Microsoft

hypothesis

Datasikkerhedsindeks

Tendenser, indsigt og
strategier til at sikre data

Forord

I en tid, der defineres af en stor mængde data, står det mere og mere klart, at dataene er selve livsnerven i en organisation. De mange data, der genereres og bruges af organisationer, understøtter vigtige driftsaktiviteter, informerer strategisk og global beslutningstagning og skaber nye fremtidsmuligheder for organisationerne. Data er ikke blot en ressource – de er selve hjertet i moderne virksomheder.

Men denne øgede afhængighed af data viser også de barske realiteter, at sårbarheder i de digitale skygger er reelle og hurtigt voksende. Cybertrusler, brud på datasikkerheden og insider-risikohændelser er ikke længere sjældne tilfælde – de er overalt og eskalerer, hvilket udgør en risiko for organisationer, der er afhængige af data. Vi foretog for nylig en undersøgelse blandt beslutningstagere, hvoraf 89 % sagde, at de betragter deres datasikkerhedsniveau som afgørende for deres generelle succes.

I dette whitepaper ser vi nærmere på denne grundlæggende nødvendighed: beskyttelse af din organisations data. Mit team og jeg er glade for at dele vores resultater med dig – og håber på at starte en dialog om, hvordan vi i fællesskab kan styrke datasikkerheden. Vores erfaringer viser, at datasikkerhed har nået et kritisk punkt. Selvom beslutningstagere inden for sikkerhed er enige om, at det er vigtigt for at sikre deres data – og de fleste siger, at de er trygge ved, hvad de foretager sig – oplever de samtidig et væld af datasikkerhedshændelser og -udfordringer. Og 80 % af de ledere, vi talte med, erkender, at en integreret tilgang – med den bedste samlede pakkeløsning – er bedre end punktløsninger, men de fleste virksomheder bruger stadig et fragmenteret multiværktøjssystem til at beskytte deres data – hvilket ofte resulterer i flere sikkerhedshændelser i stedet for færre.

Du er meget velkommen til at læse og dele denne seneste rapport og behandle den som begyndelsen på nye samtaler med vores teams om, hvordan vi bedst kan hjælpe med at sikre vores kollektive fremtid.

Rudra Mitra
Corporate Vice President
Microsoft Data Security and Compliance

Introduktion

Forebyggelse af brud på datasikkerheden og andre sikkerhedshændelser er fortsat en konstant bekymring for beslutningstagerne inden for sikkerhed og risici – og en hjørnesten i ethvert cybersikkerhedsprogram – fordi et enkelt brud på datasikkerheden kan medføre betydelige omdømmemæssige og økonomiske konsekvenser. Organisationer har til opgave at beskytte en lang række følsomme data – herunder medarbejder- og kundeoplysninger, immaterielle rettigheder, økonomiprognoser og driftsdata.

Med henblik på at forstå de nuværende praksis og tendenser inden for datasikkerhed samt identificere, hvordan organisationer kan forbedre datasikkerheden, har Microsoft lavet en aftale med et uafhængigt undersøgelsesbureau, Hypothesis Group, om at foretage en multinational undersøgelse blandt mere end 800 datasikkerhedseksperter. Denne rapport præsenterer fem vigtige resultater fra undersøgelsen, herunder tendenser, indsigt og strategier til at sikre data.

Vigtige resultater

1

Beslutningstagere mener, at de er beskyttet, men virkeligheden fortæller noget andet.

De fleste beslutningstagere siger, at de er tilfredse med og trygge ved deres datasikkerhedsløsninger, men de oplever stadig i gennemsnit 59 datasikkerhedshændelser om året med dyre konsekvenser.

2

Flere værktøjer på hånden er ikke lig med større datasikkerhed eller effektivitet – det er lige modsat.

80 % af beslutningstagere er enige om, at omfattende, integrerede løsninger er bedre end manuelle kvalitetsløsninger – og alligevel er organisationers tilgang til værktøjer fortsat fragmenteret med anvendelse af over 10 datasikkerhedsværktøjer i snit. Men dem, der har flest værktøjer, oplever også flere datasikkerhedshændelser. Derfor tyder det på, at jo større værktøjsspredningen er, jo svagere er sikkerheden.

3

Organisationer oplever fortsat stress pga. eksterne og interne datasikkerhedshændelser, især inden for virksomhedsdata.

50 % af de adspurgte organisationer har oplevet et ransomware- eller malwareangreb inden for det seneste år – og mange beslutningstagere tror ikke, at deres organisation er fuldt ud parat til at forebygge og tackle fremtidige angreb. Internt er ondsindede insidere en af de største bekymringer. Derudover er organisationer stærkt bekymrede over sårbarheden af deres virksomhedsdata. Dette understreger igen behovet for en sikkerhedsplatform, der håndterer risici på en omfattende måde.

Vigtige resultater

4

Organisationer har brug for skyen og AI til at skabe digital transformation – men det er også de mest sårbare dataplaceringer.

Cloud-applikationer og AI-teknologi er blevet afgørende for organisationers samarbejde og produktivitet – men denne udvikling har også skabt mere dynamiske og mangesidede risici. Efterhånden som organisationer tager AI til sig, bliver det afgørende at styrke datasikkerheden for at muliggøre ansvarlig og sikker brug.

5

Automatisering og AI er en lovende vej fremad mod større beskyttelse.

Organisationer ønsker, at deres teams bruger mindre tid på opdagelse og mere tid på forebyggelse af sårbarheder. Automatisering kan give teams mulighed for at fokusere mere på proaktive tiltag, mens brugen af AI til datasikkerhed hjælper organisationer med at være mere strategiske og blive klogere på fremtidige trusler.

1

Beslutningstagere mener, at de er beskyttet, men virkeligheden fortæller noget andet.

Beslutningstagere mener, at de er beskyttet, men virkeligheden fortæller noget andet.

På overfladen udstråler beslutningstagere en høj grad af tillid til og tilfredshed med deres datasikkerhedsløsninger. De fleste organisationer er enige om, at deres datasikkerhedskontroller er tilstrækkelige til at forhindre brud på datasikkerheden. De føler, at de ved, hvor de fleste af deres data findes, og at de kan opdage de fleste risici mht. data.

