INNOFACTOR

Trygge ansatte gir konkurransefortrinn

Trygge ansatte gir konkurransefortrinn:

En guide til identitetshåndtering og tilgangsstyring

- Les ekspertenes betraktninger
- Hvorfor identitet er viktig mens du forbereder deg for NIS2-compliance?
- Beste praksis fra bedrifter og kommuner
- Internasjonal forskning

Et inspirasjonshefte fra Innofactor

INNOFACTOR

Fordi det er virksomhetskritisk

Det er lenge siden fremadrettede ledere oppfattet IKT-sikkerhet som unødvendig og «kjekt å ha». Mediene florerer av kjente norske konsern og offentlige virksomheter som opplever store, dels kritiske utfordringer etter å ha bli rammet av ulike former for digital kriminalitet. Utsagnet om at «det handler om ikke «om» man blir rammet, men når» er illustrerende for hvor viktig det er at flere prioriterer investeringer i sikkerhet. Som pandemien har lært oss på nytt: Innsatsen må rettes der trusselen er størst. Mer enn åtte av ti sikkerhetsbrudd skjer fordi ledere og ansatte lures til å gjøre en feil. Derfor er også diskusjoner rundt IKT-sikkerhet løftet helt opp i toppledelsen og styrene.

Hvorfor identitet er viktig mens du forbereder deg for NIS2-compliance?

NIS2-direktivet fra EU transformerer cybersikkerhetslandskapet og pålegger strenge tiltak for organisasjoner som tilbyr kritisk infrastruktur. Direktivet bygger på sin forgjenger med mål om å styrke cybersikkerheten til vesentlige enheter innen EU. Vedtatt i 2016, trådte det i kraft i mai 2018, og den oppdaterte NIS2-versjonen ble offisielt vedtatt i november 2022, og ble effektiv fra 16. januar 2023.

Organisasjoner har nå frem til 17. oktober 2024 for å integrere dets bestemmelser i nasjonal lovgivning.

NIS2 gjelder for enheter med 50 ansatte og en årlig omsetning på €10 millioner som tilbyr avgjørende tjenester til den europeiske økonomien. Dette inkluderer både EU-baserte og ikke-EU-organisasjoner som tilbyr tjenester innen EU. Manglende overholdelse kan føre til betydelige bøter, frysing av sertifiseringer og begrensninger på lederfunksjoner.

Sikkerhet som ikke forringer brukeropplevelsen

Da en global pandemi var et faktum, ble virksomheter og organisasjoner kastet ut i en situasjon preget av uvisshet og frykt for fremtiden. To år ut i pandemien, ser vi tydelig hvordan IAM har hjulpet virksomheter i en uforutsett og ny tilværelse der arbeidsplassen har gått fra å være et sted, til å bli en tilværelse. I denne settingen seiler IAM (identity and access management) som en kritisk forutsetning for å beskytte virksomheten og dens ansatte ved å beskytte tilgangen til data og ressurser. I god IAM-praksis gjøres dette uten å forringe brukeropplevelsen – snarere tvert imot. Ved rask og trygg innlogging på virksomhetens enheter og applikasjoner, øker de ansattes produktivitet og effektivitet.

Handler om mer enn sikkerhet

IAM gjør at ledere innen sikkerhet- og risikohåndtering kan gå fra å være tjenestetilbydere til å fungere som rådgivere som støtter virksomhetens verdiskapning. IAM gjort rett skaper konkurransefortrinn fordi ansatte opplever at de kan enklere tilpasse seg fleksible arbeidsformer, med mindre frykt for å gjøre feil. Like viktig er det et viktig virkemiddel for å få nye ansatte eller innleide ressurser raskt opp og stå, eller at tilganger automatisk tas bort når vedkommende slutter i jobben. Like viktig er god IAM for å sikre etterlevelse av regler og retningslinjer knyttet til sensitive persondata, der begrep som GDPR, Schrems2 og NIS2 har endret spillereglene for alle bedrifter.

