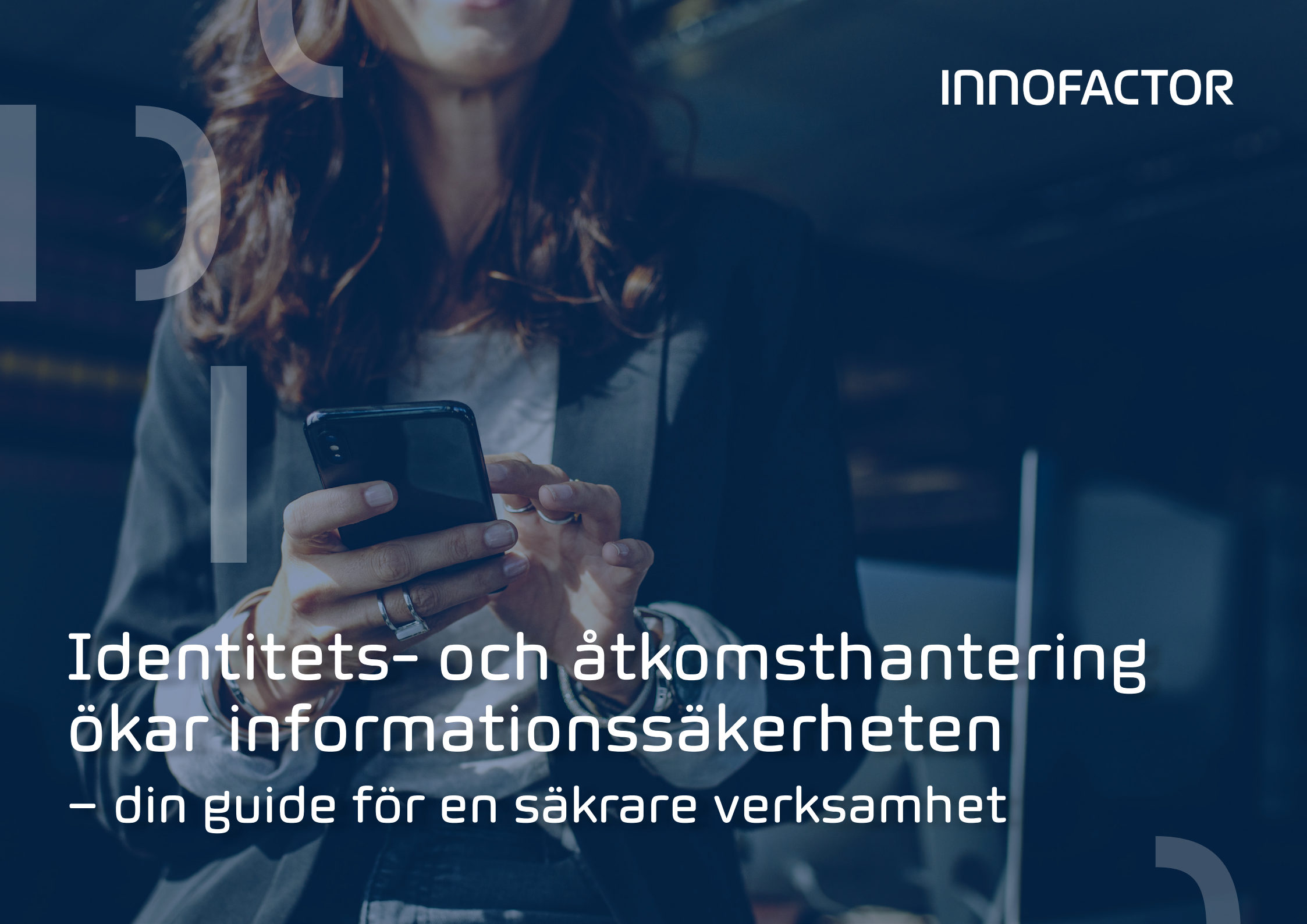


INNOFACTOR

Identitets- och åtkomsthantering ökar informationssäkerheten

– din guide för en säkrare verksamhet

Identitets- och åtkomsthanteringen, IAM, är centrala och oskiljaktiga komponenter i en alltmer digital värld.

I den här guiden får du ta del av konkreta kundberättelser och IT-experters syn på hur ett framgångsrikt IAM-arbete kan öka informationssäkerheten, underlätta medarbetarnas vardag och spara avsevärt med både tid och pengar. Du får även inblick i en färsk trendrapport, som bland annat presenterar utvecklingen av investeringar inom den globala cybersäkerhetsbranschen.

