En genomgång av säkerhetsincidenter och åtgärder avseende molntjänster

JOHN ZIEGENBEIN OCH VIKTOR BERGSTRÖM

FOI-R--5825--SE
ISSN 1650-1942 December 2025

John Ziegenbein och Viktor Bergström

En genomgång av säkerhetsincidenter och åtgärder avseende molntjänster

Titel	En genomgång av säkerhetsincidenter och åtgärder avseende molntjänster
Title	A review of cloud incidents and security controls

Rapportnr/Report no	FOI-R--5825--SE
Månad/Month	December
Utgivningsår/Year	2025
Antal sidor/Pages	66
ISSN	1650-1942
Uppdragsgivare/Client	Försvarsmakten
Forskningsområde	Cyberförsvar och cybersäkerhet
FoT-område	Inget FoT-område
Projektnr/Project no	E38079
Godkänd av/Approved by	Emil Hjalmarson
Ansvarig avdelning	Cyberförsvar och ledningsteknik
Exportkontroll	Innehållet är granskat och omfattar ingen information som är underställd exportkontrollagstiftningen.

Bild/Cover	Shutterstock

Sammanfattning

Molnteknologi har under senare år fått en betydande ökning i användning, bland annat som en lösning på det kontinuerligt växande behovet av beräkningskapacitet, exempelvis inom områden för artificiell intelligens. Samtidigt ökar antalet säkerhetsincidenter i molntjänster varje år, vilket understryker behovet av fördjupad kunskap om molnsäkerhet för att möjliggöra användning i säkerhetskänsliga sammanhang.

Denna rapport syftar till att utvärdera incidenter och säkerhetsåtgärder relaterade till molnsäkerhet. Genomgång av fem populära säkerhetsramverk utförs för att identifiera överlappande åtgärder och säkerhetskategorier. Vidare analyseras 157 rapporterade molnincidenter från de senaste 10 åren. Incidenterna analyseras med avseende på orsak till incidenten, med hjälp av de säkerhetskategorier som identifieras i tidigare steg. Även konsekvenserna av dessa incidenten analyseras. Slutligen analyseras hur de vanligast förekommande orsakerna bakom molnincidenterna kunde ha förhindrats baserat på de identifierade säkerhetsåtgärderna.

Resultaten av analysen pekar på att incidenterna i stor utsträckning beror på enklare felkonfigurationer, främst inom områdena identitets- och åtkomsthantering, infrastruktur samt dataskydd. En vanligt återkommande orsak till incidenter är publikt åtkomliga molnbaserade resurser utan tillräcklig åtkomstkontroll eller utan kryptering av känslig information. Säkerhetsramverken är omfattande och komplexa, vilket gör dem svåra att följa i praktiken. Samtidigt finns flera säkerhetsåtgärder som återkommer i alla ramverk, vilket tyder på en viss samsyn inom branschen. Dessa gemensamma åtgärder presenteras och diskuteras i rapporten. Resultaten visar också att molnsystem ofta snabbt blir komplexa, något som många organisationer har svårt att hantera på ett säkert sätt. Att använda säkerhetslösningar från molnleverantören kan underlätta, men kräver ofta specialiserad kompetens.

Nyckelord: moln, molnsäkerhet, molnarkitektur, molnincidenter, säkerhetsramverk

Summary

Cloud technology has exploded in popularity, partly as a solution to the continuously increasing demands on computing power posed by new technologies such as artificial intelligence. Furthermore, the amount of reported cloud-related security incidents is increasing steadily year by year. Thus, if cloud computing is to be used within security critical systems, building knowledge about cloud security is a top priority.

This report aims to evaluate incidents and security mitigations related to cloud security. Five popular security frameworks are examined in order to identify overlapping mitigations and security controls. These identified categories are then used to analyze 157 reported cloud incidents from the last 10 years. Furthermore, the consequences of these incidents are also examined. Lastly, security controls which help prevent many of the most common causes of identified incidents are presented.

The results of this evaluation points to a large amount of simpler misconfigurations, mostly within the areas identity and access management, infrastructure, as well as data protection. A recurring cause of incidents is publicly accessible resources that lack sufficient access control or fail to encrypt sensitive information. The security frameworks examined are comprehensive and complex, but contain a large overlap with regards to several recurring controls shared between the frameworks. These overlapping mitigations are presented and discussed in the report. The results further point to cloud systems tend to quickly become complex, which many organisations struggle to manage securely. Use of provider-specific security solutions can aid in managing this complexity substantially, but may require specialized competence.

Keywords: cloud, cloud security, cloud architecture, cloud incidents, security frameworks

Innehåll

1 Inledning

De stora framstegen inom exempelvis artificiell intelligens, maskininlärning, simulering samt rendering av grafik ställer högre krav på datorkraft än någonsin. Genom större, globalt utspridda, datacenter som drivs och förvaltas av molntjänstleverantörer kan organisationer expandera sina verksamheter och nyttja den datorkraft som krävs utan att själva behöva bygga och underhålla egna serveranläggningar.

Nedan följer några exempel på kommersiella organisationer som för närvarande nyttjar molntjänster i sina verksamheter:

- **Netflix**[1]
  Videoströmningstjänsten *Netflix* använder molntjänster från molnleverantören *Amazon Web Services (AWS)*[2] för att lagra, hantera och strömma högupplöst video till miljontals användare världen över.
- **Spotify**[3]
  Musikströmningstjänsten *Spotify* nyttjar sedan 2016 molntjänster från molnleverantören *Google Cloud Platform (GCP)*[4] för att lagra, hantera och strömma ljuddata till flera miljoner kunder runt om i världen [1], [2].
- **eBay**[5]
  Det multinationella auktionssajten *eBay* använder sedan 2010 molntjänster från molntjänstleverantören *Microsoft Azure* för att tillgängliggöra auktionsajten till hela världen [3].

Under de senaste åren har även statliga aktörer, såsom myndigheter och andra offentliga institutioner, börjat uppmärksamma molnet som en viktig teknologi. En av de större nationerna som har gjort investeringar i molnlösningar är USA, där de bland annat har utvecklat en strategi för att modernisera sin IT-infrastruktur inom militären genom initiativ såsom *Joint Warfighter Cloud Capability (JWCC)* [4], [5]. Detta program syftar till att med hjälp av kommersiella molnleverantörer skapa en flexibel och säker molnplattform som stödjer behovet hos diverse leverantörer till USA:s försvarsdepartement[6] att snabbt kunna hantera och bearbeta stora mängder data. I Europa har liknande initiativ påbörjats, såsom studien *Cloud Intelligence for Decision Support and Analysis (CLAUDIA)*, för att analysera behovet av att använda moln i försvarstillämpningar [6]. Studien fastslog att molnteknologier erbjuder stora fördelar, såsom förbättrad interoperabilitet mellan medlemsländer, snabbare databehandling och ökad flexibilitet vid hantering av kritiska resurser och information i realtid.

Säkerheten för molnbaserade system innefattar inte bara den administrativa hanteringen av molnmiljön, utan även faktorer som den komplexa nätverksdesignen och webbsäkerheten för de tjänster som ska driftas i molnet. Detta leder till en systemkomplexitet som snabbt blir svåröverskådlig, vilket syns i den stora mängd

[1] `https://www.netflix.com/se-en/`
[2] `https://aws.amazon.com/`
[3] `https://open.spotify.com/`
[4] `https://cloud.google.com/`
[5] `https://www.ebay.com/`
[6] USA:s försvarsdepartement syftar i detta fall på *United States Department of Defense (DoD)*.

molnrelaterade säkerhetsincidenter som rapporteras varje år. En studie av det franska försvarföretaget Thales från 2024 visade att 44 % av organisationer från 18 olika länder bland 37 branscher hade drabbats av minst en molnrelaterad dataläcka, varav 14 % rapporterade minst en läcka under 2024 [7]. Vidare sågs en ökning av molnbaserade intrång med 75 % 2023 jämfört med 2022, enligt en rapport från det amerikanska IT-säkerhetsföretaget CrowdStrike [8]. Ett exempel på ett omfattande intrång är dataläckan från bank- och finanskoncernen *Capital One* år 2019, där cirka 106 miljoner individers kredit- och bankkortsuppgifter komprometterades till följd av bland annat en felkonfigurerad brandvägg [9]. Generellt visar den stora mängden molnbaserade incidenter som rapporteras ett växande behov av både effektiva molnsäkerhetsåtgärder och en ökad teknisk kompetens inom området.

Den ständigt ökande användningen av molntjänster förväntas bidra till en utvidgad attackyta för stora delar av samhällets IT-infrastruktur. Användningen av molnbaserade lösningar inom säkerhetskänslig verksamhet kan vara attraktiv ur både ett ekonomiskt och logistiskt perspektiv, men medför samtidigt potentiella säkerhetsrisker. Mot denna bakgrund är en fördjupad kompetens inom molnsäkerhet en nödvändig förutsättning om molnteknologi ska kunna tillämpas på ett säkert sätt.

1.1 Syfte

Denna studie syftar till att öka kunskapen om molnsäkerhet och undersöka hur teknologin kan användas effektivt inom säkerhetskänslig verksamhet. Vidare ämnar studien att analysera konkreta tekniska brister som lett till molnsäkerhetsincidenter samt vad det finns för åtgärder för att förhindra dessa incidenter.

1.2 Forskningsfrågor

I syfte att tillhandahålla och utveckla kunskap om molnsäkerhet avser denna studie att besvara följande forskningsfrågor:

- Vilka typer av sårbarheter har orsakat molnbaserade säkerhetsincidenter under de senaste tio åren?
- Vilka säkerhetsåtgärder rekommenderas av erkända institutioner och auktoriteter inom molnsäkerhet?
- Vilka av de identifierade säkerhetsåtgärderna förhindrar eller mitigerar vanligt förekommande orsaker till de analyserade säkerhetsincidenterna?

1.3 Avgränsningar

Studien som beskrivs i denna rapport behandlar molnsäkerhet i publika molntjänster ur ett praktiskt molntjänstanvändarperspektiv. Detta innebär att de delar av systemet som molntjänstleverantören ansvarar över inte beaktas. Incidenter som beror på själva molntjänstleverantören bedöms således huvudsakligen vara utanför ramen för

studien. Rent organisatoriska metoder samt strategier för kompetensutveckling eller träning av personal ingår inte i studien.

2 Bakgrund

The National Institute of Standards and Technology (NIST) Special Publication 800-145 [10] definierar molntjänster enligt följande:

> Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

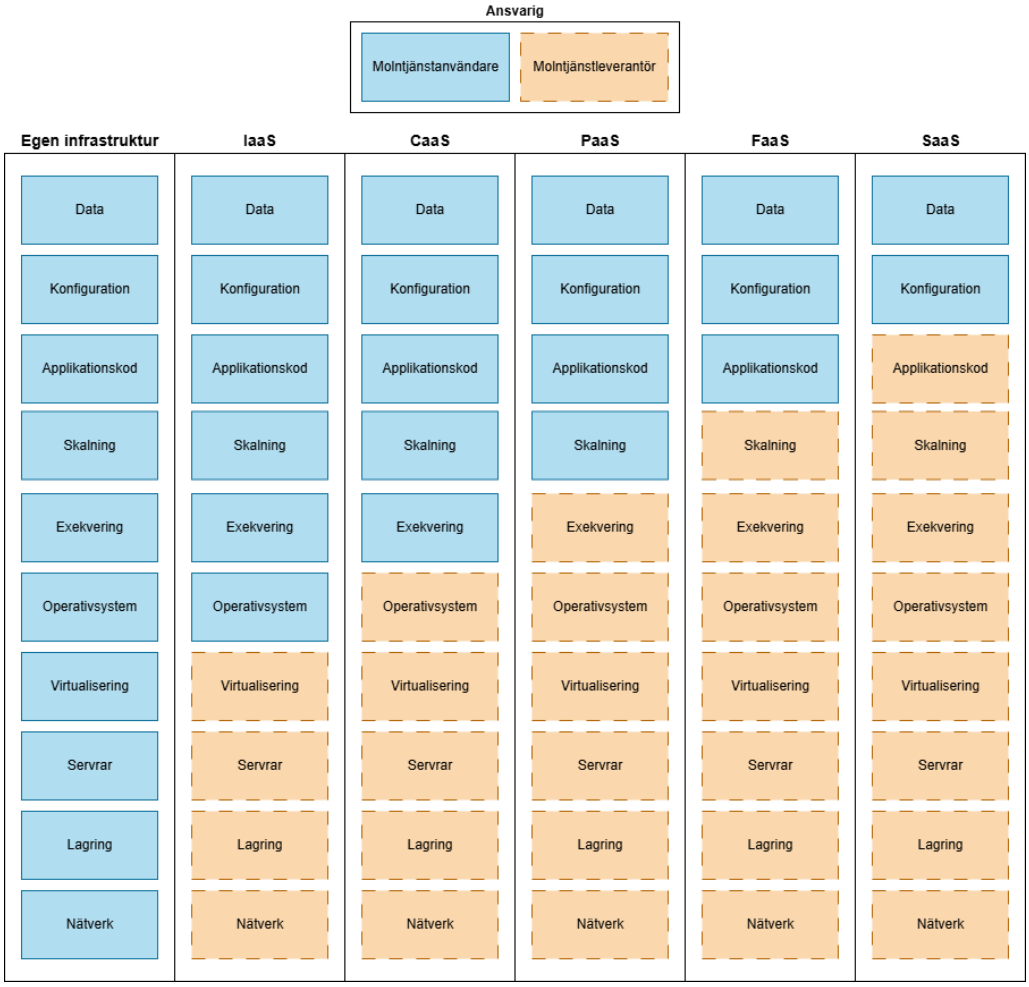
Molntjänster omfattar därmed tillgång till datorkapacitet från en delad pool av fysiska resurser. Definitionen betonar även att resurser ska kunna provisioneras snabbt och enkelt, med minimal interaktion med tjänsteleverantören.

Molntjänstleverantörer realiserar molntjänster genom att tillhandahålla datorkapacitet från sina globala infrastrukturer, vilka består av flera datacenter som är sammankopplade för att bilda egna globala nätverk. Dessa nätverk delas vanligtvis in i regioner, som i sin tur delas upp i tillgänglighetszoner (eng. availability zones), vilka består av ett eller flera datacenter. Kunden väljer från vilka regioner och tillgänglighetszoner resurser ska provisioneras. Åtkomsten till den tilldelade delen av datorkapacitetspoolen separeras med hjälp av virtualisering.

2.1 Molntjänstemodeller

NIST SP 800-145 [10] definierar tre huvudtyper av molntjänstemodeller, baserade på den ansvarsmodell som tillämpas mellan användaren och molntjänstleverantören. De tre huvudtyperna av molntjänstemodellerna är *Infrastructure as a Service* (IaaS), *Platform as a Service* (PaaS), och *Software as a Service* (SaaS). Utöver dessa har molntjänstleverantörer efter behov introducerat ytterligare två typer av molntjänstemodeller: *Container as a Service* (CaaS), som etablerades genom Kubernetes [11], samt *Function as a Service*, ofta benämnd *serverless*, som populariserats genom AWS Lambda [12].

För att beskriva ansvarsfördelningen för olika molntjänstemodeller mellan molntjänstleverantörer och deras användare brukar den delade ansvarsmodellen (eng. shared responsibility model) användas. Den delade ansvarsmodellen för respektive typ av molntjänst illustreras i figur 2.1.



Figur 2.1: Ansvarsfördelningen för olika typer av molntjänstemodeller.

De fem typerna av molntjänstemodeller som tillhandahålls av molntjänstleverantörer idag beskrivs nedan[13] [14] [15]:

- **IaaS**
  Molntjänstleverantören tillhandahåller och hanterar hela den fysiska infrastrukturen, såsom beräkningskraft, lagring, nätverk och virtualisering. Ansvaret för att konfigurera, underhålla och administrera virtuella maskiner samt tillhörande programvara ligger dock på användaren. Exempel på IaaS-tjänster är AWS Elastic Compute Cloud (EC2), Azure Virtual Machines och Google Compute Engine.
- **CaaS**
  Molntjänstleverantören tillhandahåller möjlighet att drifta containrar (istället för virtuella maskiner som används vid IaaS). Användaren ansvarar för allt som finns inom containern. Exempel på CaaS tjänster är AWS ECS, Azure Container Instances, och Google Cloud Run. De molntjänstleverantörer som nämnts ovan har även separata tjänster för att drifta Kubernetes kluster.
- **PaaS**
  Molntjänstleverantören tillhandahåller hela exekveringsmiljön. Användaren behöver enbart tillhandahålla kod för att drifta tjänsten. Exempel på PaaS tjänster är AWS Elastic Beanstalk, Azure App Service, och Google App Engine.

- **FaaS**
  Molntjänstleverantören erbjuder möjligheten att drifta en funktion som utför en specifik uppgift. Likt PaaS behöver användaren bara tillhandahålla kod, men har dessutom delegerat bort konfiguration och hantering av upp- och nerskalning till molntjänstleverantören. Exempel på FaaS tjänster är AWS Lambda, Azure Functions, och Google Cloud Run Functions.
- **SaaS**
  Molntjänstleverantören ansvarar för både applikationskoden och driften av systemet. Detta innebär att användaren enbart har ansvar för konfiguration och data i applikationen. Exempel på kända SaaS-tjänster är Shopify, Zoom och Dropbox.

Molntjänstemodeller med större andel ansvar hos molntjänstleverantören, som FaaS och SaaS, kan anses gynnsamma från ett säkerhetsperspektiv då de reducerar den driftsmässiga komplexiteten hos användarnas del av systemet. Dock medför de minskad flexibilitet och kontroll jämfört med exempelvis IaaS, vilket kan vara problematiskt beroende på syftet med att nyttja molntjänsten. Det finns ofta restriktioner på vad som går att göra med tjänster där stort ansvar placeras på molntjänstleverantören. Ett exempel är FaaS där det typiskt finns hårda krav på maximal exekveringstid för driftade funktioner.

I moderna molnsystem kombineras ofta olika molntjänster med olika ansvarsmodeller. Således finns vanligtvis inte en ren fördelning av ansvar, utan användaren måste själv hålla reda på gällande ansvarsmodell för respektive molntjänster.

2.2 Molndistributionsmodeller

Molntjänster kan även kategoriseras utifrån olika distributionsmodeller. NIST SP 800-145 [10] beskriver fyra huvudsakliga modeller för distribution av molntjänster.

