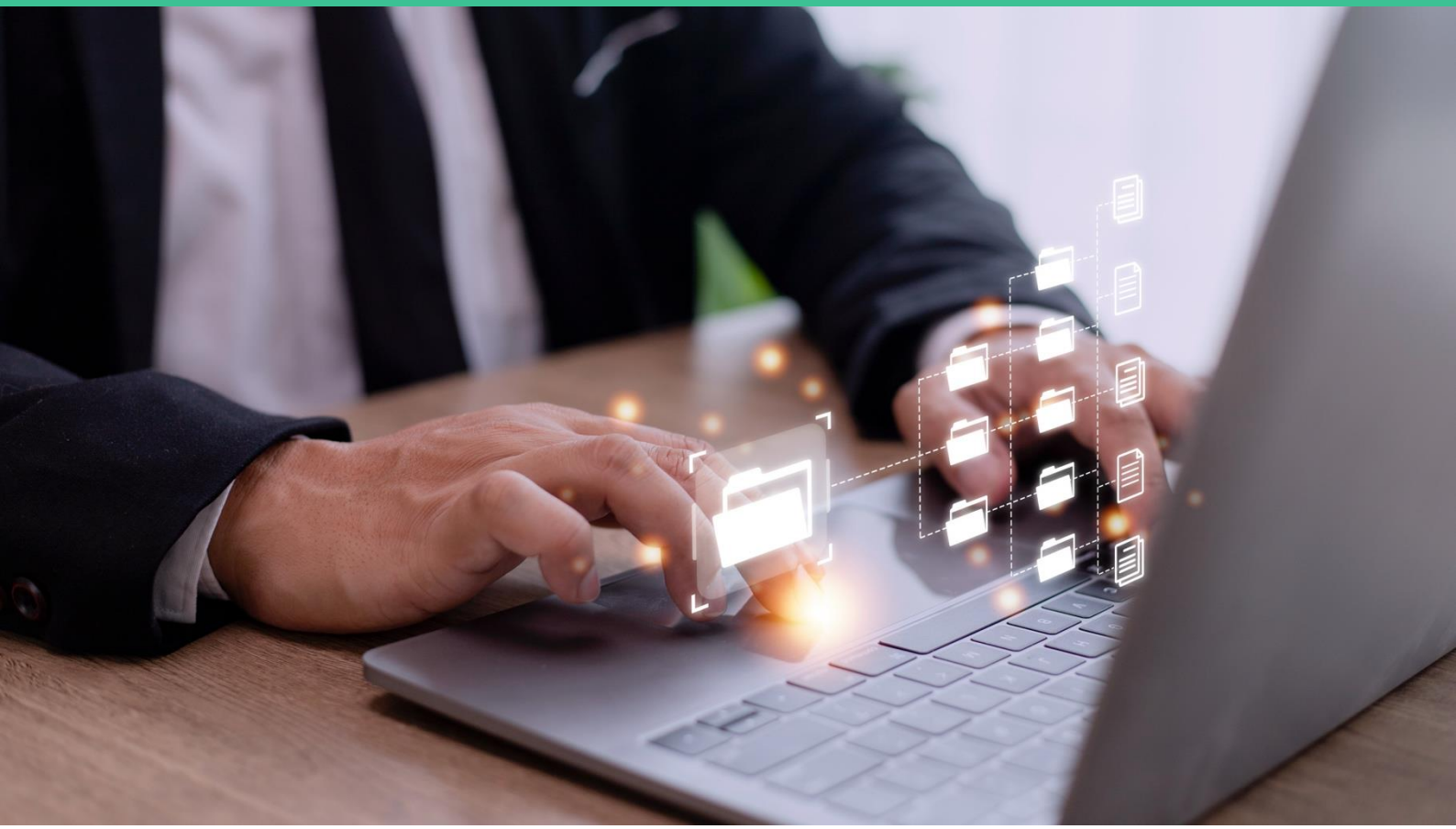
Complior

Säker Lagring

eBook

Säker lagring är avgörande för att skydda känslig information och förhindra obehörig åtkomst. Den här e-boken belyser vikten av att klassificera data och lagra den på ett säkert sätt, samt hur man möter lagkrav och minskar säkerhetsrisker. Oavsett verksamhet är säker lagring en viktig del i cybersäkerhetsstrategin för trygg och effektiv informationshantering.



