Transport- och kommunikationsverket
Cybersäkerhetscentret

Anvisning – Incidenthantering i molnmiljöer

Traficoms publikationer
18/2023

Innehåll

Sammanfattning

Användning av molntjänster är i många organisationer en del av den normala verksamheten. Molntjänster utnyttjas i processer som är viktiga och till och med kritiska för affärsverksamheten. Att dessa molntjänster fungerar pålitligt och på ett informationssäkert sätt är i många organisationer en förutsättning för den dagliga affärsverksamheten och för att den ska fortgå på ett smidigt sätt.

Upprätthållande av informationssäkerheten kräver dock kontinuerligt arbete och utveckling av verksamheten. I denna anvisning berättas om hur organisationer kan förbereda sig för informationssäkerhetsincidenter i molntjänster och för hur de ska agera i situationer där man misstänker att en informationssäkerhetsincident har inträffat i en molnmiljö.

I synnerhet följande är viktiga faktorer:

1. Informationssäkerhet vid anskaffning av tjänster

Om ni har för avsikt att skaffa nya molntjänster, se till att tillräcklig uppmärksamhet ägnas åt tjänstens informationssäkerhet redan i anskaffningsskedet. Vid användning av molntjänster är det möjligt att på ett enklare och ofta förmånligare sätt skapa lösningar med bättre informationssäkerhet än i en datorhall. Detta förutsätter att även kunderna har tillräcklig kompetens.

2. Modell med delat ansvar i olika typer av tjänster

I synnerhet i molntjänster av IaaS- och PaaS-modell är det den organisation som använder tjänsten som bär en stor del av ansvaret för informationssäkerheten i den. Beträffande underhållet av dessa tjänster är det mycket viktigt att säkerställa att de resurser för underhåll som finns tillgängliga för organisationen är tillräckliga och att de har tillräcklig kompetens i informationssäkerhet. Vad gäller informationssäkerhet i molntjänster krävs särskilt specialkompetens i dessa tjänster. Många informationssäkerhetsincidenter startar från en felaktigt konfigurerad tjänst eller från en ändring som försämrar konfigurationens informationssäkerhet. Möjligheten för fel minskar när det säkerställs att de personer som ansvarar för konfigurationerna har tillräckliga kunskaper i ämnet.

3. Flerfaktorsautentisering

Det är värt att satsa på att skydda molntjänster. En av de grundläggande sakerna är att det inte är möjligt att logga in i tjänsterna med enbart en kombination av ett användarnamn och ett lösenord. Se till att flerfaktorsautentisering är i bruk i alla era molntjänster, för alla användargrupper.

4. Övning av incidenter

Man bör förbereda sig för incidenter. Även om man har gjort stora satsningar på informationssäkerheten, är en incident alltid möjlig. Upprättande av planer för hantering av incidenter och övning av incidenter ger trygghet om en riktig incident någon gång inträffar.

5. Åtgärder för beredskap

Incidenter har i regel en viss livscykel, som omfattar olika steg. I denna anvisning beskrivs stegen och de viktigaste uppgifterna i varje steg. Säkerställ att ni i er organisation har tillräcklig förmåga att genomföra åtgärder för incidenthantering. Ofta kräver dessa åtgärder att man har gjort förberedelser, till exempel infört tillräcklig loggning och upprättat en process för säkerhetskopiering, vars funktion har kontrollerats genom testning.

6. Anlitande av experthjälp vid incidenter

Om det inträffar en informationssäkerhetsincident i en organisation är det möjligt att det behövs experthjälp för att utreda den. Det är skäl att för säkerhets skull avtala om sådan experthjälp redan i förväg.

1 Inledning

1.1 Syftet med anvisningen

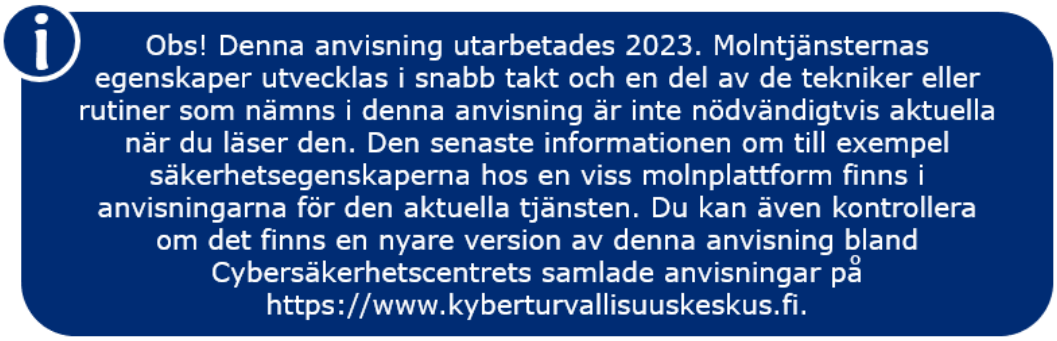
Syftet med denna anvisning, som har upprättats av Cybersäkerhetscentret vid Transport- och kommunikationsverket Traficom, är att ge organisationer råd för hur de kan förbereda sig för informationssäkerhetsincidenter i molntjänster och hur de ska agera i situationer där man misstänker en informationssäkerhetsincident i en molnmiljö. Anvisningen är avsedd för alla organisationer, oavsett storlek och bransch.

Denna anvisning beskriver följande steg i livscykeln för informationssäkerhetsincidenter:

- Observation av informationssäkerhetsincidenter – i anvisningen berättas om hur man kan upptäcka informationssäkerhetsincidenter i molnmiljöer.
- Agerande vid en incident – anvisningen omfattar de viktigaste åtgärderna som en organisation ska vidta vid en incident.
- Återställande efter en incident – i anvisningen beskrivs hur affärsverksamheten kan återställas efter en informationssäkerhetsincident i en molntjänst.

Anvisningen ingår i en serie anvisningar från Cybersäkerhetscentret som beskriver återhämtningen från olika typer av informationssäkerhetsincidenter. I de övriga delarna av serien berättas om återställande från andra incidenter än sådana som inträffar i molnmiljöer. Hela anvisningsserien finns på Cybersäkerhetscentrets webbplats.

I publikationen Ohjeita pilvipalvelujen turvallisuudesta yksityishenkilöille, pienyhteisöille ja -yrityksille (Anvisningar för säkerheten i molntjänster för privatpersoner, smågrupper och små företag) berättas allmänt om säkerheten i molntjänster[1]. Försörjningsberedskapscentralen har publicerat en handbok för beslutsfattare på företag som funderar på att införa molntjänster eller utvidga användningen av sådana till kritiska funktioner[2].



1.2 Vad betyder en informationssäkerhetsincident i en molnmiljö?

Informationssäkerhetsincidenter är oväntade eller icke-önskade händelser eller serier av händelser där säkerheten för data eller tjänster som ska skyddas äventyras. I denna anvisning definierar vi en informationssäkerhetsincident i en

[1] https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/ohjeita-pilvipalvelujen-turvallisuudesta-yksityishenkiloille-pienyhteisoille-ja
[2] https://www.huoltovarmuuskeskus.fi/files/dfd001d3135a6a37876a5afe88ba2a816156e8ae/huoltovarmuutta-pilvipalveluilla-230306.pdf

molnmiljö som en säkerhetsincident, där de data som äventyrats har lagrats i en molntjänst eller där den tjänst som är föremål för säkerhetshändelsen är en molntjänst.

Med molntjänster avses sådana IT-applikationer eller plattformstjänster som en kund använder, som produceras i en tjänsteleverantörs maskinvarumiljö, som används över ett telekommunikationsnät och vars tekniska detaljer till vissa delar ligger på tjänsteleverantörens ansvar och är dolda för kunden. Ur kundens synvinkel är molnresurserna alltid tillgängliga, de är enkla att anpassa efter varje behov och prissättningen baserar sig i allmänhet på användningen. Molntjänsterna förutsätter inte att kunden investerar i utrustning eller förbinder sig till en långvarig prenumeration.

I molnmiljöer förekommer olika slags informationssäkerhetsincidenter, vars typiska grundorsaker är:

- Svaga eller läckta användarnamn och lösenord, eller andra hemligheter, med hjälp av vilka en obehörig aktör kan få tillgång till data och tjänster som finns i molnet. Det finns en risk för detta i synnerhet när flerfaktorsautentisering (MFA) inte används eller när hemligheter såsom åtkomstnycklar (eng. access key) har hanterats ovarsamt, till exempel som en del av källkoden till ett program.
- Användning av standardkonfigurationer av molnmiljön som leder till att data, funktioner eller applikationer får mer synlighet i det offentliga nätet än det var tänkt.
- Uppluckrande av bra informationssäkerhetsinställningar som tidigare använts, varvid en oväntad möjlighet öppnar sig i tjänsterna för nätbrottslingar.
- En sårbarhet i kundens arbetsbörda, till exempel i en virtuell maskin eller en container.

Ovanstående situationer kan undvikas genom god kännedom om användningen av molnet, genom en fungerande konfigurations- och ändringshantering samt genom en aktiv uppföljning av sårbarheter i informationssäkerheten.

Europeiska byrån för nät- och informationssäkerhet Enisa[3] har bedömt att angripare riktar angrepp mot molnmiljöer bland annat på följande sätt:

- genom att utnyttja sårbarheter i molnmiljön
- genom att med hjälp av social hacking få tillgång till inloggningsuppgifter (eng. credentials) till molnmiljöer
- genom att utnyttja felaktigt konfigurerade containerdefinitioner
- genom att få fotfäste i molninfrastrukturen, gränssnitten eller säkerhetskopior i molnet.