Samtidig oplever organisationer fortsat en betydelig mængde af datasikkerhedshændelser – i gennemsnit 59 inden for de seneste 12 måneder, og en femtedel af dem betragtes som "alvorlige". Konsekvensen af disse hændelser er udbredt, da organisationer anslår, at de samlede økonomiske omkostninger ved deres mest alvorlige datasikkerhedshændelse i gennemsnit er ca. 244.000 USD – hvilket betyder, at årlige hændelser kan koste op til 15 millioner USD. Ud over disse omkostninger siger fire ud af 10 beslutningstagere også, at driftsomkostningerne til genoprettelse efter en datasikkerhedshændelse og mistet indtjening som følge af skade på omdømmet er en stor bekymring.

Derudover står 92 % over for udfordringer – primært på områder som omkostninger, integration og tid til at implementere – hvilket hæmmer deres evne til at investere yderligere i datasikkerhed og understreger behovet for mere budgetvenlige og arbejdseffektive løsninger.

Opfattelsen af tillid til datasikkerhedsparathed adskiller sig fra den virkelighed, som organisationer oplever. Selvom det er vigtigt for organisationer at vide, hvor data er placeret, samt opdage risici, er disse foranstaltninger hver for sig ikke nok til at hjælpe organisationer med at forhindre de hændelser, der holder beslutningstagere inden for datasikkerhed og risici oppe om natten.

Som en CISO (Chief Information Security Officer) inden for finansielle tjenester udtrykker det: "Det går ikke at fortælle min bestyrelse, at "dataene blev sikret, men blot ikke beskyttet tilstrækkeligt" – vi ønsker for alt i verden ikke, at vores bank bryder ned og ender på forsiden af Wall Street Journal."

59

Gennemsnitligt antal datasikkerhedshændelser i de seneste 12 måneder

OP TIL

15 mio. USD

Årlige omkostninger ved alvorlige sikkerhedshændelser

2

Flere værktøjer på hånden er ikke lig med større datasikkerhed eller effektivitet – det er lige modsat.

Flere værktøjer på hånden er ikke lig med større datasikkerhed eller effektivitet – det er lige modsat.

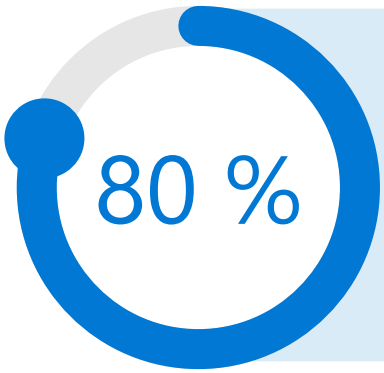
Organisationer er ved at indse, at en mangeårig tilgang med punktløsninger har skabt huller i synligheden og effektiviteten pga. siloopdelte datasikkerhedsværktøjer. Denne tendens viger nu for et ønske om at have en integreret løsning til datasikkerhed, og 80 % er enige om, at en omfattende datasikkerhedsplatform med integrerede løsninger er bedre end at bruge flere kvalitetsløsninger, der skal integreres og administreres manuelt.

Men selv om langt de fleste anser integrerede løsninger for at være overlegne, er brugen af datasikkerhedsværktøjer produktiv og fragmenteret.

Som følge heraf rapporterer organisationer, at de bruger 10 datasikkerhedsværktøjer i gennemsnit til at håndtere datasikkerhedsrisici, herunder Forebyggelse af datatab, Information Protection, SIEM (Security Information and Event Management), Cloud Access Security Broker med flere. For organisationer med over 5.000 medarbejdere er det gennemsnitlige antal værktøjer endnu større.

Det kan skabe en falsk følelse af tryghed at have flere værktøjer på hånden, fordi dem, der bruger flere værktøjer (over 16) har større tillid til deres datasikkerhedsniveau, sammenlignet med dem, der bruger færre værktøjer (61 % vs. 56 %).

Men forskning går imod denne følelse af sikkerhed, da organisationer med 16 eller flere værktøjer også oplevede flere datasikkerhedshændelser inden for det seneste år – i gennemsnit 133 – sammenlignet med 48 hændelser for organisationer med færre værktøjer.



Er enige om, at en omfattende datasikkerheds-platform med integrerede løsninger er bedre end at bruge flere kvalitetsløsninger, der skal integreres og administreres manuelt.

2,8 x

Flere datasikkerhedshændelser inden for det seneste år

For organisationer med 16 eller flere værktøjer (sammenlignet med organisationer med færre værktøjer)

Argumentet for større datasikkerhed gennem mere integrerede løsninger og færre værktøjer bliver endnu stærkere, når man ser på synspunkterne og praksis hos dem, der foretrækker kvalitetsløsninger eller flere værktøjer.

"Hvordan vil data blive indsamlet, aggregeret og brugt fra en hel del systemer? En masse forskellige datapunkter skal samles i ét økosystem, for at det virkelig kan fungere. Ellers står du reelt set med en datasikkerhed fuld af huller som en schweizisk ost."

VP for IT
Manufacturing/Production

For det første kan flere forskellige datasikkerhedsværktøjer føre til huller i synligheden og flere skyggedata. Dem, der er bekymrede over skyggedata, er faktisk mere tilbøjelige til at foretrække kvalitetsløsninger. Det skyldes højst sandsynligt, at organisationer med en kvalitativ tilgang skal gøre en større indsats for at få et omfattende overblik over deres datasikkerhedsniveau.

For det andet skaber administrationen af siloopdelte løsninger mere kompleksitet for datasikkerhedsteams, da hver enkelt løsning kræver dedikeret personale, installation og vedligeholdelse af endpoint-agenten og forskellige nye processer. Se eksempelvis på gennemgang og sortering af advarsler – en af de opgaver, der har brug for personale og ressourcer. Et stigende antal advarsler kræver en øget indsats fra datasikkerhedsteams, når de administrerer isolerede løsninger. Organisationer med flere værktøjer oplever i gennemsnit 96 datasikkerhedsadvarsler pr. dag, mens teams med færre værktøjer oplever under halvdelen, 44. De er heller ikke i stand til at gennemgå så mange af disse advarsler som teams med færre værktøjer kan (61 % vs. 68 %). Dette medfører ofte også, at organisationer med flere værktøjer er mere reaktive i forhold til organisationer, der bruger færre værktøjer.