Innehållsförteckning

Vad är säker lagring?

Säker lagring är en viktig strategi för säkerhetsmedvetna kommuner och företag. Genom att klassificera data och information efter känslighetsgrad kan man effektivt separera Öppen information från Säkerhetsklassad information. Denna strategi innebär att säkerhetsklassad information lagras åtskilt från den öppna, inom en struktur som kallas säker lagring. Detta skyddar känslig information och minimerar risken för obehörig åtkomst.

Behov av säker lagring är stort, då företag och offentlig sektor lagrar både känslig och säkerhetsklassad information. Säker lagring baseras även mycket på vilken ambitionsnivå man har samt vilka eventuella lagkrav och andra regulatoriska krav.

Vad är syftet med säker lagring, och vilken information vill man begränsa från vem?

Syftet med säker lagring är att skydda känslig information och säkerställa att endast behöriga personer har tillgång till den. Genom att separera säkerhetsklassad information från öppna data minimeras risken för dataintrång, informationsläckage och andra säkerhetsincidenter.

Syften med säker lagring:

1. **Skydd av känslig information:** Säker lagring förhindrar obehörig åtkomst till data som kan innehålla personlig information, finansiella uppgifter eller företagshemligheter.

2. **Regelefterlevnad:** Många branscher har strikta regler och lagar för hur känslig information ska hanteras, och säker lagring hjälper organisationer att följa dessa krav.

3. **Riskhantering**: Genom att lagra information på ett säkert sätt kan företag och kommuner minska risken för dataintrång och dess potentiella konsekvenser.

Vilken information vill man begränsa och från vem?

Personuppgifter

Information som rör individer, såsom namn, adresser och personnummer, bör begränsas för att skydda individers integritet.

Affärshemligheter

Företagsstrategier, kundlistor, forskningsresultat och andra affärskritiska uppgifter behöver skyddas från obehöriga, särskilt från konkurrenter eller externa hotaktörer som kan utnyttja informationen för att skada verksamheten.

Finansiell information

Ekonomiska rapporter, betalningsuppgifter och transaktionshistorik är känsliga data som måste skyddas för att förhindra bedrägeri, stöld eller missbruk. Obehörig tillgång till denna typ av information kan leda till omfattande ekonomiska skador.

Kritisk infrastruktur

Information som rör infrastruktur inom IT, energiförsörjning, transporter och liknande områden är ofta mål för spionage eller cyberattacker. Att skydda dessa system är avgörande för att undvika störningar i samhällsfunktioner och förhindra potentiella katastrofer orsakade av intrång.

Gemensamma säkerhets principer

Trots att organisationernas behov av säker lagring varierar, finns det flera gemensamma säkerhets principer som bör vara en del av varje strategi. Dessa principer hjälper till att säkerställa att information hanteras och lagras på ett säkert sätt, oavsett var eller hur den lagras.

1 Klassificering av information

Att klassificera information baserat på dess känslighet är en grundläggande åtgärd för att tillämpa rätt säkerhetsstrategier. Genom att klassificera information i kategorier som exempelvis "offentlig", "intern", "konfidentiell" eller "kritisk" kan organisationer säkerställa att rätt säkerhetsåtgärder appliceras beroende på datans känslighet. Klassificering hjälper även till att avgöra vilka åtkomstkontroller som ska tillämpas och hur informationen får delas både inom och utanför organisationen.

Klassificering med säkerhetsetiketter

För att underlätta hanteringen av klassificerad information kan säkerhetsetiketter användas. En säkerhetsetikett är en märkning som tilldelas data baserat på dess klassificering. Dessa etiketter synliggör datans känslighet för användare och system, vilket gör det lättare att följa riktlinjer för hur informationen ska hanteras. Säkerhetsetiketter kan appliceras manuellt av användare eller administratörer, men även automatiseras baserat på fördefinierade regler och mönster.

Exempelvis kan ett dokument som innehåller personuppgifter automatiskt få etiketten "konfidentiell", vilket gör att åtkomst begränsas och ytterligare säkerhetsåtgärder, som kryptering och åtkomstloggning, aktiveras. Genom att använda säkerhetsetiketter kan organisationer säkerställa att datan hanteras korrekt genom hela livscykeln – från skapande till arkivering eller radering.