Trevlig läsning!

INNOFACTOR

En affärskritisk utmaning

Idag betraktas informationssäkerheten inte längre enbart som en extra kostnad. Allt fler företag och organisationer inser också värdet av en hög informationssäkerhet och attityden till cyberattacker har på senare tid blivit alltmer proaktiv. Trots det rapporterar medier regelbundet om verksamheter som utsatts för attacker och som utöver kritiska data även har förlorat sitt anseende.

Investeringarna i informationssäkerhet inriktas mot de områden där riskerna upplevs som störst. Syftet med identitets- och åtkomsthanteringslösningarna är att skydda den anställdes identitet med hjälp av dataskydd och på så sätt förebygga dataintrång. Idag beror 80 procent av dataintrången på fel som användare orsakar.

INNOFACTOR

Höga investeringar informationssäkerhet

I Gartner Groups "CIO Agenda 2021" uppgav de tillfrågade företagen att satsningar på cybersäkerhet är deras viktigaste investering. Upp till 61 procent av IT-cheferna planerade ytterligare investeringar för att förbättra informationssäkerheten. Enligt Gartners undersökning utnyttjas automatisering och machine learning på senare tid i allt större utsträckning, eftersom cyberattacker kan förebyggas mer proaktivt med hjälp av artificiell intelligens (AI).

Bättre säkerhet och ökad produktivitet

Corona-pandemin försämrade framtidsutsikterna för många företag och organisationer och har ökat osäkerheten. Efter två pandemiår kan vi konstatera att lösningar för identitets- och åtkomsthantering i hög grad har underlättat i övergången mot en ny, mer platsoberoende och hybrid arbetskultur. I denna nya värld spelar IAM-lösningarna en betydande roll när det gäller att skydda ditt företags data och resurser.

Korrekt genomförd IAM effektiviserar produktiviteten genom att möjliggöra en smidig tillgång till utrustning och applikationer, utan att försämra användarupplevelsen.

Inte enbart en fråga om informationssäkerhet

IAM ger personer med ansvar för säkerhet och riskhantering möjlighet att stödja affärsverksamheten bättre. En IAM-lösning kan i bästa fall nämligen bli en konkurrensfördel, genom att ge medarbetarna större möjligheter att arbeta flexibelt och säkert från den plats som passar dem bäst.

IAM är också ett viktigt verktyg vid on- och off-boarding. Det ger nyanställda enkel tillgång till organisationens resurser och när någon slutar blir det lätt att kontrollera och utan dröjsmål ta bort alla åtkomsträttigheter. En god identitets- och åtkomsthantering säkerställer också att regler kring digital hantering av personuppgifter såsom GDPR- och Schrems II efterlevs.

Proaktivt beslutsfattande allt viktigare

Proaktivitet och förutseende blir allt viktigare för att planera den övergripande säkerheten i en organisations och för att kunna driva verksamhet. I Gartners studie betonas bl a att fokus inom informationssäkerhet- och administration måste riktas mot innovation och strategier som tar hänsyn till de utmaningar som den digitala omställningen innebär.

En annan viktig aspekt som Gartner-studien lyfter är hur organisationernas informationssäkerhet kan förbättras i praktiken. För att minska riskerna i samband med dataintrång är det viktigt att varje medarbetare förstår och tar ansvar för sin egen informationssäkerhet. Tydliga rutiner i verksamheten underlättar för organisationen när riskerna ökar. En identitets- och åtkomsthantering som är djupt rotad i organisationskulturen innebär en bättre beredskap för eventuella förändringar i omvärlden.

INNOFACTOR

FAKTA

Identitets- och åtkomsthantering i ett nötskal

Syftet med identitets- och åtkomsthanteringen (IAM) är att trygga organisationens data, utrustning och medarbetare så att arbetet kan utföras på ett produktivt och säkert sätt, oberoende av tid och plats. IAM bör därför vara en integrerad del av organisationens verksamhet. Ett korrekt förhållnings- och tillvägagångssätt bidrar inte bara till att det blir enklare att anpassa sig till nya krav, behov och regler. Det underlättar även anpassningen till plötsliga förändringar inom organisationen eller i omvärlden.

Ett kvalitativt IAM-arbete ger både god säkerhet och bättre användarupplevelse. Innan din verksamhet investerar och implementerar i teknik för identitetsstyrning och administration (IGA) är det viktigt att organisationen planerar införandet i olika steg och etablerar ett officiellt IAM-program.