Endelig indikerer flere værktøjer også, at organisationer skal gøre en omfattende indsats for at integrere indsigt og afhjælpningsplaner, og oplysninger kan gå tabt. Da der blev spurgt om de største datasikkerhedsudfordringer, er omkostningerne ved at implementere eller vedligeholde – og udfordringerne med at integrere –datasikkerhedsløsninger rangeret som de to vigtigste områder.

Det betyder længere og langsommere processer, hvor 37 % af dem, der bruger 16 eller flere værktøjer, rapporterer, at de har brug for en måned eller mere til at udføre en datasikkerhedsundersøgelse, sammenlignet med kun 21 % af dem med færre værktøjer.

"Lige nu kravler vi. Alle vores systemer alle deres egne portaler, egne værktøjer og egne måder at håndtere tingene på. Hver person bidrager hver især med deres ekspertise på hver enkelt område. Herefter beslutter alle i fælleskab, hvad der foregår, og vi tager hånd om det derfra. Så det består af lidt manuelt arbejde i øjeblikket," siger en Director of Infrastructure & Operations inden for fremstilling og produktion.

Ved at fortsætte med flere løsninger ignorerer organisationer ultimativt deres egen snak om, at integrerede løsninger er overlegne, og går i den modsatte retning – hvilket koster dem tid og penge.

RESULTATER I ORGANISATIONER, DER BRUGER FÆRRE (< 16) VS. FLERE (> 16) DATASIKKERHEDSVÆRKTØJER	Et lavt antal værktøjer	Et stort antal værktøjer
Antallet af **datasikkerhedshændelser** i de seneste 12 måneder	48	133
Andel af **alvorlige** datasikkerhedshændelser	19 %	26 %
Vores aktuelle datasikkerhedsstrategi er mere **reaktiv**	31 %	40 %
Udfordret med **integration af** løsninger	24 %	39 %
Datasikkerhedsteamet bruger mest tid på **reaktioner**	19 %	26 %
Vi er **trygge** ved vores datasikkerhedsniveau	56 %	61 %
Antal advarsler, der **modtages** pr. dag i gennemsnit	44	96
Andel af advarsler, vi kan **gennemgå** pr. dag	68 %	61 %
En måned eller mere er nødvendig for at udføre en datasikkerhedsundersøgelse	21 %	37 %

3

Organisationer oplever fortsat stress pga. eksterne og interne datasikkerhedshændelser, især inden for virksomhedsdata.

Organisationer oplever fortsat stress pga. eksterne og interne datasikkerhedshændelser, især inden for virksomhedsdata.

Da faktorer i forbindelse med data – herunder de folk, der interagerer med data, datarelaterede aktiviteter samt enheder og apps, der bruges til at behandle data – konstant ændrer sig, kan datasikkerhedshændelser og brud på datasikkerheden ske uanset tid og sted. Og disse trusler kommer fra både eksterne hackere og betroet personale, herunder medarbejdere, kontraktansatte og partnere. Uanset om det er ondsindet eller utilsigtet, kan alle aktører forårsage datasikkerhedshændelser – hvilket betyder, at der er et konstant behov for sikkerhed på tværs af en lang række områder.

En VP for it inden for finansielle tjenester siger: "Det, som du forsøger at beskytte dig mod, er under konstant forandring. Det er i konstant bevægelse. Det vil altid udvikle og forandre sig og være fleksibelt. Uanset, hvilke data du beskytter, og hvor de opbevares, vil de variere mere og mere."

Datasikkerhedshændelser kan opstå fra forskellige kilder, men den eksterne trussel fra malware- eller ransomware-hændelser – forekomster, hvor skadelig software infiltrerer et system, så hackere får uautoriseret adgang til systemer eller netværk – er langt den mest almindelige, hvoraf 50 % af de adspurgte organisationer har oplevet mindst én hændelse i det forløbne år.

Derudover rammer disse angreb dér, hvor organisationer føler sig mest sårbare, og 41 % siger, at de ikke føler sig tilstrækkeligt parate til at håndtere fremtidige malware- eller ransomware-angreb inden for det næste år. Denne følelse af sårbarhed er endnu højere blandt dem, der foretrækker en kvalitativ tilgang – 44 % føler sig uforberedt på et angreb af denne art, sammenlignet med kun 36 % af dem, der foretrækker en integreret løsning.

Det er også vigtigt for beslutningstagerne at beskytte sig mod og forhindre insider-risici. 35 % siger, at de har brug for at forsvare sig mod ondsindede insidere og kompromitterede konti, og en tredjedel er bekymrede over utilsigtede insiderhændelser. Selvom ondsindede insiderhændelser muligvis ikke er den vigtigste årsag til brud på datasikkerheden, er de den anden mest almindelige type hændelser, som beslutningstagere føler sig mindst parate til at forhindre.

"Jeg bliver ringet op af en panikslagen direktør mindst én gang om måneden ... Vi har haft en hændelse, jeg har opdaget en hændelse, eller trusselsteamet har opdaget en hændelse." Nogle af disse er utilsigtede, nogle er opstået, fordi folk ikke ved eller forstår, hvad deres rettigheder giver tilladelse til."

CISO i den amerikanske regering

Insidere er betroede personer, der typisk har fået adgang til eller har viden om virksomhedens ressourcer, data eller systemer, der ikke er generelt tilgængelige for offentligheden. Datasikkerhedsrisici, der er forbundet med insidere, er derfor ofte mere vanskelige at opdage. Som Bret Arsenault, CISO for Microsoft, indikerer: "I sidste ende er det ligegyldigt, om bruddet på datasikkerheden var forsætligt eller utilsigtet. Programmer mod insider-risici bør indgå i enhver virksomheds sikkerhedsstrategi."