Automatisk klassificering

För att förenkla och effektivisera klassificeringsprocessen finns det idag avancerade verktyg som kan automatisera klassificeringen av data. Dessa system kan skanna innehållet i dokument, e-postmeddelanden och filer för att identifiera känslig information baserat på innehåll, metadata eller mönster. Till exempel kan systemet känna igen personnummer, kreditkortsnummer eller andra känsliga nyckelord, och automatiskt tilldela en lämplig säkerhetsetikett.

Automatisk klassificering minskar risken för mänskliga fel, där viktig information potentiellt kan glömmas bort eller klassificeras felaktigt. Det säkerställer också att stora mängder data kan hanteras konsekvent och med minimal administrativ insats.

Vattenmärkning

För att ytterligare skydda känslig information kan vattenmärkning användas som ett komplement till klassificering och säkerhetsetiketter. Vattenmärken kan appliceras på dokument för att synligt indikera deras känslighetsnivå, vilket gör det svårare att oavsiktligt dela eller missbruka informationen. Vattenmärken kan exempelvis inkludera etiketter som "Konfidentiellt" eller "Endast för internt bruk" direkt på dokumentets innehåll, både i digital och utskriven form.

Vattenmärken fungerar även som en avskräckande faktor för obehöriga som försöker sprida känsliga dokument, då de gör det tydligt att materialet är spårbart och märkt som känsligt. I vissa fall kan vattenmärken även innehålla information om dokumentets ägare eller skapare, vilket gör att eventuella dataläckor kan spåras tillbaka till källan.

2 Starka åtkomstkontroller

Åtkomstkontroller är en av hörnstenarna i säker lagring och en kritisk komponent för att säkerställa att endast behöriga personer får tillgång till rätt information. Genom att tillämpa granulära och flexibla åtkomstkontroller kan organisationer definiera exakt vem som har tillgång till vilken data, under vilka omständigheter och med vilka rättigheter. Detta hjälper till att minska risken för obehörig åtkomst och skyddar känslig information från att hamna i fel händer.

Rollbaserad åtkomst (RBAC) och Attributbaserad åtkomst (ABAC)

Traditionellt har rollbaserad åtkomstkontroll (RBAC) varit en vanlig metod för att hantera åtkomst inom organisationer. Denna modell tilldelar åtkomst baserat på användarens roll inom organisationen. Till exempel kan en användare med rollen "administratör" ha bredare rättigheter än en "användare", och dessa roller styr vilken information som kan ses, redigeras eller delas. RBAC är relativt enkel att implementera och förstå, men kan vara begränsad i situationer där mer flexibla och dynamiska åtkomstbeslut krävs.

Attributbaserad åtkomstkontroll (ABAC) erbjuder en mer sofistikerad och flexibel metod för att hantera åtkomst. I stället för att endast basera åtkomst på en användares roll, tar ABAC hänsyn till flera attribut (egenskaper) som kan inkludera användarens identitet, tid, plats, enhetstyp, datans känslighetsnivå och andra kontextuella faktorer. Detta ger organisationer möjlighet att skapa mer dynamiska åtkomstkontroller som kan anpassas till specifika situationer och risknivåer.

Granulära åtkomstkontroller med ABAC

Med ABAC kan åtkomstkontroller preciseras på en mycket detaljerad nivå. Några av de centrala faktorerna som kan användas i attributbaserad åtkomstkontroll inkluderar:

Vem som får åtkomst:

Tillgång baseras inte bara på användarens roll, utan också på deras individuella attribut såsom deras säkerhetscertifikat, anställningsstatus eller deras relation till den data de försöker komma åt.

När och varifrån åtkomst kan ske:

Genom ABAC kan åtkomstbeslut bero på kontextuella attribut som tid och plats. Till exempel kan en användare ha tillgång till viss information endast under kontorstid eller enbart från företagets nätverk. Om användaren försöker nå datan utanför dessa förutsättningar, kan åtkomsten nekas.

Vilken typ av åtkomst som ges:

ABAC möjliggör en finjusterad styrning av vad en användare får göra med informationen. Detta kan omfatta rättigheter som att endast läsa data, redigera den eller dela den vidare. Till exempel kan en användare ges åtkomst att läsa men inte redigera ett dokument, eller ges möjlighet att redigera en fil men inte dela den utanför organisationen.