INNOFACTOR

KUNDCASE

En säker identitetshanteringslösning för norska Betonmast

"Innofactor känner till vårt sammanhang och kan därför erbjuda fungerande lösningar och göra de anpassningar som passar bra just för oss. Det sparar både tid och pengar", säger Øyvind Tørnblad, IT-chef på norska Betonmast.

Betonmast är en av Norges största byggentreprenörer. Affärsverksamheten omfattar många olika typer av byggprojekt inom såväl privat som offentlig sektorn, allt från stora bostadsprojekt till kontorskomplex. Företaget har 16 dotterbolag i Norge och Sverige med sammanlagt cirka tusen medarbetare. För Betonmast är det viktigt att kunna erbjuda sina anställda lätt åtkomst till systemen, oberoende av om arbetet utförs ute på byggplatsen, på kontoret eller någon annanstans.

”Det är mycket viktigt att företaget har möjlighet att kontrollera medarbetarnas digitala identitet och trygga åtkomsten till de applikationer som de behöver”, betonar Øyvind Tørnblad.

Medarbetarnas användarupplevelse i centrum

Innofactor har hjälpt Betonmast att implementera Microsofts IAM- och Identity Manager-lösningar (MIM) för att administrera användaridentiteter och åtkomsträttigheter. För Betonmast var det särskilt viktigt att göra de nya lösningarna tillgängliga även för dem som inte arbetar på kontoret.

INNOFACTOR

”En del arbetar vid datorn, medan andra kanske enbart använder sin egen mobiltelefon på byggarbetsplatsen. Vi har fokuserat särskilt på användarupplevelse och på att lösningen ska vara tillgänglig för alla våra medarbetare, oberoende av roller”.

Inom IT-världen är snabba förändringar vardag. Betonmast ville därför säkerställa att de nya lösningarna är dynamiska, lätta att ta i bruk och anpassar sig till förändringar i omvärlden.

”Vi engagerade en projektledare från Innofactor som vi har ett nära samarbete med. Det är en stor fördel för oss att vi vid behov kan konsultera toppexperter från Innofactor som är insatta i våra lösningar och mål”, säger Øyvind Tørnblad.

Samarbetet med Innofactor möjliggör vid behov också snabba ändringar.

”Personligen anser jag att det är viktigt att vi kan genomföra små förändringar på ett smidigt sätt. Samarbetet med Innofactors lösningsorienterade konsulter sparar både tid och pengar.”

Fler bör tänka på helhetsbilden

Med Microsoft Identity Manager och de lösningar som har införts med hjälp av Innofactor kan Betonmast på ett smidigt sätt ha koll på de anställdas identiteter på ett smidigt sätt i flera olika system. I likhet med andra organisationer många olika slags IT-system. På grund av att informationssäkerhetsriskerna ökar är identitets- och åtkomsthanteringen viktigare än någonsin.

INNOFACTOR

”Vi måste ha en säker identitetshantering, eftersom vi inte på något sätt kan riskera att en medarbetare som lämnar företaget fortfarande har åtkomst till något av våra system. Därför fäster vi särskild uppmärksamhet vid informationssäkerhet och identitetshantering med SaaS-applikationer. Detta är också viktigt med tanke på GDPR.”

Enligt Øyvind Tørnblad tar företag inte en tillräckligt övergripande hänsyn till sin informationssäkerhet när de inför nya applikationer.

”Vi vill hantera alla våra system på ett övergripande sätt. Det känns mer tryggt när vi beaktar identitetshantering och informationssäkerhet i alla delar av vår verksamhet.”

Betonmast blev en del av AF Gruppen 2019 och fick då hela koncernens IT-funktioner på sitt ansvar, inkl licenser, informationssäkerhet och support. Koncernen hade även sedan tidigare ett starkt kunnande inom informationssäkerhet. Koncernen valde ändå att dra nytta av Innofactors kompetens för att integrera Microsoft Identity Manager och applikationer.

”MIM-identitetsportalen är nu direkt länkad till andra system som används inom AF Gruppen. Det gör att det identitetshanteringsarbetetillsammans med Innofactor har fått ännu större betydelse”, säger Øyvind Tørnblad.