OVERSIGT OVER DATASIKKERHEDSHÆNDELSER

Årsager til datasikkerhedshændelser	De mest almindelige hændelser i de seneste 12 måneder	Uforberedt på at forhindre dem i de næste 12 måneder
Malware eller ransomware	**50 %**	**41 %**
Kompromitterede konti	**38 %**	**35 %**
DoS-angreb (Denial of Service)	**35 %**	**33 %**
Uagtsomme insidere	**32 %**	**29 %**
Utilsigtede insiderhændelser	**31 %**	**32 %**
Ondsindede insidere	**31 %**	**35 %**
Fysisk ejendom	**29 %**	**29 %**

De datasikkerhedsløsninger, som organisationer vælger, skal også fungere for en række forskellige følsomme data, herunder virksomhedsdata af høj værdi, driftsdata og private oplysninger. I løbet af datasikkerhedshændelserne i de seneste 12 måneder har 74 % af organisationerne haft virksomhedsdata eksponeret, 65 % oplevede, at driftsdata blev kompromitteret, og 58 % oplevede, at private oplysninger blev gjort sårbare. Blandt de forskellige typer af data, er immaterielle rettigheder, it- og netværksdesign og PII ofte blevet kompromitteret eller eksponeret.

Fremadrettet betragter 77 % af organisationerne virksomhedsdata, såsom immaterielle rettigheder og kildekode, som de mest sårbare. Dette skyldes primært, at virksomhedsdata spiller en afgørende rolle i fastlæggelsen af konkurrencemæssige fordele og generering af indtægter. Det kan dog være udfordrende at identificere og klassificere disse data, da traditionel mønstergenkendelse, faste udtryk eller teknologi til funktionstilpasning muligvis ikke identificerer indhold, der mangler specifikke strengformater eller nøgleord, på en effektiv måde. Til gengæld har organisationer brug for mere avancerede teknologier til at hjælpe med at opdage og beskytte disse sårbare følsomme data.

TYPER AF DATA, DER ER MEST I FARE OVER DE NÆSTE 12 MÅNEDER

77 % **virksomhedsdata**		64 % **driftsdata**		63 % **private oplysninger**	
Immaterielle rettigheder	**30 %**	It- og netværksdesign	**29 %**	Personidentificerbare oplysninger (PII)	**31 %**
Kildekode	**28 %**	Regnskaber	**18 %**	HR-oplysninger (lønsystem, CV'er osv.)	**21 %**
Forretningsplaner	**27 %**	Salgs- og indtægtsrapporter	**15 %**	PCI-data (Payment Card Industry)	**18 %**
Forretningshemmeligheder	**24 %**	Indkøb og faktura	**12 %**	Beskyttede sundhedsoplysninger (PHI)	**18 %**
Dokumenter om fusion og overtagelse	**20 %**	Juridiske dokumenter/ aftaler	**12 %**	Legitimationsoplysninger	**17 %**
Specifikationer for byggeri	**18 %**	Produktionsprocesser/ batchfiler	**11 %**		

4

Organisationer har brug for skyen og AI til at skabe digital transformation – men det er også de mest sårbare dataplaceringer.

Organisationer har brug for skyen og AI til at skabe digital transformation – men det er også de mest sårbare dataplaceringer.

Samarbejde via cloud-applikationer og -platforme – kombineret med ny AI-teknologi – øger medarbejdernes produktivitet betydeligt og muliggør fleksible arbejdsordninger, hvilket gør cloud-applikationer og AI-teknologi afgørende for organisationer. I gennemsnit bruger organisationer nu 147 public cloud-tjenester, der spænder over SaaS, PaaS og IaaS.[1] Og 66 % af organisationerne har udviklet en AI-strategi, hvoraf 36 % allerede er i gang med at implementere den.[2] Denne udvikling har imidlertid skabt mere dynamiske og mangesidede risici pga. udfordringen med at opstille en klar definition af datagrænser på tværs af forskellige miljøer.

1. Measuring Risk and Risk Governance, Cloud Security Alliance (CSA), 2022
2. Microsofts AI-forskning i datasikkerhed, Hypothesis, marts 2023

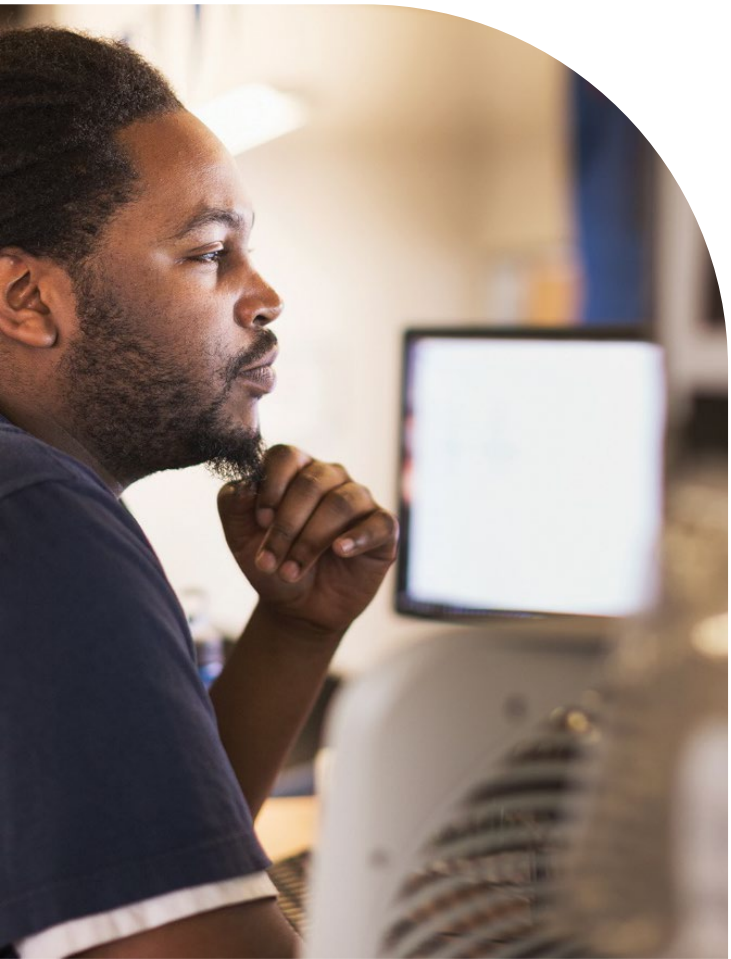
Det er blevet endnu vigtigere at have den rigtige datasikkerhedsløsning til disse dataplaceringer med høj produktivitet. I de seneste 12 måneder har 42 % af organisationerne rapporteret sikkerhedshændelser i cloud-storage og 31 % i mails, chatbeskeder eller onlinemødeværktøjer. Hændelser synes at være mest udbredte på områder, hvor produktiviteten og samarbejdet er størst.