Fördelar med ABAC i Säker lagring

Dynamisk och flexibel åtkomsthantering:

Genom att använda flera attribut och kombinera dem kan organisationer implementera mer avancerade regler för åtkomst. Detta är särskilt användbart i komplexa miljöer där användare behöver tillgång till olika typer av information beroende på kontexten.

Förbättrad säkerhet:

Genom att inkludera faktorer som plats och tid kan ABAC säkerställa att åtkomst endast ges under säkra och kontrollerade förhållanden, vilket minskar risken för obehörig åtkomst vid exempelvis nätverksintrång eller stulna inloggningsuppgifter.

Bättre efterlevnad:

Med ABAC kan organisationer säkerställa att deras åtkomstpolicyer följer specifika lagar och regulatoriska krav, genom att precisera och automatisera åtkomstregler baserat på de krav som ställs på olika typer av information.

Exempel på användning av ABAC

En anställd kan ha tillgång till en intern rapport när de är på företagets nätverk under arbetstid, men nekas åtkomst när de försöker logga in från en personlig enhet utanför arbetstiden.

Känslig data, såsom affärshemligheter eller personuppgifter, kan automatiskt skyddas beroende på vilken enhet som används, vilket gör att endast enheter som uppfyller säkerhetskraven får full åtkomst.

3 Säker informationsdelning

Säker informationsdelning och samarbete

Att kunna dela information säkert är en kritisk funktion för många organisationer, särskilt de som arbetar i projekt med externa partners, leverantörer eller konsulter. För att säkerställa att känslig information inte hamnar i fel händer krävs robusta verktyg och metoder som gör det möjligt att dela filer och dokument på ett säkert sätt, samtidigt som åtkomsten kontrolleras noggrant.

Krypterad informationsdelning

För att skydda data under överföring och lagring används krypterade kommunikationskanaler. Genom att använda verktyg som möjliggör krypterad delning av filer och dokument kan organisationer säkerställa att endast behöriga mottagare får åtkomst till informationen. Kryptering gör det omöjligt för obehöriga att läsa innehållet, även om det skulle avlyssnas eller stjälas under transport.

Granulär åtkomst vid informationsdelning

Det är viktigt att kunna dela information med rätt personer och med rätt behörigheter. Ett effektivt verktyg för informationsdelning gör det möjligt att:

- **Ställa in olika åtkomstnivåer**, såsom "läs endast", "redigera" eller "dela vidare".
- **Återkalla åtkomst** om det skulle behövas, exempelvis om mottagaren inte längre behöver åtkomst eller om säkerhetskraven förändras. Detta ger organisationen full kontroll över den delade informationen under hela delningsprocessen

Säker läsare för läs-endast åtkomst

En vanlig lösning för att förhindra obehörig spridning eller missbruk av delad information är att använda en **säker läsare.** Detta innebär att mottagaren endast kan läsa informationen via en säker visningsapplikation som förhindrar:

- **Kopiering av text och innehåll.**
- **Nedladdning av dokumentet till en personlig enhet.**
- **Skärmdumpning eller andra sätt att extrahera information.**

Denna metod säkerställer att informationen kan delas på ett kontrollerat sätt och minimerar risken för att känsliga data sprids vidare, även om dokumentet har delats med externa parter.

Användningspolicys baserade på mottagare

En annan viktig aspekt av säker informationsdelning är att tillämpa **individuella policys** beroende på mottagaren och deras roll i organisationen eller projektet. Exempelvis:

- **Externa konsulter** kan tillåtas att öppna ett dokument, men en policy kan tvinga det att öppnas i "läs-endast" läge och med en synlig vattenstämpel som indikerar att dokumentet är konfidentiellt. Detta vattenmärke kan också innehålla mottagarens namn eller e-postadress för att avskräcka från otillåten spridning.

- **Projektanställda** eller interna teammedlemmar kan ges fullständig redigeringsåtkomst till dokumenten. Detta kan inkludera möjligheten att öppna och bearbeta filer i ordinarie program, som exempelvis Microsoft Word, för att underlätta det dagliga arbetet med projektmaterialet.

Genom att ha **granulära användningspolicys** baserade på mottagarens relation till organisationen säkerställs att varje individ får exakt den nivå av åtkomst som krävs för deras uppgifter, och inget mer.