- **Publika moln (eng. public cloud)**
  Molninfrastruktur tillhandahålls av en molntjänstleverantör till allmänheten över ett offentligt nätverk. Den underliggande hårdvaran delas således mellan olika organisationer, även om de logiska resurserna är isolerade från varandra.
- **Privata moln (eng. private cloud)**
  Molntjänster tillhandahålls till en enskild organisation. Infrastrukturen driftas i organisationens lokaler (s.k. *on-site private clouds*) eller hos en eller flera värdorganisationer (s.k. *outsourced private clouds*) eller i en kombinerad konstellation.
- **Kollektiva moln (eng. community cloud)**
  Infrastruktur tillhandahålls till ett begränsat kollektiv av organisationer med delade intressen[7]. Likt för privata moln kan infrastruktur i kollektiva moln driftas i organisationernas egna lokaler eller hos en tredje part. Driften och hanteringen av resurserna kan åläggas klienterna eller värdorganisationen alternativt fördelas mellan dem. Dessa moln är inte tillgängliga för parter utanför kollektivet.

[7] Detta kan vara delade uppdrag, säkerhetskrav, policyer, etc.

- **Hybridmoln (eng. hybrid cloud)**
  Hybridmoln kombinerar åtminstone ett privat och ett publikt moln. Ett exempel på vanlig användning är integrering av egen infrastruktur i ett hybridmoln för att bibehålla fullständig kontroll över känslig information.

Utöver de molndistributionsmodeller som NIST SP 800-145 beskriver, finns även multimoln (eng. multi cloud). Multimolnsystem kombinerar åtminstone två separata molnplattformar från olika molntjänstleverantörer [16].

2.3 Molntjänstleverantörer

Molntjänster är en väletablerad sektor med ett uppskattat globalt marknadsvärde på cirka 390 miljarder dollar år 2025. Denna siffra förväntas öka, med en fortsatt årlig tillväxttakt omkring 28 % [17].

De olika molntjänstleverantörernas marknadsandelar varierar något mellan kvartalen, men tabell 2.1 redovisar uppskattade marknadsandelar för de största aktörerna under det tredje kvartalet 2025.

Tabell 2.1: Uppskattade marknadsandelar för de största molntjänstleverantörerna under Q3 2025.

Företag	**Marknadsandel**
AWS	30 %
Azure	20 %
GCP	13 %
Alibaba Cloud	4 %
Oracle Cloud	3 %
Salesforce Cloud	2 %
IBM Cloud	2 %
Tencent Cloud	2 %

AWS innehar den största marknadsandelen med cirka 30 %, följt av Microsoft Azure med 20 % och GCP med 13 %. Därefter minskar marknadsandelarna avsevärt, där Alibaba Cloud, Oracle Cloud, Salesforce Cloud, IBM Cloud och Tencent Cloud vardera står för omkring 2–4 %. Samtliga av de tre största molntjänstleverantörerna har globalt distribuerad infrastruktur och erbjuder motsvarande lösningar inom de flesta typer av tjänster.

2.4 Vanligt förekommande molntjänster

I följande punktlista beskrivs några av de vanligast förekommande molntjänsterna. Listan är långt ifrån fullständig, men syftar till att ge en översikt över det nuvarande utbudet av molntjänster.

Beräkningskapacitet (eng. compute):

- **Virtuella Maskiner (VM)**: Driftsättning av virtuella maskiner.
- **Container-tjänster**: Driftsättning och orkestrering av containrar.

- **Hanterad applikationsplattform**: Fullständig utvecklings- och driftmiljöer för applikationer.
- **Molnfunktioner**: Driftsättning av funktioner som exekveras automatiskt i respons till konfigurerbara händelser.

Lagring:

- **Blocklagring**: Persistent lagring på blocknivå.
- **Hinkar**: Persistent lagring på objektnivå.
- **Fillagring**: Persistent lagring på filsystemsnivå.
- **Databaser**: Relations- och NoSQL-databaser.
- **Hemlighetsvalv**: Lagring och hantering av hemligheter såsom kryptografiska nycklar.

Nätverk:

- **Virtuella nätverk**: Realisering av virtuella nätverk inom molnmiljön.
- **Routing**: Routing mellan de virtuella nätverken inom molnmiljön.
- **VPN**: Krypterad nätverksåtkomst till virtuellt molnnätverk från externt nätverk.
- **Lastbalansering**: Fördelning av inkommande nätverkstrafik till molnmiljön.
- **DNS**: Intern domännamnssystem för resurser inom ett molnnätverk.
- **Nätverksbrandvägg**: Brandvägg med filtrering på nätverkslagret.
- **Web Application Firewall (WAF)**: Applikationslager-brandvägg.

Identitetshantering:

- **Identitetshantering**: Centraliserad identitetshantering kopplad till samtliga tjänster inom ett molnsystem.
- **Organisatoriska enheter**: Gruppering och klassificering av identiteter avseende behörigheter.

Övervakning:

- **Monitorering**: Centraliserad monitorering av resurser och konfigurationsändringar inom ett molnsystem.
- **Loggning**: Centraliserad loggning av resurser och konfigurationsändringar inom ett molnsystem.

I tabell 2.2 presenteras leverantörsspecifika exempel på vanliga tjänster från AWS, Azure och GCP.

Tabell 2.2: Exempel på leverantörsspecifika implementationer av vanligt förekommande molntjänster.

Typ av tjänst	AWS	Azure	GCP
Virtuella maskiner (VM)	EC2 [18]	Virtual Machines [19]	Compute Engine [20]
Containrar	ECS [21] och EKS [22]	AKS [23]	GKE [24]
Hanterad applikationsplattform	Elastic Beanstalk [25]	App Service [26]	App Engine [27]
Molnfunktioner	Lambda [28]	Functions [29]	Cloud Functions [30]

Typ av tjänst	AWS	Azure	GCP
Blocklagring	EBS [31]	Managed Disks[32]	Persistent Disks [33]
Hinkar	S3 [34]	Blob Storage [35]	Cloud Storage [36]
Fillagring	EFS [37]	Files [38]	Filestore [39]
Relations-databas	RDS [40]	SQL Database [41]	Cloud SQL [42]
NoSQL-databas	DynamoDB [43]	Cosmo DB [44]	Firestore [45]
Hemlighetsvalv	Secrets Manager [46]	Key Vault [47]	Secrets Manager [48]
Virtuella nätverk	VPC [49]	Virtual Network [50]	VPC [51]
Routing	Transit Gateway [52]	Virtual Wan [53]	Cloud Router [54]
VPN	Site-to-Site VPN [55]	VPN Gateway[56]	Cloud VPN [57]
Lastbalansering	ELB [58]	Load Balancer[59]	Load Balancing [60]
DNS	Route 53 [61]	DNS [62]	Cloud DNS [63]
Klassisk brandvägg	Network Firewall [64]	Firewall [65]	Cloud Firewall [66]
WAF	WAF [67]	WAF [68]	Cloud Armor [69]
Identitet- och åtkomshantering (IAM)	AWS IAM [70]	Entra ID [71]	GCP IAM [72]
Organisatoriska enheter	Organizations [73]	Management Groups [74]	Folders [75]
Monitorering	Cloudwatch [76]	Monitor [77]	Cloud Monitoring [78]
Loggning	Cloudwatch Logs [79]	Monitor Logs [80]	Cloud Logging [81]

2.5 Molnsäkerhet

Molnsäkerhet har blivit en central fråga i takt med den ökade användningen av molntjänster inom både offentlig och privat sektor. Ofta lyfts de risker som kommer med att bruka publika molntjänster, såsom förlust av rådighet och suveränitet över systemet. Detta kapitel lyfter några säkerhetsfördelar som finns med att bruka molntjänster.

2.5.1 Centraliserad säkerhetshantering

En av säkerhetsfördelarna med att bruka molntjänster är att det medför användandet av molntjänstleverantörernas välbeprövade lösningar för centraliserad

säkerhetshantering. Centraliserad säkerhetshantering innebär att alla säkerhetsrelaterade åtgärder och policyer kan styras från en central punkt.

I följande punktlista beskrivs några förmågor som de tre stora molntjänstleverantörernas säkerhetshantering stödjer:

- infrastruktur som kod (eng. Infrastructure as Code, IaC), som kan granskas av automatiska kodanalysverktyg vid utrullning
- genom användning av centraliserad identitetshantering, som kan definiera och begränsa användares och applikationers rättigheter enligt principen om lägsta behörighet (eng. Principle of Least Privilege, PoLP), kan organisationer effektivt förhindra obehörig åtkomst och begränsa skador vid eventuella intrång
- skyddsräcken för behörigheter (eng. permission guardrails) kan implementeras via automatiserade policyer och regelverk som övervakar och kontrollerar åtkomstnivåer.
- säkerhetsverktyg som ofta är integrerade i molntjänsterna kan kontinuerligt övervaka och analysera trafik och användarbeteenden, vilket möjliggör förmågan att tidigt identifiera avvikelser och hot

Molntjänstleverantörerna har stöd för att skapa system som innefattar säkerhetsåtgärder utifrån mallar som utgår från genomarbetade ramverk såsom *AWS Landing Zone Accelerator*[8], *Azure Landing Zone*[9] och *Google Cloud Landing Zone*[10]. Dessa mallar sätter upp en grundläggande struktur för organisationen i molnmiljön utifrån praxis som beskrivs i varje molntjänstleverantörs ramverk för att designa molntjänster på ett hållbart, skalbart och säkert sätt.[11]. Det finns även etablerade mallar för att sätta upp molntjänster som behöver möta högre regulatoriska krav, såsom AWS LZA Trusted Secure Enclaves Sensitive Edition (TSE-SE)[12] och App Service Secure Baseline[13].

2.5.2 Säkerhetslösningar för molnbaserade system

Molnsäkerhet är en stor bransch, vilket medför att det finns flera säkerhetslösningar ute på marknaden specifikt för molnbaserade lösningar, även från leverantörer som inte själva tillhandahåller molntjänster.

Säkerhetslösningar för molnbaserade system är utformade för att hantera de unika utmaningar som uppstår i molnet, såsom delat ansvar mellan kund och leverantör, skydd av data som lagras på flera geografiska platser samt hantering av komplexa åtkomstkontroller. Vid implementation av molnsystem är det därmed fördelaktigt att överväga vad dessa typer av säkerhetslösningar ger för fördelar till den tjänst eller system som ska driftas. Några säkerhetslösningar för molnlösningar presenteras i följande punktlista med korta beskrivningar[82]:

[8] https://aws.amazon.com/solutions/implementations/landing-zone-accelerator-on-aws/
[9] https://learn.microsoft.com/azure/cloud-adoption-framework/ready/landing-zone/
[10] https://cloud.google.com/architecture/landing-zones
[11] Så kallade Well architected-frameworks
[12] https://github.com/aws-samples/landing-zone-accelerator-on-aws-for-tse-se
[13] https://github.com/Azure/appservice-landing-zone-accelerator/blob/main/scenarios/secure-baseline-multitenant

- **Cloud Security Posture Management (CSPM)**
  Lösning för att hantera risker genom att identifiera och flagga för konfigurationsfelaktigheter i molninfrastrukturen. Vidare hjälper dessa verktyg till med att kartlägga efterlevnadskontroller och dess implementering.
- **Cloud Workload Protection Platform (CWPP)**
  Lösning för att säkra både värd och containerbaserade arbetsbelastningar mot hot. Inkluderar oftast exekveringsskydd, sårbarhetshantering och nätverkssegmentering.
- **Cloud Access Security Broker (CASB)**
  Lösning som sitter mellan användare och applikationer för att övervaka all aktivitet och påtvinga säkerhetsriktlinjer. Dessa riktlinjer handlar ofta om exempelvis autentisering, auktorisering och samlad inlogging (eng. single sign-on, SSO).
- **Cloud Detection and Response (CDR)**
  Lösning som är molnbaserade systems motsvarighet till Endpoint Detection and Response (EDR) och Network Detection and Response (NDR) som återfinns i traditionella IT-system. CDR kan ses som en specialiserad form av Extended Detection and Response (XDR), som kan övervaka molnmiljön och agera utifrån insamlad information.
- **Cloud Infrastructure Entitlement Management (CIEM)**
  Lösning för att säkerställa att åtkomstprofiler inte innefattar för breda behörigheter. Dessa används ofta för att hjälpa organisationer följa principen om lägsta behörighet.
- **Data Security Posture Management (DSPM)**
  DSPM är ett verktyg som skyddar känslig data genom automatiserad övervakning och klassificering.
- **Cloud-Native Application Protection Platform (CNAPP)**
  Plattform som innefattar flera av ovanstående lösningar, vilken ofta innefattar aggregering av insikter från andra säkerhetslösningar.

2.5.3 Flexibilitet

Molnsäkerhet möjliggör flexibilitet i säkerhetsåtgärderna. Eftersom molnresurser kan anpassas efter behov kan säkerhetslösningar dynamiskt justeras i takt med att organisationens verksamhet växer eller förändras.

De tre största molntjänstleverantörerna har en stor mängd datacenter vilket medför en redundans på infrastrukturskapacitet. Det är därmed möjligt att bygga system där haveri i ett datacenter kan hanteras genom fortsatt drift med hjälp av andra tillgängliga datacenter. Mängden datacenter möjliggör även lagring av säkerhetskopior i separata datacenter i separata regioner. Eftersom datacentren är geografiskt utspridda är det osannolikt att alla slås ut samtidigt vid en katastrof eller annan oönskad händelse [83][84][85].

2.6 Tidigare studier

I detta kapitel presenteras tidigare FOI-studier som gjorts med anknytning till molntjänster.

En rapport av Henrik Karlzén [86] från 2012 beskriver molnets möjligheter och begränsningar. Rapporten beskriver fördelar som att användare av molntjänster inte behöver fokusera på att bygga upp och förvalta den tekniska infrastrukturen och samtidigt enbart betala för den datorkraft och lagring som används. Rapporten beskriver även risker med molnet som hög komplexitet, stor attackyta samt tilliten till molntjänstleverantörerna. Dessutom adresseras begränsningar med potentiella lösningar som exempelvis homomorfisk kryptering och betrodda plattformar (eng. trusted platforms). Slutligen nämns också hur den delade infrastrukturen kan medföra säkerhetsrisker som dataläckage utan gedigen resursisolering.

I rapporten *Risker med virtualisering av IT-system* [87] beskriver Eidenskog och Karresand olika tekniska och administrativa risker som uppstår vid virtualisering av IT-system. Författarna diskuterar risker med virtuella beståndsdelar som exempelvis hur sårbarheter i nätverkskort, grafikkort och ljudenheter kan ge upphov till dataläckage mellan olika virtuella maskiner. Administrativa risker med förvaltning av virtuella miljöer adresseras också där komplexiteten som virtualisering medför lyfts.

En annan tillämpning av moln är vid distribuering av *industriella informations- och styrsystem (ICS)*. I en intervjustudie av Hunstad och Karresand [88] diskuteras möjligheter och risker med att använda molntjänster i ICS-tillämpningar. Författarna adresserar affärsmässiga fördelar med reducerade kostnader och den utökade tillgängligheten till centrala system som molnet erbjuder. Exempelvis nämns de globalt spridda redundanta servrar som molntjänstleverantörerna tillhandahåller som en viktig tillgång för att upprätthålla en gedigen nivå av feltolerans i diverse styrsystem. Samtidigt beskriver rapporten molnets risker avseende angrepp på exempelvis webbgränssnitt, lagring av data hos extern part samt förlorad rådighet till utlokaliserade ICS. Baserat på dessa risker utformar författarna olika råd, exempelvis kopplade till noggrann riskanalys, säkra protokoll, detaljerad loggning och att fördelaktiga avtal med molntjänstleverantören förhandlas fram.

I ett memo av Ronnie Johansson[89] undersöks forskningen kring begreppet *combat cloud* som handlar om att nyttja den kommersiella molntekniken i försvarstillämpningar. Författaren tar upp amerikanska militära initiativ som JWCC och lyfter risker med molnets kommunikationsbegränsningar, såsom för långa svarstider eller för hög latens. Vidare nämner skribenten hur kantdatabehandling (eng. edge computing) kan nyttjas för att tillhandahålla snabbare lokal databearbetning och lagring. Memot adresserar även vikten av att säkerställa säkerheten i dessa system för att exempelvis motverka intrång och avlyssning.

3 Metod

Med syfte att bilda en översikt av rekommenderade åtgärder från erkända institutioner och auktoriteter, samt orsak till molnincidenter under de senaste tio åren utfördes en studie bestående av följande två delar:

- **Genomgång av säkerhetsåtgärder från kända molnsäkerhetsramverk**: I studiens första del genomfördes en litteraturgenomgång av välkända molnsäkerhetsramverk, där säkerhetsåtgärderna kategoriseras och analyseras.
- **Genomgång av rapporterade molnincidenter**: I den andra delen utfördes en litteraturstudie av rapporterade molnincidenter från de senaste 10 åren. Molnincidenterna analyserades och dataextraktion gjordes utifrån orsak till att incidenten uppstått och bedömd konsekvens. Därefter grupperades incidenterna efter författarnas bedömning av orsak till incidenten utifrån samma kategorisering som gjordes för säkerhetsåtgärdena i första delen av studien.

3.1 Genomgång av säkerhetsåtgärder

Molnsäkerhetsramverken som användes för att samla säkerhetsåtgärder identifierades genom att söka efter forskningsartiklar som granskade molnsäkerhetsramverk. Sökningen för forskningsartiklar gjordes i Google Scholar med söktermen ”cloud security framework” och filtrerades på artiklar som publicerats de senaste tio åren. Artiklarna sorterades utifrån relevans. Forskningsartiklarna som identifierades lista molnsäkerhetsramverk var *An analysis of cloud security frameworks, problems and proposed solutions*[90] och *Cloud Standards in Comparison: Are New Security Frameworks Improving Cloud Security?[91]*. Ytterligare ramverk identifierades genom explorativa sökningar på internet med Google som sökmotor.

Ramverken togs enbart med om de var specifika för molnet, vilket exkluderade generiska cybersäkerhetsramverk, såsom *ISO 27001*[14]. Följande ramverk identifierades:

- Cloud Control Matrix (CCM) av Cloud Security Alliance (CSA) [92]
- Well-architected Framework Security Pillar av AWS [93]
- Well-architected Framework Security Pillar av Azure [94]
- Well-architected Framework Security, Privacy and Compliance Pillar av GCP [95]
- ISO-27017 [96]
- NIST SP 500-292 [97]
- NIST Special Publication 800-144 [98]
- CSA Security Guidance [99]
- CSA Star [100]
- Foundational Cloud Security with CIS Benchmarks [101]
- Cloud Companion Guide for CIS Controls v8.1 [102]
- ENISA Cloud Security Guide [103]

[14]https://www.iso.org/standard/27001

- FedRamp [104].