1.3 Utmärkande egenskaper hos molnmiljöer ur incidenthanteringens perspektiv

Informationssäkerhetsincidenter i molnmiljöer har några utmärkande egenskaper. Det är bra för molntjänsternas kunder att beakta dessa egenskaper, så att de kan agera så effektivt som möjligt vid en incident.

[3] Enisas rapport på engelska: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

1.3.1 Insyn i tjänsteleverantörens processer

Användningen av en molntjänst är en utkontraktering, där kunden helt eller delvis överlåter utvecklingen och underhållet av den tjänst som köps till tjänsteleverantören. Det är bra att vara medveten om att beslutet om att ta i bruk molntjänsten samtidigt är ett beslut att lita på molnleverantören och informationssäkerhetsnivån i de tjänster som den tillhandahåller.

Molntjänster är förknippade med avtalsvillkor för ansvarsfördelningen som sätter gränser för insynen i tjänsteleverantörens processer eller för möjligheten till ett aktivt samarbete. Ur informationssäkerhetsperspektiv innebär detta att när kundorganisationen ska välja en molnleverantör, borde organisationen innan tjänsten skaffas noggrant studera tjänsteleverantörens dokumentation, där de processer och hanteringsmetoder för informationssäkerheten som används beskrivs, inklusive verksamhetsmodeller för informationssäkerhetsincidenter och vilken stödnivå som är tillgänglig vid en incident.

Det är bra att observera att vissa informationssäkerhetsegenskaper hos molntjänster kan vara produkter med tilläggsavgift vars ibruktagande kräver både investeringar och specialkunskaper.

1.3.2 Modell med delat ansvar

Molnleverantören och molntjänstens kund delar alltid på ansvaret för informationssäkerheten i tjänsten. Typen av molntjänst (SaaS, PaaS eller IaaS) och avtalet med tjänsteleverantören samt vilka tjänster som används bestämmer hur ansvaret är fördelat mellan parterna. Ansvarsfördelningen syns även vid incidenter:

Infrastructure-as-a-Service (IaaS): I IaaS-modellen tillhandahåller molnleverantören en skalbar IT-infrastruktur, där kunden tar i bruk valfria tjänster, till exempel virtuella maskiner, internetanslutningar och lagringskapacitet. I praktiken finns tjänsterna fysiskt i tjänsteleverantörens datacenter, och tjänsteleverantören ansvarar för utrustningens fysiska säkerhet. Kunden har ansvar för att säkerställa säkerheten för de tjänster den använder och de data som den lagrar, inklusive exempelvis definition av användare och behörigheter, konfiguration av molnresursernas informationssäkerhet, hantering av sårbarheter i containrar och operativsystem, upptäckt och avvärjning av angrepp, spegling av tjänsterna samt tillräcklig säkerhetskopiering. Vid en informationssäkerhetsincident har kunden i stor utsträckning ansvar för utredningen av incidenten och för de korrigerande åtgärderna om incidenten inte gäller prenumerations- och administrationssystem eller produktionens infrastruktur som ligger på tjänsteleverantörens ansvar.

Platform-as-a-Service (PaaS): I PaaS-modellen tillhandahåller molnleverantören en plattform för utveckling och publicering av applikationerna. Kunden tar i bruk valfria tjänster på plattformen, vilka vanligtvis inkluderar förutom utvecklingsverktyg och en plattform för körning av kod, även lagrings- och hanteringstjänster för filer och data. I PaaS-modellen ansvarar kunden för att säkerställa säkerheten för sin utvecklingsmiljö, sina applikationer och de data som lagras samt för att trygga åtkomsthanteringen i tjänsterna. Vid en informationssäkerhetsincident har kunden huvudansvaret för utredningen av incidenten, men molnleverantören kan fungera som samarbetspartner.

Software-as-a-Service (SaaS): I SaaS-modellen tillhandahåller molnleverantören sina kunder en färdig applikation, som i allmänhet används via det offentliga nätet, det vill säga med en internetuppkoppling. I SaaS-modellen ansvarar tjänsteleverantören för säkerheten i applikationens infrastruktur och den egentliga applikationen. Kunden ansvarar dock i viss mån för säkerheten vid användningen av applikationen, till exempel hanteringen av användare, behörigheter och identifieringsverktyg. Utredningen av en incident sker i samarbete med molnleverantören, eftersom kunden troligtvis inte har tillgång till applikationens loggdata och andra uppgifter som behövs i utredningen av incidenten. I SaaS-tjänster kan det finnas avgiftsbelagda tilläggsfunktioner för informationssäkerheten som hänför sig till exempelvis identifieringsverktyg, kryptering av information och tillgången till användningsloggar.

Molntjänsternas kunder bör alltid sätta sig in i ansvarsfördelningsmodellen för den tjänst som skaffas, så att missförstånd och otrevliga överraskningar i fråga om säkerheten och incidenthanteringen kan undvikas.

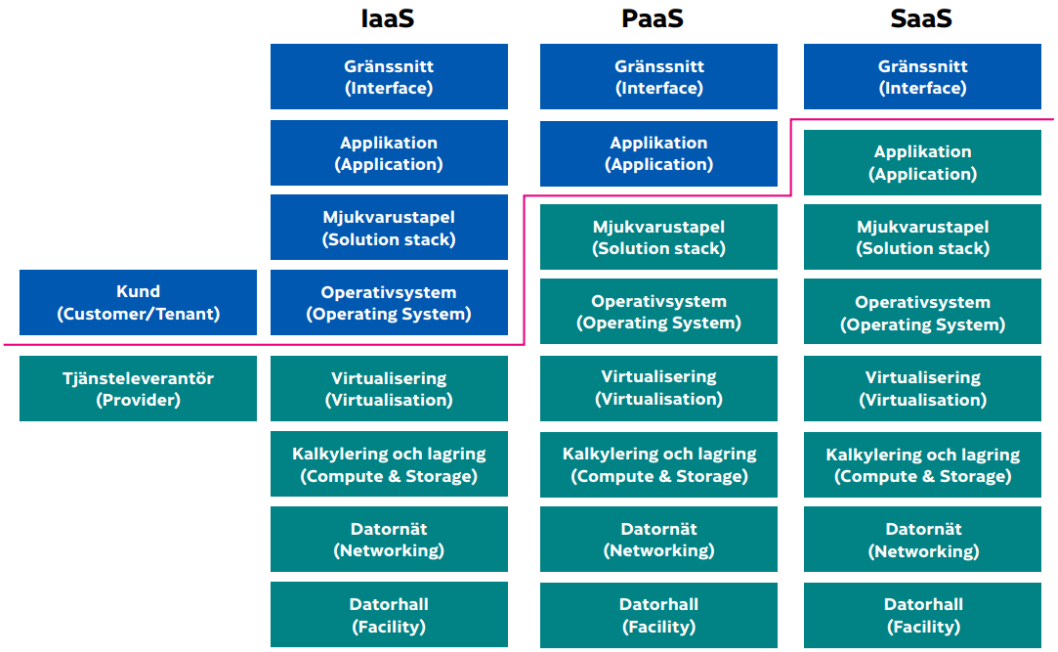


Bild 1. En typisk modell för ansvarsfördelning. Källa: Säkerhetskriterier för molntjänster (PiTuKri)

1.3.3 Behövlig specialkompetens för incidentutredning

Molnmiljöer kan vara komplicerade och innehålla mycket data. Dessutom kan de vara föremål för ständiga ändringar, vilket gör att utredningen av incidenter är en uppgift som kräver specialkompetens.

Leverantörer av molntjänster kan tillhandahålla tjänsteavtal på olika nivåer som påverkar hurdant stöd leverantörerna ger vid incidenter. På marknaden för experttjänster finns det dessutom specialiserade leverantörer som kan hjälpa till vid utredningen av och återställandet efter incidenter.

I många fall är det till nytta att organisationen i förväg ingår avtal med tjänsteleverantörer som skulle kunna hjälpa vid en incident. Det är värt att upprätta avtal i förväg, så att man när en incident pågår inte behöver använda tid till avtalsförhandlingar.

Organisationen ska även säkerställa att dess egen IT-personal har tillräckliga kunskaper och färdigheter i molntjänster och hur sådana används på ett säkert sätt. Kunskaperna om molntjänster kan utvecklas genom utbildningar och genom att skaffa yrkescertifikat för tjänsterna.

Kunskaperna om incidenter kan utvecklas genom övning, och det berättas det mer om i kapitel 2.3 Övning av informationssäkerhetsincidenter i molnmiljöer.

1.3.4 Tjänstens informationssäkerhetsegenskaper kan bero på ett avtal eller en licens

I en del molntjänster kan det finnas avgiftsbelagda tilläggsfunktioner för informationssäkerheten som hänför sig till exempelvis identifieringsverktyg, kryptering av information och tillgången till användningsloggar. Å andra sidan kan de informationssäkerhetsegenskaper som molntjänsterna använder även vara knutna till hurdan licens som har skaffats för tjänsten. I IaaS- och PaaS-modellerna är många tekniker för informationssäkerhet som till exempel ger effektivare övervakning av miljön och informationssäkerhetsincidenter ofta belagda med en tilläggsavgift.

En organisation som skaffar eller använder molntjänster bör sätta sig in i tjänstens egenskaper, licenser och tjänstemodeller för att kunna försäkra sig om att helheten uppfyller organisationens informationssäkerhetskrav.