INNOFACTOR

FAKTA

Visste du att:

- 65 % av dagens dataintrång orsakas av bristfällig lösenordshantering*
- Hela 82 % av överträdelserna beror på den mänskliga faktorn *
- Utpressningsprogram är det vanligaste och mest växande hotet mot små och medelstora företag i Europa **
- Attacker och dataintrång är mycket dyrt; Till exempel gav ransom-attacken mot Kalix Kommun i december 2021 upphov till miljonkostnader, trots att kommunen inte betalade lösen ***

*https://www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf

**https://www.europarl.europa.eu/news/sv/headlines/society/20220120STO21428/cybersakerhet-de-vanligaste-och-storsta-cyberhoten-under-2021-grafik

***https://www.svt.se/nyheter/lokalt/norrbotten/it-attacken-mot-kalix-kommun-detta-har-hant

KUNDCASE

IAM-lösning gav norska Bjørnafjorden kontroll efter kommunsammanslagning

När de norska kommunerna Os och Fusa slogs samman till kommunen Bjørnafjorden uppstod behovet av en övergripande identitetslösning. Kommunen tog hjälp av Innofactor för att införa en IAM-lösning och göra en utredning av data- och IT-säkerheten i den nya kommunen.

Bjørnafjordens kommun i Norge bildades i januari 2020. Den nya kommunen har knappt 25 000 invånare och cirka 1 800 anställda.

IT-chefen för Bjørnafjorden, Espen Harald Haga, berättar att Os och Fusa efter sammanslagningen beslutade att avveckla sina tidigare servercentraler och sin infrastruktur. På den nya kommunens IT-avdelning arbetar nu sammanlagt 11 personer.

”IT-avdelningarna i Fusa och Os började samarbeta redan 2018. På hösten började vi fundera på vilken IT-lösning som skulle lämpa sig bäst för den nya kommunen Bjørnafjorden”, berättar Haga.

Äntligen kontroll på informationshanteringen

De två tidigare kommunerna kom redan från början överrens om att en övergripande identitets- och åtkomsthanteringslösning (IAM) var viktig för helheten.

INNOFACTOR

”Tidigare behärskade vi inte identitetshanteringen tillräckligt väl. Det visade sig särskilt när nya medarbetare började sina anställningar och gamla slutade. Informationen om att anställningarna hade upphört nådde ofta inte fram till IT-avdelningen, vilket innebar att tidigare anställda kunde ha fortsatt åtkomst till kommunens informationssystem. Detta var ett allvarligt problem för informationssäkerheten.”

Med den insikten började kommunerna kartlägga egenskaper och skillnader i olika IAM-lösningar. Valet föll till slut på en One Identity-lösning som baserar sig på Microsoft Identity Manager (MIM). Bjørnafjorden tog hjälp av Innofactors experter för att införa den nya lösningenoch övergick samtidigt till en e-postlösning baserad på Exchange Online.

”Identitetshantering var ett delområde som vi från början saknade sakkunskap inom. Vi hade inte heller resurser för att själva införa lösningarna, därför vände vi oss till Innofactor”, förklarar Haga.

Enklare och säkrare åtkomsthantering

MIM-lösningen har kopplats till Microsoft Azure AD (Active Directory) för att kunna hantera medarbetares åtkomst till informationsmiljöer och andra nätresurser utifrån vilken AD-grupp varje medarbetare tillhör.

”Nu fungerar våra on- och offboarding-processer betydligt bättre. Bland annat skapas konton för nya användare automatiskt.”

INNOFACTOR

För att kunna utföra vissa arbetsuppgifter behöver kommuner ofta tillgång till olika, ibland även äldre, applikationer som inte nödvändigtvis integreras i de IAM-lösningar som används. Även IT-avdelningen i Bjørnafjorden behöver därför fortfarande radera användare som slutat manuellt från dessa applikationer. I Bjørnafjorden har den processen dock förbättrats genom att det numera skickas ett automatiskt larm till IT-avdelningen när någon slutat. Efter larmet raderas användaruppgifterna manuellt från de applikationer som inte kan hanteras centralt.

Innofactors analys ett viktigt steg i att stärka säkerheten

Den norska informationssäkerhetsmyndighet Norwegian National Security Authority (NSM) konstaterade år 2021 i sin rapport om de nationella riskerna att norska företag under år 2022 löper avsevärda risker att utsättas för utpressningsprogram.

Inom Bjørnafjorden är hotet om utpressningsprogram välkänt. Många norska kommuner har redan varit tvungna att betala ett högt pris för liknande cyberattacker. Också enligt en utredning som gjorts av World Economic Forum ser IT-säkerhetscheferna utpressningsprogrammen som det största hotet mot organisationernas informationssäkerhet.