INNOFACTOR

Ledere må være offensive

Gartner uttaler seg om viktigheten av å ta en offensiv posisjon. De mener sikkerhetsledere må ha fokus på innovasjon, utforme fremadrettede strategier, og sikre at sikkerheten støtter den digitale endringen som skjer på tvers av virksomheten. Her er det viktig å jobbe med holdninger og spre kunnskap slik at hele organisasjonen tar eierskap til sikkerhet. Det vil dramatisk redusere risikoen for sikkerhetsbrudd. I et stadig mer opphetet risikomiljø, vil en offensiv sikkerhetstilnærming lede virksomheten gjennom digitale usikkerhet. Bedrifter med IAM forankret i organisasjonen, er langt bedre rustet til å møte akutte situasjoner som krever endring og omstilling i bedriften. Ledere må være offensive Gartner uttaler seg om viktigheten av å ta en offensiv posisjon. De mener sikkerhetsledere må ha fokus på innovasjon, utforme fremadrettede strategier, og sikre at sikkerheten støtter den digitale endringen som skjer på tvers av virksomheten. Her er det viktig å jobbe med holdninger og spre kunnskap slik at hele organisasjonen tar eierskap til sikkerhet. Det vil dramatisk redusere risikoen for sikkerhetsbrudd. I et stadig mer opphetet risikomiljø, vil en offensiv sikkerhetstilnærming lede virksomheten gjennom digitale usikkerhet. Bedrifter med IAM forankret i organisasjonen, er langt bedre rustet til å møte akutte situasjoner som krever endring og omstilling i bedriften.

FAKTABOKS

Dette er IAM

Identity and Access Management (IAM) designes for å sikre virksomhetens data, maskiner og ansatte uansett tid og sted, derigjennom øke mulighetene til effektivt og sikkert arbeid. IAM er et arbeid som til enhver tid skal være aktivert i en bedrift. Det ikke et engangstiltak, men et viktig element i en organisasjons stadige omstilling og endring. Med en riktig tilnærming til IAM får virksomheten bedre evne til å tilpasse seg nye krav, behov og regler, og kan være til uvurderlig hjelp når uforutsette situasjoner oppstår, og nødvendige endringer må gjøres. IAM gjort rett gir både god sikkerhet og gode brukeropplevelser. Før anskaffelse og distribusjon av teknologi for identitetsstyring- og administrasjon (IGA), må bedriften gjennomgå nødvendige planleggingsfaser og iverksette et formelt IAM-program.

INNOFACTOR

Forberedelser til NIS2

- **Identifikasjon og demping av risiko:** Gjennomfør en grundig risikovurdering på tvers av virksomheten for å identifisere sårbarheter og formulere en plan for å redusere dem.
- **Forsterkning av tilgangskontroll:** Styrk tilgangskontrollen gjennom robust Identity governance og definisjon av detaljerte autorisasjonspolicyer for spesifikke ressurser.
- **Beskyttelse av privilegert tilgang:** Implementer beste praksis som minst privilegium-tilgang for å beskytte mot potensielle angrep som utnytter privilegerte kontoer.
- **MFA mot phishing:** Rull ut Multi-Factor Authentication (MFA) mot sosial ingeniørkunst for å bekjempe angrep uten å forstyrre brukeropplevelsen.
- **Styrking av forsvar mot ransomware:** Proaktivt forsvare seg mot ransomware med løsninger som endpoint privilege management og robust antivirus.
- **Sikker programvareforsyning:** Gjennomgå programvareforsyningen din og vurder implementering av en løsning for håndtering av hemmeligheter for å redusere risikoen for angrep gjennom forsyningskjeden.
- **Adopsjon av Zero Trust-strategi:** Omfavn en Zero Trust-tilnærming, inkludert robust Identity management, kontinuerlig autentisering og trusselanalyse for sterk sikkerhet.

Viktigheten av identitet for NIS2-compliance

I riket av cybersikkerhet og overholdelse er Identitet bindeleddet. Effektiv identitetsadministrasjon etablerer ansvar, sikrer tilgangskontroll og gir en lett tilgjengelig revisjonsspor. Med kartlegging til ISO 27001 kan organisasjoner dra nytte av eksisterende sertifiseringer for å oppfylle NIS2-kravene og dermed spare tid og ressurser.

Konsekvenser av manglende overholdelse: En advarsel

Manglende overholdelse av NIS2 kan føre til betydelige bøter, frysing av sertifiseringer og begrensninger på lederfunksjoner. Essensielle enheter og viktige enheter står overfor varierende botnivåer basert på sektor og omsetning.

Sikring av forsyningskjeden din: Ut over vurderinger

Å sikre integriteten til forsyningskjeden er avgjørende under NIS2. Organisasjoner må implementere sikkerhetstiltak, gjennomføre vurderinger og revisjoner av leverandørrisiko og opprettholde løpende overvåking for å redusere generell risiko.