1.3.5 Datainsamling vid incidenter

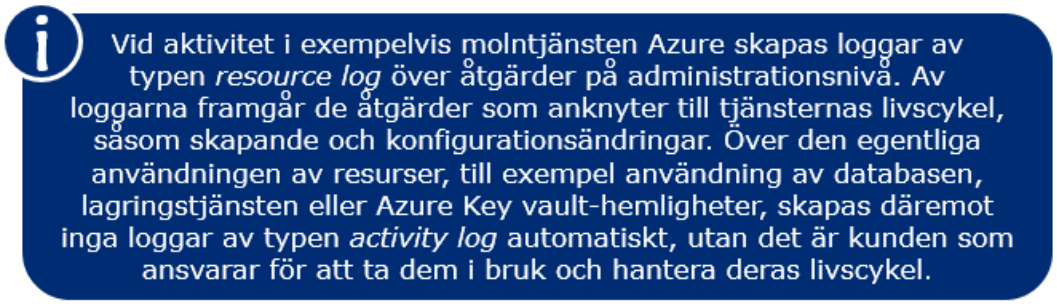
Utredningen av en incident i en molnmiljö beror i stor utsträckning på vilka loggdata som används. Huruvida tjänsterna producerar och samlar in loggdata beror på tjänsten och dess konfiguration. Om kunden inte har samlat in loggdata kan det vara svårt eller omöjligt att bevisa incidenten.

Många molnplattformar samlar in loggdata om IaaS- och PaaS-tjänster automatiskt på det så kallade **kontrollplanet** (eng. control plane, ibland även management plane). Kontrollplan avser de användargränssnitt, verktyg och gränssnitt som kundens administrationspersonal använder för att beställa och konfigurera molntjänsterna. Exempelvis införande av nya tjänster och befullmäktigande av nya administratörer på plattformen lagras typiskt i kontrollplanets logg, utan att kunden har förstått att ta i bruk en sådan auditlogg.

Loggens lagringstid varierar, och huruvida den räcker till bör kontrolleras i plattformstjänsten. Lagringstiden kan vara till exempel några månader, varvid det kan vara svårt att undersöka misstänkt missbruk som pågått en längre tid. Vanligtvis är det möjligt att spara loggar längre än standard mot en tilläggsavgift.

Molntjänster används på det så kallade **data- eller applikationsplanet** (eng. data plane eller application plane). Användningshändelser på denna nivå är exempelvis inloggning på en virtuell maskin, nedladdning av en fil från ett molnlagringsutrymme och operationer som anknyter till data i databastjänsten. Tillgången till användningsloggar på denna nivå beror ofta på vilka förfaranden som kunden har infört och som tjänsteplattformarna tillhandahåller mot en tilläggsavgift. Det kan hända att molntjänsten inte automatiskt producerar några loggar alls över dessa händelser, utan det är kunden som ska ta dem i bruk och hantera loggarnas livscykel.

I **SaaS-tjänster** samlas loggdata in av tjänsteleverantören. Vid ibruktagande av SaaS-tjänster ska det säkerställas att tjänsteleverantörens loggningspraxis uppfyller de krav som organisationen ställt på loggningen. Det ska till exempel vara möjligt att undersöka användningshändelser och misstänkta missbruk. I en del tjänster kan sådana här loggar vara tillgängliga för kunden, i andra förutsätter de sökningar av tjänsteleverantören och ibland skapas inga loggar alls.



Utöver loggarna kan molntjänster göra det möjligt att följa nättrafiken (eng. network flow logs), varvid det är möjligt att analysera molnets arbetsbördor, till exempel datatrafiken i virtuella maskiner, containrar och applikationer.

1.3.6 DevOps-praxis

Den nutida applikationsutvecklingen baserar sig på DevOps-praxis, där kod, automation och reproducerbarhet står i fokus. Särskilt vanliga är sådana här automationer i molnmiljöer.

I praktiken innebär det att det är möjligt att automatisera kundens andel av molntjänsternas ibruktagande, konfiguration, införande i produktion och uppföljning av produktionen samt göra den till en reproducerbar modell. Det gör återställandet efter incidenter mer flexibelt. Kunden kan ha möjlighet att återställa applikationen och dess stödtjänster från källkoder och säkerhetskopior av data antingen till samma ställe, till ett annat ställe hos samma molnleverantör eller ibland, genom mindre ändringar, till en annan tjänsteleverantörs miljö. Enligt god praxis innehåller källkoden ingen information om behörigheter (till exempel koder, nycklar och certifikat), utan de hanteras separat.

Viktiga saker att observera i fråga om DevOps-praxis är med tanke på incidenter att tillgången till källkoden och säkerhetskopior av data har säkerställts. Bäst görs

detta så att säkerhetskopior har sparats i olika typer av tjänster (till exempel databas vs. objektlagring), de är skyddade med åtkomsträttigheter på olika nivåer och i mån av möjlighet även spridda till ett eget datacenter, till en geografiskt annan lagringsplats i samma molntjänst eller helt och hållet till en annan molntjänst. Mer information om säkerhetskopiering finns i kapitel 2.2.7 Säkerställ tillräckliga rutiner för säkerhetskopiering och återställande.

2 Beredskap

Ett centralt sätt att minska incidenternas allvarlighetsgrad samt möjliggöra snabb återhämtning och att affärsverksamheten kan fortsätta är att förbereda sig för incidenter. Organisationen kan bedöma sin beredskap genom att använda till exempel Cybersäkerhetscentrets Cybermätare[4]. En i förväg upprättad incidenthanteringsplan ger ett bra utgångsläge för hur man ska agera när en incident inträffar. Organisationen ska även säkerställa att olika åtgärder, till exempel att låsa användarkoder, blockera servrar och enheter från nätet samt begränsa nättrafiken till skadliga IP-adresser eller domännamn, är tekniskt möjliga samt att personalen även har kompetens och anvisningar för att genomföra dem.

Det är viktigt att samla in, sammanställa och övervaka loggdata för att kunna upptäcka incidenter i tid. Loggdata gör det även möjligt att utreda incidenter grundligt och på så sätt göra den eventuella rensningen och återställandet av miljön snabbare. Cybersäkerhetscentret har utarbetat anvisningar för hur man samlar in och använder loggdata[5]. Beroende på vilka system en organisation använder, krävs vanligtvis dessutom lösningar på nätverks- och systemnivå för omfattande övervakning.

2.1 Administrativa åtgärder

När incidenter inträffar är det nästan alltid fråga om hektiska situationer då organisationen prövas hårt. Man kan försöka underlätta situationen i förväg genom att göra upp planer och öva på verksamhetsmodeller för incidenter. Dessa åtgärder säkerställer att incidenthanteringsgruppen när situationen pågår kan koncentrera sig på att utreda incidenten, då de viktiga verksamhetssätt, ansvar, roller och förfaranden som behövs i situationen redan är bekanta.

2.1.1 Känn din molntjänst

Det första steget i beredskapen är att identifiera vilka molntjänster organisationen använder: en typisk nutida IT-miljö består av till exempel flera SaaS-tjänster samt en eller flera molnplattformar (till exempel Azure, AWS eller Google Cloud). Organisationen kan även använda en lösning med flera molntjänster (eng. multicloud), där tjänster på flera molnplattformar används.

Organisationen bör bilda sig en uppfattning om sin molntjänsthelhet och säkerheten för den genom att ta reda på till exempel:

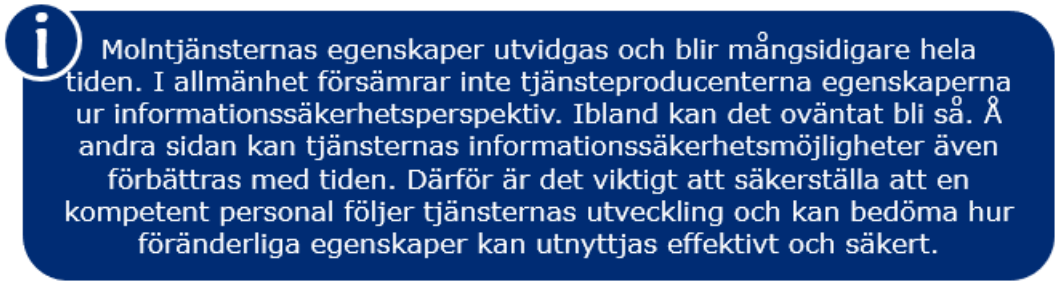
- Vilka molntjänster och molnleverantörer som den använder sig av.
- Vad som sägs i avtalen och tjänstevillkoren om fördelningen av säkerhetsansvaret mellan den organisation som använder tjänsten och molnleverantören (den så kallade modellen med delat ansvar, se kapitel 1.3.2).
- Vilka data och datatyper (till exempel kundinformation, sekretessbelagd information) som behandlas i respektive tjänst. Man bör i synnerhet känna till i vilka molntjänster personuppgifter som omfattas av dataskyddsförordningen behandlas.
- Hur behörigheterna i molntjänsterna har definierats och hur det säkerställs att åtkomsten följer principen om lägsta behörighet.

[4] https://www.kyberturvallisuuskeskus.fi/sv/vara-tjanster/lagesbild-och-natverksledarskap/cybermataren
[5] https://www.kyberturvallisuuskeskus.fi/sv/aktuellt/anvisningar-och-guider/sa-har-samlar-du-och-anvander-loggdata

- Huruvida olika typer av miljöer (till exempel test och produktion) har skiljts åt.
- Hur molntjänsten har segmenterats på nätverksnivå.
- Huruvida förbindelser har öppnats från molnet till datacentret.
- Vilka identiteter applikationerna och automationerna använder, och hurdana rättigheter de har.
- Vilka olika slags molntjänster och -resurser som används, och hurdana egenskaper de har ur informationssäkerhetsperspektiv.
- Var tjänsterna och data finns (geolokalisering). Har tjänsterna speglats på flera ställen för att minska risken med en enskild geografisk plats?
- Hur tjänsterna och data för närvarande skyddas mot cyberhot.
- Hurdana loggar tjänsterna producerar, var de sparas och hur länge de finns tillgängliga.
- Hur incidenter och larm i loggdata och säkerhetsprodukterna övervakas.
- Hurdana rutiner för säkerhetskopiering och återställande som har införts i respektive tjänst.