Genomgång av ramverk gjordes individuellt och filtrerades ytterligare baserat på följande krav:

- **Krav 1**: Ramverket tillhandahåller en direkt eller indirekt lista rekommendationer för säkerhetsåtgärder vid design av molnsystem för en molntjänstanvändare. Generella exempel på områden som bör behandlas vid design av molnsystem anses inte som tillräckligt konkreta för att inkludera.
- **Krav 2**: Ramverket är mindre än 10 år gammalt, alternativt kontinuerligt uppdaterad för att kunna presentera tillräckligt relevant och specifik information med hänsyn till moderna molnsystem.
- **Krav 3**: Ramverket tillhandahåller en stor mängd rekommendationer på åtgärder som kunde lyftas och generaliseras till leverantörsagnostiska mitigeringar. Ramverk som endast består av konkreta rekommendationer för hur leverantörsspecifika tjänster avgränsas bort.

Utifrån dessa tre krav kvarstod fem ramverk som de främst relevanta för studien.

- CCM av CSA
- Well-architected Framework Security Pillar av AWS
- Well-architected Framework Security Pillar av Azure
- Well-architected Framework Security, Privacy and Compliance Pillar av GCP
- Cloud Companion Guide for CIS Controls v8.1.

Säkerhetsåtgärder från samtliga ramverk extraherades sedan. För att enbart få med åtgärder som var relevanta för denna studie filtrerades åtgärderna ytterligare. Åtgärder som ej ansågs addressera ett tillräckligt konkret problem eller problemområde valdes bort. Som exempel bedömdes *AWS SEC01-BP08: ”Evaluate and implement new security services and features regularly”* inte uppfylla krav, medan *Azure: ”Establish processes to manage the identity lifecycle”* ansågs vara tillräckligt konkret. Åtgärderna fick således vara relativt generella, men inte alltför övergripande.

Åtgärderna grupperades sedan genom en systematisk genomgång av samtliga 333 åtgärder. Varje åtgärd sammanfattades först i ett fåtal ord, varefter sammanfattningarna analyserades och de med liknande innebörd grupperades till underkategorier. Underkategorierna grupperades sedan vidare in i fem huvudkategorier. Grupperingen och filtreringen utfördes gemensamt av två forskare för att minska risken för feltolkningar.

3.2 Genomgång av incidenter

För den lista av incidenter som skapats har följande söktermer använts:

- cloud breaches
- cloud security incidents
- cloud breaches database
- cloud incident database.

För dessa söktermer har de första 5 sidorna på Google granskats efter sammanställningar av molnincidenter. Från de relevanta källorna som identifierats utifrån söktermerna har vidare snöbollning[15] tillämpats för att identifiera ytterligare sammanställningar av molnincidenter.

De sammanställningar av molnincidenter som hittades presenteras i tabell 3.1.

Tabell 3.1: Översikt av identifierade molnincidentssammanställningar.

Sammanställning	Inkluderad	Incidenter	Beskrivning
breaches.cloud [105]	Ja	22	Databasen förvaltas av PrimeHarbor Technologies, LLC och tillåter öppna bidrag från allmänheten. Varje incident är försedd med referenser till trovärdiga källor.
Cloud security alliance [106]	Ja	22	Indirekt databas förvaltad av CSA, en av de ledande auktoriteterna inom molnsäkerhet. Företagets Top Threats to Cloud Computing innehåller en mängd referenser till molnincidenter.
Arcserve [107]	Ja	7	Artikel utgiven av cybersäkerhetsföretaget Arcserve, med länkar till trovärdiga källor.
aws-customer-security-incidents [108]	Ja	61	Open Source-sammanställningar förvaltad av fristående individ. Alla incidenter har tydliga referenser till trovärdiga källor.
s3-leaks [109]	Ja	38	Open Source-sammanställning förvaltad av fristående individ. Alla incidenter har tydliga referenser till trovärdiga källor.
Cloudcomputing News [110]	Nej	10	Nyhetskälla där bland annat incidenter rapporteras. Saknar tillförlitliga referenser till källor för många av incidenterna.
Cloud threat landscape [111]	Ja	116	Databas förvaltad av Wiz, ett väletablerat molnsäkerhetsföretag. Databasen inkluderar referenser till trovärdiga källor.

För den manuella filtreringen av incidenter från dessa sammanställningar inkluderades incidenter utifrån följande inkluderingskrav:

- **Relevant för dagens molnsystem**
  Incidenten måste skett inom de senaste 10 åren (2015 eller senare).
- **Hänvisar till trovärdiga källor**
  Incidenten måste ha rapporterats av en källa som bedöms trovärdig av författarna.
- **Tillräckligt med information**
  Incidenten måste vara tillräckligt väl dokumenterad för att möjliggöra extrahering av information angående orsak till incidenten och konsekvensen.

I denna filtrering har även duplicerade incidenter från olika databaser tagits bort.

Dataextraktion har genomförts med avseende på år, organisation, orsak till incidenten och konsekvens. Dataextraktionen gjordes för varje incident individuellt av två forskare och eventuella avvikelser i bedömningen diskuterades för att fastslå en slutlig bedömning. Orsak till att incidenten uppstått har bedömts enligt samma kategorier som kategorisering av säkerhetsåtgärden som beskrevs i avsnitt 3.1. Då en incident kan ha uppstått på grund av flera orsaker, är det möjligt att en incident innefattar flera kategorier. Det har även lagts till en kategori, kallad okänd, för de incidenter där företag antingen inte vet hur incidenten har uppstått eller inte tillhandahåller denna information. Även en kategori för mänskliga sårbarheter har lagts till där incidenter som uppstår av antingen social manipulation eller okunskap faller in.

[15] Snöbollning är en metod för att hitta relevanta källor eller referenser genom att använda redan identifierade källor som en utgångspunkt.

4 Genomgång av säkerhetsåtgärder

Efter en genomgång av CSA:s (CCM), Cis Controls v8.1 samt de tre stora molntjänstleverantörernas ramverk för säker molnarkitektur, identifierades fem övergripande kategorier för molnsäkerhet:

- infrastrukturhantering
- identitets- och åtkomsthantering
- dataskydd
- applikationssäkerhet
- loggning och monitorering

4.1 Infrastrukturhantering

Kategorin för infrastrukturhantering täcker molnsystemets nätverkstopologi, samt konfigureringen av grundläggande nätverkstjänster. Detta innefattar till exempel:

- de subnät som existerar i molnsystemet
- de molntjänster som existerar i varje subnät
- de logiska kopplingar som finns mellan de olika subnäten
- hur interna molnnätverk ansluts till internet
- konfiguration av nätverkstjänster och -system, vilket innefattar exempelvis:
  - DNS
  - DHCP
  - NAT
  - brandväggar
  - nätverksbaserade intrångs- och preventionssystem.
- hur infrastrukturen konfigureras och distribueras
- regioner och tillgänglighetszoner där molnsystemet ska driftas.

Utifrån genomgången av säkerhetsåtgärderna identifierades tolv underkategorier vilka listas i tabell 4.1.

Tabell 4.1: Underkategorier med antal tillhörande åtgärder från molnsäkerhetsramverken som kategoriserats som infrastruktur samt antal procent av åtgärderna som tillhör underkategorin. Procent avrundat till närmaste heltal. En åtgärd kan tillhöra flera underkategorier och summan av underkategoriernas andelar kan därmed överstiga 100 %.

Underkategori	Tillhörande åtgärder	Andel av åtgärder
Nätverkssegmentering	26	46 %
Användning intrångspreventionsverktyg	8	14 %
IaC med användning av statisk analys	7	13%
Minimering av publik exponering	6	11 %
Perimeterhärdning	4	7 %
Trafikinspektion	3	5%
Arkitekturspecifikation för nätverk	2	4 %
Portbaserad åtkomstkontroll	2	4 %
Skydd mot DDoS	1	2 %

Underkategori	Tillhörande åtgärder	Andel av åtgärder
Hantering av hybrida molnlösningar	1	2 %
Säker migrering från egen infrastruktur	1	2 %
DNS för interna resurser	1	2%

Inom kategorin för infrastrukturshantering rekommenderade många av ramverken samma åtgärder. Exempel på åtgärder som lyftes av en majoritet av ramverken ges i tabell 4.2. Följande åtgärder är exempel på konkreta rekommendationer tagna från ramverken, och ingår i de underkategorier som presenterades i tabell 4.1.

Tabell 4.2: Identifierade åtgärder som rekommenderas av ett flertal av molnsäkerhetsramverken inom kategorin infrastrukturshantering.

Åtgärd	Inkluderas i antal ramverk	AWS	Azure	GCP	CCM	CIS
Definiera säkerhetsklasser och segmentera samt mikrosegmentera nätverket utifrån dessa säkerhetsklasser	5	✓	✓	✓	✓	✓
Använd grundläggande brandväggar, applikationsbrandväggar samt Next Generation Firewalls (NGFW)	5	✓	✓	✓	✓	✓
Använd nätverksbaserade intrångs- och preventionssystem	5	✓	✓	✓	✓	✓
Använd Infrastructure as Code (IaC) samt statisk analys av denna	4	✓	✓	✓	✗	✓
Minimera publik exponering	4	✓	✓	✓	✗	✓
Använd isolerade molnbaserade virtuella/privata nätverk	4	✓	✓	✓	✓	✗

4.2 Identitets- och åtkomsthantering

Samtliga autentiseringsmekanismer vid åtkomst av resurser inom molnsystem utgör en egen kategori. Kategorin för identitets- och åtkomsthantering täcker samtliga autentiseringsmekanismer vid åtkomst av resurser. Identitets- och åtkomsthantering kategorin innefattar till exempel:

- åtkomst till hantering av molnsystemet genom den använda molnplattformen
- åtkomst till öppna portar för tjänster inom molnsystemet

- åtkomst till användarkonton på operativsystemnivå inom IaaS-tjänster
- system för att federera åtkomst centralt, samt associera dem med ovanstående identiteter.

Utifrån genomgången av säkerhetsåtgärderna identifierades 14 underkategorier vilka listas i tabell 4.3.

Tabell 4.3: Underkategorier med antal tillhörande åtgärder från molnsäkerhetsramverken som kategoriserats som identitets- och åtkomsthantering, med antal procent av åtgärderna som tillhör underkategorin. Procent avrundat till närmaste heltal. En åtgärd kan tillhöra flera underkategorier och summan av underkategoriernas andelar kan därmed överstiga 100 %.

Underkategori	**Tillhörande åtgärder**	**Andel av åtgärder**
Centraliserad IAM	17	20 %
Rollbaserad åtkomsthantering	14	16 %
Starka inloggningsmekanismer	12	14 %
Åtkomsthantering för externa parter	10	12 %
Principen om lägsta behörighet	10	12 %
Hantering av privilegierade användare	7	8 %
Uppdelning av ansvarsområden	6	7 %
Skyddsräcken för behörigheter	4	5 %
Segmentering av organisationer	3	4 %
Tidsbegränsade åtkomstnycklar	3	4 %
Organisationsövervakning	2	3 %
Terminering av konton	2	3 %
Glasbrytarkonto	2	3 %
Unika identiteter	1	1 %

Inom kategorin för identitets- och åtkomsthantering rekommenderade många av ramverken samma åtgärder. Exempel på åtgärder som lyftes av en majoritet av ramverken ges i tabell 4.4. Följande åtgärder är exempel på konkreta rekommendationer tagna från ramverken, och ingår i de underkategorier som presenterades i tabell 4.3.

Tabell 4.4: Identifierade åtgärden som rekommenderas av ett flertal av molnsäkerhetsramverken inom kategorin identitets- och åtkomsthantering.

Åtgärd	**Inkluderas i antal ramverk**	**AWS**	**Azure**	**GCP**	**CCM**	**CIS**
Använd rollbaserad tillgång	5	✓	✓	✓	✓	✓
Använd starka lösenord	5	✓	✓	✓	✓	✓
Använd flerfaktorsautentisering (eng. multi factor authentication, MFA)	5	✓	✓	✓	✓	✓
Använd principen om lägsta behörighet	5	✓	✓	✓	✓	✓

Åtgärd	Inkluderas i antal ramverk	AWS	Azure	GCP	CCM	CIS
Använd uppdelning av ansvarsområden (eng. separation of duties, SoD)	5	✓	✓	✓	✓	✓
Bruka skyddsräcken för behörigheter	4	✓	✓	✓	✓	✗
Använd en centraliserad identitetsintygare (eng. identity provider, IdP) (federera vid behov)	4	✓	✓	✓	✗	✓
Gruppera och klassificera identiteter med hjälp av organisatoriska enheter	3	✓	✓	✗	✗	✓
Använd temporära inloggningsuppgifter	3	✓	✓	✗	✗	✓

4.3 Dataskydd

Kategorin för dataskydd täcker hantering av data både i vila och vid överföring. Detta innefattar exempelvis:

- kryptering av privat data i vila
- hashning av exempelvis lösenord
- lagring av hemligheter
- protokoll som används vid kommunikation.

Utifrån genomgången av säkerhetsåtgärderna identifierades 10 underkategorier vilka listas i tabell 4.5.

Tabell 4.5: Underkategorier med antal tillhörande åtgärder från molnsäkerhetsramverken, med antal procent av åtgärderna som tillhör underkategorin. Procent avrundat till närmaste heltal. En åtgärd kan tillhöra flera underkategorier och summan av underkategoriernas andelar kan därmed överstiga 100 %.

Underkategori	Tillhörande åtgärder	Andel av åtgärder
Dataklassifikation	23	27 %
Data i vila	14	16 %
Nyckelhantering	14	16 %
Kryptering	13	15 %
Data vid överföring	13	15 %
Säkerhetskopior	5	6 %
Förvaring av hemligheter	5	6 %
Gallring av data	3	4 %
Data vid beräkning	3	4 %
Använd verktyg för dataskydd	1	1 %

Inom kategorin för dataskydd rekommenderade många av ramverken samma åtgärder. Exempel på åtgärder som lyftes av en majoritet av ramverken ges i tabell 4.6. Följande åtgärder är exempel på konkreta rekommendationer tagna från ramverken, och ingår i de underkategorier som presenterades i tabell 4.5.

Tabell 4.6: Identifierade åtgärden som rekommenderas av ett flertal av molnsäkerhetsramverken inom kategorin dataskyddskonfiguration.

Åtgärd	**Inkluderas i antal ramverk**	**AWS**	**Azure**	**GCP**	**CCM**	**CIS**
Inför en process för dataklassificering	5	✓	✓	✓	✓	✓
Kryptera känslig data i vila	5	✓	✓	✓	✓	✓
Använd rekommenderade moderna primitiver för kryptering och hashning	5	✓	✓	✓	✓	✓
Använd rekommenderade moderna protokoll för all nätverkskomunikation	5	✓	✓	✓	✓	✓
Inför en process för att skapa, radera, och rotera nycklar	5	✓	✓	✓	✓	✓
Använd ett hemlighetsvalv för förvaring av hemligheter	4	✓	✓	✓	✓	✗
Inför en process för att radera data	4	✓	✓	✗	✓	✓

4.4 Applikationssäkerhet

Kategorin för Applikationssäkerhet är inte specifikt för molnet, men tas upp som en kategori då applikationssäkerhet fortsätter vara viktigt även efter migrering till molnet.

Det finns även exempel där sättet molnet är implementerat på gör att vissa attacker är mer effektiva än om det inte skulle vara en molnmiljö. Ett exempel är att Server-Side Request Forgery (SSRF) attacker mot VM i molnet kan få tillgång till metadatatjänsten för VM:en. Metadatatjänster (eng. Instance Metadata Service, IMDS) tillhandahålls för varje VM i molnet och används för att tillgängliggöra metadata relaterat till resursen, exempelvis IAM-nycklar som den aktuella instansen körs med. Det bör noteras att svagheten med att IAM-nycklar exponeras via IMDS är välkänd, och att den nyare versionen IMDSv2 införts för att motverka just denna exponering. IMDSv2 kräver att en åtkomstnyckel används för att få åtkomst till metadatatjänsten. Åtkomstnyckeln erhålls genom ett anrop med en specifik HTTP-header. Eftersom de flesta typer av SSRF-attacker inte möjliggör manipulation av headers reduceras risken avsevärt för att metadatatjänsten ska kunna utnyttjas som en attackvektor.

Kategorin utgörs till exempel av:

- konfiguration av utvecklingsmiljö
- konfiguration av driftmiljö
- design och testning av applikation
- driftsättning av applikation
- hantering av tredjeparts-bibliotek och applikationer
- underhåll och vidareutveckling.

Utifrån genomgången av säkerhetsåtgärderna identifierades 10 underkategorier vilka listas i tabell 4.7.

Tabell 4.7: Underkategorier med antal tillhörande åtgärder från molnsäkerhetsramverken, med antal procent av åtgärderna som tillhör underkategorin. Procent avrundat till närmaste heltal. En åtgärd kan tillhöra flera underkategorier och summan av underkategoriernas andelar kan därmed överstiga 100 %.

Underkategori	Tillhörande åtgärder	Andel av åtgärder
Hantering av tredjepartsprodukter och tjänster	14	29 %
Deklarativ härdad operativsystemskonfiguration	9	18 %
Kodanalys	7	14 %
Följ standarder för säker applikationsutveckling	7	14 %
Använd verktyg för utrullning	6	12 %
Automatiserade tester	5	10 %
Utred rotorsak för upptäckta sårbarheter	4	8 %
Penetrationstester	4	8 %
Verifiera komponenters riktighet	1	2 %
Lista tillåten mjukvara	1	2%

Inom kategorin för applikationssäkerhet rekommenderade många av ramverken samma åtgärder. Exempel på åtgärder som lyftes av en majoritet av ramverken ges i

tabell 4.8. Följande åtgärder är exempel på konkreta rekommendationer tagna från ramverken, och ingår i de underkategorier som presenterades i tabell 4.7.

Tabell 4.8: Identifierade åtgärden som rekommenderas av ett flertal av molnsäkerhetsramverken inom kategorin applikationssäkerhet.

Åtgärd	**Inkluderas i antal ramverk**	**AWS**	**Azure**	**GCP**	**CCM**	**CIS**
Skapa en process för att hantera tredjepartsapplikationer och bibliotek	5	✓	✓	✓	✓	✓
Härda driftmiljöer (på operativsystemsnivå)	5	✓	✓	✓	✓	✓
Utför kodanalys	5	✓	✓	✓	✓	✓
Använd verktyg för utrullning av kod	5	✓	✓	✓	✓	✓
Använd automatiserade tester	4	✓	✓	✗	✓	✓

4.5 Monitorering och loggning

Monitorering och loggning är en övergripande kategori, där bevakningen av samtliga resurser i molnsystemet inkluderas. Detta inkluderar till exempel övervakning av:

- nätverkstrafik
- molntjänstadministrering (eng. control plane)
- försök till autentisering
- beräkningsresurser
- hinkar och databaser
- nyckelhantering.