”Till följd av hotet om utpressningsprogram beslutade vi att ta hjälp av Innofactors experter för att genomföra en säkerhetskartläggning. Även om många delar redan var i gott skick visade det sig att kartläggningen var mycket nyttig. Den gav oss värdefulla tips om hur vi kan förbättra vår beredskap inom informationssäkerhet ytterligare”, säger Tom Ruben Bratholmen, IT-konsult i Bjørnafjorden.

Bratholmen berättar att kommunens IT-avdelning varje fredag fokuserar särskilt på informationssäkerheten. Genomgången omfattar aktuella hot, sårbarheter och rekommendationer som gäller samt konkreta metoder för att förbättra cybersäkerheten.

"Det är viktigt att beakta informationssäkerheten hela tiden – inte först när skadan redan har skett."

IT Manager Espen Harald Haga är mycket nöjd med samarbetet med Innofactor och de positiva effekter som informationssäkerhetsutredningen och identitetslösningen har fört med sig.

”Innofactor har mycket kunniga och trevliga experter. Det var viktigt för oss när vi valde lösningsleverantören”, säger Haga.

5 skäl till att IAM ger konkurrensfördelar

1. Med hjälp av IAM får användarna tillgång till de resurser de behöver, vid rätt tidpunkt och på rätt grunder.

2. IAM är en nödvändig komponent för att garantera säker åtkomst till resurser i komplexa miljöer i enlighet med informationssäkerhetskraven.

3. När du genomför ett IAM-projekt rekommenderas, utöver teknisk kunskap, också affärsmässig kompetens och visioner som möjliggör ett mer flexibelt och informationssäkert arbete.

4. Med tillgång till moderna IAM-verktyg blir identitetshanteringen snabbare och billigare. Utan IAM-verktyg tvingas organisationer göra saker manuellt som kan automatiseras, vilket leder till mer arbete och därmed även dolda kostnader. *

5. En IAM-lösning gör det lättare att växa sin affärsverksamhet och införa nya applikationer.

---

* https://www.gartner.com/en/doc/738620-guide-to-initiating-and-running-an-effective-iam-program

INNOFACTOR

Spara tid och resurser med välplanerad IAM

Företag kan hantera fler risker på kortare tid och medarbetarna kan arbeta på det sätt de anser bäst. Ett viktigt nyckelord är automatisering.

Engelsmannen Stephen Isherwood har arbetat i Norge sedan 2002 och har inom IT-branschen blivit känd för sin gedigna IAM-kompetens. Isherwood började sin karriär inom energisektorn och har arbetet inom såväl små startup-bolag som storföretag, och sedan 2021 på Innofactor.

Bakom övergången låg Isherwoods vilja att hjälpa kunder med informationssäkerhets- och nätverksteknik och i synnerhet IAM-lösningar.

”Det kändes lockande att få dyka ännu djupare i IAM”, säger han.

Han fördjupade sig ursprungligen i identitets- och åtkomsthanteringens värld redan 2016. Då arbetade han på ett företag med vid den tidpunkten några tusen anställda, spridda över mer än 30 verksamhetsställen. Företaget tillämpade rutiner för distansarbete som låg före sin tid och hade ett stort antal användare med åtkomsträttigheter som skulle hanteras och vid behov återkallas.

”Vi hade behov av en mer omfattande användarhantering och därför började vi använda Microsoft Identity Manager (MIM). Genom att administrera användarnas identitet säkerställde vi att medarbetarna kunde arbeta tryggt, oberoende av var de befann sig”.

Framgångsreceptet – IAM-program och väl fungerande säkerhetsprocesser

Det första projektet företaget genomförde gav ett stort mervärde när tusentals användare lades till i IT-miljön genom ett stort företagsförvärv med en tight tidplan.

”Vi lyckades snabbt lägga till nya användare i våra system, eftersom vi hanterade identiteter och redan hade integrerat våra lösningar med de system som HR använde. På så sätt blev IAM en kritisk komponent för affärsverksamheten”, berättar Isherwood.

En korrekt identitetshantering förbättrar organisationens informationssäkerhet, vilket gör det möjligt att fatta smidiga beslut och reagera på förändringar.