Det är bra att känna till hurdana beroenden och inverkan molntjänsterna har med tanke på övriga tjänster och organisationens affärsverksamhet, till exempel:

- Hur skulle en informationssäkerhetsincident i en viss molntjänst påverka organisationens övriga IT-system?
- Hur skulle en informationssäkerhetsincident i en viss molntjänst påverka organisationens affärsprocesser?



2.1.2 Planera och dokumentera åtgärder för incidenthantering

Incidenthanteringsplan: Upprättande av en incidenthanteringsplan är en bra övning, där organisationen kan bedöma till exempel vilka roller, kommunikationskanaler och utomstående aktörer (till exempel juridiska tjänster, tjänster för kriskommunikation, utredning av incidentens omfattning och allvarlighetsgrad) som behövs vid en incident samt definiera hurdana händelser som i organisationen definieras som incidenter som initierar incidenthanteringsprocessen. I incidenthanteringsplanen beskrivs även den beslutskedja som ska följas vid en incident. En färdig incidenthanteringsplan utgör stommen i incidenthanteringen, och det är möjligt att i förväg öva på att följa den. Med hjälp av incidenthanteringsplanen kan man även inom organisationen förklara och ge utbildning i verksamhetsmodellen som ska följas vid incidenter.

Utöver en incidenthanteringsplan kan exempelvis följande dokumentation vara till nytta:

Kontaktuppgifter: Kontaktuppgifter för de aktörer som behövs i incidenthanteringen (till exempel organisationens beslutsfattare, det tekniska stödet och tjänsteleverantörerna).

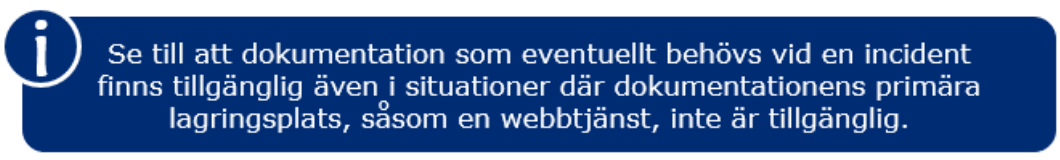
Arkitektur och teknisk dokumentation: Beskrivningar av arkitekturen i organisationens molnmiljöer samt teknisk dokumentation, till exempel molnresursernas konfigurationer. När modern DevOps-praxis tillämpas är molnresursernas konfigurationer i allmänhet tillgängliga i form av kod. Det är vanligtvis möjligt att skapa automatisk teknisk dokumentation även genom att ladda ner en konfiguration av SaaS- och PaaS-komponenterna från molnet. Det är bra att göra på det här sättet alltid efter ändringar om ändringarna inte genomförs med kod och DevOps- automation.

Datainventering: Med hjälp av datainventering eller motsvarande dokumentation är det möjligt att ta reda på i vilka system eller på vilka lagringsställen det finns personuppgifter. Den informationen behövs i utredningen av incidenters konsekvenser och identifieringen av informationssäkerhetsincidenter.

Anvisningar för incidenthantering: anvisningar för till exempel hur man inom incidenthanteringen kan genomföra tekniska åtgärder såsom isolera enheter, samla in bevismaterial eller återställa data från säkerhetskopior. De tekniska åtgärderna för utredning och återställande omfattar ofta bland annat administrativa element i fråga om roller, ansvar och skyldigheter, vilket är en viktig orsak till att planera och dokumentera dessa förfaranden i förväg. Till exempel insamling och behandling av loggdata omfattas av lagstiftningsmässiga skyldigheter. För att sådana skyldigheter ska kunna beaktas på ett tillräckligt sätt vid en incident, ska åtgärderna planeras och dokumenteras i förväg. Observera även att anvisningarna ska stämma överens med incidenthanteringsplanen, så att till exempel beslutskedjan motsvarar den som har fastställts i incidenthanteringsplanen.

Mall för incidenthanteringslogg: en mall som används för att föra en händelselogg över incidenten. Åtminstone ska man i förväg komma överens om vilket system eller vilken lagringsplats som vid en incident används för att föra och upprätthålla en händelselogg, samt säkerställa att tillräckliga förfaranden tillämpas för att skydda informationen.

Årsklocka för incidenthanteringen och molnmiljöernas säkerhet: Både incidenthanteringsåtgärderna och informationssäkerheten som helhet är processer som ska upprätthållas och utvecklas regelbundet. Se till att exempelvis uppdatering av incidenthanteringsplanen, övning av incidenter och granskning av bästa säkerhetspraxis för molnplattformarna ingår i organisationens årsklocka.



2.1.3 Definiera roller och ansvar inom incidenthanteringen

Se till att din organisation har en aktuell incidenthanteringsplan, där det har avtalats om rollerna och ansvaren vid incidenter.

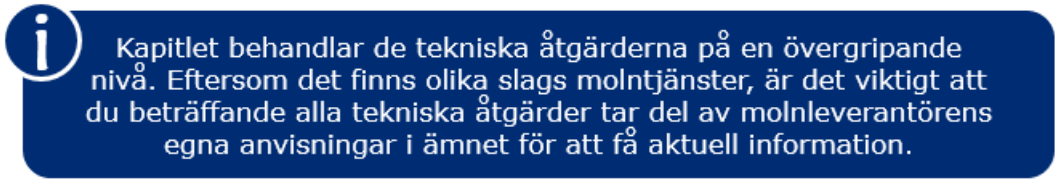
En incident kräver samarbete mellan organisationens olika aktörer. Vid en incident bildas en så kallad incidenthanteringsgrupp med åtminstone en person som representerar ledningen och en teknisk expert. Om möjligt ska det i gruppen även finnas experter inom kommunikation och juridik samt den tekniska expertis som krävs för utredningen av incidenten. Uppgiftsrollerna och de ansvaren som hänför sig till dem i fråga om informationssäkerhetsincidenter beskrivs i exempelvis finansministeriets anvisning Ohje tietoturvapoikkeamatilanteiden hallinnasta (Anvisning om hantering av informationssäkerhetsincidenter)[6]. Om organisationen inte har tillgång till ovanstående resurser kan den efter eget gottfinnande anlita utomstående experter till hjälp vid hanteringen och utredningen av situationen. Det är bra att i förväg planera ytterligare kompetens som eventuellt behövs vid en incident.

Vid definitionen av roller och ansvar är det viktigt att beakta även tjänsteleverantörernas roll vid incidenter. Det är bra att skriftligt komma överens med tjänsteleverantörerna om verksamhetsmodellen för incidenter. För molnleverantörerna är det bra att i avtalsvillkoren eller annan dokumentation kontrollera hurdan hjälp molnleverantören kan ge vid incidenter. Säkerställ även att tjänsteleverantörernas kontaktuppgifter snabbt kan hittas i en nödsituation.

I situationer där det är fråga om en personuppgiftsincident kan molnleverantören i egenskap av personuppgiftsbiträde vara skyldig att hjälpa till i utredningen av ärendet.

2.2 Tekniska åtgärder

I detta kapitel beskrivs viktiga tekniska åtgärder som kan användas för att förbättra beredskapen för incidenter.



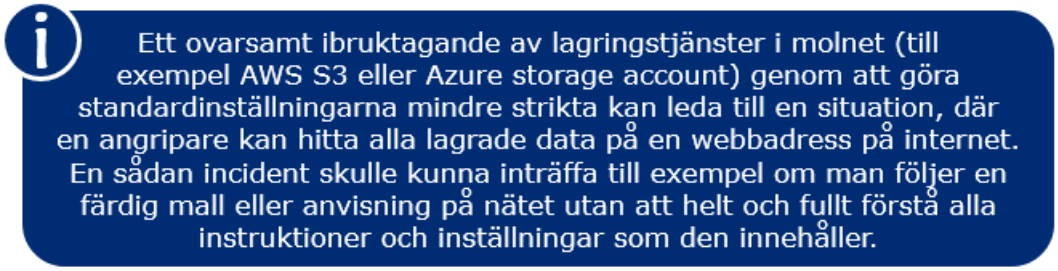
2.2.1 Planera molnmiljön med omsorg

Angripare kan få tillträde till en molnmiljö genom att till exempel utnyttja en sårbarhet eller komma över en behörig användares användar- och identifieringskoder. Tjänsten ska planeras så att, även om en angripare skulle lyckas ta sig in i tjänsten, ger tillträde till ett ställe inte tillträde överallt. Man kan prata om en så kallad sprängradie (eng. blast radius), det vill säga vilken omfattning konsekvenserna av angreppet kan få.

I molntjänster är det typiskt att om uppgifter läcker ut från en felaktigt konfigurerad lagringstjänst, läcker i allmänhet allt ut på en gång. Därför är det särskilt viktigt att sörja för åtkomsthanteringen av resurserna och att begränsa

[6] https://julkaisut.valtioneuvosto.fi/handle/10024/79258

gränssnittens synlighet så att de inte är nåbara på nätverksnivå från hela internet, vilket vanligtvis gäller som standard i molntjänster.



Man strävar efter att minimera konsekvenserna av eventuella angrepp med hjälp av den så kallade Zero Trust-planeringsmodellen, exempelvis genom att minimera användarnas och tjänsternas åtkomst till olika tjänster:

- Ge användarna så låga behörigheter som möjligt: ge behörighet till endast de resurser och tjänster som de behöver.
- Verifiera användaren och enheten med hjälp av flera behörighetsuppgifter vid tidpunkten för användningen.
- Ge högre behörigheter endast för de tidpunkter då de behövs (så kallad Just-In-Time-åtkomst).

Försök även dela in tjänsterna du använder på molnplattformen i logiska helheter, till exempel:

- Genom att dela in i logiska helheter – såsom varje applikation, dess data och stödtjänster – under olika konton eller prenumerationer.
- Genom att dela in olika typer av miljöer i infrastrukturhelheter enligt användningsändamål (till exempel utveckling, testning och produktion).