Utifrån genomgången av säkerhetsåtgärderna identifierades 8 underkategorier vilka listas i tabell 4.9.

Tabell 4.9: Underkategorier med antal tillhörande åtgärder från molnsäkerhetsramverken, med antal procent av åtgärderna som tillhör underkategorin. Procent avrundat till närmaste heltal. En åtgärd kan tillhöra flera underkategorier och summan av underkategoriernas andelar kan därmed överstiga 100 %.

Underkategori	Tillhörande åtgärder	Andel av åtgärder
Loggning	22	40 %
Resursövervakning	9	16 %
Logganalys	8	15 %
Avvikelsehantering	5	9 %
Loggskydd	5	9 %
Användning av verktyg för intrångsskydd	3	6 %
Loggaggregering	2	4 %
Tidssynkronisering	2	4 %

Inom kategorin för monitorering och loggning rekommenderade många av ramverken samma åtgärder. Exempel på åtgärder som lyftes av en majoritet av ramverken ges i tabell 4.10. Följande åtgärder är exempel på konkreta rekommendationer tagna från ramverken, och ingår i de underkategorier som presenterades i tabell 4.9.

Tabell 4.10: Identifierade åtgärden som rekommenderas av ett flertal av molnsäkerhetsramverken inom kategorin monitorering och loggning.

Åtgärd	Inkluderas i antal ramverk	AWS	Azure	GCP	CCM	CIS
Använd ett centraliserat loggsystem för alla typer av loggar	5	✓	✓	✓	✓	✓
Aggregera och analysera loggarna i det centraliserade loggsystemet	5	✓	✓	✓	✓	✓
Skydda loggar mot icke autentiserad access och radering	5	✓	✓	✓	✓	✓

För kategoriseringen av incidenter, valdes att huvudsakligen inkludera de fall då intrång och onaturligt beteende har skett under längre tid, eller då betydande mängder data har exfiltrerats utan att ha satt igång något larm. Detta för att inte alla typer av intrång eller felanvändning skulle klassificeras under monitorering och loggningskategorin.

5 Analys av molnincidenter

Detta kapitel presenterar resultaten från analysen av molnincidenter som inträffat under de senaste tio åren. Inledningsvis redovisas orsaker till molnincidenterna i avsnitt 5.1, följt av en genomgång av molnincidenternas konsekvenser i avsnitt 5.2.

5.1 Orsak till molnincidenter

Totalt 157 molnincidenter, insamlade från incidentdatabaserna, bedömdes av författarna och sorterades baserat på orsak till att incidenten uppstod utifrån brist av de kategorier av säkerhetsåtgärder som presenterade i kapitel 4. Här har social manipulation samt okänd orsak till incidenten lagts till som kategorier för de incidenter som orsakats av social manipulation eller där organisationen inte vet eller inte vill delge orsaken till incidenten. Följande tabell visar de bedömda orsakerna till att incidenter uppstått för incidenterna.

Tabell 5.1: Sårbarhetskategorier hos de observerade molnincidenterna. Procent avrundade till närmast heltal. En incident kan vara resultatet av flera sårbarheter, och summan av kategoriernas andelar kan därmed överstiga 100 %.

Kategori	**Antal**	**Andel av incidenter**
Brister i identitets- och åtkomsthantering	91	58%
Brister i dataskydd	67	43%
Brister i infrastrukturhantering	63	40%
Brister i applikationssäkerhet	35	22%
Okänd orsak till incidenten	28	18%
Brister i monitorering och loggning	20	13%
Mänskliga brister	18	12%

Som kan observeras består en stor del av incidenterna av brister i identitet- och åtkomsthantering, dataskyddskonfiguration och infrastrukturshantering. Brister i applikationssäkerhet, brister i monitorering och loggning samt mänskliga brister är orsak till en del av incidenterna, men inte i samma utsträckning. Vidare kan man se att nästan en femtedel av incidenterna har bedömts bero på okända anledningar. I följande avsnitt presenteras incidenterna för varje kategori mer detaljerat.

5.1.1 Brister i infrastrukturhantering

Majoriteten av infrastrukturrelaterade intrång berodde på att att resurser, som endast borde vara tillgängliga från vissa subnät, var exponerade mot internet. Exempel på incidenter där anledningen var exponerade resurser inkluderar 2024 Tunefab Converter, 2024 Zenlayer, 2024 Wurk, 2023 Deposit Files och 2017 CloudPets, där databaser var öppna utan krav på autentisering. Detta inkluderar även hinkar, vilka ofta var exponerade mot internet. I många incidenter låg en felkonfigurerad brandvägg bakom den publika exponeringen.

Utöver exponerade resurser mot internet observerades även några mer komplexa incidenter där bristfällig nätverkssegmentering möjliggjorde lateral förflyttning inom det interna nätverket som organisationerna skapat. Exempel på detta är 2024 MITRE, 2023 Microsoft AI och 2019 Capital One.

Slutligen identifierades några exempel på felkonfigurerade nätverkstjänster, såsom felkonfigurerad DNS i 2025 U.S. Centers for Disease Control and Prevention och 2025 Mastercard, samt felkonfigurerad WAF i 2019 Capital One.

5.1.2 Brister i identitets- och åtkomsthantering

Drygt 58 % av de observerade incidenterna bedömdes bero på en sårbarhet relaterad till identitets- och åtkomsthantering. Av dessa 91 incidenter berodde 53 på att åtkomsthantering saknades för resurserna. Majoriteten av dessa resurser var dessutom åtkomliga från internet, vilket medförde att obehöriga kunde nå dem.

Tio av incidenterna berodde på att en tidigare anställd nyttjat sitt konto från anställningen för att komma åt data. Således saknades en tillförlitlig process för terminering av identiteter och konton.

Ett annat återkommande problem var att svaga inloggningsmekanismer användes. Förekommande brister inkluderade återanvändning av lösenord i databaser från tidigare dataläckor som kunde utnyttjas av angripare, användning av enkla lösenord samt avsaknad av MFA.

I många incidenter fanns åtkomsthantering, men den var otillräcklig. Den vanligast förekommande bristen var att åtkomstprofiler generellt sett hade för omfattande behörigheter. I vissa fall uppstod även incidenter på grund av användning av nycklar utan giltighetstid. Ytterligare exempel på felkonfigurationer inkluderar incidenterna 2017 Paytm och 2017 Dow Jones Index, där regler infördes som krävde autentisering, men inte att användaren var autentiserad inom den avsedda organisationen. Detta medförde att alla autentiserade AWS-användare kunde komma åt resurserna.

I fem av fallen har incidenten uppstått som följd av att resurser delats med en extern part i form av konsulter vars konton blivit övertagna.

5.1.3 Brister i dataskydd

Brister i dataskydd var den näst vanligaste kategorin bland incidenterna. Inom denna kategori var det vanligaste orsaken otillräcklig hantering av hemligheter, vilket förekom i 33 av totalt 67 incidenter. Vanligtvis förekom dessa hemligheter i form av autentiseringsnycklar, såsom moln- och databasåtkomstnycklar, som förvarades utan användning av ett valv, lösenordsskydd eller liknande. Nycklar förvarades ofta i klartext i konfigurationsfiler.

Bristande kryptering av känsliga data i vila var också vanligt förekommande. Totalt 30 incidenter inkluderade dataexfiltrering av okrypterad känslig information från hinkar och databaser.

Ett fåtal incidenter involverade avsaknad av, eller användning av föråldrade eller otillräckliga krypteringsalgoritmer vid lagring av lösenord i vila. Exempel på detta var

2024 Fujitsu, 2020 Live Auctioneers och 2018 Limoges Jewelry. Det är värt att notera att det inte observerades några incidenter med otillräcklig kryptering eller att utdaterade protokoll användes för data vid överföring.

5.1.4 Brister i applikationssäkerhet

Brister i applikationssäkerhet var en relativt vanlig orsak till incidenter och identifierades som en av orsakerna i 22 % av incidendenterna. Den största delen med 13 av 35 (37 %) av bristerna i applikationssäkerhet var vanligt förekommande säkerhetsbrister, som inte har något direkt anknytning till molnet, såsom brister i API-säkerhet. I två av dessa incidenter, 2021 LinkedIn och 2019 Facebook utnyttjades applikationernas förväntade beteende för att extrahera data på ett sätt som inte var avsett.

Tolv av de 35 (34 %) bristerna i applikationssårbarheter var sårbarheter i tredjepartsprodukter eller bibliotek. Vissa sårbarheter utgjordes av nolldagsattacker, men majoriteten bestod av redan kända CVE:er som funnits tillgängliga under en längre tid.

För sex av de bedömda incidenterna var orsaken till incidenten att åtkomstnycklar funnits i källkoden, såsom i APK:er (reedorz och Cameo) eller javascript (Indias National Logistics Portal-Marine.

Resterande fyra incidenter (Grafana Labs, SAFE Wallet, Juniper Networks och CommuteAir) för brister i applikationssäkerhet bedömdes vara sårbarheter i verktyg för utrullning av kod.

5.1.5 Brister i monitorering och loggning

I 20 av de analyserade incidenterna bedömdes bristande monitorering och loggning ha möjliggjort incidenten eller förstärkt konsekvenserna av den inträffade incidenten. I många av dessa incidenter rör det sig om omfattande mängder data som exfiltrerats från organisationens interna molnnätverk under längre tidsperioder, såsom i fallen 2025 Office of the Comptroller of the Currency, 2023 Toyota och 2019 Alibaba. I andra incidenter rör det sig om publika resurser som lagrar känslig information och därigenom har lett till långvariga läckor. Att dessa resurser exponerats mot internet under en längre period indikerar brister i monitoreringen. Exempel på fall där känslig data exponerats mot internet under en längre tid är 2023 KidSecurity, 2021 Cognyte, och 2018 Imperva.

En annan förekommande typ av incident är att nya molnresurser skapas och används under en längre tid utan att något system eller logganalysverktyg larmar om avvikande aktivitet inom organisationen, som vid 2024 Meson Network. Detta kan möjliggöra olika typer av brytning av kryptovaluta. Alternativt kan molnresurser tas bort utan korrekt övervakning, såsom i fallet med 2024 NCS.

Liksom för infrastrukturincidenter uppmärksammades även här ett antal incidenter där attacker skulle kunna ha motverkats genom bättre monitorering av trafiken inom organisationenens interna molnnätverk, exempelvis 2024 MITRE, 2024 Hugging Face och 2023 Okta.

5.1.6 Mänskliga brister

Även om ett system är väl härdat finns det fortfarande en möjlighet för fientliga aktörer att utnyttja anställda med befogade behörigheter. Det går således inte alltid att säkra ett system med rent tekniska lösningar.

Av de 18 incidenterna som bedömdes orsakas av mänskliga brister uppstod 15 (83 %) av incidenterna inom denna kategori av olika typer av social manipulation. Ett av de mer sofistikerade exemplen är 2025 SAFE Wallet där en APT stal 1,4 miljarder dollar i kryptovaluta. Ingångsvektorn var att nyttja social manipulation för att få åtkomst till en utvecklares dator, som sedan användes för att injicera illvillig javascript-kod. Social manipulation har även använts för att ta sig förbi MFA-lösningar genom att hotaktören etablerat kontakt med offret och utgett sig för att vara exempelvis supportpersonal. Social manipulation kan delvis motverkas genom tekniska lösningar såsom nedlåsning och kontroll av klienter eller e-postfilter, men det finns alltid en överhängande risk att dessa åtgärder inte täcker in alla möjliga hot.

De resterande tre incidenterna uppstod på grund av att privata molnnycklar lagts upp i publika kodförråd (eng. repositories) hos GitHub som hotaktörer sedan använt för att få tillgång till molnmiljön.

5.1.7 Okänd orsak

För vissa incidenter har organisationer inte offentliggjort hur intrånget inträffade. Således var en kategorisering inte möjlig. Detta kan delvis förklaras av att de vill värna sitt rykte och därför undviker att dela detaljer om hur deras säkerhetsmekanismer brustit. I andra fall har företagen uppgett att de helt enkelt inte vet hur angriparen tagit sig in i systemen. Detta kan bero antingen på att angriparen raderat spår efter intrånget eller att organisationen saknat tillräcklig övervaknings- och loggningsförmåga.

5.2 Konsekvenser av molnincidenter

De rapporterade konsekvenserna för dessa molnincidenter presenteras i följande tabell.

Tabell 5.2: Rapporterade konsekvenser av de analyserade molnincidenterna. Procent avrundade till närmast heltal. En incident kan ha flera konsekvenser, och summan av konsekvensernas andelar kan därmed överstiga 100 %.

Konsekvens	**Antal**	**Andel av incidenter**
Dataexfiltrering	125	80%
Resursövertagning	17	11%
Borttagning av data	5	3%
Inga konsekvenser	12	8%

5.2.1 Dataexfiltrering

Exfiltrering av data var den absolut vanligaste konsekvensen som cirka 80 % av incidenterna resulterade i. Detta kan förklaras genom att konsekvensen är bred och inkluderar incidenter när någon typ av skyddsvärd data blivit stulen. I denna konsekvens ingår även incidenter där hotaktörer stulit kryptovaluta.

Vad följderna för organisationerna blir från dataexfiltreringen beror till stor del på hur känsliga de data som stulits är. Det finns dokumenterade fall där väldigt känsliga data läckts, såsom 2017 US Government där data tillhörande USA:s militär legat okrypterade i publika hinkar, men det finns även fall där mindre känsliga data stulits.

De flesta av de observerade incidenterna framstår som opportunistiska attacker, där angriparen identifierat en sårbarhet och därefter utnyttjat den för att uppnå ekonomisk vinning. Möjligheterna uppstod ofta genom exploatering av nya sårbarheter i välanvända tredjepartsbibliotek, genom identifiering av publika resurser utan åtkomsthantering, genom social manipulation i form av nätfiske eller genom att molnnycklar återfunnits i publika källor. I vissa fall utnyttjades övertagandet av resurser även för att genomföra nätfiskeattacker mot andra företag via den kompromitterade organisationens betrodda domän.

Det förekom också incidenter där dedikerade APT-grupper riktade sig mot specifika företag som bedömdes vara särskilt attraktiva mål. Det mest framträdande exemplet var 2025 Bybyit SAFE Wallet, där en APT-grupp fokuserade på att stjäla en stor mängd kryptovaluta. Dessutom observerades incidenter som var personligt motiverade, exempelvis hämnd eller vedergällning efter uppsägningar.

Sammanfattningsvis styrs konsekvenserna av angriparens motivation. Opportunistiska aktörer tenderar att söka ekonomisk vinning, medan APT-grupper kan ha mycket varierande motiv beroende på grupp och tillhörighet. Det är även troligt att mer avancerade hotaktörer besitter kompetens och resurser för att forska på sårbarheter hos molnleverantören för att kunna slå mot alla dess kunder.

5.2.2 Resursövertagning

I de flesta incidenterna, 11 av 17, där resurser tagits över har detta resulterat i olika typer av kryptobrytning, där antingen företagets molnresurser eller företagets klientdatorer har använts för att bryta kryptovaluta. I två av fallen för resursövertagning har hotaktören kommit åt företagets AWS Simple Email Service[16] och skickat nätfiskeförsök via e-post från företagets domän. I två fall har en aktör tagit över resurser och konfigurerat om DNS för att visa olämpliga bilder för företagets anställda. Det observerades i ett fall att en tidigare anställd loggat in på samma konto som den hade vid anställning och stängt ner servrar. I ett av fallen utfördes en gisslanattack där data krypterades och användes för att utpressa företaget.

[16] AWS Simple Email Service är AWS molnbaserade e-posttjänst [112].

5.2.3 Radering av data

I 4 av 5 incidenter där radering av data skett har det gjorts av en tidigare anställd på företaget. I det resterande fallet har data tagits bort i samband med att den blivit stulen.

5.2.4 Inga konsekvenser

12 av de totalt 157 bedömda incidenterna resulterade inte i några konsekvenser. Av dessa 12 incidenter antas 10 vara utan konsekvens på grund av att forskare rapporterat säkerhetshålen innan en hotaktör kunnat utnyttjat sårbarheten. Här har företagen behandlat dessa sårbarheter som incidenter, även att ingen konsekvens medföljt. För de resterande två incidenterna har andra säkerhetsfunktioner förhindrat konsekvens. 2023 Sumo Logic identifierade att en hotaktör loggat in och försökt exfiltrera data. Dessa data var dock krypterade med nycklar som hotaktören inte fick tillgång till och konfidentialiteten bedöms därmed vara intakt. 2025 Grafana Labs identifierade en incident tack vare en säkerhetsteknik kallad *canary tokens* eller *honeytoken*. Detta är en vilseledningsteknik där konton utan behörigheter skapas och inloggningsuppgifter för dessa konton publiceras på olika ställen, såsom privata kodförråd eller användares enheter. Tack vare canary tokens identifierades intrånget och hotaktören kunde avlägsnas innan hotaktören lyckades få tillgång till andra konton. Fördelen med canary tokens är att stränga övervakningsregler kan sättas upp som varnar när inloggning sker på dessa konton, då det inte finns någon anledning att dessa konton ska användas i vanliga fall.

6 Diskussion

I detta kapitel diskuteras studiens resultat. I avsnitt 6.1 diskuteras orsaker till molnrelaterade säkerhetsincidenter, följt av en utvärdering av de utvalda säkerhetsramverken i avsnitt 6.2, baserad både på genomgången av ramverken och på de analyserade incidenterna. I avsnitt 6.3 rekommenderas åtgärder mot vanligt förekommande säkerhetsbrister bakom de analyserade incidenterna. Därefter följer en översikt av de problem runt ofullständig rådighet som tillkommer vid användning av molntjänster i avsnitt 6.4. Potentiella begränsningar med studien diskuteras i avsnitt 6.5 medan avsnitt 6.6 ger förslag på framtida forskning.