Anpassade säkerhetsnivåer beroende på typ av dokument

Olika typer av information, såsom ritningar, ekonomiska rapporter eller projektdokument, kräver olika nivåer av säkerhet beroende på hur känsliga de är och vem de delas med. Organisationer bör kunna ställa in specifika säkerhetsprinciper för olika typer av information

- **Ritningar** kan till exempel delas med externa byggentreprenörer med möjlighet att endast läsa och kommentera utan att ladda ner dokumentet.

- **Rapporter** kan delas med finansiella partners med åtkomst till både läs- och redigeringsmöjligheter, beroende på deras roll i projektet.

Förhindrande av spridning och missbruk

En av de största utmaningarna med informationsdelning är att förhindra att delad information sprids vidare utan kontroll. Det finns flera tekniker och verktyg som kan användas för att minimera dessa risker:

- **Blockera bifogningar i e-postmeddelanden:** Delad information kan konfigureras så att den inte kan bifogas i e-postmeddelanden eller laddas upp till externa lagringsytor som molntjänster. På detta sätt kan organisationen säkerställa att känslig data förblir inom kontrollerade kanaler och inte sprids okontrollerat.

- **Spårbarhet och revisionsloggning:** All delad information bör vara spårbar. Detta innebär att organisationen kan se vem som har öppnat, redigerat eller delat dokumentet, samt när och var detta skedde. Spårbarhet ger en extra nivå av ansvarsskyldighet och säkerhet, vilket avskräcker obehörig användning av delad information.

Vattenmärkning för ökad säkerhet

Att använda **vattenmärkning** är ett effektivt sätt att ytterligare skydda delad information. Genom att tillämpa automatiska vattenmärken på dokument, som anger att materialet är konfidentiellt eller tillhör en viss avdelning, kan organisationer tydligt visa att informationen är skyddad. Vattenmärken kan också inkludera mottagarens namn eller e-postadress, vilket skapar en avskräckande effekt och gör det möjligt att spåra eventuella läckor.

4 Förhindra datastöld och spridning

Starka säkerhetsåtgärder för att skydda information:

För att skydda information från att stjälas eller spridas, medvetet eller omedvetet, är det avgörande att införa starka säkerhetsåtgärder. Dessa säkerhetsåtgärder hjälper organisationer att hantera både interna och externa hot, och säkerställa att känslig information förblir skyddad.

Här är några av de viktigaste åtgärderna:

Datakryptering både i vila (lagrad) och under överföring:

Kryptering är en grundläggande säkerhetsmetod för att skydda data från obehörig åtkomst. Genom att kryptera information både när den lagras och när den överförs mellan system säkerställs att även om data fångas upp, kan den inte tolkas utan rätt krypteringsnyckel.

Dataläckageskydd (Data Loss Prevention, DLP):

DLP-system används för att identifiera och blockera otillåtna överföringar av känslig information, såsom personuppgifter eller företagshemligheter. Dessa system övervakar och analyserar dataflöden, både internt och externt, och kan automatiskt vidta åtgärder som att blockera eller varna när känslig data försöker lämna organisationens nätverk på ett otillåtet sätt.

Automatisk upptäckt (discovery) av känslig data:

Moderna säkerhetssystem kan automatiskt skanna och identifiera känslig information i organisationens nätverk, dokument och e-post. Denna automatiska upptäckt säkerställer att även oupptäckt eller oklassificerad känslig data kan lokaliseras och skyddas. Systemet kan till exempel upptäcka personuppgifter, finansiella data eller immateriella rättigheter, och säkerställa att dessa uppgifter hanteras i enlighet med företagets policyer och regelverk som GDPR.

Automatisk etikettering av känslig data:

När känslig data identifieras kan system för automatisk etikettering tillämpa säkerhetsetiketter baserat på datans innehåll eller kontext. Detta innebär att all känslig information automatiskt får rätt etikett, som "konfidentiell" eller "endast för internt bruk", utan att användaren behöver ingripa manuellt. Automatisk etikettering bidrar till att säkerställa att säkerhetsåtgärder tillämpas konsekvent och att rätt skyddsnivå appliceras på all känslig data

Användarutbildning:

Även de bästa tekniska lösningarna kan inte helt eliminera den mänskliga faktorn. Användarutbildning är en viktig del av säkerhetsarbetet. Genom att utbilda anställda i att förstå vikten av att skydda känslig information och hur man undviker vanliga säkerhetsrisker, som phishing eller osäker hantering av data, kan organisationer minska risken för oavsiktliga säkerhetsincidenter. Det är särskilt viktigt att användare lär sig identifiera varningar från säkerhetssystem och följa interna rutiner för informationshantering.