Se till att åtkomsten mellan dessa helheter är begränsad eller förhindrad.

Användarnamn som ger åtkomst till flera helheter eller miljöer bör användas endast för administration. Sådana behörigheter bör användas enligt exempelvis Just-In-Time-principen och användningen av dem övervakas.

Det är i allmänhet möjligt att begränsa oförutsedda ändringar i molnet. Det är en god idé att i mån av möjlighet definiera till exempel molntjänster, datatjänster och containerregister som används för hantering av hemligheter så att det inte är möjligt att förstöra innehållet i dem utan påtvingad fördröjning.

2.2.2 Följ de rutiner som tjänsteleverantörerna gett anvisningar om

Molnmiljöer kännetecknas av att de förnyas och förändras i snabb takt. Många molnleverantörer strävar efter att informera sina användare om ändringar samt upprätthålla aktuella anvisningar för vilka de bästa rutinerna för att använda och administrera tjänsterna är, vilket inkluderar informationssäkerhet. Beakta åtminstone följande för att säkerställa att tjänsten är informationssäker:

- Följ meddelanden om de molntjänster som används (till exempel e-postmeddelanden och webbplatser). I meddelandena kan det finns information om till exempel nya säkerhetsfunktioner eller kända sårbarheter.

- Följ tjänsteleverantörernas rekommendationer om säkerhet vid både ibruktagandet och användningen av molntjänsterna. Internationella tjänsteleverantörers anvisningar hittas med sökorden ”security best practices”. Underlåtenhet att följa säkerhetsrekommendationer borde alltid vara ett medvetet och motiverat beslut av organisationen. I en del molntjänster finns det automation som stöder informationssäkerheten (eng. exempelvis security defaults eller guardrails), med hjälp av vilka konfigurationer och ändringar i molnet kan låsas eller göras säkrare. Dessa möjligheter varierar från en tjänsteleverantör till en annan.

- Skärp tjänsterna enligt tjänsteleverantörens anvisningar för skärpning (till exempel säker konfiguration, urbruktagande av standardlösenord och -konton och liknande). Internationella tjänsteleverantörers anvisningar hittas med sökorden ”hardening guide”.

- Se till att de nya tjänster och resurser som skapats i molnmiljön uppfyller kraven genom att införa standardiserade riktlinjer (eng. policy) och modeller (eng. template). De standardiserade riktlinjerna och modellerna skapar standardinställningar för sina objekt i enlighet med bestämmelserna. Riktlinjerna kan man själv skapa så att de motsvarar organisationens krav och arkitektur. På molnplattformarna kan det även erbjudas färdiga kravmallar till exempel baserade på god praxis (till exempel AWS Well-Architected Framework och Azure Architecture Center).

- Använd den kodautomation som tjänsteleverantören stöder i hanteringen av molntjänsterna (Infrastructure-as-Code, IaC), varvid konfigurationernas livscykel och ändringshanteringen blir tydligare. Användningen av IaC hänger samman med god DevOps-praxis och snabbar upp skapandet av nya resurser och återställandet av tjänsterna vid allvarliga störningar.

- Övervaka så att din molnmiljö överensstämmer med god praxis. För detta ändamål kan du använde både automatiserade bedömningar (till exempel Azure Security Score och Defender for Cloud eller AWS Security Hub) eller en extern granskning.

- Studera tjänsteleverantörernas dokumentation om incidenthantering. På molnplattformarna finns anvisningar om incidenthantering från respektive tjänsteleverantör. Ta i bruk de tekniska lösningar enligt anvisningarna som lämpar sig för din organisations lösning.

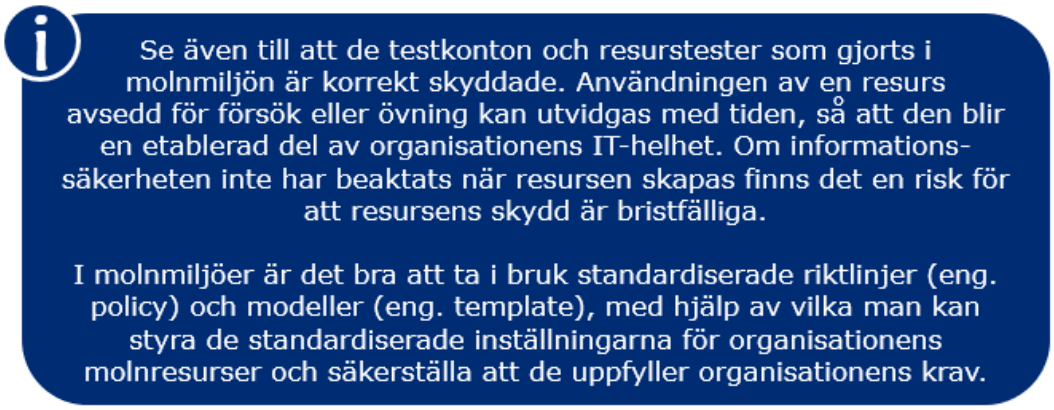
2.2.3 Säkerställ säkerheten i utvecklings- och produktionsmiljöer

Uppmärksamhet ska även ägnas åt informationssäkerheten för den applikationsutveckling som sker i molnmiljöer. Samtidigt som det finns mycket anvisningar om processmodellen för säker applikationsutveckling[7], är det skäl att ägna uppmärksamhet även åt säkerheten i själva utvecklings- och produktionsmiljöerna, till exempel:

- Planera utvecklings- och produktionsmiljöerna på ett sådant sätt att miljöer för olika ändamål finns i olika infrastrukturhelheter.

[7] Ett exempel på en anvisning: https://www.kyberturvallisuuskeskus.fi/sv/publikationer/saker-utveckling-med-sikte-pa-godkannande

- CI/CD-automationer är ett vanligt sätt att göra intrång i molntjänsters produktionsmiljöer. Kom ihåg att sörja för informationssäkerheten även för dessa system.
- Påbörja informationssäkerhetsarbetet i ett så tidigt skede av utvecklingen som möjligt (ofta används termen ”vänsterförflyttning” med hänvisning till placeringen på projektets tidslinje, eng. shift left). Beakta informationssäkerheten i samband med utvecklingen med hjälp av olika verktyg och tekniker som säkerställer informationssäkerheten. När informationssäkerheten integreras på rätt sätt i utvecklingspipelinen kan man undvika att konfigurationer som inte uppfyller kraven på informationssäkerhet eller sårbara komponenter används.
- Planera en CI/CD-automation där inställningarna för och uppdateringarna av applikationen kan göras endast med en viss användarkod. Användningen av denna kod ska omfattas av informationssäkerhetsövervakningen för att kontrollera om det förekommer avvikelser i användningen av den.



2.2.4 Minska angreppsytan

Med organisationens angreppsyta avses dess informationssystem, tjänster och kommunikationsportar som är öppna mot det offentliga nätet och som en angripare skulle kunna göra ett angrepp mot – åtminstone i teorin. Begreppet angreppsyta konkretiserar det faktum att ju fler informationssystem och -tjänster som är öppna mot nätet, i desto större utsträckning bör organisationen även kunna upptäcka eventuella angrepp och förhindra dem. Gör följande för att minska angreppsytan:

- Se till att organisationen använder endast sådana molntjänster och -resurser som den behöver.
- Skärp de tjänster som används i enlighet med anvisningarna för skärpning (se kapitel 2.2.2 Följ de rutiner som tjänsteleverantörerna gett anvisningar om).
- Tänk på att angreppsytan blir större även av behörigheter som getts användarna och som är för omfattande med tanke på arbetsuppgifterna. Se till att användarnas behörigheter följer principen om lägsta behörighet och att administratörskoder avsedda för särskilda arbetsuppgifter och andra högre behörigheter inte används i det dagliga arbetet.
- Skapa en process genom vilken onödiga tjänster och resurser samt användare och behörigheter tas ur bruk regelbundet.

2.2.5 Fastställ en kostnadsbudget för resursanvändningen

Ibland kan en angripares åtgärder omfatta aktivering av molnets resurser så att användningen av molnet orsakar en betydande ekonomisk skada för kunden. För att begränsa en sådan effekt ska man sätta upp regler för molnets prenumerationer och konton som begränsar aktiveringen av dyra resurser samt fastställa en kostnadsbudget, som det inte är möjligt att förbigå utan ägarens godkännande. Molnplattformarnas egenskaper i fråga om dessa funktioner varierar, och man bör sätta sig in i dem när plattformarna tas i bruk.

2.2.6 Säkerställ åtkomsten till tjänster i nödsituationer

Säkerställ beträffande molnplattformar att organisationen har konfigurerat åtkomstförfaranden för nödsituationer i dem (eng. emergency access). Syftet med dessa förfaranden är att säkerställa att kunden i alla situationer har möjlighet att hantera sina molntjänster.

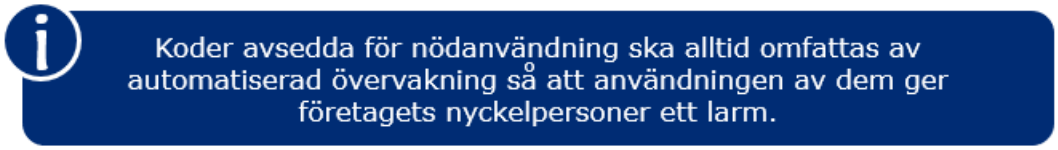
Dessa åtkomstförfaranden kan behövas i undantagssituationer, där till exempel den autentiseringsmetod för många användare (till exempel en autentiseringsapplikation) som organisationen normalt använder inte är tillgänglig. Administratörerna har i nödsituationer möjlighet att identifiera sig i tjänsten på olika sätt. Dessa användarkoder används endast i undantagsfall, och man ska utarbeta rutiner för skapandet och förvaringen av dem. Koderna ska vara avsedda endast för nödanvändning av organisationen och därför inte vara kopplade till de anställdas koder eller identifieringsverktyg.