6.1 Orsaker till molnrelaterade säkerhetsincidenter

Baserat på resultatet från incidentkategoriseringen i avsnitt 5.1, kan det konstateras att en vanlig orsak till molnrelaterade säkerhetsincidenter är generella felkonfigurationer. Med hänsyn till omfattningen av de incidenter som orsakats av dessa generella felkonfigurationer, samt att även organisationer med hög mognadsgrad har drabbats, tolkar författarna det som en tydlig indikation på den konfigurationskomplexitet som präglar molnmiljöer. Vissa organisationer har helt saknat säkerhetskontroller, medan de flesta incidenter har inträffat när enskilda resurser inte omfattats av befintliga kontroller. Problemet rör således främst bristande översikt över systemets konfiguration, särskilt avseende identitets- och åtkomsthantering. Åtgärder såsom effektiv användning av skyddsräcken för behörigheter och organisatoriska enheter anses lämpliga för att stärka identitets- och åtkomsthantering. IaC är en lämplig metod för att undvika uppenbara felkonfigurationer i infrastrukturen genom att undvika eventuella fel vid manuell konfiguration.

Tjänster för att hantera organisatoriska enheter, såsom AWS Organizations [73], Azure Management Groups [74] och GCP Folders [75], bidrar både till nätverkssegmentering och identitets- och åtkomsthantering. De möjliggör separation av miljöer, som exempelvis produktion och utveckling, till olika molnnät, samtidigt som molnkonton kan organiseras och grupperas med relaterade behörigheter. Ofta integreras dessa organisatoriska enheter med övervakningssystem, exempelvis AWS Cloudwatch [76], Azure Monitor [77], eller GCP Cloud Logging [78], vilket ytterligare underlättar hanteringen av identiteter i systemet.

Skyddsräcken för behörigheter gör det möjligt att definiera strikta ramar för vilka åtgärder som inte får utföras inom olika delar av organisationen. Redan vid systemets design kan det därmed fastställas vilka operationer som ska begränsas och säkerställa att otillåtna åtgärder aldrig utförs.

Genom att använda IaC tillsammans med statisk analysverktyg för all konfiguration inom molnsystemet blir det avsevärt svårare att skapa resurser som lämnas oövervakade, vilket har visat sig vara en vanlig orsak till incidenter. Om manuella ändringar i molnmiljön endast tillåts via uppdateringar av infrastrukturkoden skapas en enhetlig översikt över samtliga resurser och deras konfigurationer, vilket i sin tur

bidrar till en mer robust och säker infrastruktur. IaC-verktyg finns tillgängliga specifikt för molntjänstleverantörer som AWS CloudFormation [113], Azure Resource Manager [114], och GCP Infrastructure Manager [115]. Det är även möjligt att använda ett mer övergripande verktyg såsom Terraform [116].

Det faktum att många enkla felkonfigurationer har observerats kan betraktas som oroväckande. Mer sofistikerade attacker, exempelvis de som lyfts i avsnitt 5.1.1, ställer avsevärt högre krav på ett systems säkerhet än vad som krävs för att undvika de enklare konfigurationsfelen. Det framstår därför som osannolikt att en stor andel av de undersökta organisationerna har uppnått en säkerhetsmognad som är tillräcklig för att stå emot en mer motiverad angripare. I ett sådant scenario ställs inte enbart krav på den externa perimetern, utan även på att det interna nätverket är tillräckligt segmenterat. Detta förutsätter i sin tur, som ett minimum, en välfungerande och centraliserad identitets- och åtkomsthantering, samt adekvat monitorering och loggning, vilket är något som författarna uppfattat saknats i en stor del av organisationerna som drabbats av de analyserade incidenterna.

Flera återkommande säkerhetsproblem har identifierades av författarna utifrån genomgång av incidenterna i kapitel 5:

- inventering och klassificering av lagrade data genomförs inte
- kryptering av data i vila används sällan
- granskning av tredjepartstjänster och externa bibliotek är otillräcklig
- system- och mjukvaruuppdateringar försummas
- mjukvaruutvecklare har bristfällig kompetensen inom cybersäkerhet
- överblick över identiteter inom organisationen saknas
- principerna om lägsta behörighet och ansvarsfördelning följs inte konsekvent
- tillämpning av nolltillit sker i mycket begränsad utsträckning, vilket innebär att exempelvis en felkonfigurerad brandvägg kan ge djupgående åtkomst i nätverket
- monitorering och larmfunktioner saknas ofta, även vid avvikande beteenden såsom omfattande dataöverföring från interna databaser till externa mottagare
- bristande nätverkssegmentering är vanligt förekommande, och mikrosegmentering uppfattas användas i mycket liten omfattning.

Utifrån dessa observationer kan det diskuteras i vilken utsträckning organisationerna har designat sina molnsystem med säkerhet i åtanke. Rimligtvis har många organisationer försökt designa sina system med hänsyn till säkerhet, potentiellt även utifrån ett säkerhetsramverk. I så fall kan en slutsats vara att molnsäkerhet är så pass komplext att även organisationer med stora resurser ofta misslyckats i implementeringen. Alternativt finns möjligheten att incitamenten för att prioritera säkerhet inte har varit tillräcklig stora inom många organisationer.

Då molnsystems komplexitet diskuteras är det viktigt att beakta de säkerhetslösningar som erbjuds av molntjänstleverantörerna. Dessa säkerhetslösningar syftar till att förenkla molnsäkerhetsarbetet genom att automatisera etablerade säkerhetsåtgärder inom olika säkerhetskategorier. Därigenom kan behovet av djupgående säkerhetskompetens vid systemdesign minska något. Användningen av dessa tjänster innebär dock potentiellt ytterligare kostnader, eftersom flera olika molntjänster ofta krävs och prissättningen är baserad på resursförbrukning. Dessutom krävs en ny form av leverantörsspecifik kompetens för att kunna använda och kombinera tjänsterna på ett effektivt sätt. Det kan även konstateras att ett ökat beroende av

molnsäkerhetstjänster medför en högre grad av leverantörsinlåsning, vilket i sin tur kan försvåra en framtida migrering till andra leverantörer. Vidare ställer dessa typer av säkerhetslösningar även vidare krav på tillit till leverantören. Användningen av säkerhetsrelaterande molntjänster bör övervägas, men bör inte ses som enkla eller färdiga lösningar vilka garanterar molnsäkerhet.

6.2 Säkerhetsramverk

Genomgång av de utvalda säkerhetsramverken visar ett genomgående tema – samtliga ramverk är mycket omfattande och innehåller ofta över hundra sidor med listor över krav och kontroller. Att följa ett sådant ramverk i detalj utgör därför en mycket resurskrävande uppgift. En möjlig förklaring är att ramverken är avsedda att vara så generella som möjligt. I praktiken innebär detta dock potentiellt att organisationer måste analysera och anpassa åtgärderna utifrån sina specifika behov, vilket kan introducera en mängd oavsiktliga säkerhetsbrister.

Vidare saknas konkreta mekanismer för att säkerställa huruvida de hundratals individuella kraven faktiskt är uppfyllda, utan att beakta den höga tolkningsgraden som präglar många av åtgärderna. Detta tyder på att den mest utmanande delen av att implementera ett säkerhetsramverk inte nödvändigtvis är själva implementeringen, utan snarare tolkningen och verifieringen av kraven.

Ytterligare en punkt som bör uppmärksammas är att standarder för molnsäkerhet för närvarande i stor utsträckning drivs av molntjänstleverantörerna. Aktörer som ISO och NIST, vilka inom många andra områden har en ledande roll, har hittills inte varit drivande i den tekniska utvecklingen av molnsäkerhetsstandarder eller rekommendationer.

Från resultaten kan det utläsas att säkerhetsramverken lägger extra vikt på vissa typer av åtgärder. Exempelvis omfattar 46 % av infrastruktursåtgärderna nätverkssegmentering i olika former. Dock bör för stor vikt inte läggas vid dessa siffror då underkategorierna är olika omfattande och på olika nivå av konkretisering. En bättre skärning kan vara att utvärdera vilka konkreta säkerhetsåtgärder som rekommenderas av flera ramverk. Utifrån de 333 säkerhetsåtgärder från de fem ramverk som sammanställdes i ett begränsat antal underkategorier i kapitel 4, kan ett betydande överlapp noteras mellan samtliga ramverk. Detta indikerar förekomsten av ett stort antal säkerhetsåtgärder som branschen i stor utsträckning är överens om, exempelvis:

- autentisering för samtliga resurser via centraliserad identitetsleverantör och ZTNA eller motsvarande; all åtkomst bör regleras av en centraliserad policy snarare än separata policyer för varje instans.
- tidsbegränsade autentiseringsuppgifter (eng. temporary credentials) baserade på central autentisering
- principen om lägsta behörighet och ansvarsfördelning för identiteter och grupper inom organisationen
- användning av organisatoriska enheter för att hantera och gruppera konton, samt logiskt separerade miljöer för exempelvis produktion och utveckling.
- användning av skyddsräcken för behörigheter inom de organisatoriska enheterna för att förbjuda aktiviteter som aldrig ska kunnas utföras.
- kryptering av känsliga data i vila

- lagring av hemligheter med hjälp av hemlighetsvalv eller lösenordsskyddade mekanismer
- segmentering av nätverk baserat på användning med hjälp av:
  - subnät
  - brandväggar
  - begränsad exponering mot internet.
- process för uppdatering av tredjepartsmjukvara
- systemutvecklingslivscykel för egenutvecklade applikationer
- loggning och övervakning av samtliga åtkomstförsök och avvikelser i nätverkstrafik
- konfiguration endast via IaC.

Även om fullständig regelefterlevnad enligt ramverk kräver hundratals kontroller, kan organisationer uppnå en relativt hög säkerhetsnivå om åtgärderna i punktlistan implementeras konsekvent. Dock är implementationen av enbart dessa 12 åtgärder en komplex uppgift som kräver specifik kompetens.

Som tidigare nämnt i avsnitt 6.1, är det möjligt att få tillgång till många av dessa åtgärder genom molntjänstleverantörernas egna säkerhetslösningar. Att nyttja molntjänstleverantörens egna lösningar innebär lägre krav på grundkompetens jämfört med att själv implementera ett säkert molnsystem. Dessa lösningar har dessutom fördelen att de är skräddarsydda för den specifika molntjänsten, vilket exempelvis tillåter skalbarhet, tillgänglighet samt unika förmågor som bland annat övervakning av alla administrativa ändringar. Författarna anser att samtliga erbjudna säkerhetstjänster från använd molntjänstleverantör åtminstone bör utvärderas när säkerhetskritiska molnsystem designas.

6.3 Rekommenderade åtgärder mot de vanligast förekommande säkerhetsbristerna i molnsystem

Utifrån de analyserade incidenterna upptäcktes tydliga överlapp i vilka säkerhetsbrister som hade utnyttjats. Detta avsnitt diskuterar de identifierade säkerhetsbristerna och presenterar förslag på säkerhetsåtgärder som hade kunnat förhindra eller mitigerat respektive incident. Som tidigare nämnt kan en enskild incident orsakas av flera brister, vilket innebär att procenten i följande avsnitt överstiger 100 %.

6.3.1 Publika resurser utan åtkomsthantering

Orsaken till en stor del av säkerhetsincidenterna var att resurser med privat data befann sig publikt tillgängliga, helt utan åtkomsthantering. Dessa resurser var vanligtvis hinkar eller databaser, men det förekom även andra resurser som till exempel verktyg för utrullning (Tesla). Totalt bedömdes ungefär 36 % av de analyserade incidenterna orsakas av publika resurser utan åtkomsthantering.

Lösningen på detta problem kan framstå som enkelt: säkerställ att resurser som inte ska vara publikt tillgängliga omfattas av åtkomsthantering och exponera inte dessa resurser mot internet. I praktiken är detta problem dock mer komplext, eftersom det i stor utsträckning kräver att organisationer har översikt över samtliga resurser som driftas. Vissa resurser, såsom publika webbsidor, ska dessutom vara publikt tillgängliga utan åtkomsthantering, vilket innebär att det inte är möjligt att låsa ned samtliga resurser.

De säkerhetsåtgärder som identifierats i ramverken för att hantera detta problem omfattar regelbaserad hantering av resurserna utifrån både infrastruktur- och åtkomstperspektiv. Infrastrukturella regler kan implementeras genom att använda IaC tillsammans med verktyg för statisk kodanalys. Den statiska analysen kan varna molntjänstanvändaren när publikt tillgängliga resurser avses skapas, vilket möjliggör en bedömning av huruvida exponeringen är avsiktlig eller om resursen har konfigurerats felaktigt. För åtkomsthanteringen rekommenderas användning av en central IAM, där skyddsräcken för behörigheter kan skapas. Genom dessa skyddsräcken är det möjligt att begränsa åtkomsträttigheter för behörighetsprofiler och därigenom minska risken för oavsiktlig exponering av resurser.

Dessa säkerhetsåtgärder är enbart effektiva om de faktiskt tillämpas på de relevanta resurserna. Med den komplexitet som molntjänster ofta medför är det möjligt att organisationer som drabbats av de analyserade incidenterna redan hade implementerat de tidigare beskrivna säkerhetsåtgärderna, men att dessa inte tillämpats på de specifika resurser som utnyttjats. Felkonfigurationer i molntjänster är vanliga, och branschen har uppmärksammat att sådana felkonfigurationer ofta är orsaken till att incidenter uppstår. För att hantera dessa felkonfigurationer har verktyg utvecklats som syftar till att identifiera och förebygga vanliga förekommande felkonfigurationer. CSPM-lösningar är exempel på sådana verktyg och avser att öka säkerheten genom att övervaka organisationens resurser samt analysera resurserna för vanliga felkonfigurationer.

6.3.2 Bristfällig hantering av hemligheter

Ungefär 25 % av de analyserade incidenterna har bedömts orsakats eller förvärrats av otillräcklig hantering av hemligheter. Dessa hemligheter var ofta i form av åtkomstnycklar till molntjänstanvändare eller databaser. I de analyserade incidenterna befann sig hemligheterna i publikt tillgängliga resurser utan åtkomstkontrol, i konfigurationsfiler samt i olika typer av klientkod, såsom APK:er och javascript-kod.

- **Åtkomstnycklar till molnplattformen**:
  En vanlig orsak till de analyserade incidenterna var att tidsobegränsade åtkomstnycklar hade lagts upp i publika källor, såsom Github eller APK:er. Molntjänstanvändare behöver utbildning i att hantera åtkomstnyckeln som en hemlighet, på samma sätt som användarnamn och lösenord till molntjänstplattformen. Det är även rekommenderat att bruka tidsbegränsade åtkomstnycklar för att begränsa skadan vid eventuell exponering. Molntjänstanvändares behörigheter bör dessutom minimeras för att ytterligare minska exponering vid eventuellt röjda hemligheter. För att motverka att

hemligheter inkluderas i källkod kan även statisk kodanalys användas för att identifiera vanliga nyckelformat i koden.

- **Hantering av drifthemligheter**:
  För att minska exponeringen av hemligheter i molnmiljön rekommenderas användning av hemlighetsvalv. Dessa hemlighetsvalv krypterar hemligheter och har inbyggd åtkomsthantering för tillgång till hemligheterna. I de fall där användning av hemlighetsvalv inte är möjligt bör åtminstone hemligheter vara krypterade när de befinner sig i vila.

6.3.3 Okrypterad data i vila

I 19 % av de analyserade incidenterna observerade författarna att känslig data förvarades okrypterad i vila. Om data hade varit krypterad i vila hade incidenten åtminstone delvis kunnat mitigerats. Det är oklart om organisationerna ansåg att kryptering av data i vila inte var nödvändig, eller om detta missats för särskilda resurser. Molntjänstleverantörerna är medvetna om att okrypterad data i vila är ett problem och har på senare tid infört kryptering av data i vila som standard för lagringsresurser[17][18]. För att identifiera resurser där standardkonfigurationen för kryptering av data i vila har inaktiverats kan statisk analys av IaC användas. För att säkerställa att resurser krypterar data i vila kan även DSPM-lösningar implementeras.

6.3.4 Sårbarheter i applikationskoden

Ungefär 16 % av de analyserade incidenterna har orsakats av sårbarheter i applikationskoden. Detta omfattar både sårbarheter i egenutvecklad kod och sårbarheter i tredjepartsbibliotek och -produkter. Sårbarheter i applikationskoden är inte en molnspecifik säkerhetsbrist, utan påverkar traditionella IT-miljöer i lika hög grad. För att förebygga sårbarheter i egenutvecklad kod bör etablerade säkra utvecklingsprocesser följas. Applikationskoden bör dessutom testas för sårbarheter, både genom statisk kodanalys och genom penetrationstester.

För tredjeparsbibliotek och -produkter är hantering av nolldagssårbarheter svåra att hantera. Däremot bör kända sårbarheter i tredjeparsbibliotek och -produkter upptäckas och åtgärdas i största möjliga utsträckning. Upptäckt av kända sårbarheter i tredjepartsbibliotek och -produkter kan automatiseras genom sårbarhetshanteringsprocesser, där verktyg jämför de versionerna av tredjepartsbiliotek och -produkter som används mot databaser över kända sårbarheter[19].

6.3.5 Bristfällig intrångsdetektion

I 13 % av de analyserade incidenterna bedömde författarna att intrångsdetektering och övervakning varit otillräcklig. Om intrång hade upptäckts tidigare skulle incidenten eventuellt ha kunnat förhindras genom att avlägsna hotaktören innan denna fått

[17] https://docs.aws.amazon.com/AmazonS3/latest/userguide/default-encryption-faq.html
[18] https://azure.microsoft.com/en-us/blog/announcing-default-encryption-for-azure-blobs-files-table-and-queue-storage/
[19] Som till exempel https://www.cve.org/

tillgång till data eller påverkat resurser. Säkerhetsåtgärderna från säkerhetsramverken rekommenderar användning av olika verktyg för intrångsdetektion. Det finns flera etablerade typer av intrångsdetektionsverktyg på marknaden, som till exempel NDR, XDR och CDR, som med fördel kan användas vid nyttjandet av molntjänster.

6.3.6 Svaga inloggningsmekanismer

För 8 % av de analyserade incidenterna har forskarna bedömt att svaga inloggningsmekanismer till molnplattformen varit en bidragande orsak till incidenten. Samtliga av de tre stora molntjänstleverantörerna erbjuder möjligheter att definiera och hävda policyer för inloggningsmekanismer. Det är rekommenderat att samtliga molntjänstanvändarkonton omfattas av starka inloggningsmekanismer, vilket innefattar MFA och acceptabel nivå av komplexitet på lösenord.

6.3.7 Aktiva molntjänstkonton för tidigare anställda

8 % av de analyserade incidenterna har orsakats av tidigare anställda som använt de molntjänstkonton som personen haft tillgång till under sin anställning. För att förhindra att tidigare anställda behåller åtkomst till molntjänstkonton bör offboarding av anställda automatiseras och inkludera de berörda molntjänstkontona.

Sammanfattningsvis hade majoriteten av incidenterna kunnat förhindrats eller mitigerats genom implementering av ett fåtal säkerhetsåtgärder, vilka är relativt enkla att införa.