5 Spårbarhet och loggning

Tydlig spårbarhet genom loggning av alla åtkomstförsök och datatransaktioner är en avgörande komponent för att kunna upptäcka, utreda och förhindra säkerhetsincidenter. Loggning fungerar som en "svart låda" för systemet, vilket ger insyn i hur data hanteras och används. Genom att övervaka och dokumentera varje interaktion med känslig information, skapas ett ovärderligt verktyg för både proaktiv och reaktiv säkerhetshantering.

Vad bör loggningen omfatta?

Effektiv loggning ska täcka flera aspekter av dataåtkomst och användning för att säkerställa full spårbarhet:

Vem som har fått åtkomst: Identifiering av användaren (inklusive deras roll eller behörigheter) som försöker få tillgång till information. Detta inkluderar både interna användare och externa parter, såsom konsulter eller leverantörer. Loggen ska även kunna kopplas till individens autentiseringsmetod (t.ex. lösenord, tvåfaktorsautentisering).

När åtkomsten skedde: Exakta tidsstämplar för varje åtkomstförsök eller datatransaktion. Genom att veta när en specifik åtgärd inträffade kan organisationen snabbt identifiera misstänkta eller obehöriga åtkomstförsök under oregelbundna tider, såsom utanför ordinarie arbetstider.

Varifrån åtkomsten gjordes: Information om den plats eller enhet där åtkomsten skedde, såsom IP-adress, nätverksplats eller vilken enhet som användes (exempelvis mobil, dator eller surfplatta). Detta gör det möjligt att spåra om åtkomsten gjorts från säkra nätverk eller från potentiellt osäkra eller otillåtna platser.

Vad användaren har gjort med informationen: Det är inte bara viktigt att veta att någon har fått tillgång till data, utan även vad de gjort med den. Loggningen bör omfatta vilka filer eller data som har öppnats, ändrats, delats, kopierats eller raderats. Detta ger en fullständig bild av användarens aktivitet och kan hjälpa till att identifiera potentiellt skadliga beteenden, som att kopiera stora mängder data eller dela känslig information med obehöriga.

Säkerhetsincidenter och utredning

En välutvecklad loggningsfunktion ger organisationer möjlighet att snabbt och effektivt identifiera potentiella säkerhetsincidenter. Vid ett dataintrång eller annan säkerhetsöverträdelse kan loggarna analysera exakt hur intrånget skedde, vilka data som exponerades och hur stort hotet var. Detta möjliggör en snabb och målinriktad respons, inklusive att isolera händelsen, stoppa ytterligare intrång och genomföra återställningsåtgärder.

Regelefterlevnad och rapportering

I många branscher, särskilt inom offentlig sektor, finans och hälso- och sjukvård, krävs det att organisationer följer specifika lagar och regleringar som kräver spårbarhet. Exempel på sådana regleringar inkluderar GDPR (General Data Protection Regulation), som kräver att organisationer kan visa att personuppgifter hanteras på ett säkert sätt och att alla åtkomstförsök till dessa data dokumenteras. Loggar hjälper organisationer att uppfylla dessa krav genom att tillhandahålla en historik av hur data har hanterats och av vem.

Om en organisation drabbas av en säkerhetsincident där känslig information äventyras, måste den ofta rapportera till tillsynsmyndigheter. Tydliga och detaljerade loggar gör det möjligt för organisationen att snabbt sammanställa den nödvändiga informationen och bevisa att lämpliga åtgärder vidtagits för att skydda data. Detta kan minska böter och andra påföljder samt förbättra förtroendet hos kunder och affärspartners.

