret i uautoriseret brug af AI, har større behov for visse typer kontroller. **Blandt brugere med uautoriseret brug af AI har 42 % brug for kontroller til at identificere risikable brugere baseret på AI-forespørgsler, sammenlignet med 30 % for dem, hvor der ikke forekommer uautoriseret brug. Desuden har 40 % af de organisationer, der beskæftiger sig med uautoriseret brug af AI, brug for kontroller til at administrere livscyklussen for data (såsom opbevarings- og sletningsprotokoller), sammenlignet med 27 % af virksomheder uden dette problem.**

De 5 vigtigste datasikkerhedskontroller, der er nødvendige for AI

Forhindr, at følsomme data uploades til AI	43 %
Logfør alle aktiviteter og alt indhold i AI-værktøjer med henblik på potentielle undersøgelser eller hændelsesrespons	42 %
Bloker brugeradgang til uautoriserede AI-værktøjer	42 %
Undervis medarbejderne i sikker brug af AI-værktøjer	42 %
Identificer risikable brugere baseret på AI-forespørgsler	41 %

Vejen frem

For at opretholde et effektivt datasikkerhedsniveau har teams brug for et komplet sæt kontroller til at opdage, beskytte og styre deres data i AI-apps. Her er tre vigtige strategier, som teams kan bruge:

Skab større synlighed af brugen af AI-apps og de data, der flyder igennem dem: Benyt datasikkerhedsværktøjer, der kan registrere brugen af AI-apps. Disse værktøjer giver indsigt i en omfattende liste over anvendte AI-apps sammen med deres risikoprofiler, herunder oplysninger som understøttede datasikkerhedskontroller og overensstemmelse med forordninger. Brug værktøjer, der kan give ensartet klassificering af følsomme data i AI-interaktioner og vise tendenser for, hvordan data flyder gennem AI-apps.

Udvikl og håndhæv politikker: Opret politikker, der er baseret på den indsigt, der opnås fra analysen. Disse politikker kan omfatte retningslinjer for godkendte AI-apps og procedurer til blokering eller begrænsning af medarbejdernes brug af ikke-godkendte apps. Selv i godkendte AI-apps kan du oprette detaljerede politikker, så ikke-følsomme data kan flyde frit, samtidig med at brugen af følsomme og forretningskritiske data begrænses. Dette kan omfatte blokering af visse handlinger for at beskytte datasikkerheden, f.eks. indsættelse af følsomme data i browserbaserede AI-værktøjer.

Vurder regelmæssigt risici, og juster politikker: Generér regelmæssigt rapporter, der viser risikoniveauerne for de anvendte AI-apps, tendenser for, hvordan følsomme data flyder gennem disse apps, samt brugeraktiviteten omkring disse apps. Dette er en hjælp til at vurdere det overordnede risikolandskab og træffe informerede beslutninger om de mest relevante datasikkerhedspolitikker.

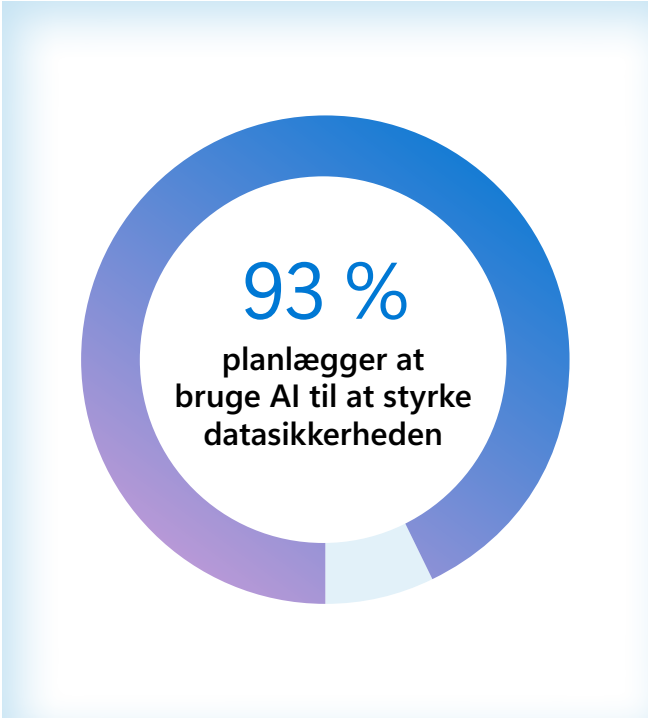
3

Beslutningstagerne er optimistiske med hensyn til AI's potentiale til at fremme deres datasikkerhedsindsats