Formaliser beredskapsplanen din for hendelser: Rask rapportering er nøkkelen

NIS2 krever rask rapportering av hendelser. Etablering av en godt strukturert beredskapsplan for hendelser, sammen med løsninger som Okta, hjelper til med å rekonstruere tidslinjer for effektiv rapportering.

INNOFACTOR

Sikker identitetsløsning for alle ansatte i Betonmast

– Det er en kjempefordel at Innofactor kjenner løsningene våre og kan snu seg fort rundt. Det sparer vi både tid og penger på, sier IT-sjef Øyvind Tørnblad i Betonmast.

Som en av Norges største byggentreprenører, er Betonmast involvert i alt fra store boligprosjekter til næringsbygg i både privat og offentlig sektor. Entreprenørselskapet har rundt 1000 medarbeidere i 16 underselskaper i Norge og Sverige. Derfor har det vært viktig å kunne tilby ansatte en brukervennlig og tilgjengelig løsning som fungerer godt uansett om de befinner seg på kontoret eller ute i felten.

– Det er ytterst viktig at vi har kontroll på de digitale identitetene til de ansatte, og sikker tilgangsstyring for alle de ulike tjenestene de bruker, forteller IT-sjef Øyvind Tørnblad i Betonmast.

Sikre medarbeideropplevelser

Innofactor har hjulpet Betonmast med å rulle ut Microsofts IAM-løsninger (Identity and Access management) og Microsoft Identity Manager (MIM) for å kunne administrere identiteter og tilgangsstyring av brukernes rettigheter og tillatelser.

For Betonmast har det vært spesielt viktig at disse løsningene ikke bare skal være forbeholdt de som sitter på kontoret.

– Noen jobber på PC-er, mens andre bare bruker privateide mobiltelefoner ute i felten. Det har vært viktig for oss å ha fokus på medarbeideropplevelsen, og at alle skal kunne bruke løsningen uansett om de jobber som funksjonærer eller fagarbeidere, sier Tørnblad.

Har leid inn fast prosjektleder

I en hektisk IT-hverdag endrer behovene seg raskt. For Betonmast har det vært avgjørende at løsningene de velger må være dynamiske og enkelt kan tilpasses og endres.

– Vi har leid inn en prosjektleder fra Innofactor som vi jobber tett med. Det er også en kjempefordel at vi har enkel tilgang på dyktige konsulenter som kjenner løsningene og målene våre.

Det gjør at konsulentene kan snu seg fort rundt og komme raskt i gang med å løse oppgavene.

– Det er viktig for meg at man ikke lager kjempeprosjekter av hver minste ting, men kan jobbe med konsulenter som er løsningsorienterte. Det sparer vi både tid og penger på.

Mange tenker ikke på helheten

Med Microsoft Identity Manager og løsningene Innofactor har satt opp, får Betonmast håndtert identiteten til medarbeiderne på tvers av mange ulike fagsystemer. I dagens trusselbilde har dette blitt viktigere enn noensinne, spesielt med tanke på at Betonmast i liket med de fleste andre bedrifter knytter seg opp mot stadig flere ulike skyløsninger og ulike fagsystemer.

– Da må vi ha kontroll på identitetene. Ellers kan du risikere at en ansatt som slutter fortsatt har tilgang til enkelte systemer uten at du er klar over det. Derfor er sikkerheten rundt skyløsninger og identitetshåndtering noe vi må ha fokus på. Ikke minst er dette viktig med tanke på GDPR, sier Tørnblad.

Han mener mange virksomheter altfor ofte tar i bruk nye skyløsninger ukritisk, uten å tenke helhetlig rundt sikkerhet.

– For meg er det en trygghet å vite at vi jobber med identitetshåndtering og sikkerhet. Vi ønsker fremtidig full kontroll på dette.

Betonmast ble i 2019 en del av AF Gruppen, og i den forbindelse overtok nå i høst (2021) AF Gruppen IT-drift, lisens, sikkerhet og support. AF Gruppen har selv solid sikkerhetskompetanse, men har valgt å gå til Innofactor for hjelp med deler av integrasjonene mot Microsoft Identity Manager.

– Identitetsportalen er nå knyttet opp mot AF Gruppens sentrale systemer. Det betyr bare at jobben vi har gjort rundt identitet, og den lokale tilnærmingen vi har til medarbeiderne våre, er viktigere enn noensinne, avslutter Tørnblad.