”Vi var helt redo för distansarbete när samhället stängdes ner första gången på grund av pandemin. Tack vare tidigare investeringar i IAM kunde vi enkelt ordna det stöd som behövdes för de anställdas hemmakontor i över 30 länder. Allt inom 24 timmar.”

Receptet för framgången var:

- Microsoft Azure Active Directory,
- distanskopplingar,
- identitets- och åtkomsthanterings-program,
- fungerande processer för att minska informationssäkerhetsriskerna.

Spår en framtid utan brandväggar

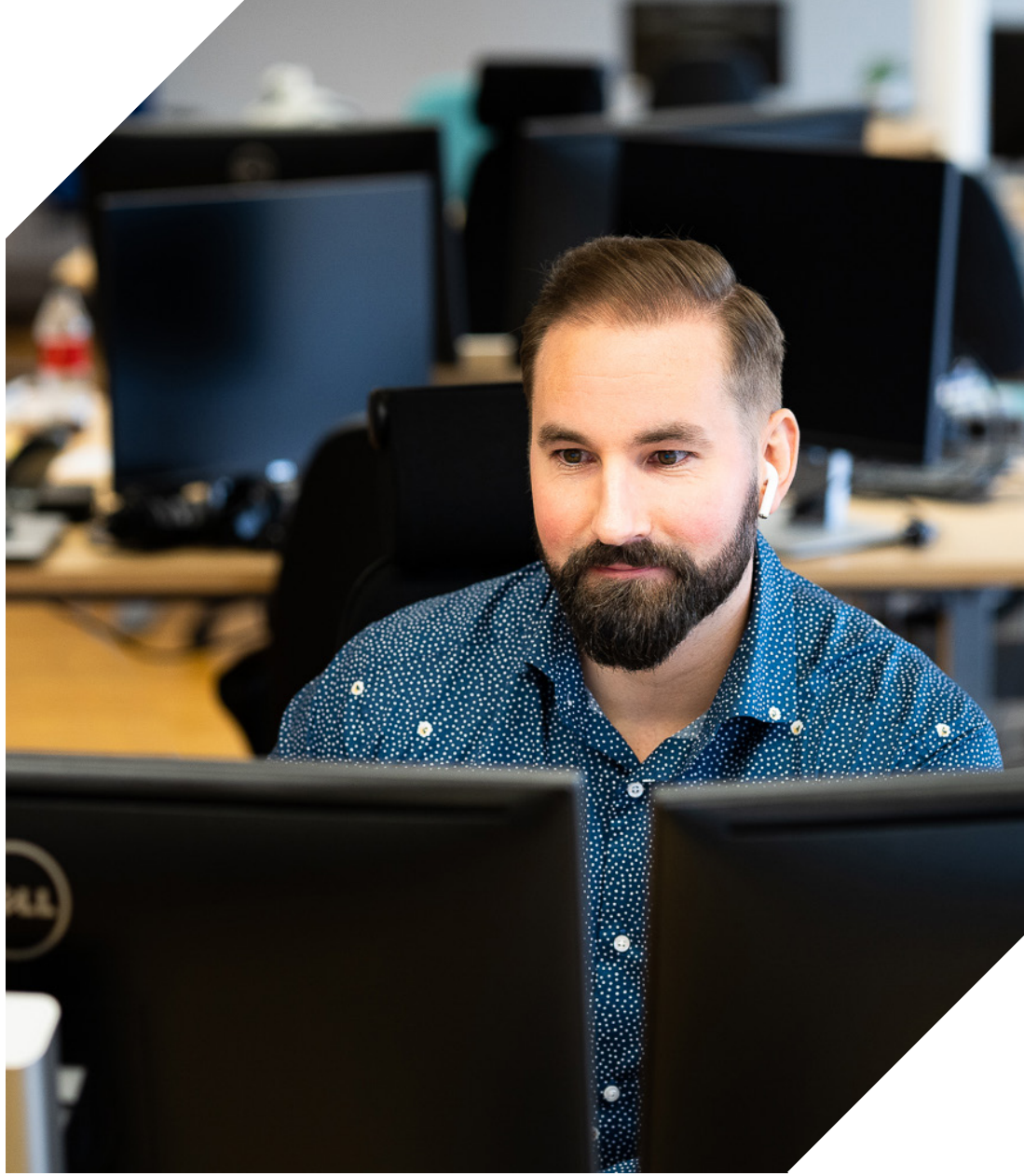
På Innofactor arbetar Stephen Isherwood med kundrelationer där den gemensamma nämnaren är komplexitet och höga krav på dataskydd. Han tror att Microsofts programvara redan nu är så avancerad att den här typen av företag efter några år kanske inte längre behöver brandväggar.