Undersøgelser af datasikkerhed er stærkt afhængige af AI

Størstedelen (88 %) af organisationerne investerer allerede i AI for at forbedre deres registrerings- og responsindsats – identifikation af følsomme data, registrering af unormal aktivitet og automatisk beskyttelse af data i risikozonen. **77 % af organisationerne mener, at AI vil fremskynde disse processer, og 76 % mener, at det vil forbedre nøjagtigheden af deres registrerings- og responsstrategier.**

Mens 73 % af beslutningstagerne giver udtryk for bekymringer for at bruge AI til at styrke datasikkerheden, siger 50 %, at det ikke har hindret dem i at bruge AI til at styrke datasikkerheden, og kun 23 % siger, at det har holdt dem tilbage. Samlet set planlægger hele 93 % i det mindste at bruge AI til at styrke datasikkerheden på trods af deres bekymringer.

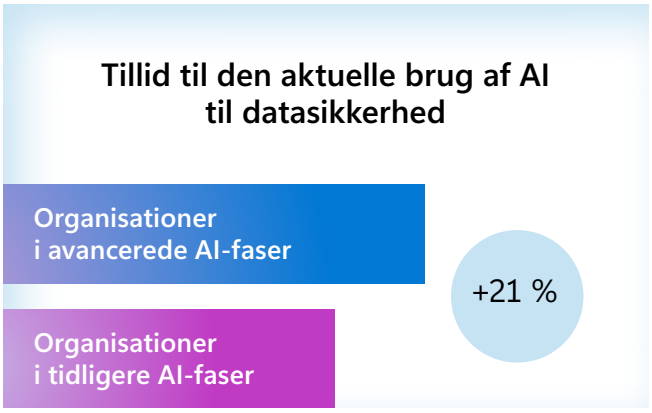


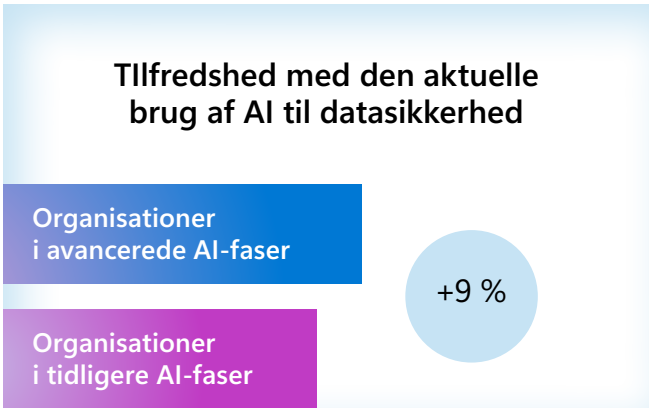
Brug af AI til at styrke datasikkerhed øger synlighed, tillid og tilfredshed

En af de vigtigste fordele ved at bruge AI til at styrke datasikkerheden er dens evne til at øge synligheden på tværs af systemer, hvilket afbøder et fremtrædende problem, som beslutningstagerne har med at vide, hvor data lagres, og hvordan de klassificeres (20 %).[1] 88 % af beslutningstagerne inden for datasikkerhed mener, at integrationen af AI i datasikkerhedsløsninger vil give teams større indsigt, og dette vil gøre det muligt for organisationer at behandle og analysere langt flere data, end de ellers ville kunne. Mellemstore organisationer fokuserer først og fremmest på at reducere kortsigtede risici, f.eks. minimering af menneskelige fejl i deres datasikkerhedsprocesser. Rent faktisk prioriterer 43 % af de mellemstore virksomheder at reducere risici, der er forårsaget af menneskelige fejl, i sammenligning med kun 37 % af de ekstra store virksomheder.

I modsætning hertil er større virksomheder mere avancerede i deres tilgang og lægger større vægt på langsigtede risici og behovet for tilpasning. Med det højere niveau af raffinement får datasikkerhedsteams mulighed for bedre at tilpasse sig skiftende risici, hvilket er en topprioritet for 49 % af de ekstra store virksomheder, sammenlignet med 43 % af de mellemstore organisationer.