FAKTABOKS

Visste du at...

- Beredskapen for å håndtere omfattende cyberangrep mot Norge har store mangler.
- Det mangler helhetlig styring og koordinering av IT-sikkerhet på tvers av statlige etater.
- Evnen til å oppdage digitale angrep i Norge er for dårlig.

Kilde: NSM

Ny identitetsløsning ga Bjørnafjorden kontroll etter kommunesammenslåingen

Da to kommuner skulle slås sammen, ble behovet for en solid identitetsløsning for alle ansatte tydelig. Innofactor har hjulpet til med å sette opp løsningen, og har også gjennomført en omfattende sikkerhetsvurdering av den nye kommunens IT-løsninger.

Bjørnafjorden kommune så dagens lys i januar 2020, da kommunene Os og Fusa ble slått sammen. Kommunen har i underkant av 25.000 innbyggere og rundt 1800 ansatte.

Espen Harald Haga er leder for IT-avdelingen i Bjørnafjorden, og forteller at både Fusa og Os hadde sine egne datasentre og sin egen infrastruktur – men i forbindelse med sammenslåingen ble alt samlet. IT-avdelingen i den nye kommunen består av 11 personer, inkludert en lærling.

– Men IT-avdelingene i Fusa og Os begynte å samarbeide allerede i 2018. På høsten begynte vi å se på hvordan den nye IT-løsningen for Bjørnafjorden skulle bli, forteller Haga.

De to kommunene ble tidlig enige om at det var nødvendig å få på plass en skikkelig løsning for identitetshåndtering (Identity and Access Management – IAM).

– Det var ikke god nok kontroll på identiteter, noe vi så for eksempel når nye medarbeidere begynte eller sluttet. I mange tilfeller fikk ikke IT beskjed, og medarbeidere kunne bli liggende i AD etter at de hadde sluttet. Det var et sikkerhetsproblem, sier Haga.

INNOFACTOR

Endelig kontroll på onboarding og offboarding

Kommunene begynte derfor å se på ulike identitetsløsninger, og landet til slutt på One Identity, en løsning basert på Microsoft Identity Manager (MIM).

Konsulenter fra Innofactor har jobbet sammen med Bjørnafjorden for å få satt opp den nye ID-løsningen, i tillegg til en ny e-post-løsning basert på Exchange Online.

– Identitetshåndtering var et kompetanseområde vi på den tiden ikke hadde. Vi har ikke ressurser og kapasitet til å holde på med dette selv, derfor ønsket vi heller å kjøpe dette som en tjeneste fra Innofactor, sier Haga.

MIM-løsningen er koblet opp mot Microsoft Azure AD, slik at tilganger til filområder og andre nettverksressurser kan styres basert på hvilke grupper i AD ansatte er medlem av.

– Nå har vi mye bedre kontroll på onboarding og offboarding, og nyansatte kommer inn i AD via personalmelding.

I en kommune kan det ofte være mange ulike fagsystemer og mange spesialtilpassede løsninger. Bjørnafjorden har som mål at flest mulig av fagsystemene skal omfattes av identitetsløsningen, men det er likevel enkelte spesialsystemer der man er nødt til å manuelt fjerne tilganger fra ansatte som slutter.

– Det har vi løst med automatisk epostvarsling til IT hver gang noen slutter, slik at vi manuelt får fjernet tilganger fra de systemene som ikke styres via AD, sier Haga.

INNOFACTOR

Fikk en full sikkerhetsgjennomgang av Innofactor

Nasjonal Sikkerhetsmyndighet (NSM) slår i sin rapport Nasjonalt Digitalt Risikobilde 2023 fast at det er svært høy risiko for at norske virksomheter vil utsettes for løsepengevirus i løpet av 2022. Dette er en trussel IT-avdelingen i Bjørnafjorden kommune er høyst oppmerksomme på, ikke minst etter at det nylig har vært eksempler på løsepengeangrep som har fått alvorlige konsekvenser for andre kommuner.

– Vi vil nødig havne i en slik situasjon, og fikk derfor bistand fra Innofactor til å gjøre en sikkerhetsrevisjon. Selv om gjennomgangen viste at mye allerede var bra hos oss, var det veldig nyttig. Vi fikk mange konkrete tips om hva vi kunne forbedre, sier Tom Ruben Bratholmen, IT-konsulent i Bjørnafjorden.