För användarkoder som skapats för nödsituationer rekommenderas att man använder en så stark identifieringsmetod som möjligt, till exempel säkerhetsnyckeln FIDO2. FIDO2-nyckeln är fysisk, så det är möjligt att förvara den i ett låst utrymme, till exempel företagets kassaskåp.

Det är bra om användningen av åtkomstförfarandena för nödsituationer omfattas av informationssäkerhetsövervakningen så att användning av koderna ger upphov till ett larm. På så vis är det möjligt att reagera på eventuella missbruk av koderna.

Koder som skapats för nödanvändning ska testas med planerade mellanrum för att säkerställa att nödvändiga personer känner till de olika skedena av användningen av dem och att koderna fortfarande fungerar.

Se dessutom till att automatik som hänför sig till rensning och radering av användarkoder och behörigheter, eller riskbaserade rutiner för åtkomsthantering (till exempel Conditional Access) inte av misstag förhindrar nödkodernas funktion.



2.2.7 Säkerställ tillräckliga rutiner för säkerhetskopiering och återställande

Se till att tillräckliga rutiner för säkerhetskopiering och återställande har skapats för molntjänsterna[8]. På en molnplattform kan en del rutiner för återställande automatiskt vara i användning, till exempel spegling av tjänster i fler än en datorhall. Det är dock bra att observera att kunden på molnplattformar får de tjänster som han eller hon betalar för: I praktiken är mer avancerade och säkra rutiner för säkerhetskopiering och återställande i allmänhet tjänster som tillhandahålls mot en tilläggsavgift och som används endast om organisationen har köpt dem och integrerat dem i sina tjänster.

Om din organisation inte har tagit i bruk säkerhetskopieringstjänster för molntjänsterna eller säkerställt spegling av tjänsterna på flera geografiska platser[9], har dessa rutiner sannolikt inte genomförts automatiskt av tjänsteleverantören. Utan tillräckliga rutiner för säkerhetskopiering och återställande kan organisationen till följd av en incident i värsta fall förlora alla resurser som den har byggt upp och alla data som den har lagrat i molnet.

Vid användning av containerbaserade arbetsbördor (till exempel Docker) kan tjänsterna och applikationerna i allmänhet återställas snabbare än tjänster baserade på operativsystem. Vid återställande är det viktigt att de register som används för fördelningen av containrar fortfarande är tillgängligt eller att ett sådant kan sättas upp och containrarna skapas på nytt från källkoderna.

Säkerställ tillräckliga rutiner för säkerhetskopiering genom att planera av vilka molnresurser det måste finnas säkerhetskopior och hur ofta kopior ska göras. På molnplattformar finns det separata tjänster och arkitekturrekommendationer för hur säkerhetskopiering kan utföras. Observera när du planerar hur säkerhetskopieringen ska utföras att om du sparar säkerhetskopiorna i samma molnmiljö som deras källmaterial, kan säkerhetskopiorna utsättas för samma informationssäkerhetsangrepp. I värsta fall skulle ett angrepp mot molnmiljön således kunna förstöra både de ursprungliga tjänsterna och de data de innehåller samt deras säkerhetskopior. Säkerhetskopiorna kan spridas från källsystemen till åtskilda konton (till exempel eng. AWS account) eller prenumerationer (esim. eng. Azure subscription).

Det rekommenderas att återställande av säkerhetskopior testas regelbundet både som en teknisk åtgärd och som en del av krisövningen. Se även kapitel 2.3 Övning av informationssäkerhetsincidenter i molnmiljöer.

2.2.8 Definiera och utför loggning

Tillräcklig loggning spelar en viktig roll i observationen och utredningen av informationssäkerhetsincidenter. Loggar som kunden samlat in kan vara det enda sättet att bevisa att en informationssäkerhetsincident har inträffat.

[8] Det är bra om planeringen baserar sig på den målsättning för återställningstid och den målsättning för återställning av data (eng. Recovery Time Objective (RTO) och Recovery Point Objective (RPO)) som satts upp för tjänsterna. Ytterligare information (på finska) om kontinuitetshantering och planeringen av den finns till exempel i anvisningen VAHTI 2/2016, Toiminnan jatkuvuuden hallinta (Hantering av verksamhetens kontinuitet) på https://julkaisut.valtioneuvosto.fi/handle/10024/75168.

[9] Det är bra att observera att om tjänsteleverantören har placerat molnresurser på endast en geografisk plats kan dessa utsättas för störningar om en störning riktas mot infrastrukturen på platsen i fråga.

När loggning planeras är det bra att observera att loggar kan innehålla personuppgifter och att lagstiftningen ställer krav på hanteringen av loggar[10].

Se till att din organisation har infört tillräckliga loggningsförfaranden i molntjänsterna. På molnplattformar kan man fastställa regler för loggningen (eng. data collection rules) som definierar insamlandet av loggen. Om insamlingen av loggdata från olika tjänster inte har definierats kan insamlingen av loggdata för att utreda en incident visa sig vara mycket svårt.

Beträffande loggar kan du fundera på till exempel följande:

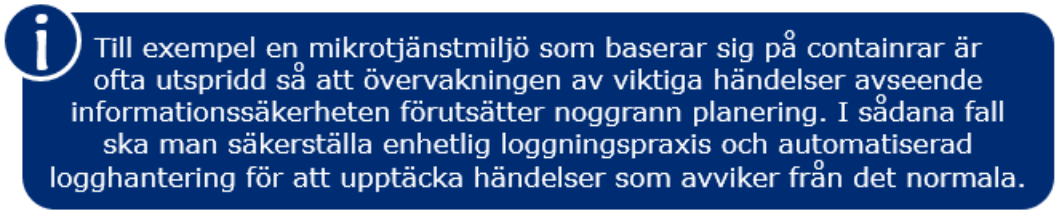
- Är det möjligt att i loggarna se ändringar i molntjänsternas konfigurationer och ändringar som gäller administratörer?
- Är det möjligt att i loggarna se vem som har använt en tjänst/resurs samt när och var han eller hon har gjort det?
- Hur länge är olika loggar tillgängliga?
- Vem har åtkomst till loggarna? Åtkomsten ska vara strikt begränsad och hanteringen av loggarna ska övervakas.
- Är loggarna och de tjänster som används för att spara dem skyddade från ändringar? Loggarnas integritet, det vill säga oföränderlighet, ska säkerställas, så att loggdata är tillförlitliga. Utredningen av en informationssäkerhetsincident i en molnmiljö försvåras avsevärt om angriparen har möjlighet att förstöra loggar.
- Hur kan nätverksloggar (eng. network flow logs) tas i bruk och behövs det specialkompetens eller -verktyg för att analysera dem?

Ämnet behandlas även ovan i kapitel 1.3.5 Datainsamling vid incidenter.

2.2.9 Övervaka miljöer och upptäck incidenter

Observation av incidenter i en molntjänsts normala verksamhet och datatrafik kräver att den följs upp. På molnplattformar är det möjligt att ta i bruk olika typer av övervakningsverktyg, i allmänhet mot en tilläggsavgift. I SaaS-tjänster, som finns i en IT-miljö som administreras av en tjänsteleverantör, ansvarar vanligtvis tjänsteleverantören för observationen av incidenter.

Det är centralt för observationen av de incidenter som förekommer i en tjänst att förstå tjänstens normala verksamhet och datatrafik (eng. baseline). När man känner till de normala användningssätten och -mängderna samt trafiken kan man upptäcka verksamhet och trafik som avviker från det.



Ytterligare information om observationen av incidenter i kapitel 4 Upptäckt av informationssäkerhetsincidenter.

[10] Ytterligare information om hanteringen av loggdata finns i till exempel Cybersäkerhetscentrets anvisningar på https://www.kyberturvallisuuskeskus.fi/sv/aktuellt/anvisningar-och-guider/sa-har-samlar-du-och-anvander-loggdata

2.2.10 Planera det tekniska genomförandet av utredningar av incidenter

Planera som en del av de tekniska beredskapsåtgärderna hur den tekniska utredningen av incidenten i praktiken kunde genomföras:

- Finns tillräckliga loggar tillgängliga och vem har åtkomst till dem vid en incident? Hur kan loggdata förvaras på ett sätt som möjliggör senare undersökning och användning av dem som bevis?
- Används en miljö där incidenten kan undersökas? I idealfallet utreds inte incidenten i samma miljö som angriparen har tillträde till. På molnplattformar kan det till exempel vara möjligt att skapa en separat undersökningsmiljö (eng. forensic investigation environment).
- Vet man hur man gör rätt slags sökningar i loggdata för att utreda vad som har hänt? Det samlas mycket loggdata, och det kan vara svårt att hitta de data som behövs. Det är bra att sätta sig in i loggningens format och hur man gör loggsökningar vid en tidpunkt då ingen incident pågår.
- Se till att det finns skriftliga metodanvisningar för den tekniska utredningen av incidenten och att de personer som gör den tekniska utredningen har tillräcklig kompetens för uppgiften.

2.3 Övning av informationssäkerhetsincidenter i molnmiljöer

Ett effektivt sätt att förbereda sig på incidenter utöver den administrativa och tekniska beredskapen, är att öva på hur man ska agera när en incident inträffar. Vid en incident behöver organisationen förutom upprätthålla sin normala affärsverksamhet, även utreda en incident, där det krävs såväl snabba beslut som åtgärder. Övning av incidenter gör organisationen bekant med de rutiner, den beslutsmodell, de roller och ansvar samt viktiga åtgärder som ska följas vid en incident. Med hjälp av övning har de som är delaktiga i den faktiska incidenten redan en god uppfattning om ovanstående, vilket hjälper dem att agera på överenskommet sätt.