Generelt rapporterer organisationer, der er længere fremme med at bruge AI til at styrke datasikkerheden, meget højere niveauer af tillid og tilfredshed med deres datasikkerhedsstrategier. **Blandt de virksomheder, der er i de avancerede faser af AI-implementering, føler 90 % sig ekstremt eller meget trygge ved deres brug af AI til styrke datasikkerheden, sammenlignet med 69 % i de tidligere faser. Tilsvarende giver 76 % af organisationerne med avanceret brug af AI udtryk for tilfredshed med deres datasikkerhedsløsninger, mens kun 67 % af organisationerne, der er i de tidligere faser, er tilfredse.**





1. En undersøgelse fra september 2024 blandt beslutningstagere inden for datasikkerhed, styring, overensstemmelse og beskyttelse af personlige oplysninger, bestilt af Microsoft og foretaget af MDC Research

Organisationer reducerer antallet af datasikkerhedshændelser og forbedrer administration af advarsler ved hjælp af AI

Organisationer, der bruger AI til at styrke deres datasikkerhedsaktiviteter, melder om væsentligt færre advarsler. **De, der har implementeret AI-drevne datasikkerhedsværktøjer, modtager gennemsnitligt 47 advarsler pr. dag, sammenlignet med 79 advarsler for de, der ikke har. Og de, der bruger AI, kan gennemse 66 % af deres advarsler pr. dag, mens organisationer, der ikke bruger AI, kun kan gennemse 60 %.**

Endvidere er de, der bruger AI til at styrke datasikkerheden, mere tilbøjelige til også at bruge AI til at afbøde risici (56 % sammenlignet med 26 %). Reduktionen i antallet af advarsler sammen med den øgede evne til at afbøde dem ved hjælp af AI ser ud til at have haft en dramatisk indvirkning på det samlede antal datasikkerhedshændelser. Organisationer, der har implementeret AI for at styrke datasikkerheden, oplever en reduktion på 65 % i datasikkerhedshændelser sammenlignet med dem, der ikke bruger AI til at styrke datasikkerheden.

AI forventes at have den største indflydelse på respons

Når det drejer sig om registrering, forventer 33 % af beslutningstagerne, at AI kan hjælpe med at identificere unormal aktivitet, mens 23 % mener, at AI kan hjælpe med til at undersøge potentielle datasikkerhedshændelser. Yderligere 22 % ser muligheden for, at AI kan give anbefalinger til bedre sikring af deres datamiljøer.

Beslutningstagerne forventer dog, at AI vil have den største indflydelse, når det handler om reaktionen på hændelser. 34 % mener, at AI automatisk kan blokere ureglementeret deling af følsomme data, og 32 % siger, at AI vil beskytte data i fare. Yderligere 26 % mener, at AI bidrager til at afhjælpe datasikkerhedsrisici og anvende passende kontroller, mens lige så mange forventer, at AI automatisk gør opmærksom på risikabel brugeradfærd.

Vejen frem

Integration af AI i datasikkerhedsløsninger kan hjælpe ved at tilbyde teams realtidsvejledning, opsummeringsfunktioner og understøttelse af naturligt sprog for at fremhæve områder, der ellers kunne være overset. Dette kan også fremskynde undersøgelse og styrke ekspertisen i datasikkerhedsteams. Her kan du se, hvordan disse funktioner kan gøre en forskel:

Opsummering af advarsler: Undersøgelser kan være overvældende på grund af den store mængde kilder, der skal analyseres, og mangfoldigheden af politikregler. Ved at integrere AI i forebyggelse af datatab (DLP) og håndtering af insiderrisici (IRM) kan teams hurtigt få en advarselsoversigt, herunder kilden, politikregler og brugerrisikoindsigter, så de kan forstå, hvilke følsomme data der blev kompromitteret og den tilknyttede brugerrisiko.

Kontekstafhængig kommunikation: Organisationer skal overholde lovkrav omkring virksomhedskommunikation, hvilket ofte kan kræve en omfattende gennemgang af overtrædelser. AI kan hjælpe datasikkerhedsteams med at vurdere indhold i forhold til bestemmelser og virksomhedspolitikker for at fremhæve kommunikation med høj risiko, der kan føre til en datasikkerhedshændelse.