Bratholmen forteller at IT-avdelingen nå har begynt med en fast sikkerhetsdag hver fredag, hvor de blant annet går gjennom kjente sårbarheter, anbefalinger og hvilke konkrete tiltak de kan gjøre for å forbedre IT-sikkerheten.

– Det er viktig å ha fokus på sikkerhet hele tiden, slik at det ikke bare blir skippertak.

IT-leder Espen Harald Haga er veldig fornøyd med samarbeidet med Innofactor og oppfølgingen de har fått både gjennom sikkerhetsrevisjonen og oppsett av identitetsløsningen.

– Vi opplever at Innofactor har veldig god kompetanse og flinke folk. Dette er noe som også var viktig for oss ved valg av leverandør, avslutter Haga.

INNOFACTOR

FAKTABOKS

5 grunner til at god IAM gir konkurransefortrinn

- IAM legger til rette for at de riktige menneskene får tilgang til de riktige ressursene, til riktig tid og av riktige årsaker
- IAM er kritisk for å sikre riktige tilganger til ressurser på tvers av stadig mer kompliserte teknologimiljøer, og for å møte stadig strengere sikkerhetskrav
- IAM krever ikke bare teknisk ekspertise, men forretningsferdigheter som gjør det enklere å skape sikkerheten som gir en mer fleksibel og trygg arbeidsstyrke
- Virksomheter som utvikler solide ferdigheter innen IAM, kan redusere kostnadene for identitetsadministrasjon. Bedrifter uten nedfelte IAM-programmer vil bruke langt mer på IAM-tiltak, og oppnå mindre, enn bedrifter med IAM-programmer*
- Virksomheter med godt forankret IAM kan enklere støtte nye forretningsinitiativer.

Kilde: Gartner Research – Guide to Initiating and Running an Effective IAM Program

God IAM gir store forretningsgevinster

Bedriften kan raskere ta mer risiko og de ansatte får jobbe slik de selv ønsker. Et viktig stikkord på veien er automatisering.

Engelske Stephen Isherwood har jobbet i Norge siden 2002, og gjort bergenser av seg underveis. Etter å ha jobbet i energisektoren for store globale bedrifter og mindre oppstartsselskaper meldte han i 2021 overgang til Innofactor.

Ønsket var å komme inn i et fagmiljø der han fikk muligheten til å bistå selskapets kunder med sikkerhet og nettverksteknologi generelt, og IAM spesielt.

- Det var forlokkende å kunne gå enda mer i dybden av IAM, sier han.

Han ble for alvor faglig oppslukt i identitetsstyring og tilgangshåndtering i 2016. Da jobbet han i et selskap med flere tusen ansatte på over 30 lokasjoner, utstrakt bruk av hjemmekontor, og stor hyppighet av ansatte og konsulenter som måtte gis og fratas tilgang til IT-miljøet.

- Vi behøvde større kontroll. Derfor introduserte vi Microsoft Identity Manager. Med styring på identiteten til den enkelte kunne vi sikre at folk kunne jobbe trygt uansett hvor de var, sier han.

INNOFACTOR

Stor verdi ved milliardoppkjøp

Det første prosjektet ga stor verdi til bedriften ved et milliardoppkjøp der flere tusen ansatte raskt skulle innlemmes i IT-miljøet.

- Fordi vi hadde kontroll på identitetene og var integrert mot HR-systemene kunne vi raskere få de nye brukerne opp og stå. IAM var plutselig blitt forretningskritisk, sier han.

I tillegg fremhever han at IAM gjør at ledere kan få en større appetitt for å ta risiko, fordi sikkerheten i mindre grad blir en hemsko.

- Da samfunnet stengte ned første gangen i forbindelse med pandemien hadde vi alt klart slik at alle kunne jobbe hjemmefra. På grunn av tidligere investeringer i IAM var vi klare for å støtte samtlige ansatte på hjemmekontor i over 30 land. Alt var gjort på under et døgn, sier han.

Oppskriften handlet om on-premise Microsoft Azure AD, ende til ende IP-nettverk, programvare for å kontrollere identiteter og enheter, globalt DNS, og gode prosesser for håndtering av IT-sikkerheten og for å redusere risiko.

En fremtid uten bokser og brannmurer

I Innofactor jobber Isherwood med kunder der fellesnevneren er komplekse IT-miljø med store krav til compliance. Han mener at programvaren til Microsoft nå er så komplett at vi om få år ikke trenger dedikerte bokser og maskiner for å håndtere sikkerheten.