Administrationen af denne type hændelser kræver ressourcer, og 79 % af organisationerne rapporterer, at deres datasikkerhedsteam har brug for flere medarbejdere til at administrere vigtige ansvarsområder inden for datasikkerhed på en effektiv måde. Men blandt de organisationer, der hævder at have brug for flere medarbejdere, foretrækker de fleste (57 %) en kvalitativ tilgang. Denne præference fremhæver, at organisationer, der bruger flere løsninger, har svært ved at identificere de reelle risici blandt de mange brugeraktiviteter.

OVERSIGT OVER DATAPLACERINGER

Dataplaceringer	Kompromitteret i de seneste 12 måneder	Mest i fare
Cloud-storage (f.eks. Box, OneDrive, Google Drive)	42 %	54 %
Mails/chat/onlinemødeværktøjer	31 %	39 %
Platform-as-a-Service (PaaS)	29 %	34 %
Infrastructure-as-a-Service (IaaS)	28 %	36 %
AI (f.eks. ChatGPT, Bard osv.)	27 %	38 %
SaaS-baserede databaser/datasøer	27 %	41 %
Endpoints/enheder	25 %	36 %
On-premises-lagre/filshares/databaser	24 %	28 %
Skyggedata	21 %	23 %
Line of business-applikationer	17 %	25 %
Udviklerværktøjer	16 %	23 %

Med over en tredjedel af – og stigende – organisationer, der implementerer AI-strategier, bliver AI taget i brug med hidtil uset hastighed – meget hurtigere end ibrugtagning af cloud-løsninger og mail førhen. Efterhånden som organisationer tager AI til sig, bliver det afgørende at styrke datasikkerheden for at muliggøre ansvarlig brug og forebygge risici. AI betragtes som en placering, der er mest i fare for datasikkerhedshændelser i forhold til andre steder, og 27 % af organisationerne har oplevet et brud på datasikkerheden for AI. Organisationers bekymringer omkring risiciene ved at bruge AI er centreret omkring manglende kontrol over data, der deles med AI, manglende kontrol til at opdage og afbøde risikabel brug af AI, manglende gennemsigtighed omkring, hvordan generative AI-modeller trænes, samt lækage af fortrolige oplysninger via AI.



"AI er godt for produktivitet og effektivitet, men omfatter potentielle sikkerheds- og datarisici." udtaler en beslutningstager inden for sikkerhed i virksomhed.

Selvom der er bekymringer omkring AI, kan beslutningstagere også se potentialet, især da leverandører på markedet udvikler innovationer, der kan hjælpe virksomheder gennem ansvarlig brug af AI. De vigtigste kontroller, som organisationer rapporterer, at de behøver for yderligere at kunne udnytte AI, er at opdage skadeligt eller risikabelt indhold i AI, kryptere, maskere eller anonymisere data, før de kan uploades til AI, samt identificere følsomme data genereret af AI.

DE 5 VIGTIGSTE DATASIKKERHEDSKONTROLLER, DER ER NØDVENDIGE FOR AI

1. **Opdage skadeligt eller risikabelt indhold** i AI
2. **Kryptere, maskere eller anonymisere data,** før de kan uploades til AI
3. **Identificere følsomme data** genereret af AI
4. **Forhindre, at følsomme data uploades** til AI
5. **Opdage manipulation af modeller eller data** i AI

5

Automatisering og AI er en lovende vej fremad mod større beskyttelse.

Automatisering og AI er en lovende vej fremad mod større beskyttelse.

I en ideel verden uden begrænsninger, der er baseret på organisatoriske prioriteter eller budget, vil halvdelen af organisationerne gerne være mere proaktive omkring datasikkerhedsmanagement og bruge mere tid på ting som opdagelse af følsomme data og relaterede risici omkring dem samt forebyggelse af datasikkerhedshændelser. Men i øjeblikket bruger over halvdelen af organisationerne mest tid på at fokusere på reaktive foranstaltninger som registrering af hændelser, reaktion og undersøgelser. Denne registrering af og reaktion på datasikkerhedshændelser er samtidig tidskrævende – det tager de fleste organisationer ca. en måned at løse en datasikkerhedshændelse, og for nogle kan det tage op til seks måneder at løse problemet.

Fordelen ved ibrugtagning af en mere proaktiv strategi ses tydeligt, da de adspurgte organisationer, der er mere proaktive og allerede oplever mindre dyre datasikkerhedshændelser, er mere tilbøjelige til at undersøge disse hændelser på under en måned, og de har større tillid til, at deres forsvarskontroller er tilstrækkelige til at forhindre brud på datasikkerheden.

Selvom organisationerne er klar over, at proaktive datasikkerhedsforanstaltninger kan være med til at reducere datasikkerhedsrisici, er de ikke kommet videre med implementeringen af disse foranstaltninger. Dem, der f.eks. ønsker at være mere proaktive ved at afsætte mere tid til forebyggelse, er mere tilbøjelige til at vælge kvalitetsløsninger. Dette kræver i virkeligheden en større indsats i håndteringen af reaktive foranstaltninger, når registreringssignaler og responskontroller indføres.