”I framtiden behöver vi bara terminalutrustning, ett användarkonto och en internetanslutning. Åtkomst ges via den programvara som kontrollerar åtkomsten och autentiseringen sker utifrån identiteten.”

Isherwood menar att Microsoft tack vare sina enorma resurser har de bästa förutsättningarna att nå framgång på IAM-marknaden. Microsoft är känt som en föregångare när det gäller informationssäkerhet och för sin förmåga att anamma modern funktionalitet samt inte minst för sina experter och analytiker.

”Microsofts IAM-lösningar har många olika egenskaper, vilket enligt min åsikt gör Microsoft till en ledande aktör i branschen. Deras lösningar minskar sannolikheten för attacker och utpressningsprogram.”

Nya krav av typen GDPR och Schrems II kommer öka inkomsterna ytteligare för Microsoft, eftersom de har höga krav på hanteringen av IT-miljön och de data som lagras.



INNOFACTOR

Automatisering är A och O

Stephen Isherwood betonar att **IT-experternas krav håller på att bli så omfattande och komplicerade att verksamhetsmodellerna måste förändras.** De strategiska arbetsuppgifterna kräver alltmer tid och därför måste tidsresurserna effektiviseras. Det väckte hans intresse för automatisering av olika affärsprocesser.

”Många processer kan förenklas och effektiviseras med hjälp av automatisering. Sådana situationer är till exempel när en ny medarbetare börjar, någon slutar eller när en persons arbetsuppgifter väsentligt förändras. Sådana processer kan vi automatisera genom att skapa arbetsflöden som även förbättrar informationssäkerheten och minskar antalet fel.”

Med automatisering är målet betydande tidsbesparingar.

”När arbetsflödet har utförts på rätt sätt, är det tillförlitligt och fungerar alltid perfekt.”

Dessutom ger det arbetsgivaren tillgång till en loggbok som kan ge snabba svar vid eventuella problem.

”Vi kan erbjuda flera nyttiga mervärden för dem som arbetar med dataskydd”, tillägger Stephen Isherwood.

Viktigt att känna till verksamhetskraven

Enligt Isherwood behöver man vara affärsorienterad för att vara en bra IAM-expert.

”Det behövs mer än teknikkunskap. Vi digitaliserar processerna inom affärsverksamheten. Det en stor fördel att kunna förstå dessa och värdekedjan. När du ska skapa lösningar som stöder organisationens arbetssätt.”

Han rekommenderar en visualisering av arbetsstegen för att kunna kartlägga olika skeenden i affärsprocesserna.

”Det är viktigt att ha en djupgående förståelse för kundens processer. Först därefter väljer man teknik och funktionalitet samt genomför en riskanalys. På så sätt kan vi analysera om enskilda användares inloggning sker från de platser där vi antar att de äger rum.”