- Vi vil ikke trenge mer enn en enhet, en brukerkonto og tilgang til internett. Det meste vil være programvaredefinert, og autorisering vil skje basert på identiteten.

Han fremhever at Microsoft er best plassert i dette markedet sett i lys av at de er den største spilleren, anerkjennes for sine sikkerhetsvisjoner, har evnen til å gjennomføre, og løftes frem av de fremste ekspertene og analytikerne.

- I mine øyne er Microsoft best i klassen på IAM. De har så mange funksjoner at det for eksempel vil være mulig å unngå hacking eller at bedriften blir utsatt for ransomware.

Like viktig er de nye behovene som tvinges frem av nye regler som GDPR og Schrems II som stiller strenge krav til kontroll i IT-miljøet, og nye retningslinjer til lagring.

Automatisering er alfa og omega

Isherwood fremhever at kravene til IT-ekspertene begynner å bli så mange og komplekse, at det haster med å endre hvordan IT-avdelingen jobber. Tid må hele tiden frigjøres til å håndtere mer strategiske oppgaver. Han er derfor særlig opptatt av automatisering.

- Mange prosesser kan forenkles og forbedres ved å automatisere prosesser knyttet til hva som skal skje når en ansatt starter eller slutter i jobben, eller om vedkommende bytter tittel eller avdeling. Her kan det settes opp regler som skaper automatiske handlinger som gir større sikkerhet, forenkler arbeidsoppgaver og som gir trygghet for at alt gjøres riktig, sier han.

Dette vil føre til relativt store kostnadsbesparelser, særlig de indirekte oppgavene som mennesker slipper å huske eller håndtere. Med automatisering løses det automagisk.

- Når oppgaven først er satt opp så er det pålitelig. Det fungerer som det skal hver eneste gang.

I tillegg vil arbeidsgiver ha et revisjonsspor som gir raske svar ved behov.

- Der har vi veldig mye bra og viktig for alle som jobber med compliance, sier han.

Må kjenne forretningsbehovene

Isherwood mener at den gode IAM-eksperten må være forretningsdrevet.

- Det behøves mer enn kompetanse på teknologien. Vi skal digitalisere forretningsprosesser og må derfor ha forståelse for driverne i de ulike avdelingene, og i verdikjedene. Det gjør at vi kan digitalisere på en måte som støtter arbeidsformene.

Han anbefaler å tegne opp flytdiagrammer for de mange arbeidsprosess-ene for å kartlegge alle stegene og oppgavene i en prosess.

- Dette med å virkelig forstå oppgaven er det kritiske. Deretter handler det om å velge teknologien og funksjonene som best støtter oppgavene, og balansere dette opp mot en risikovurdering. Da får vi muligheten til å raskt avdekke om påloggingar knyttet til enkeltbrukere skjer fra steder der vi har mistanke for å tro at de ikke befinner seg.

Driverne for IAM

Det er ved å knytte sammen systemer og oppgaver at forenklingene og forbedringene skjer, og rundt identitet er det særlig viktig at HR og IT jobber tett sammen.

- Det er når vi knytter sammen systemene at vi skaper de virkelig store gevinstene med smarte integrasjoner. HR burde også drive dette fordi god datakvalitet gagner alle.

Han identifiserer flere åpenbare triggere som viktige for å sette fart på en IAM-investering.

- Den åpenbare er at HR og IT er fremadrettede og driver dette selv. Like viktig er det i forkant av store endringer på arbeidsplassen som et oppkjøp eller ved sammenslåinger.

- Sikkerhet er den viktigste driveren. Den største risikoen er knyttet til mennesker som blir hacket. Ved å beskytte identiteten bedre kan vi ta ned risikoen betraktelig, og det er et språk som forretningsledere forstår.

FAKTABOKS

Investeringene i sikkerhet er rekordhøy i 2024

I følge Gartner Groups prognose fra september 2023 øker de globale investeringene i teknologi og tjenester for IT-sikkerhet og risikohåndtering med 14 prosent i 2024, til et nivå på 188 milliarder amerikanske dollar. Dette er mer en dobling fra det som ble brukt i 2020. Veksten kommer i stor grad av trender som skyteknologi (+24,7%) og mer hybride arbeidsformer, til reguleringer som tvinger organisasjoner til å forsterke sine sikkerhetsmurer. Veksten innen IAM stiger med hele 14,8 prosent.