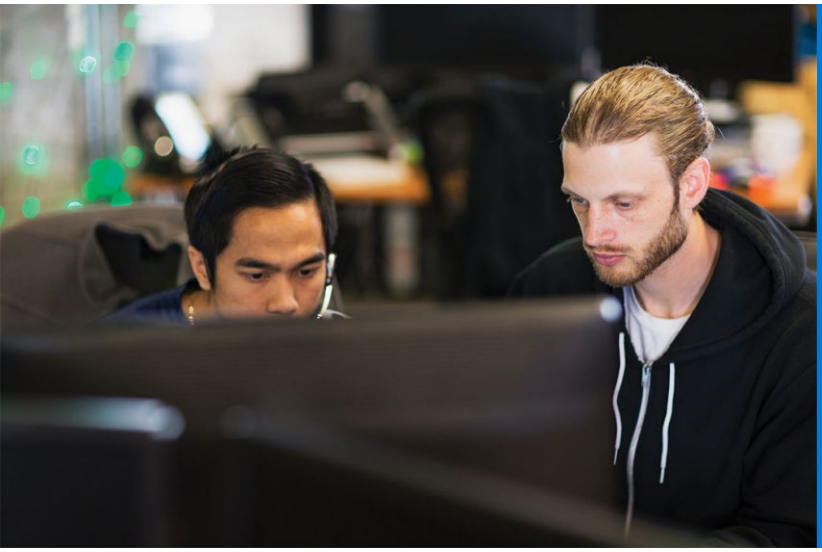
RESULTATER I ORGANISATIONER, DER ER MERE PROAKTIVE VS. REAKTIVE

	Mere proaktive	Mere reaktive
De gennemsnitlige omkostninger som følge af en datasikkerhedshændelse i de seneste 12 måneder	**207.000 USD**	**330.000 USD**
Udføre en datasikkerhedsundersøgelse på under en måned i gennemsnit	**80 %**	**68 %**
Vores forsvarskontroller er tilstrækkelige til at forhindre brud på datasikkerheden	**77 %**	**68 %**

Organisationer er på udkig efter teknologi, der kan hjælpe dem med at afsætte mere tid til proaktive aktiviteter pga. begrænsede ressourcer og medarbejdere, og fordi allokeringen af indsatsen mellem aktiviteter muligvis ikke er ideel. Automatisering er én måde, hvorpå organisationer kan afsætte tid til en mere proaktiv tilgang til datasikkerhed. 74 % af de adspurgte organisationer foretrækker semiautomatiseret eller fuldt automatiseret risikoafhjælpning, så sikkerhedsteams kan minimere konsekvenserne af potentielle datasikkerhedshændelser, i stedet for manuelle gennemgange. Desuden genkender organisationer mange andre opgaver, hvor automatisering kan hjælpe, såsom oprettelse af datasikkerhedsrapporter, automatisering af workflows for hændelsesstyring samt reaktion på og undersøgelse af hændelser. De fleste af de vigtigste opgaver, som sikkerhedsteams ønsker at automatisere, er reaktive foranstaltninger. Ved at automatisere disse opgaver kan organisationer aflaste deres datasikkerhedsteams, så de kan være mere proaktive.

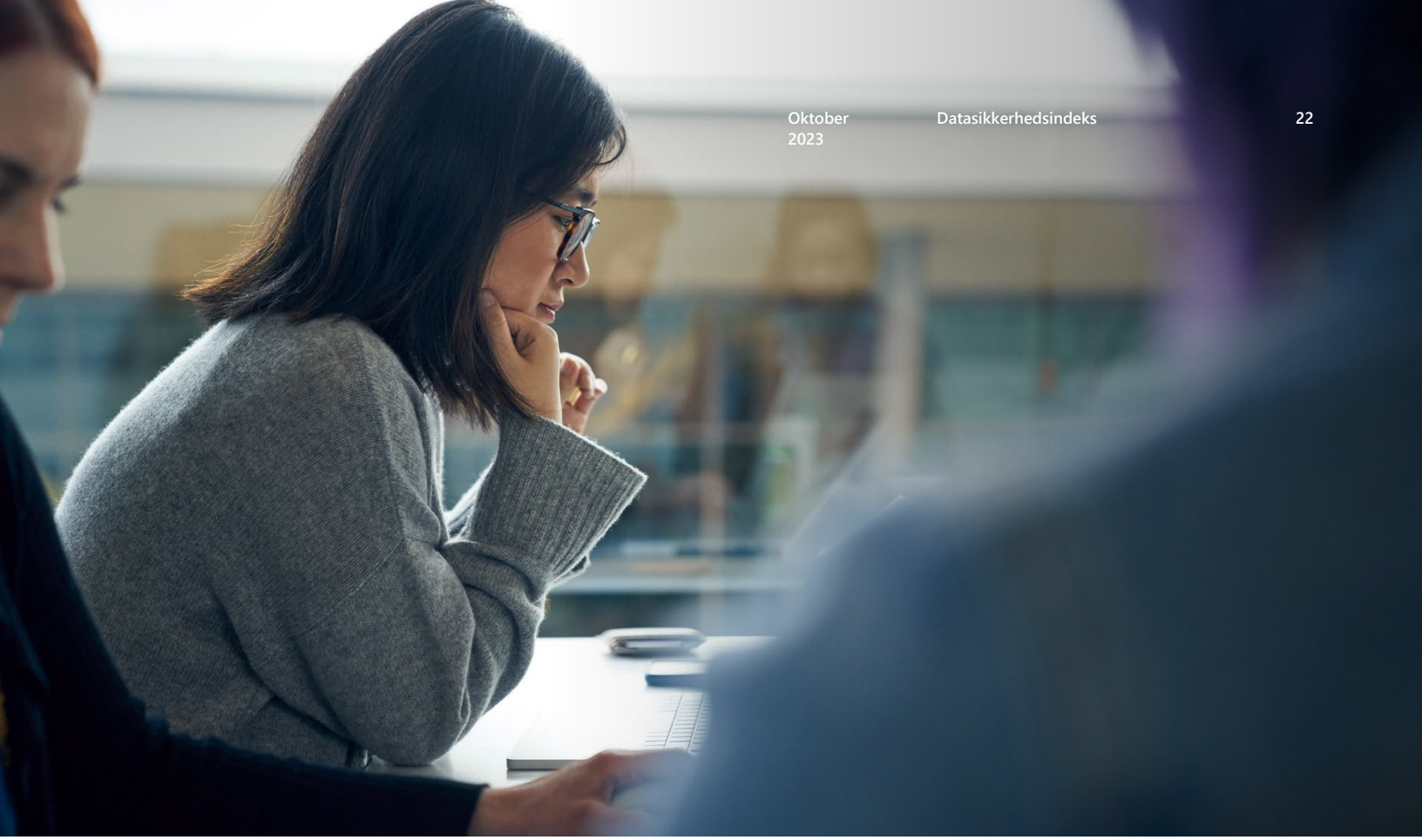
DE 5 VIGTIGSTE OMRÅDER, HVOR DATASIKKERHEDSTEAMS FORETRÆKKER AUTOMATISERING/AFHJÆLPNING