6.4 Ofullständig rådighet

Vid användning av molntjänster uppstår risker kopplade till att molntjänstanvändaren inte har fullständig rådighet över det underliggande IT-systemet. Under vissa omständigheter kan molntjänstleverantören försöka få åtkomst till data som lagras i användares molntjänster. Leverantören har även möjlighet att stänga ned tjänster som driftas i dess infrastruktur. Att hantera de utmaningar som följer av denna begränsade kontroll innebär ofta ökad komplexitet och ytterligare beräkningsmässiga kostnader. I följande punktlista diskuteras några av dessa utmaningar samt möjliga åtgärder för att hantera dem:

- **Data i vila och under överföring**: Molntjänstleverantörer kan potentiellt försöka få tillgång till data som ligger i vila eller överförs mellan tjänster. För att motverka detta kan data krypteras, vilket innebär att även om molntjänsteleverantören får åtkomst kan innehållet inte tolkas. En konsekvens av detta är att tjänster för hantering av krypteringsnycklar ej får befinna sig i molnet, vilket utesluter användningen av leverantörens egna nyckelhanteringstjänster. Det krävs därför en extern lösning utanför molnmiljön för att tillhandahålla dekrypteringsnycklar för att behålla kontroll över data i vila och under överföring.

- **Data vid beräkning**: En molntjänsteleverantör kan i teorin försöka läsa data i minnet under pågående beräkningar. En strategi för att motverka detta är att använda hybridsystem där känsliga data bearbetas i lokala datacenter och krypteras innan de skickas till molnet. Nackdelen med hybridsystem är att molnets beräkningsresurser då inte kan nyttjas för behandling av känsliga uppgifter. Ett annat alternativ är homomorfisk kryptering, som möjliggör beräkningar på krypterad data och därmed tillåter användning av molnresurser utan dekryptering. Tekniken är dock omogen och medför i dagsläget en mängd begränsningar, såsom hög beräkningskostnad, begränsat stöd för olika datatyper och operationer, samt bristande integration med stora delar av molnekosystemet. Ett mer etablerat alternativ är att använda betrodda exekveringsmiljöer, såsom *Intel Software Guard Extensions (SGX)*[20], *AMD SEV-SNP*[21] *(Secure Encrypted Virtualization – Secure Nested Paging)* och *AWS Nitro Enclaves*[22]. Dessa lösningar kräver dock fortsatt tillit till leverantörer.
- **Drift**: En molntjänsteleverantör kan eventuellt välja att stänga ner en molntjänst. Leverantörer stänger rutinmässigt ner tjänster som bryter mot dess användarvillkor, men det kan även uppstå situationer där ekonomiska, juridiska, eller politiska påtryckningar leder till avstängning. Ett aktuellt exempel är att Microsoft stängde ned en tjänst som tillhörde Israels militär, med hänvisning till att den användes för massövervakning av civila, vilket strider mot Microsoft Azures användarvillkor[23]. För att mitigera denna risk kan organisationer använda multimolnlösningar eller upprätthålla färdiga alternativ hos andra leverantörer eller i egna datacenter. Detta medför dock betydande kostnader och ökad komplexitet, både avseende förvaltning av alternativlösningen och drift av egen infrastruktur.

Samtliga av de tre stora molntjänstleverantörerna arbetar aktivt med initativ för att möjliggöra suveräna molnlösningar inom EU, såsom AWS European Sovereign Cloud[24], Azure Data Guardian[25] och GCP soveregin cloud[26].

Sammanfattningsvis bör rådighet beaktas när säkerhetskänsliga system designas för molnet. Det är ett ofrånkomligt faktum att en viss grad av tillit till molntjänstleverantören är nödvändig. Även om tekniker såsom säkra enklaver, attestation och alternativa arkitekturella lösningar kan reducera risken, kvarstår det grundläggande beroendet av leverantören, eftersom denne äger och kontrollerar den underliggande infrastrukturen.

[20] https://www.intel.com/content/www/us/en/products/docs/accelerator-engines/software-guard-extensions.html
[21] https://www.amd.com/en/developer/sev.html
[22] https://aws.amazon.com/ec2/nitro/nitro-enclaves/
[23] https://blogs.microsoft.com/on-the-issues/2025/09/25/update-on-ongoing-microsoft-review/
[24] https://aws.eu/
[25] https://blogs.microsoft.com/blog/2025/06/16/announcing-comprehensive-sovereign-solutions-empowering-european-organizations/
[26] https://cloud.google.com/sovereign-cloud

6.5 Studiens begränsningar

Molnsäkerhet är ett omfattande och komplext område, och det har därmed inte varit möjligt att täcka hela fältet inom ramen för denna studie. Den sökning som genomförts för att identifiera molnsäkerhetsramverk har varit ytlig, vilket innebär att det finns en risk att välkända ramverk har missats. Det bör dock betonas att studiens mål inte var att identifiera samtliga befintliga molnsäkerhetsramverk och extrahera alla åtgärder ur dessa, utan snarare att samla in tillräckligt med information för att skapa en övergripande förståelse av vilka typer av säkerhetsåtgärder som vanligtvis förekommer i ramverk. Det har inte heller funnits möjlighet för författarna att sätta sig in på djupet för varje säkerhetsåtgärd, utan det har krävts en balansgång mellan djup och bredd.

Säkerhetsramverken betonar även behovet av viktiga processer för drift av molnsystem. Exempelvis innehåller CCM kontroller för riskhantering, incidenthantering, granskning och assurans, interoperabilitet samt kontinuitet- och resiliensstrategier. Dessa kontroller har inte placerats i någon specifik sårbarhetskategori, då de sprider sig över en bredare grund för säkerhetsarbetet och därmed berör alla kategorier i viss mån. Vidare är dessa typer av kontroller inte unika för molnplattformar, utan återfinns generellt inom förvaltning av IT-system. Liksom i traditionell drift är dessa processer en väsentlig del av säkerhetsarbetet.

Det finns ett stort antal kända incidenter för molnlösningar, vilka ökar i antal dagligen. Att gå igenom alla dessa incidenter har inte varit möjligt för denna studie. Det har inte heller varit möjligt att studera varje utvald incident djupgående, utan många har analyserats ytligt. I denna studie var syftet inte att skapa en uttömmande lista av incidenter, utan att bygga en tillräcklig stor incidentlista av relevanta incidenter för att bygga förståelse för hur och varför molnincidenter uppstår, samt att kunna dra rationella slutsatser utifrån resultaten.

De incidenter som analyserats inträffade under de senaste tio åren. Eftersom molnteknik fortfarande är ett relativt ungt område, och att utvecklingen sker i snabb takt, är det sannolikt att att en del av de specifika bristerna eller sårbarheterna som ledde till incidenterna har hunnit bli inaktuella. Samtidigt är det svårt att fastställa ett optimalt tidsintervall för analys, eftersom ett alltför snävt tidsspann skulle reducera mängden tillgängliga incidenter och därmed försvåra möjligheten att dra tillförlitliga slutsatser på grund av ett otillräckligt empiriskt underlag.

Vidare bygger studien enbart på incidenter som har publicerats öppet. Det är rimligt att anta att ett omfattande mörkertal förekommer. Incidenter som inte publicerats öppet behöver inte nödvändigtvis vara kopplade till samma typ av sårbarheter eller leda till liknande konsekvenser som de som analyserats. Därmed kan den bild som framkommer i studien endast delvis spegla verkligheten.

Slutligen medför denna typ av forskning där man samlar incidenter, att man studerar bristfälliga system i större utsträckning än välfungerande molnlösningar. Detta kan leda till en negativ vinkling över molnlösningars säkerhet. Studien har delvis balanserat denna effekt genom att även inkludera säkerhetsramverk för molnlösningar. Hur dessa ramverk i praktiken implementeras av organisationer är emellertid betydligt svårare att undersöka, då sådan information sällan är offentligt tillgänglig.

6.6 Framtida forskning

Författarna identifierar flera intressanta möjliga inriktningar för framtida forskning inom molnsäkerhet. Ett område är studier som jämför eller utvärderar specifika molnsäkerhetstjänster. Exempelvis skulle säkerhetslösningar som tillhandahålls av molnjänstleverantörer, såsom Trusted Secure Enclave med AWS Landing Zone, kunna analyseras.

Vidare framstår säkerhetsrelaterade fallgropar vid migration mellan leverantörer eller från lokal infrastruktur, som ett relevant forskningsområde. De rådighetssutmaningar som följer av användningen av molntjänster har inte behandlats genomgående i denna studie, men är av central betydelse för att avgöra om moln kan användas i säkerhetskänsliga verksamheter. Forskning kring molnsuveränitet och rådighet utgör därmed en potentiellt värdefull inriktning. Även mer varierade distributionsmodeller, såsom hybridmoln och multimoln, kan vara av intresse att titta närmare på. Slutligen finns stora möjligheter att studera specifika typer av sårbarheter och motsvarande säkerhetsåtgärder ur ett mer tekniskt perspektiv, exempelvis i kombination med konkreta fallstudier eller praktiska demonstrationer.

7 Slutsatser

I denna rapport presenteras en litteraturstudie där fem etablerade ramverk för molnsäkerhet har analyserats i syfte att identifiera och sammanställa centrala säkerhetsåtgärder inom området. Molnincidenter från de senaste tio åren har samlats in och analyserats utifrån orsak till att incidenten uppstod och konsekvensen av incidenten. Slutligen analyseras hur de vanligaste molnincidenterna kunde ha förhindrats baserat på de identifierade säkerhetsåtgärderna.

I studien har följande forskningsfrågor besvarats.

Forskningsfråga 1: Vilka typer av sårbarheter har orsakat molnbaserade säkerhetsincidenter under de senaste tio åren?

Den största andelen av de analyserade incidenterna kan härledas till generella felkonfigurationer. Det är sannolikt att många av de felkonfigurerade resurserna i molntjänsterna inte har fångats upp av säkerhetsprocesser eller rutiner alternativt inte har övervakats på ett strukturerat sätt.

Denna typ av brister har observerats även hos organisationer med hög säkerhetsmognad. Detta tyder på att det generellt är svårt för organisationer att upprätthålla en fullständig överblick över sina data och resurser i molnmiljöer. För att bemöta mer avancerade attacker kan det förväntas kräva en betydligt högre grad av säkerhetsmognad inom organisationen, vilket i praktiken innebär behov av personal med djup kompetens inom molnarkitektur och molnsäkerhet. För att hantera denna komplexitet bör det dessutom finnas redundans i dessa roller, eftersom det kan vara svårt för nya medarbetare att snabbt sätta sig in i systemen.

Forskningsfråga 2: Vilka säkerhetsåtgärder rekommenderas av erkända institutioner och auktoriteter inom molnsäkerhet?

Befintliga ramverk för molnsäkerhet är omfattande och kan vara svåra att implementera i praktiken, delvis eftersom de tenderar att omfatta hundratals individuella åtgärder. Ramverken innehåller dessutom en hög grad av tolkningsutrymme, vilket ställer krav på kompetens hos den som implementerar dem. Verifiering av huruvida en åtgärd har implementerats korrekt kan sällan genomföras formellt, utan verifieringen förlitar sig i stor utsträckning på expertis hos den som utformar molnsystemet.

Många av de säkerhetslösningar som utvecklats för att hantera molnsäkerhet kräver leverantörsspecifik kompetens, vilket i sin tur kan innebära leverantörsinlåsning. Trots skillnader mellan leverantörsspecifika molnlösningar identifieras i samtliga ramverk ett antal övergripande säkerhetsmekanismer som återkommer oberoende av leverantör. En mer översiktlig sammanställning av många av dessa åtgärder återfinns i samtliga tabeller i kapitel 4. Utöver detta bedöms, med hänsyn till forskningsfråga 1, ett särskilt värde i användning av organisatoriska enheter, skyddsräcken för behörigheter samt IaC. Ett system som från början är designat med dessa åtgärder i åtanke har potential att växa utan att enkla konfigurationsfel går förbi obemärkta.

Forskningsfråga 3: Vilka av de identifierade säkerhetsåtgärderna förhindrar eller mitigerar vanligt förekommande orsaker till de analyserade säkerhetsincidenterna?

De vanligaste säkerhetsbristerna som förekommer i de analyserade incidenterna är främst inom områdena identitets- och åtkomsthantering, infrastruktur samt dataskyddskonfiguration. Den orsak som förekommer vid flest incidenter är publikt åtkomliga resurser, helt utan åtkomstkontroll. Dessa incidenter hade kunnat förhindrats eller mitigerats genom att utnyttja statisk kodanalys av IaC, samt att etablera tydliga skyddsräcken för behörigheter. Säkerhetslösningar, som till exempel CSPM, hade även kunnat användas för att identifiera dessa felkonfigurationer. Bristfällig hantering av hemligheter var också en vanligt förekommande orsak bakom de analyserade incidenterna. De incidenter som orsakats av röjda drifthemligheter, kunde ha mitigerats med hjälp av användning av hemlighetsvalv. För de incidenter som orsakats av röjda åtkomstnycklar till molnplattformen, hade dessa incidenter mitigerats med hjälp av exempelvis tidsbegränsade åtkomstnycklar, minimala behörigheter för molnanvändare och statisk kodanalys. Utöver dessa åtgärden identifierades ytterligare mitigering för att undvika vanligt förekommande orsaker till incidenter, vilka återfinns i avsnitt 6.3.

Denna studie har enbart undersökt rapporterade molnincidenter och därmed inte tagit hänsyn till fall där organisationer har implementerat välfungerande molnsäkerhet. Därmed är det inte möjligt att dra några slutsatser om huruvida molnbaserade system är svårare eller enklare att konstruera på ett säkert sätt jämfört med traditionella IT-system. Den slutsats som kan dras är att molnsystem generellt introducerar nya attackytor och att molnsystem snabbt tenderar att utvecklas till komplexa miljöer, vilket många organisationer har svårt att hantera på ett säkert sätt.

Sammanfattningsvis tyder resultaten i denna rapport på att organisationer har problem med att överblicka resurser i ett molnsystem. Vidare tenderar molnsystem att snabbt blir komplexa när de växer. Säkerhetsramverk för molnsystem existerar, men de är omfattande och kan vara svårtolkade. Det finns dock en tydlig branschkonsensus mellan ramverken avseende leverantörsagnostiska säkerhetsåtgärder. För att implementera dessa åtgärder krävs både domänspecifik kompetens och leverantörsspecifik kunskap. Denna kompetens är sannolikt både eftertraktad och kostsam, vilket även sannolikt kommer öka i takt med att molnsystem används alltmer.

Trots dessa utmaningar är det möjligt att, genom att designa ett system med några centrala säkerhetsåtgärder i åtanke, undvika många vanligt förekommande felkonfigurationer.

Referenser

[1] Google Cloud. ”Spotify: Google Cloud Customer Case Study”. Hämtad: 2025-11-20. (2025), URL: https://cloud.google.com/customers/spotify/.

[2] G. Leygues. ”Spotify chooses Google Cloud Platform to power data infrastructure”. Hämtad: 2025-11-20. (2016-02), URL: https://cloud.google.com/blog/products/gcp/spotify-chooses-google-cloud-platform-to-power-data-infrastructure.

[3] Microsoft Corporation. ”eBay and Microsoft Announce Cloud Computing Agreement - Stories — news.microsoft.com”. Hämtad: 2025-03-11. (2010), URL: https://news.microsoft.com/2010/07/12/ebay-and-microsoft-announce-cloud-computing-agreement/?msockid=22de974a1c696efb02b182e61d116f62.

[4] U.S. Department of Defense. ”Department of Defense Announces Joint Warfighting Cloud Capability Procurement — defense.gov”. Hämtad: 2025-02-20. (2022), URL: https://www.defense.gov/News/Releases/Release/Article/3239378/department-of-defense-announces-joint-warfighting-cloud-capability-procurement/.

[5] Defense Information Systems Agency (DISA). ”DISA Hybrid Cloud Broker / HaC”. Hämtad: 2025-11-20. (2025), URL: https://hybridcloud.disa.mil/.

[6] European Defence Agency. ”Combat Cloud: EDA Study Shows Benefits of Cloud Computing for EU Militaries”. Hämtad: 2025-03-11. (2024), URL: https://eda.europa.eu/news-and-events/news/2024/01/25/combat-cloud-eda-study-shows-benefits-of-cloud-computing-for-eu-militaries.

[7] Thales Group, ”2024 Thales Cloud Security Study - Global Edition”, Thales Group, 2024, An in-depth study on cloud security trends, challenges, and solutions based on responses from 3,000 participants across 18 countries and 37 industries. URL: http://cpl.thalesgroup.com/cloud-security-research.

[8] CrowdStrike Inc., ”CrowdStrike 2024 Global Threat Report”, CrowdStrike Inc., 2024, Comprehensive analysis of global cyber threats, focusing on cloud exploitation, generative AI, and identity-based attacks. URL: https://www.crowdstrike.com.

[9] S. Khan, I. Kabanov, Y. Hua och S. Madnick, ”A Systematic Analysis of the Capital One Data Breach: Critical Lessons Learned”, *ACM Trans. Priv. Secur.*, årg. 26, nr 1, 2022-11, ISSN: 2471-2566. DOI: 10.1145/3546068.

[10] T. G. Peter Mell. ”The NIST Definition of Cloud Computing”. Hämtad: 2025-03-07. (2011), URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.

[11] B. Burns, B. Grant, D. Oppenheimer, E. Brewer och J. Wilkes, ”Borg, Omega, and Kubernetes”, *Communications of the ACM*, årg. 59, nr 5, s. 50–57, 2016. DOI: 10.1145/2890784.

[12] Amazon Web Services. ”Amazon Web Services Announces AWS Lambda”. Hämtad: 2025-10-06. (2014-11), URL: https://press.aboutamazon.com/2014/11/amazon-web-services-announces-aws-lambda.

[13] Amazon Web Services. ”Types of Cloud Computing”. Hämtad: 2025-02-10. (2025), URL: https://aws.amazon.com/types-of-cloud-computing/.

[14] Google Cloud. ”PaaS vs IaaS vs SaaS”. Hämtad: 2025-02-10. (2025), URL: https://cloud.google.com/learn/paas-vs-iaas-vs-saas.

[15] Microsoft Azure. ”Types of Cloud Computing”. Hämtad: 2025-02-10. (2025), URL: https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/types-of-cloud-computing/.

[16] Google Cloud. ”What is Multicloud?” Hämtad: 2025-11-17. (2023), URL: https://cloud.google.com/learn/what-is-multicloud.