Naturligt sprog i søgeordsforespørgsel: Søgning i forbindelse med undersøgelser kan være et komplekst og tidskrævende workflow, hvilket ofte kræver brug af et forespørgselssprog for søgeord. Med AI bliver det muligt for datasikkerhedsteams at indsætte søgeprompter i et naturligt sprog for at strømline søgningens start og give mulighed for mere avancerede undersøgelser.

Endelige anbefalinger

1 Beskyt dig mod datasikkerhedshændelser ved at implementere en integreret platform

Implementering af en fuldt integreret datasikkerhedsplatform tilbyder en mere sikker og strømlinet strategi i et landskab, der er i konstant udvikling. Dette reducerer kompleksiteten og øger synligheden, samtidig med at beskyttelsen forbedres. En integreret tilgang kan hjælpe organisationer med at forbedre administrationen af datasikkerhed ved at centralisere datasikkerhedskontroller og give ensartet synlighed på tværs af data, brugere og aktiviteter og dermed styrke og strømline registrering og beskyttelse mod datarisici. Da 82 % af organisationerne er enige om, at en integreret platform er den bedste løsning, er det ikke kun en fordel at gå i gang med konsolidering – det er bydende nødvendigt.

2 Optimer synligheden af den interne brug af AI for at vurdere de nødvendige kontroller for medarbejdernes brug af AI, der ikke påvirker produktiviteten

I takt med at AI bliver mere almindelig på arbejdspladsen, kan det forstærke de eksisterende risici og introducere nye risici. Organisationer indrømmer, at de bliver nødt til at gøre mere for at beskytte mod usikker brug af AI. Anvendelse af indbyggede kontroller og synlighed i AI-apps er af afgørende vigtighed for at opretholde datasikkerheden uden at afbryde produktiviteten. Undervisning af medarbejdere i sikker brug af AI kan hjælpe organisationer med at minimere risikabel adfærd, samtidig med at det sikrer, at teams fortsætter med at drage fordel af disse effektive værktøjer.

3 Opgrader din datasikkerhedsstrategi med hjælp fra AI

AI gør det muligt for datasikkerhedsteams at fokusere på mere strategiske initiativer i stedet for at reagere på konstante trusler og en stor mængde advarsler. Virksomheder, der er i de avancerede faser af AI-implementeringen, er mere trygge og tilfredse med deres datasikkerhedsløsninger end virksomheder, der lige er startet. Ved at implementere AI som en del af en omfattende datasikkerhedsstrategi kan organisationer få bedre synlighed og styrke deres evne til at registrere og reagere på risici, hvilket i sidste ende styrker deres overordnede datasikkerhedsforhold.

Undersøgelsesmål

Målene for undersøgelsen omfattede:

1. Få indblik i datasikkerhedslandskabet, herunder prioriteter og tankegange, udfordringer samt årsagen og konsekvenserne af datasikkerhedshændelser.
2. Udforske datasikkerhedens fremtid, herunder hvilke strategier og innovationer, der er på vej, samt hvordan organisationer har planer om at investere i fremtiden.
3. Afdæk AI's rolle i forbedring af datasikkerhed og den rolle, AI spiller i beskyttelse af data.

Metode

En 20-minutters multinational onlineundersøgelse blev gennemført mellem den 5. til 23. august 2024 blandt 1.376 beslutningstagere inden for datasikkerhed.

Spørgsmålene var centreret omkring datasikkerhedslandskabet og -hændelser i sammenligning med 2023. Undersøgelsen i år indeholdt desuden spørgsmål om sikring af medarbejdernes brug af AI og brugen af AI til at styrke datasikkerhed.

Rekruttering af målgruppe

For at opfylde screeningkriterierne skal beslutningstagerne inden for datasikkerhed være:

- CISO og tilsvarende beslutningstagere (C-2 og derover) med ansvar for datasikkerhed
- Arbejde i virksomhedsorganisationer (i forskellige størrelser med over 500 medarbejdere)
- Blanding af regulerede og ikke-regulerede brancher (uden uddannelse, offentlige myndigheder, eller non-profit)

Af de 1.376 adspurgte beslutningstagere inden for datasikkerhed i undersøgelsen var antallet af deltagere efter land følgende:

- USA: 302
- Storbritannien: 305
- Indien: 301
- Brasilien: 158
- Frankrig: 156
- Australien: 154

hypothesis Microsoft Security