Reaktiv	1	Oprette automatiserede workflows for hændelsesstyring og -respons
	2	Oprette datasikkerhedsrapporter
Reaktiv	3	Reagere på og inddæmme datasikkerhedshændelser
	4	Dirigere hændelser til de rigtige teams (f.eks. SOC, juridisk afdeling, HR) under efterforskningen
	5	Efterforske datasikkerhedshændelser



"Der er så mange følsomme data, der skal evalueres manuelt. AI kan hjælpe med at fremskynde vores teams reaktionstider og beskytte data, når vi mangler ressourcer."

Beslutningstager inden for sikkerhed i Storbritannien



Brug af AI til datasikkerhed kan også hjælpe organisationer med at være mere strategiske og blive klogere på fremtidige trusler. Teknologien fremskynder reaktionen på registrerede hændelser, så datasikkerhedseksperter får mere tid til yderligere efterforskning. Tilsvarende automatisering nævner organisationer mange scenarier, hvor AI kan hjælpe med at levere stærkere sikkerhed, **så deres team sparer tid.** De vigtigste scenarier for brug af AI omfatter automatisk blokering af upassende datadeling, registrering af kritiske datasikkerhedsrisici/ unormale dataaktiviteter og efterforskning af potentielle datasikkerhedshændelser.

Ved at udnytte fordelene ved AI og automatisering – og bevæge sig i retning af mere integrerede løsninger – kan organisationer indføre en mere proaktiv datasikkerhedsstrategi og forberede sig på en mere sikker fremtid.

VIGTIGSTE SCENARIER, HVOR AI BRUGES

Automatisk blokere upassende datadeling

Registrere kritiske datasikkerhedsrisici/ unormale dataaktiviteter

Anbefalinger til bedre beskyttelse af dit datamiljø

Undersøge potentielle datasikkerhedshændelser

Finjustere datasikkerhedspolitikker

Endelige anbefalinger

- Indfør en integreret platform for at styrke datasikkerhedsniveaet
- Beskyt dig mod datasikkerhedshændelser både udefra og indefra med en dybdegående tilgang til forsvar
- Opgrader dine datasikkerhedsstrategier med AI og automatisering

Indfør en integreret platform for at styrke datasikkerhedsniveaet

Ifølge resultaterne i denne undersøgelse kan færre løsninger skabe mere sikkerhed. Det kan virke ulogisk, men organisationer skal bekæmpe den falske selvsikkerhed, der opstår ved at have en lang række isolerede løsninger. Leverandørkonsolidering giver en strategisk tilgang, der ikke kun reducerer omkostningerne, men også øger sikkerheden.

Beslutningstagere inden for datasikkerhed kan påbegynde denne transformation ved at give deres teams mulighed for at afsætte mere tid til strategisk arbejde såsom at undersøge og planlægge nye sikkerhedskontroller samt optimere sikkerhedspolitikker – hvilket 84 % af beslutningstagerne er enige om, at de ønsker at gøre. Denne proces indebærer udskiftning af ældre siloopdelte løsninger, der ofte betragtes som "markedets bedste", men som ikke kan integreres med andre værktøjer på en effektiv måde.

Beslutningstagere kan fremme et tæt samarbejde med deres teams for at opstille mål for programmål for datasikkerhed og nøgletal (KPI'er). De kan derefter gøre fremskridt ved at definere løsningskravene og identificere funktioner, der ikke er til forhandling. Denne tilgang giver dem mulighed for at udpege leverandører, der kan levere værktøjer, som er i overensstemmelse med de overordnede mål. Det afgørende er, at det fremmer en fremtidsrettet tankegang og hjælper teams med ikke at fokusere for meget på eksisterende praksis eller isolerede use cases, så de kan implementere nødvendige ændringer i retning af en mere integreret tilgang.

En integreret datasikkerhedsplatform bør give sikkerhedsteams mulighed for at udføre alle disse vigtige opgaver problemfrit:

1. Opdage og beskytte følsomme data i deres digitale landskab.
2. Registrere kritiske risici i forbindelse med disse data.
3. Forhindre uautoriseret brug af følsomme data, uden at det påvirker deres lovlige forretningsaktiviteter.

Ved at implementere en integreret datasikkerhedsstrategi kan organisationer opnå et højere beskyttelsesniveau og samtidig forenkle deres sikkerhedsinfrastruktur.

Beskyt dig mod datasikkerhedshændelser både udefra og indefra med en dybdegående tilgang til forsvar

Datasikkerhedshændelser skyldes normalt eksterne hackere, ondsindede insidere eller utilsigtede insiderhændelser. Organisationerne skal træffe foranstaltninger for at beskytte deres data, både ved at forhindre uautoriseret adgang fra eksterne trusler og ved at mindske risikoen for insidertyveri eller utilsigtet dataeksponering.

Organisationer kan tackle disse udfordringer ved at indføre en dybdegående tilgang til datasikkerhed. Denne strategi svarer til et museums beskyttelse af uvurderlige kunstværker: avancerede sikkerhedskameraer, der er udstyret med oplysninger om trusler, overvåger besøgende, billetsystemer styrer identitet og adgang til museet, og strenge sikkerhedsforanstaltninger omkring kunstværkerne fungerer på samme måde som datasikkerhedskontroller, der beskytter dine værdifulde data. Disse foranstaltninger modvirker potentielle hændelser, uanset om de stammer fra eksterne aktører eller enkeltpersoner, der allerede er i organisationens miljø.