[17] SRG Research. ”Cloud Market Growth Rate Rises Again in Q3, Biggest Ever Sequential Increase”. Hämtad: 2025-11-17. (2023), URL: https://www.srgresearch.com/articles/cloud-market-growth-rate-rises-again-in-q3-biggest-ever-sequential-increase.

[18] Amazon Web Services. ”Amazon EC2 (Elastic Compute Cloud) Documentation”. Hämtad: 2025-10-13. (2025), URL: https://docs.aws.amazon.com/ec2/.

[19] Microsoft Corporation. ”Azure Virtual Machines Documentation”. Hämtad: 2025-10-13. (2025), URL: https://learn.microsoft.com/en-us/azure/virtual-machines/.

[20] Google LLC. ”Google Cloud Compute Engine Documentation”. Hämtad: 2025-10-13. (2025), URL: https://cloud.google.com/compute/docs.

[21] Amazon Web Services. ”Amazon Elastic Container Service (ECS)”. Hämtad: 2025-10-13. (2025), URL: https://aws.amazon.com/ecs/.

[22] Amazon Web Services. ”Amazon Elastic Kubernetes Service (EKS)”. Hämtad: 2025-10-13. (2025), URL: https://aws.amazon.com/eks/.

[23] Microsoft Corporation. ”Azure Kubernetes Service (AKS)”. Hämtad: 2025-10-13. (2025), URL: https://azure.microsoft.com/en-us/services/kubernetes-service/.

[24] Google LLC. ”Google Kubernetes Engine (GKE)”. Hämtad: 2025-10-13. (2025), URL: https://cloud.google.com/kubernetes-engine.

[25] Amazon Web Services. ”AWS Elastic Beanstalk”. Hämtad: 2025-10-13. (2025), URL: https://aws.amazon.com/elasticbeanstalk/.

[26] Microsoft Corporation. ”Azure App Service”. Hämtad: 2025-10-13. (2025), URL: https://azure.microsoft.com/en-us/products/app-service/.

[27] Google LLC. ”Google App Engine”. Hämtad: 2025-10-13. (2025), URL: https://cloud.google.com/appengine.

[28] Amazon Web Services. ”AWS Lambda Documentation”. Hämtad: 2025-10-13. (2025), URL: https://docs.aws.amazon.com/lambda/.

[29] Microsoft Corporation. ”Azure Functions documentation”. Hämtad: 2025-10-13. (2025), URL: https://learn.microsoft.com/en-us/azure/azure-functions/.

[30] Google LLC. ”Google Cloud Functions / Cloud Run functions documentation”. Hämtad: 2025-10-13. (2025), URL: https://cloud.google.com/functions/docs.

[31] Amazon Web Services. ”Amazon Elastic Block Store (Amazon EBS)”. Hämtad: 2025-10-13. (2025), URL: https://docs.aws.amazon.com/ebs/latest/userguide/what-is-ebs.html.

[32] Microsoft Corporation. ”Overview of Azure Disk Storage - Virtual Machines”. Hämtad: 2025-10-13. (2025), URL: https://learn.microsoft.com/en-us/azure/virtual-machines/managed-disks-overview.

[33] Google LLC. ”Persistent Disk: Durable Block Storage”. Hämtad: 2025-10-13. (2025), URL: https://cloud.google.com/persistent-disk.

[34] Amazon Web Services. ”Amazon S3 (Simple Storage Service) Documentation”. Hämtad: 2025-10-13. (2025), URL: https://docs.aws.amazon.com/s3/.

[35] Microsoft Corporation. ”Azure Blob Storage Documentation”. Hämtad: 2025-10-13. (2025), URL: https://learn.microsoft.com/en-us/azure/storage/blobs/.

[36] Google LLC. ”Google Cloud Storage (GCS) Documentation”. Hämtad: 2025-10-13. (2025), URL: https://cloud.google.com/storage/docs.

[37] Amazon Web Services. ”Amazon Elastic File System Documentation”. Hämtad: 2025-10-13. (2025), URL: https://docs.aws.amazon.com/efs/.

[38] Microsoft Corporation. ”Azure Files Documentation”. Hämtad: 2025-10-13. (2025), URL: https://learn.microsoft.com/en-us/azure/storage/files/.

[39] Google LLC. ”Filestore Documentation”. Hämtad: 2025-10-13. (2025), URL: https://cloud.google.com/filestore/docs.

[40] Amazon Web Services. ”Amazon Relational Database Service (Amazon RDS)”. Hämtad: 2025-10-13. (2025), URL: https://aws.amazon.com/rds/.

[41] Microsoft Corporation. ”Azure SQL Database”. Hämtad: 2025-10-13. (2025), URL: https://azure.microsoft.com/en-us/services/sql-database/.

[42] Google LLC. ”Cloud SQL”. Hämtad: 2025-10-13. (2025), URL: https://cloud.google.com/sql.

[43] Amazon Web Services. ”Amazon DynamoDB”. Hämtad: 2025-10-13. (2025), URL: https://aws.amazon.com/dynamodb/.

[44] Microsoft Corporation. ”Azure Cosmos DB”. Hämtad: 2025-10-13. (2025), URL: https://azure.microsoft.com/en-us/services/cosmos-db/.

[45] Google LLC. ”Cloud Firestore”. Hämtad: 2025-10-13. (2025), URL: https://cloud.google.com/firestore.

[46] Amazon Web Services. ”AWS Secrets Manager”. Hämtad: 2025-10-14. (2025), URL: https://aws.amazon.com/secrets-manager/.

[47] Microsoft Corporation. ”Azure Key Vault”. Hämtad: 2025-10-14. (2025), URL: https://azure.microsoft.com/en-us/products/key-vault/.

[48] Google LLC. ”Google Secret Manager”. Hämtad: 2025-10-14. (2025), URL: https://cloud.google.com/secret-manager.

[49] Amazon Web Services. ”Amazon Virtual Private Cloud (VPC) Documentation”. Hämtad: 2025-10-14. (2025), URL: https://docs.aws.amazon.com/vpc/latest/userguide/.

[50] Microsoft Corporation. ”Azure Virtual Network”. Hämtad: 2025-10-14. (2025), URL: https://azure.microsoft.com/en-us/products/virtual-network/.

[51] Google LLC. ”Google Cloud Virtual Private Cloud (VPC) Documentation”. Hämtad: 2025-10-14. (2025), URL: https://cloud.google.com/vpc/docs.

[52] Amazon Web Services. ”AWS Transit Gateway”. Hämtad: 2025-10-14. (2025), URL: https://aws.amazon.com/transit-gateway/.

[53] Microsoft Corporation. ”Azure Virtual WAN”. Hämtad: 2025-10-14. (2025), URL: https://azure.microsoft.com/en-us/products/virtual-wan/.

[54] Google LLC. ”Google Cloud Router”. Hämtad: 2025-10-14. (2025), URL: https://cloud.google.com/network-connectivity/docs/router.

[55] Amazon Web Services. ”AWS Site-to-Site VPN”. Hämtad: 2025-10-14. (2025), URL: https://aws.amazon.com/vpn/.

[56] Microsoft Corporation. ”Azure VPN Gateway”. Hämtad: 2025-10-14. (2025), URL: https://azure.microsoft.com/en-us/products/vpn-gateway/.

[57] Google LLC. ”Google Cloud VPN”. Hämtad: 2025-10-14. (2025), URL: https://cloud.google.com/network-connectivity/docs/vpn.

[58] Amazon Web Services. ”AWS Elastic Load Balancing Documentation”. Hämtad: 2025-10-14. (2025), URL: https://docs.aws.amazon.com/elasticloadbalancing/latest/userguide/.

[59] Microsoft Corporation. ”Azure Load Balancer Overview”. Hämtad: 2025-10-14. (2025), URL: https://learn.microsoft.com/en-us/azure/load-balancer/load-balancer-overview.

[60] Google LLC. ”Google Cloud Load Balancing Documentation”. Hämtad: 2025-10-14. (2025), URL: https://cloud.google.com/load-balancing/docs.

[61] Amazon Web Services. ”Amazon Route 53 – DNS Service”. Hämtad: 2025-10-14. (2025), URL: https://aws.amazon.com/route53/.

[62] Microsoft Corporation. ”Azure DNS”. Hämtad: 2025-10-14. (2025), URL: https://azure.microsoft.com/en-us/products/dns/.

[63] Google LLC. ”Google Cloud DNS Documentation”. Hämtad: 2025-10-14. (2025), URL: https://cloud.google.com/dns/docs.

[64] Amazon Web Services. ”AWS Network Firewall”. Hämtad: 2025-10-14. (2025), URL: https://aws.amazon.com/network-firewall/.

[65] Microsoft Corporation. ”Azure Firewall”. Hämtad: 2025-10-14. (2025), URL: https://azure.microsoft.com/en-us/products/azure-firewall/.

[66] Google LLC. ”Google Cloud Firewall Rules”. Hämtad: 2025-10-14. (2025), URL: https://cloud.google.com/vpc/docs/firewalls.

[67] Amazon Web Services. ”AWS WAF – Web Application Firewall”. Hämtad: 2025-10-14. (2025), URL: https://aws.amazon.com/waf/.

[68] Microsoft Corporation. ”Azure Web Application Firewall (WAF)”. Hämtad: 2025-10-14. (2025), URL: https://learn.microsoft.com/en-us/azure/web-application-firewall/.

[69] Google LLC. ”Google Cloud Armor – Web Application Firewall (WAF)”. Hämtad: 2025-10-14. (2025), URL: https://cloud.google.com/armor.

[70] Amazon Web Services. ”AWS Identity and Access Management (IAM)”. Hämtad: 2025-10-14. (2025), URL: https://aws.amazon.com/iam/.

[71] Microsoft Corporation. ”Microsoft Entra ID (Azure Active Directory)”. Hämtad: 2025-10-14. (2025), URL: https://learn.microsoft.com/en-us/entra/identity/.

[72] Google LLC. ”Google Cloud Identity and Access Management (IAM)”. Hämtad: 2025-10-14. (2025), URL: https://cloud.google.com/iam.

[73] Amazon Web Services. ”AWS Organizations”. Hämtad: 2025-10-14. (2025), URL: https://aws.amazon.com/organizations/.

[74] Microsoft Corporation. ”Azure Management Groups”. Hämtad: 2025-10-14. (2025), URL: https://learn.microsoft.com/en-us/azure/governance/management-groups/.

[75] Google LLC. ”Google Cloud Resource Hierarchy – Organizations and Folders”. Hämtad: 2025-10-14. (2025), URL: https://cloud.google.com/resource-manager/docs/cloud-platform-resource-hierarchy.

[76] Amazon Web Services. ”Amazon CloudWatch”. Hämtad: 2025-10-14. (2025), URL: https://aws.amazon.com/cloudwatch/.

[77] Microsoft Corporation. ”Azure Monitor”. Hämtad: 2025-10-14. (2025), URL: https://azure.microsoft.com/en-us/products/monitor/.

[78] Google LLC. ”Google Cloud Monitoring”. Hämtad: 2025-10-14. (2025), URL: https://cloud.google.com/monitoring.

[79] Amazon Web Services. ”Amazon CloudWatch Logging”. Hämtad: 2025-10-14. (2025), URL: https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/WhatIsCloudWatchLogs.html.

[80] Microsoft Corporation. ”Azure Monitor Logs”. Hämtad: 2025-10-14. (2025), URL: https://learn.microsoft.com/en-us/azure/azure-monitor/logs/data-platform-logs.

[81] Google LLC. ”Google Cloud Logging”. Hämtad: 2025-10-14. (2025), URL: https://cloud.google.com/logging.

[82] Wiz. ”Cloud Security Tools”. Hämtad: 2025-11-17. (2023), URL: https://www.wiz.io/academy/cloud-security-tools.

[83] Microsoft Azure, *Benefits of Cloud Migration*, Hämtad: 2025-03-03. URL: https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/benefits-of-cloud-migration.

[84] Google Cloud, *Advantages of Cloud Computing*, Hämtad: 2025-03-03. URL: https://cloud.google.com/learn/advantages-of-cloud-computing.

[85] S. J. TP, ”Advantages and Security Challenges of Cloud Computing–Overview”, *International Journal of Computer Science and Mobile Computing*, årg. 9, nr 12, s. 76–85, 2020-12. URL: https://ijcsmc.com/docs/papers/December2020/V9I12202018.pdf.

[86] H. Karlzén, ”Molnet – möjligheter och begränsningar”, FOI, Totalförsvarets Forskningsinstitut (Swedish Defence Research Agency), Stockholm, Sweden, tekn. rapport FOI-R–3381–SE, 2012-02, s. 19.

[87] D. Eidenskog och M. Karresand, ”Risker med virtualisering av IT-system”, Totalförsvarets forskningsinstitut (FOI), Stockholm, Sweden, tekn. rapport FOI-R–4448–SE, 2017-07.

[88] A. G. Hunstad och M. Karresand, ”Molntjänster inom industriella informations- och styrsystem”, FOI, Totalförsvarets forskningsinstitut, Stockholm, Sweden, tekn. rapport FOI-R–4597–SE, 2018-06, Kategoriindelning och säkerhetsutmaningar för molntjänster inom industriella system.

[89] R. Johansson, ”Avskanning av forskningsfronten inom combat cloud”, FOI, Totalförsvarets forskningsinstitut, Stockholm, Sweden, tekn. rapport FOI Memo 8142, 2023-02, Genomgång av forskningsläget för molnteknik inom försvarstillämpningar.

[90] M. Chauhan och S. Shiaeles, ”An analysis of cloud security frameworks, problems and proposed solutions”, *Network*, årg. 3, nr 3, s. 422–450, 2023.

[91] C. Di Giulio, R. Sprabery, C. Kamhoua, K. Kwiat, R. H. Campbell och M. N. Bashir, ”Cloud standards in comparison: Are new security frameworks improving cloud security?”, i *2017 IEEE 10th International Conference on Cloud Computing (CLOUD)*, IEEE, 2017, s. 50–57.

[92] Cloud Security Alliance. ”Cloud Controls Matrix”. Hämtad: 2025-10-28. (2024), URL: https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v4.

[93] Amazon Web Services. ”Security Pillar – AWS Well-Architected Framework”. Hämtad: 2025-10-28. (2024), URL: https://docs.aws.amazon.com/wellarchitected/latest/security-pillar/welcome.html.

[94] Microsoft Corperation. ”Security Pillar – Azure Well-Architected Framework”. Hämtad: 2025-10-28. (2025), URL: https://learn.microsoft.com/en-us/azure/well-architected/security/.

[95] Google Cloud. ”Security, Privacy, and Compliance Pillar – Google Cloud Well-Architected Framework”. Hämtad: 2025-10-28. (2025), URL: https://docs.cloud.google.com/architecture/framework/security.

[96] International Organization for Standardization. ”ISO/IEC 27017:2015 – Code of Practice for Information Security Controls for Cloud Services”. Hämtad: 2025-10-28. (2015), URL: https://www.iso.org/standard/43757.html.

[97] F. Liu, J. Tong, J. Mao, R. Bohn, J. Messina, L. Badger och D. Leaf, ”NIST Cloud Computing Reference Architecture”, 2011, Hämtad: 2025-10-28. DOI: 10.6028/NIST.SP.500-292.

[98] T. Grance och W. Jansen, ”Guidelines on Security and Privacy in Public Cloud Computing”, 2011, Hämtad: 2025-10-28. DOI: 10.6028/NIST.SP.800-144.

[99] Cloud Security Alliance. ”Security Guidance for Critical Areas of Focus in Cloud Computing”. Hämtad: 2025-10-28. (2025), URL: https://cloudsecurityalliance.org/research/guidance.

[100] Cloud Security Alliance. ”Security, Trust & Assurance Registry (STAR)”. Hämtad: 2025-10-28. (2025), URL: https://cloudsecurityalliance.org/star.

[101] Center for Internet Security. ”Foundational Cloud Security with CIS Benchmarks”. Hämtad: 2025-10-28. (2025), URL: https://www.cisecurity.org/insights/blog/foundational-cloud-security-with-cis-benchmarks.

[102] Center for Internet Security. ”Cloud Companion Guide for CIS Controls v8.1”. Hämtad: 2025-10-28. (2024), URL: https://www.cisecurity.org/insights/white-papers/cis-controls-v8-1-cloud-companion-guide.

[103] European Union Agency for Cybersecurity. ”Cloud Security Guide for SMEs”. Hämtad: 2025-10-28. (2015), URL: https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes.

[104] U.S. General Services Administration. ”FedRAMP Cloud Security Publication”. Hämtad: 2025-10-28. (2025), URL: https://www.fedramp.gov.

[105] PrimeHarbor Technologies, LLC. ”Breaches.Cloud: Public Cloud Security Breaches”. Hämtad: 2025-11-20. (2025), URL: https://www.breaches.cloud/.

[106] Cloud Security Alliance. ”Top Threats to Cloud Computing”. Hämtad: 2025-11-20. (2025), URL: https://cloudsecurityalliance.org/research/topics/top-threats.

[107] Arcserve. ”7 Most Infamous Cloud Security Breaches”. Hämtad: 2025-11-20. (2023-12), URL: https://www.arcserve.com/blog/7-most-infamous-cloud-security-breaches.

[108] ramimac. ”aws-customer-security-incidents: Catalog of AWS customer security breaches”. Hämtad: 2025-11-20. (2025), URL: https://github.com/ramimac/aws-customer-security-incidents.

[109] nagwww. ”s3-leaks: List of AWS S3 Leaks”. Hämtad: 2025-11-20. (2025), URL: https://github.com/nagwww/s3-leaks.

[110] Cloud Computing News (TechForge Media). ”Cloud Computing News: Latest Cloud Computing News & Insights”. Hämtad: 2025-11-20. (2025), URL: https://www.cloudcomputing-news.net/.

[111] Wiz Research. ”Cloud Threat Landscape – Incidents”. Hämtad: 2025-11-20. (2025), URL: https://threats.wiz.io/all-incidents.

[112] Amazon Web Services, Inc. ”Amazon Simple Email Service (Amazon SES)”. Hämtad: 2025-11-03. (2025), URL: https://aws.amazon.com/ses/.

[113] Amazon Web Services. ”AWS CloudFormation User Guide”. Hämtad: 2025-10-13. (2025), URL: https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/.

[114] Microsoft Corporation. ”What is Azure Resource Manager?” Hämtad: 2025-10-13. (2025), URL: https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/overview.

[115] Google Cloud. ”Infrastructure Manager Documentation”. Hämtad: 2025-11-20. (2025), URL: https://docs.cloud.google.com/infrastructure-manager/docs.

[116] HashiCorp, Inc. ”Terraform by HashiCorp”. Hämtad: 2025-10-13. (2025), URL: https://www.terraform.io/.