Det finns många olika typer av övningar för incidenter som omfattar allt från så kallade skrivbordsövningar till simulerade angrepp (eng. red teaming, purple teaming) och allt där emellan. Organisationer där incidenthanteringen inte ännu har etablerats kan ha nytta av skrivbordsövningar som illustrerar till exempel vilka ansvar och krav som gäller för olika roller vid en incident. Med hjälp av en skrivbordsövning kan man även gå igenom åtgärderna i incidenthanteringsplanen och diskutera deras konsekvenser samt på så sätt hitta utvecklingsområden i planen.

Med hjälp av övning kan man även upptäcka eventuella brister i förmågan att hantera incidenter. Genom övningar kan man även testa till exempel huruvida organisationen i sina planer och sin verksamhet har beaktat molnmiljöernas utmärkande egenskaper med tanke på incidenthanteringen som beskriv i kapitel 1.3 samt huruvida de åtgärder som räknas upp i kapitel 5 Anvisningar kan utföras av incidenthanteringsgruppen.

Oavsett övningstyp ska ett övningsscenario som är relevant för organisationen väljas när man övar på informationssäkerhetsincidenter. Beträffande molnmiljöer kan sådana scenarion vara till exempel följande typer av utgångsscenarion, genom vilka man börjar genomföra incidenthanteringsåtgärder:

- På darknet finns en ”data dump” som innehåller konfidentiella data från organisationen. Hur har den hamnat där?
- En angripare har krypterat vissa resurser i molntjänsten och kräver nu lösen. Hur kan man återställa situationen?
- Molnmiljöns övervakningsverktyg meddelar om misstänkt aktivitet på ett administratörskonto. Hur ska man göra?

Övning av incidenter kan ordnas även tillsammans med organisationens IT-tjänsteleverantörer om dessa har en central roll vid incidenter.

Ytterligare anvisningar för cyberövning och olika övningsscenarion finns på Cybersäkerhetscentrets webbplats[11].

[11] https://www.kyberturvallisuuskeskus.fi/sv/aktuellt/anvisningar-och-guider/anvisningar-och-guider-organisationer-och-foretag

3 Informationssäkerhetsincidenters livscykel

Livscykeln för en informationssäkerhetsincident består vanligtvis av följande steg:

- Observation
- Utredning av incidenten
- Återställande
- Efterverkningar av incidenten.

Alla informationssäkerhetsincidenter har i stora drag denna livscykel, oberoende av vilka tjänster eller data de påverkar. Rollen för en organisation som utsatts för en incident i livscykelns olika steg beror dock på vilken typ av molntjänst det är fråga om och vad som avtalsmässigt har överenskommits om hur man ska förfara vid incidenter. Tabellen nedan visar de viktigaste skillnaderna.

Tabell 1. Typiska ansvar för kunden i livscykeln för informationssäkerhetsincidenter i olika typer av molntjänster

Steg	IaaS	PaaS	SaaS
Observation	Kunden ansvarar för observationen av informationssäkerhetsincidenter i de molntjänster den använder. Typiska metoder för observationen är att följa upp loggkällor, använda verktyg för övervakning av informationssäkerheten, övervaka avvikelser i datatrafiken och övervaka ändringar i konfigurationer.	Kunden ansvarar för att observera informationssäkerheten i sina applikationer. Typiska metoder är övervakning av händelseloggar för applikationer och programmeringsgränssnitt (API), övervakning av ändringar i konfigurationer samt övervakningslogik per applikation som beskriver eventuella missbruk.	Kundens ansvar för observationen av informationssäkerhetsincidenter är begränsat. I allmänhet kan kunden upptäcka en sådan exempelvis om tjänstens innehåll oväntat förändras, man ser underliga användare i tjänsten eller användningen av tjänsten förhindras.
Utredning av incidenten	Kunden tar de verktyg som den använder, till exempel verktyg för informationssäkerhet, konfiguration och logganalys, till hjälp för att göra observationer och utreda situationen. Tjänsteleverantören bistår i utredningen av incidenten i allmänhet åtminstone när incidenten kan få konsekvenser även för deras operationer eller andra kunders data och tjänster.		I utredningssteget har molnleverantören en viktig roll. Kunden ska vid behov rapportera sina observationer till tjänsteleverantören.
Återställande	Kunden aktiverar åtgärder i enlighet med sin återställningsplan samt återställer data och molnresurser. I allmänhet sker återställandet i molnet genom att skapa nya tjänsteinstanser. Det är möjligt att tjänsteleverantören hjälper till med återställningsåtgärderna. Tjänsteavtalens omfattning och innehåll kan påverka hurdan hjälp som finns tillgänglig.		Återställningsförmågan beror i stor utsträckning på tjänsteleverantörens lösningar.
Efterverkningar av incidenten	Kunden utreder grundorsakerna till incidenten och analyserar hur framgångsrik hanteringen av incidenten har varit. På basis av observationerna försöker man förbättra agerandet, så att ingen liknande situation uppstår igen.		Efterverkningarna hanteras i samarbete mellan organisationen och tjänsteleverantören.

Det centrala är att förmågan att utreda incidenter och återhämta sig från dem ofta är begränsad hos organisationer som använder SaaS-tjänster: I SaaS-modellen är det ofta endast tjänsteleverantören som har sådan förmåga. Därför lämpar sig endast en del av åtgärderna i kapitel 4–6 för användare av SaaS-tjänster. I SaaS-modellen fokuserar organisationerna inom incidenthanteringen på att utreda situationen tillsammans med tjänsteleverantören samt på att informera om situationen internt inom organisationen och vid behov även utanför den, till exempel till myndigheter.

4 Upptäckt av informationssäkerhetsincidenter

Informationssäkerhetsincidenter, inklusive säkerhetsincidenter i molnmiljöer, kan upptäckas på flera olika sätt. En organisation kan själv upptäcka en incident till exempel med hjälp av övervakning eller genom att upptäcka störningar i en tjänst. Organisationen kan även få information om incidenten från en utomstående aktör, till exempel kunderna, media, white hat hackers eller tjänsteleverantören.

I detta kapitel berättas om hur molnmiljöer kan främja observationen av informationssäkerhetshändelser och -incidenter.

Larm och säkerhetspaneler

På stora molnplattformar finns det ofta paneler eller webbplatser som visas för utsedda användare inom organisationen och som beskriver läget för säkerheten i de tjänster som används. Där kan administratörerna se både säkerhetsrekommendationer för sina tjänster och larm om informationssäkerhetshändelser och -avvikelser.

De olika tjänsterna som används på molnplattformarna kan ha egna säkerhetspaneler (eng. security daschboard) som kan ge larm om misstänkt aktivitet. Till exempel molnbaserad centraliserad identitetshanteringsteknologi (till exempel Azure AD, Google Cloud Identity och Okta) kan larma användarorganisationen om misstänkt aktivitet. Sådana funktioner kan dock kräva användarlicenser på en viss nivå och införande av automation.

I SaaS-tjänster kan larm om misstänkt aktivitet komma från tjänsteleverantören eller tjänstens användare.

Molnbaserade informationssäkerhetslösningar

På stora molnplattformar erbjuds ofta olika slags säkerhetslösningar, som kan skydda de tekniker som finns i molnet (till exempel Microsoft Defender for Cloud och AWS GuardDuty). Med hjälp av dessa lösningar kan säkerheten i molnmiljöer och -resurser skyddas och övervakas. Genom sådana lösningar kan man även genomföra automatiserade arbetsflöden, som reagerar på misstänkt aktivitet. Med lösningarna kan man till exempel automatiskt isolera en enhet som man upptäckt misstänkt aktivitet på. Skapande, utveckling och administration av reglerna för dessa lösningar kräver tillräcklig resursfördelning av organisationen.

System för övervakning av informationssäkerheten

Organisationen kan öka sin observationsförmåga genom att förutom ovanstående molnlösningar även investera i ett separat system för hantering av informationssäkerhetsdata och -händelser (eng. Security Information and Event Management, SIEM). Sådana centraliserade loggningssystem kan analysera loggdata och göra observationer av informationssäkerhetshändelser i dem. Skapande, utveckling och administration av reglerna även för dessa lösningar kräver tillräcklig resursfördelning av organisationen.

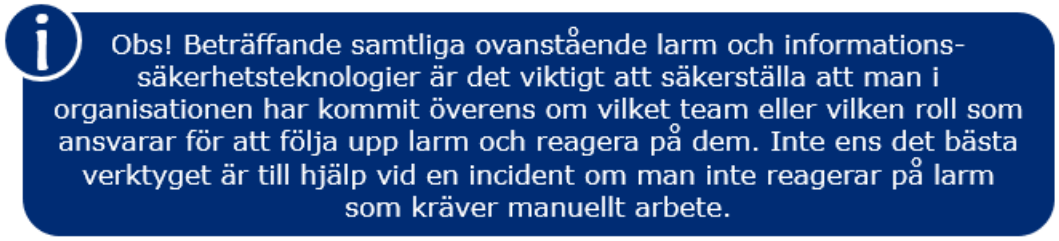
Anmälningar från tjänsteleverantörer

Ibland kommer den första observationen av en informationssäkerhetsincident från molnleverantören. I dessa fall är det viktigt att agera i enlighet med molnleverantörens anvisningar, till exempel byta lösenord och andra åtkomstuppgifter.

Var dock noggrann med att observationen verkligen kommer från molnleverantören – nätbrottslingar använder nämligen ofta namn på kända och allmänna aktörer såsom Microsoft och Amazon i sina bedrägerimeddelanden, som lätt ser ut som äkta meddelanden.