Bekæmpelse af skiftende datasikkerhedsrisici kræver en koordineret indsats i hele organisationen for at implementere denne dybdegående forsvarsstrategi. Datasikkerhedsteamets samarbejde med andre afdelinger, såsom SOC (Security Operations Center), kan optimere investeringen i datasikkerhed. Det skal bemærkes, at 66 % af de organisationer, der betragter sig selv som proaktive, interagerer med deres SOC-team, sammenlignet med 54 %, som ikke gør.

Tilsvarende teamwork på tværs af sikkerhedsteams bør datasikkerhedsløsninger også problemfrit integreres med andre systemer, f.eks. løsninger til udvidet registrering og svar (XDR) eller identitets- og adgangsadministration (IAM), for effektivt at forhindre datasikkerhedshændelser fra både eksterne og interne kilder. Disse integrationer gør det muligt for organisationer at foretage omfattende undersøgelser og reaktioner på sikkerhedshændelser, få en grundig forståelse af de berørte data, aktører og aktiviteter og reagere med flere afhjælpningskontroller. Derved kan de reagere på en informeret, præcis og hurtig måde for at minimere konsekvenserne af potentielle sikkerhedshændelser.

Opgrader dine datasikkerhedsstrategier med AI og automatisering

Automatisering og AI kan hjælpe organisationer med at være mere proaktive inden for datasikkerhed. Her er nogle anbefalinger til, hvordan din organisation kan påbegynde rejsen mod automatisering og AI:

- Opdag følsomme data: Brug AI til at hjælpe med at identificere følsomme data og anvende beskyttelsespolitikker, herunder kryptering og rettighedsstyring. Dette er især værdifuldt for forretningsdata, der kan give udfordringer i forbindelse med opdagelse via traditionelle mønstergenkendelsesteknologier. Organisationer kan udnytte klassificeringsteknologi, såsom maskinel indlæring eller AI-baserede klassificeringer, der er kendt for deres intelligens og evne til hurtigt at finde følsomt indhold baseret på datakontekst eller forretningskategori. Alternativt kan organisationer anvende præcis datamatchningsteknologi til at opdage driftsmæssige eller personlige data.

  Da branchens forordninger hele tiden er under udvikling (f.eks. GDPR, HIPAA eller PCI DSS), og datalandskabet bliver mere dynamisk, er det derudover afgørende at have avanceret klassificeringsteknologi, der let kan tilpasses til at identificere nye kategorier af følsomme data.

- Opdag kritiske datasikkerhedsrisici: Udnyt styrken ved AI til at identificere kritiske risici i forbindelse med dine følsomme data og allokere ressourcer strategisk til at håndtere potentielle højrisikohændelser. AI-teknologier kan generere advarsler i høj kvalitet, så sikkerhedsteams kan spare værdifuld tid, der ellers ville blive brugt på at gennemgå en masse falske positive advarsler. Derudover kan AI hjælpe organisationer med at identificere flygtige risici, især når ondsindede aktører forsøger at undgå at blive opdaget. Det er afgørende at bruge maskinhastighed for at være et skridt foran disse trusselsaktører.

- Forebyg datasikkerhedshændelser dynamisk: Brug AI og automatisering til automatisk at skræddersy dine kontroller til forebyggelse og afhjælpning baseret på vurderede risici, hvilket muliggør en mere fleksibel og proaktiv datasikkerhedsstrategi. Når AI-baserede løsninger registrerer og evaluerer risici, kan automatiserede kontroller til forebyggelse hurtigt gribe ind for at beskytte dataene ved at anvende kontroller til afhjælpning netop på højrisikoscenarierne. I tilfælde, hvor højrisikobrugere registrerer tidlige indikatorer for hensigt om dataeksfiltrering, kan organisationer f.eks. anvende mere stringente politikker for forebyggelse af datatab (DLP) og proaktivt være på forkant med potentielle datasikkerhedshændelser.

Vi håber, at du finder indsigten og anbefalingerne i denne rapport nyttige til at forbedre din datasikkerhed og styrke din organisation mod skiftende risici.

Du kan lære mere om Microsoft-datasikkerhed på https://aka.ms/DataSecurityNews

Detaljerede mål for undersøgelsen, metoder og detaljer om rekruttering af målgruppen

Målene for undersøgelsen omfattede:

1. Forstå datasikkerhedslandskabet, herunder prioriteter, tankegange og udfordringer

2. Kortlægge årsagen til og konsekvenserne af datasikkerhedshændelser samt identificere handlinger, som datasikkerhedsteams kan foretage for at styrke datasikkerhedsniveauet

3. Udforske fremtiden inden for datasikkerhed, herunder nye strategier og innovationer omkring brugen af AI til datasikkerhed

Metoden var:

En 15-minutters multinational onlineundersøgelse blev gennemført mellem den 28. juli til 9. august 2023 blandt 822 beslutningstagere inden for datasikkerhed.

Spørgsmålene var centreret omkring datasikkerhedslandskabet, hvordan datasikkerhedsteams allokerer deres ressourcer, datasikkerhedshændelser og holdninger til og brug af kunstig intelligens (AI) til datasikkerhed.

Med henblik på at opfylde kriterierne for screening skulle beslutningstagerne inden for datasikkerhed være:

CISO og tilgrænsende beslutningstagere (C-2 og derover) med ansvar for datasikkerhed

Arbejde i virksomhedsorganisationer (i forskellige størrelser med over 500 medarbejdere)

En blanding af regulerede og ikke-regulerede brancher (ingen uddannelsesinstitutioner, offentlige myndigheder eller nonprofitorganisationer)

Af de 822 beslutningstagere inden for datasikkerhed, der blev adspurgt i undersøgelsen, var gennemførelsen efter land:

USA	329
Storbritannien	322
Australien	171