A Samling molnincidenter

Tabell A.1: Insamlade molnincidenter

ID	År	Organisation	Referens
1	2025	Grafana Labs	https://threats.wiz.io/all-incidents/grafana-github-action-attempted-supply-chain-attack
2	2025	Office of the comptroller of the currency	https://threats.wiz.io/all-incidents/long-term-email-breach-at-occ-exposes-sensitive-bank-oversight-data
3	2025	Europcar	https://threats.wiz.io/all-incidents/europecar-gitlab-breach
4	2025	U.S. Centers for Disease Control and Prevention	https://threats.wiz.io/all-incidents/cdc-dangling-domain-hijack
5	2025	Zapier	https://threats.wiz.io/all-incidents/zapier-data-breach
6	2025	SAFE Wallet	https://threats.wiz.io/all-incidents/bybit-hack
7	2025	U.S. Agency for International Development	https://threats.wiz.io/all-incidents/usaid-cryptojacking-incident
8	2025	Mastercard	https://threats.wiz.io/all-incidents/mastercard-fixes-five-year-old-dns-typo-misconfiguration
9	2025	Unacast	https://threats.wiz.io/all-incidents/gravy-analytics-data-breach
10	2025	AngelOne	https://www.securityweek.com/indian-stock-broker-angel-one-discloses-data-breach
11	2025	Pearson	https://www.bleepingcomputer.com/news/security/education-giant-pearson-hit-by-cyberattack-exposing-customer-data/
12	2025	KiranaPro	https://techcrunch.com/2025/06/03/indian-grocery-startup-kiranapro-was-hacked-and-its-servers-deleted-ceo-confirms/
13	2024	Ticketmaster (Snowflake)	https://www.breaches.cloud/incidents/snowflake/
14	2024	Spoutible	Top threats 2024
15	2024	Trello	Top threats 2024
16	2024	Mercedes Benz	Top threats 2024
17	2024	Tangerine	Top threats 2024
18	2024	Tunefab converter	Top threats 2024

ID	År	Organisation	Referens
19	2024	Football Australia	https://cloudsecurityalliance.org/blog/2025/06/09/the-2024-football-australia-data-breach-a-case-of-misconfiguration-and-inadequate-change-control
20	2024	Otelier	https://threats.wiz.io/all-incidents/otelier-data-breach
21	2024	U.S. Department of the Treasury	https://threats.wiz.io/all-incidents/us-treasury-breach-via-beyondtrust-supply-chain-attack
22	2024	Volkswagen	https://threats.wiz.io/all-incidents/volkswagen-data-leak-through-spring-boot-actuator-misconfiguration
23	2024	ZAGG Inc	https://threats.wiz.io/all-incidents/zagg-customer-data-compromised-via-hijacked-freshclicks-bigcommerce-app
24	2024	Byte Federal	https://threats.wiz.io/all-incidents/byte-federal-data-breach-via-gitlab-vulnerability
25	2024	Ultralytics	https://threats.wiz.io/all-incidents/ultralytics-compromise
26	2024	Game Freak	https://threats.wiz.io/all-incidents/game-freak-data-leak
27	2024	Rackspace	https://threats.wiz.io/all-incidents/rackspace-incident-2024
28	2024	Fortinet	https://threats.wiz.io/all-incidents/fortinet-sharepoint-data-leak
29	2024	BORN Group	https://threats.wiz.io/all-incidents/born-group-supply-chain-attack
30	2024	Disney Slack	https://threats.wiz.io/all-incidents/disney-slack-breach
31	2024	NCS	https://threats.wiz.io/all-incidents/ncs-mass-server-deletion
32	2024	New York Times	https://threats.wiz.io/all-incidents/nyt-source-code-theft
33	2024	Disney Confluence	https://threats.wiz.io/all-incidents/club-penguin-data-theft-via-confluence
34	2024	MITRE	https://threats.wiz.io/all-incidents/mitre-breach-via-ivanti-connect-secure
35	2024	Sisense	https://threats.wiz.io/all-incidents/sisense-breach

ID	År	Organisation	Referens
36	2024	Microsoft	https://threats.wiz.io/all-incidents/microsoft-exposed-storage-with-credentials
37	2024	Hugging Face	https://threats.wiz.io/all-incidents/hugging-face-cross-tenant-access
38	2024	Fujitsu	https://www.thestack.technology/fujitsu-breach-cloud-buckets/
39	2024	Meson Network	https://threats.wiz.io/all-incidents/meson-network-cryptojacking-campaign
40	2024	Cutout.Pro	https://threats.wiz.io/all-incidents/cutoutpro-breach
41	2024	DemandScience	https://threats.wiz.io/all-incidents/pure-incubation-demandscience-breach
42	2024	WinStar	https://threats.wiz.io/all-incidents/winstar-exposed-app-database
43	2024	BMW	https://threats.wiz.io/all-incidents/bmw-exposed-cloud-storage
44	2024	Government Accountability Office	https://threats.wiz.io/all-incidents/cgi-federal-incident
45	2024	Zenlayer	https://threats.wiz.io/all-incidents/zenlayer-exposed-database
46	2024	Wurk	https://threats.wiz.io/all-incidents/wrk-exposed-database
47	2024	Juniper Networks	https://threats.wiz.io/all-incidents/juniper-support-portal-exposure
48	2024	Almerys/Viamedis	https://threats.wiz.io/all-incidents/almerys-incident
49	2024	pcTattletale	https://techcrunch.com/2024/05/25/spyware-app-pctattletale-was-hacked-and-its-website-defaced/
50	2024	BeyondTrust	https://www.beyondtrust.com/remote-support-saas-service-security-investigation
51	2024	TinaCloud	https://tina.io/blog/2024-12-tinacloud-public-disclosure-security-breach
52	2023	Toyota	Top threats 2024
53	2023	Darkbeam	Top threats 2024
54	2023	Microsoft AI	Top threats 2024
55	2023	World baseball softball confederation	Top threats 2024
56	2023	CaptainU	Top threats 2024
57	2023	Veritone AI	Top threats 2024

ID	År	Organisation	Referens
58	2023	OpenAI	Top threats 2024
59	2023	23 and Me	Top threats 2024
60	2023	KidSecurity	Top threats 2024
61	2023	Indias National Logistics Portal-Marine	Top threats 2024
62	2023	Sumo Logic	https://www.breaches.cloud/incidents/sumologic2023/
63	2023	CommuteAir	https://www.breaches.cloud/incidents/commuteair/
64	2023	Cisco WebEx	https://www.breaches.cloud/incidents/cisco-2020/
65	2023	JumpCloud	Top threats 2024
66	2023	Okta	Top threats 2024
67	2023	Fortra	Top threats 2024
68	2023	New Relic	https://threats.wiz.io/all-incidents/new-relic-incident-november-2023
69	2023	Microsoft	https://threats.wiz.io/all-incidents/microsoft-email-exfiltration-by-nobelium
70	2023	Ly corp	https://threats.wiz.io/all-incidents/line-and-naver-cloud-incident
71	2023	Rollbar	https://threats.wiz.io/all-incidents/rollbar-hack
72	2023	Retool	https://threats.wiz.io/all-incidents/retool-hack
73	2023	Fatal Model	https://threats.wiz.io/all-incidents/fatal-model-exposed-database
74	2023	DepositFiles	https://threats.wiz.io/all-incidents/depositfiles-exposed-config-file
75	2023	Cloudflare	https://web.archive.org/web/20240201200520/https://blog.cloudflare.com/thanksgiving-2023-security-incident/
76	2023	Pegasus Airlines	https://medium.com/@syednashetali/pegasus-airlines-leaked-6-5tb-of-data-in-aws-s3-bucket-mess-up-5db20d96517e
77	2022	npm	https://github.blog/2022-05-26-npm-security-update-oauth-tokens/
78	2022	PREMINT	https://www.chaincatcher.com/en/article/2076680
79	2022	Uber	https://www.halock.com/uber-is-taken-for-a-ride-by-a-hacker-again/

ID	År	Organisation	Referens
80	2022	Lastpass	https://support.lastpass.com/help/incident-2-additional-details-of-the-attack
81	2022	Medibank	https://www.bleepingcomputer.com/news/security/amazon-redshift-gets-new-default-settings-to-prevent-data-breaches/
82	2022	Sonder	https://dojmt.gov/wp-content/uploads/Consumer-Notification-Letter-816.pdf
83	2022	Teqtivity	https://www.teqtivity.com/breach-notification-statement
84	2022	Colombia airport	https://www.darkreading.com/application-security/cloud-misconfig-exposes-3tb-sensitive-airport-data-amazon-s3-bucket
85	2022	McGraw Hill	https://www.theregister.com/2022/12/20/mcgraw_hills_s3_buckets_exposed/
86	2021	Accenture	https://www.techtarget.com/searchsecurity/news/252508243/Accenture-sheds-more-light-on-August-data-breach
87	2021	LinkedIn	https://fortune.com/2021/06/30/linkedin-data-theft-700-million-users-personal-information-cybersecurity/
88	2021	Cognyte	https://www.hackread.com/cybersecurity-firm-expose-data-breach-records/
89	2021	Juspay	https://web.archive.org/web/20210127001214/https://threatpost.com/data-from-august-breach-of-amazon-partner-juspay-dumped-online/162740/
90	2021	20/20 Eye/Hearing Care network	https://www.databreaches.net/20-20-eye-care-network-and-hearing-care-network-notify-3253822-health-plan-members-of-breach-that-deleted-contents-of-aws-buckets/
91	2021	Sendtech	https://web.archive.org/web/20220923025502/https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Commissions-Decisions/Decision---Sendtech-Pte-Ltd---220721.ashx?la=en

ID	År	Organisation	Referens
92	2021	LogicGate	https://web.archive.org/web/20210519233848/https://techcrunch.com/2021/04/13/logicgate-risk-cloud-data-breach/
93	2021	Ubiquiti	https://web.archive.org/web/20210731152054/https://krebsonsecurity.com/2021/04/ubiquiti-all-but-confirms-breach-response-iniquity/
94	2021	Uran Company	https://web.archive.org/web/20221205145546/https://topdigital.agency/clear-and-uncommon-story-about-overcoming-issues-with-aws/
95	2021	reddoorz	https://web.archive.org/web/20211130202805/https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Commissions-Decisions/Decision---Commeasure-Pte-Ltd---15092021.pdf?la=en
96	2021	HPE Aruba	https://www.arubanetworks.com/support-services/security-bulletins/central-incident-faq/
97	2021	Kaspersky	https://www.bleepingcomputer.com/news/security/kasperskys-stolen-amazon-ses-token-used-in-office-365-phishing/
98	2021	Eye Care Leaders	https://dojmt.gov/wp-content/uploads/Augusta-University-Medical-Center-Consumer-Notification-Letter.pdf
99	2021	Onus	https://cystack.net/research/the-attack-on-onus-a-real-life-case-of-the-log4shell-vulnerability
100	2021	Flexbooker	https://therecord.media/booking-management-platform-flexbooker-leaks-3-7-million-user-records/
101	2020	Sina Weibo	https://www.zdnet.com/article/hacker-selling-data-of-538-million-weibo-users/
102	2020	First republic	https://www.breaches.cloud/incidents/first-republic/
103	2020	Ubiquiti	https://www.breaches.cloud/incidents/ubiquiti/
104	2020	Drizly	https://www.breaches.cloud/incidents/drizly/
105	2020	Cameo	https://www.vice.com/en/article/akwj5z/cameo-app-exposed-private-videos-user-data-passwords

ID	År	Organisation	Referens
106	2020	Open Exchange Rates	https://nakedsecurity.sophos.com/2020/03/20/exchange-rate-services-customer-details-hacked-via-aws/
107	2020	Live Auctioneers	https://www.atg.wa.gov/live-auctioneers/
108	2020	Twilio	https://web.archive.org/web/20210813010417/https://www.twilio.com/blog/incident-report-taskrouter-js-sdk-july-2020
109	2020	Natures Basket	https://web.archive.org/web/20200825004529/https://medium.com/@gchib/naturesbasket-aws-root-account-takeover-e4aa5c5e95e1
110	2020	Animal Jam	https://web.archive.org/web/20210122070047/https://www.theregister.com/2020/11/12/animal_jam_breached/
111	2020	SeniorAdvisor	https://www.hackread.com/s3-bucket-exposed-senior-us-canada-citizens-data//
112	2020	UK Consulting firms	https://www.computerweekly.com/news/252476870/Exposed-AWS-buckets-again-implicated-in-multiple-data-leaks
113	2020	Common Services Centres e-Governance Services India Limited	https://social.cyware.com/news/data-breach-in-an-indian-e-governance-website-leaks-data-of-726-million-users-54a99a3d
114	2019	Capital One	https://cloudsecurityalliance.org/blog/2019/08/09/a-technical-analysis-of-the-capital-one-cloud-misconfiguration-breach
115	2019	Alibaba	https://www.wsj.com/articles/alibaba-falls-victim-to-chinese-web-crawler-in-large-data-leak-11623774850
116	2019	Facebook	https://about.fb.com/news/2021/04/facts-on-news-reports-about-facebook-data/
117	2019	Vitagene	https://www.breaches.cloud/incidents/vitagene/
118	2019	Voova	https://nakedsecurity.sophos.com/2019/03/22/sacked-it-guy-annihilates-23-of-his-ex-employers-aws-servers/

ID	År	Organisation	Referens
119	2019	JW Player	https://web.archive.org/web/20210828044334/https://medium.com/jw-player-engineering/how-a-cryptocurrency-miner-made-its-way-onto-our-internal-kubernetes-clusters-9b09c4704205
120	2019	Malindo Air	https://www.infosecurity-magazine.com/news/malindo-air-data-breach-was-inside/
121	2019	Attunity	https://www.zdnet.com/article/aws-s3-server-leaks-data-from-fortune-100-companies-ford-netflix-td-bank/
122	2018	Tesla	https://www.cnbc.com/2018/02/21/hackers-hijack-teslas-cloud-system-to-mine-cryptocurrency-redlock.html
123	2018	Chegg	https://www.breaches.cloud/incidents/chegg/
124	2018	LA Times	https://www.breaches.cloud/incidents/latimes/
125	2018	Imperva	https://www.breaches.cloud/incidents/imperva-rds-snapshot/
126	2018	Drizly	https://www.ftc.gov/news-events/news/press-releases/2022/10/ftc-takes-action-against-drizly-its-ceo-james-cory-rellas-security-failures-exposed-data-25-million
127	2018	imToken	https://archive.ph/bRjXi
128	2018	MedCall Healthcare Advisor	https://www.healthcareitnews.com/news/update-misconfigured-database-breaches-thousands-medcall-advisors-patient-files
129	2018	Limoges Jewelry	https://thenextweb.com/security/2018/03/14/jewelry-site-accidentally-leaks-personal-details-plaintext-passwords-1-3m-users/
130	2018	Octoly	https://www.upguard.com/breaches/cloud-leak-octoly
131	2017	Accenture	http://www.zdnet.com/article/accenture-left-a-huge-trove-of-client-passwords-on-exposed-servers/
132	2017	OneLogin	https://web.archive.org/web/20210620180614/https://www.onelogin.com/blog/may-31-2017-security-incident

ID	År	Organisation	Referens
133	2017	Politifact	https://web.archive.org/web/20200806102838/https://www.washingtonpost.com/news/the-switch/wp/2017/10/13/hackers-have-turned-politifacts-website-into-a-trap-for-your-pc/
134	2017	Dataspline	https://www.linkedin.com/feed/update/urn:li:activity:7219713829528563712
135	2017	DXC	https://web.archive.org/web/20210228215919/https://www.theregister.com/2017/11/14/dxc_github_aws_keys_leaked/
136	2017	Alteryx	http://www.zdnet.com/article/alteryx-s3-leak-leaves-120m-american-households-exposed/
137	2017	National Credit Federation	https://www.upguard.com/breaches/credit-crunch-national-credit-federation
138	2017	NSA	http://www.zdnet.com/article/nsa-leak-inscom-exposes-red-disk-intelligence-system/
139	2017	AMP	https://www.theguardian.com/technology/2017/nov/02/amp-among-companies-affected-by-data-breach-of-50000-staff-records
140	2017	Viacom	https://www.theregister.co.uk/2017/09/19/viacom_exposure_in_aws3_bucket_blunder/
141	2017	TalentPen	https://www.theregister.com/2017/09/04/us_security_clearance_aws_breach
142	2017	Time Warner Cable	http://gizmodo.com/millions-of-time-warner-customer-records-exposed-in-thi-1798701579
143	2017	Creditseva	http://www.informationsecuritybuz.com/expert-comments/indian-creditseva-data-breach/
144	2017	Groupize	https://www.theregister.com/2017/08/22/open_aws_s3_bucket_leaked_hotel_booking_service_data_says_kromtech/
145	2017	Dow Jones Index	https://www.theregister.co.uk/2017/07/18/dow_jones_index_of_customers_not_prices_leaks_from_aws_repo/

ID	År	Organisation	Referens
146	2017	WWE	https://www.forbes.com/sites/thomasbrewster/2017/07/06/massive-wwe-leak-exposes-3-million-wrestling-fans-addresses-ethnicities-and-more/ #5a0bf96275dd
147	2017	Verizon	https://thehackernews.com/2017/07/over-14-million-verizon-customers-data.html
148	2017	Deep Root Analytics	https://auth0.com/blog/massive-data-leak-exposes-198-million-us-voters/
149	2017	US Government	http://gizmodo.com/top-defense-contractor-left-sensitive-pentagon-files-on-1795669632
150	2017	US National Geospatial-Intelligence Agency	https://www.theregister.co.uk/2017/06/01/us_national_geospatial_intelligence_agency_leak/
151	2017	Alliance Direct Lending Corperation	https://threatpost.com/auto-lender-exposes-loan-data-for-up-to-1-million-applicants/125216/
152	2017	CloudPets	https://threatpost.com/childrens-voice-messages-leaked-in-cloudpets-database-breach/123956/
153	2017	Paytm	https://tutorgeeks.blogspot.com/2017/04/aws-s3-bucket-misconfiguration.html
154	2016	Uber	https://www.breaches.cloud/incidents/uber/
155	2016	Democratic National Commitee	https://www.politico.com/f/?id=00000168-6161-de11-af7d-ef7327ea0000
156	2016	DataDog	https://web.archive.org/web/20201128071102/https://www.datadoghq.com/blog/2016-07-08-security-notice/
157	2016	Lynda	http://archive.today/oU2ZL

FOI
Totalförsvarets forskningsinstitut
164 90 Stockholm

Tel: 08-55 50 30 00
Fax: 08-55 50 31 00

www.foi.se