Automatisering och analys

Många moderna säkerhetssystem använder automatiserad loggning och analysverktyg för att snabbt upptäcka avvikelser i användarbeteende och potentiella säkerhetshot. Till exempel kan sådana system varna om en användare plötsligt börjar ladda ner ovanligt stora mängder data, eller om åtkomstförsök görs från en ovanlig plats. Automatiserad incidentrespons kan också användas för att blockera åtkomst omedelbart om ett potentiellt intrång upptäcks, vilket begränsar skadorna innan de hinner eskalera.

Loggningens roll i revision och säkerhetsförbättring

Loggar spelar även en viktig roll vid regelbundna säkerhetsrevisioner. Organisationer kan använda loggdata för att analysera åtkomstmönster, identifiera svagheter i åtkomstkontroller och anpassa sina säkerhetspolicyer över tid. Genom att regelbundet granska loggar kan man upptäcka och åtgärda potentiella säkerhetsbrister innan de utnyttjas av obehöriga.

6 Kryptering

Stark kryptering är en grundläggande säkerhetsåtgärd för att skydda känslig information, både när den lagras och när den överförs. Genom att kryptera data säkerställs att även om information skulle stjälas eller tappas bort, kan den inte läsas av obehöriga.

Kryptering bör användas på all känslig data, och organisationer bör regelbundet uppdatera sina krypteringsmetoder för att hålla sig i linje med de senaste säkerhetsstandarderna.

Oavsett om krypteringen sker på en lokal filserver eller i en publik molntjänst är det viktigt att uppfylla kraven för HYOK (Hold Your Own Key). Med HYOK får organisationen fullständig kontroll över sin data genom att själv skapa, lagra och hantera krypteringsnyckeln. Denna nyckel skyddas av en HSM (Hardware Security Module), vilket säkerställer att nyckeln lagras och hanteras på ett mycket säkert sätt.

Genom att använda sin egen krypteringsnyckel kan organisationen skydda sin data oberoende av tredjepartsleverantörer, och den har därmed total äganderätt och kontroll över datan. Detta innebär att krypteringsnyckeln kan lagras i Sverige, under svensk suveränitet och lagstiftning, vilket är avgörande för att säkerställa efterlevnad av lokala regler och skydd mot utländska jurisdiktioner.

Ett viktigt skydd som HYOK erbjuder är att det förhindrar att exempelvis en molnleverantör tvingas lämna ut data under lagar som FISA (Foreign Intelligence Surveillance Act) i USA, eftersom leverantören inte har tillgång till krypteringsnyckeln. Dessutom hindrar HYOK att molnleverantörens administratörer, eller en potentiell angripare som stjäl deras nycklar, kan få åtkomst till organisationens data. Genom att hålla kontroll över sin egen krypteringsnyckel minimeras risken för obehörig åtkomst och säkerställer att ingen annan än organisationen själv kan dekryptera och komma åt den känsliga informationen.

Complior

Att säkerställa en robust lösning för säker lagring kräver inte bara tekniska lösningar utan även efterlevnad av juridiska och regulatoriska krav. Genom att använda moderna metoder för kryptering och nyckelhantering kan företag och organisationer garantera full kontroll över sin data, oavsett om den lagras lokalt eller i en publik molntjänst.

Complior erbjuder en bred uppsättning säkerhetstjänster för organisationer som vill skydda sina känsligaste data. Genom sin **PCI DSS-certifierade molninfrastruktur** och tjänster som **HSM** och **Key Management Systems (KMS),** kan företag enkelt implementera säkra lösningar för lagring, nyckelhantering och efterlevnad av regler som GDPR och PCI DSS, DORA, NIS2.

Complior erbjuder en komplett lösning för säker lagring genom kryptering och nyckelhantering, oavsett om det sker lokalt eller i molnet. Vårt starka partnerskap med **archTIS** har utökat våra lösningar med **NC Protect** och **NC Encrypt**, som ger kunder möjlighet att automatiskt klassificera och skydda ostrukturerad data i Microsoft 365 och andra miljöer. Genom **HYOK (Hold Your Own Key)** och integration med lokal KMS, får kunder full kontroll över sina krypteringsnycklar, vilket garanterar datasuveränitet och skydd.

Mer information om Complior och lösningar finns här: www.complior.se/products

Complior erbjuder inte bara verktygen för säker lagring och kryptering utan också en pålitlig partner som säkerställer att organisationer kan hålla sig i linje med internationella och lokala lagar, och samtidigt behålla full kontroll över sin mest värdefulla data.


Complior