IAM behöver vara verksamhetsövergripande

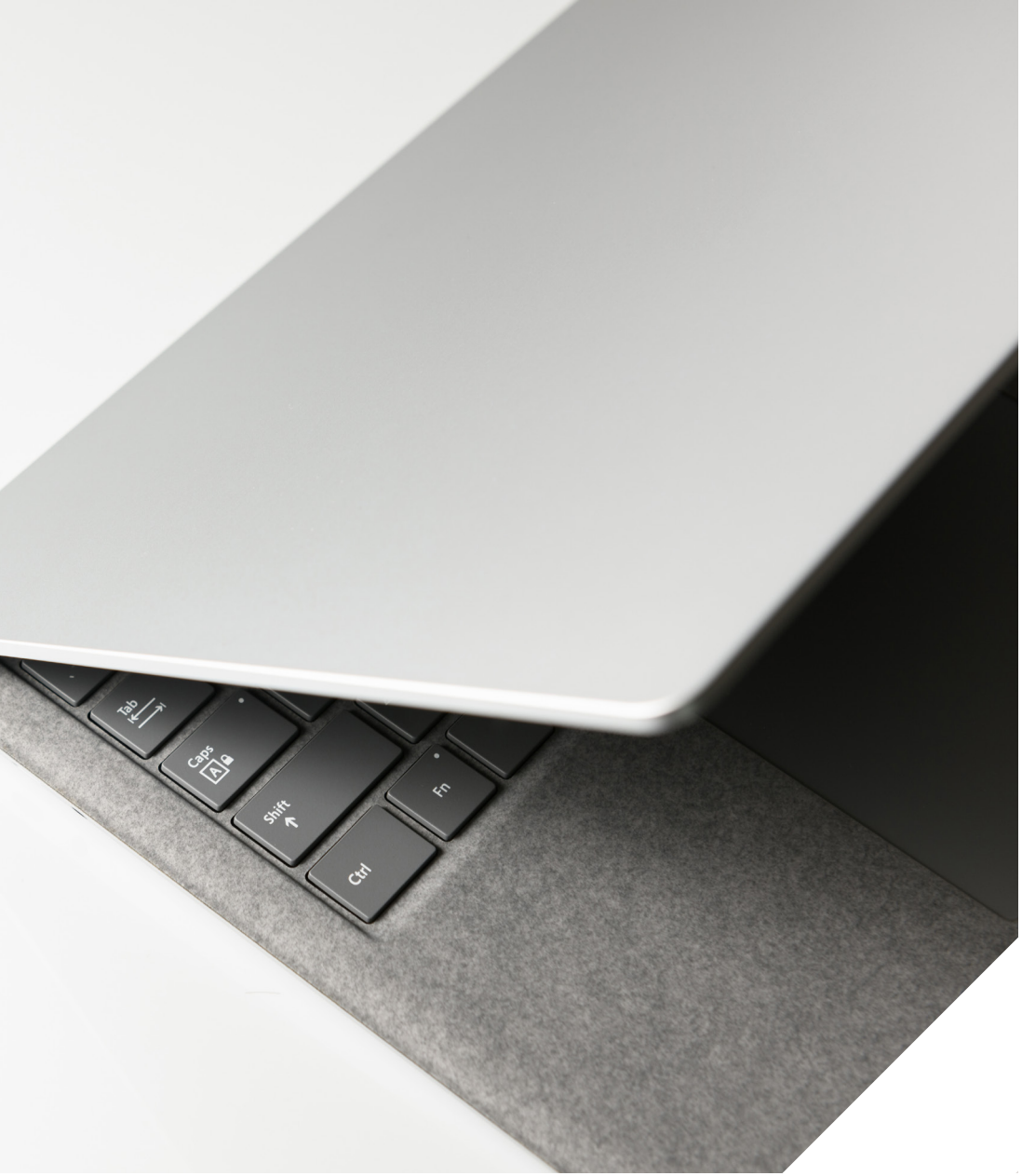
När system och arbetsprocesser integreras blir det resultat. Därför är det viktigt att IT och HR samarbetar i frågor som gäller identitet.

”När vi förenar systemen skapar vi en affärsfördel genom smart integration. HR bör vara med i detta, eftersom högklassig kvalitet på data gagnar alla”, säger Isherwood.

Några viktiga faktorer för att IAM-investeringen ska bli framgångsrik:

”HR och IT måste naturligtvis vara proaktiva och driva förändringen självständigt och på eget initiativ. Detsamma gäller till exempel vid företagsförvärv eller fusion där arbetsmiljön förändras avsevärt.”

”Informationssäkerheten är det viktigaste delområdet. Den största risken har att göra med att angrepp mot användarkontot, men genom att skydda identiteten kan vi minska den risken avsevärt. Det förstår även ledningen.”



FAKTA

Fördubblade investeringar i cybersäkerhet

Enligt Gartners prognos från maj 2021 ökade de globala investeringarna i cybersäkerhet och riskhanteringsteknik 2021 med 12,4 %, till sammanlagt 150,4 miljarder dollar. Ökningen förklaras i huvudsak avomställningen till ett distans- och hybridarbetsliv samt ökade informationssäkerhetskrav på molnplattformar.

Identitets- och åtkomsthanteringens andel av tillväxten var hela 15,6 %.

INNOFACTOR

INNOFACTOR

Ledande i Norden

Innofactor har lång erfarenhet av att hjälpa organisationer i hela Norden att skapa en modern och säker digital miljö som står emot externa hot och cyberattacker. Hos oss får du tillgång till best practice och hela vår ledande nordiska expertis inom datasäkerhet samt en gedigen kompetens om Microsofts banbrytande lösningar.

Hör av dig så berättar vi mer om hur ett samarbete med oss fungerar!
Mailto: daniel.manstrom@innofactor.com

Läs mer om vårt erbjudande inom IAM här