Anmälningar från kunder och andra aktörer

Ibland kommer de första observationerna av en informationssäkerhetsincident från kunderna, white hat hackers, oberoende informationssäkerhetsforskare eller andra oväntade aktörer. Organisationen ska ha förfaringssätt för att hantera dessa anmälningar och ändamålsenliga anvisningar för till exempel kundtjänsten. I ordnandet av processen är det till nytta att publicera lämpliga kontaktuppgifter[12].



[12] Organisationen kan till exempel ange en security.txt-fil för sin webbplats där man berättar om hur man önskar få observationer avseende informationssäkerheten och om den rekommenderade anmälningskanalen. Ytterligare information till exempel på: https://www.kyberturvallisuuskeskus.fi/sv/aktuellt/en-praxis-som-underlattar-anmalan-av-sarbarheter-anvands-annu-inte-i-finland.

5 Anvisningar

Ni kan använda checklistorna för åtgärderna i detta kapitel som hjälp när ni misstänker att det har inträffat en incident i en molnmiljö.

Checklistorna hjälper organisationen att prioritera och dela in verksamheten vid utredningen av en informationssäkerhetsincident.

5.1 Arbetsflödet för utredning av incidenter i molnmiljöer

Diagrammet på följande sida visar de viktigaste åtgärderna inom incidenthantering. Diagrammet stöder användning av checklistorna i tabellform. Organisationen har nytta av att göra upp ett flödes- eller simbanadiagram som lämpar sig för dess incidenthanteringsprocess och som överensstämmer med förfarandena i incidenthanteringsplanen.

Under incidenthanteringsprocessen är det även viktigt att föra en noggrann händelselogg över de åtgärder som vidtagits. Av loggen ska framgå vilken åtgärd som genomförts, tidsstämpeln för den och vem som utfört åtgärden.

Det är även skäl att omsorgsfullt dokumentera eventuellt bevismaterial. Det bör antecknas vem som samlat in materialet, vad materialet består av samt var och när det har samlats in. En omsorgsfullt upprättad händelselogg underlättar avsevärt utredningen samt samarbetet med polisen och datasäkerhetsforskarna.

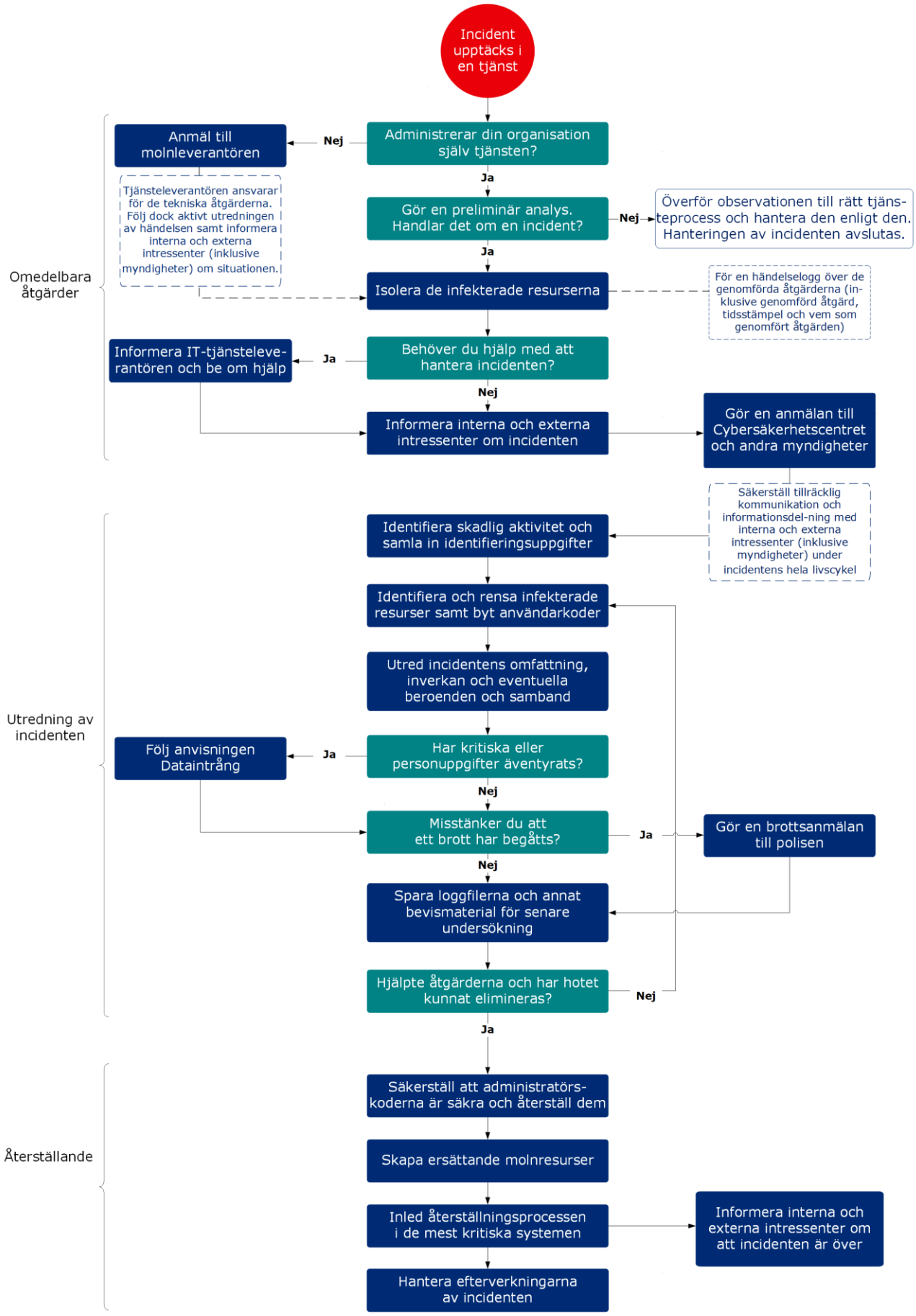


Bild 2. Arbetsflöde för incidentutredning i molnmiljöer, förenklat diagram

5.2 Omedelbara åtgärder

Stegets mål	Syftet med de omedelbara åtgärderna är att skydda kritiska data i miljön, förhindra att angriparen får fotfäste i miljön och förbereda inledande av återställningsprocessen.	
Steg	**Syfte**	**Åtgärder**
Incident upptäcks i en tjänst		
Administrerar din organisation själv tjänsten? **Anmäl till molnleverantören**	I utredningen av incidenten kan hjälp behövas från molnleverantören eller IT-partnern. Vilka stödtjänster som finns tillgängliga varierar enligt vilket tekniskt område incidenten riktar sig mot och huruvida det är kunden eller tjänsteleverantören som ansvarar för området. IaaS, PaaS: Kontakta eventuella IT-partner eller molnleverantören om incidenten hör till deras ansvarsområde. SaaS: Organisationen som producerar molntjänsten är oumbärlig i utredningen av situationen. Observera att tjänsteavtalet kan fastslå att organisationen är skyldig att informera tjänsteleverantören om incidenten.	Lokalisera incidenten: identifiera den eller de tjänster där den eventuella incidenten förekommer och ta reda på huruvida de administreras av din organisation eller om det är din molnleverantör eller IT-partner som ansvarar för dem. Om tjänsten administreras av tjänsteleverantören eller IT-partnern, **kontakta tjänsteleverantörens stödkanal**. Tjänsteleverantören ansvarar för de tekniska åtgärderna, men följer dock utredningen av incidenten och sörjer för bland annat kommunikationen med interna och externa intressenter (inklusive myndigheter). Gå till steg "Isolera de infekterade resurserna". Om tjänsten administreras av din egen organisation, gå vidare i incidenthanteringsprocessen (gå till steg "Gör en preliminär analys").
Gör en preliminär analys. Handlar det om en incident?	Alla larm och observationer avseende informationssäkerheten leder inte till incidenthanteringsåtgärder. En del larm är så kallade falska alarm. En del larm och störningar hanteras som en del av organisationens normala operativa verksamhet. Organisationen ska definiera hur allvarlig en informationssäkerhetshändelse eller -händelsekedja ska vara för att den ska initiera incidenthanteringsprocessen. <u>Inled vid behov åtgärder för kontinuitetshantering</u> Beroende på hur allvarlig incidenten är och för att säkerställa affärsverksamhetens kontinuitet kan det vara nödvändigt att inleda undantagsförfaranden, övergå till att använda en tillfällig webbplats och vidta andra liknande åtgärder för kontinuitetshantering. Man kan även i vissa fall bli tvungen att inleda partiella återställningsåtgärder för att säkerställa affärsverksamhetens kontinuitet. I idealfallet börjar man återställa systemen först när man genom en analys av grundorsakerna till incidenten har försäkrat sig om att angriparen inte längre har tillträde till miljöerna. Med tanke på affärsverksamhetens kontinuitet kan man dock inte nödvändigtvis vänta tills utredningen är färdig, utan för att säkerställa kontinuiteten kan det hända att man blir tvungen att inleda ett partiellt återställande redan tidigare. I sådana fall finns det en risk för att systemet efter återställandet fortfarande är sårbart och att en ny incident inträffar.	Gör en preliminär analys: Undersök informationen om larmet eller någon annan indikation som du har fått och använd nödvändiga ytterligare källor för att bedöma huruvida det verkar vara fråga om en informationssäkerhetsincident. Om du bedömer att det är eller kan vara fråga om en informationssäkerhetsincident, gå vidare till följande steg i incidenthanteringsprocessen. I övriga fall ska det arbetsflöde som fastställts i respektive fall följas. Hanteringen av incidenten avslutas. Gör en bedömning av hur allvarlig situationen är och inled vid behov åtgärder för kontinuitetshantering (undantagsförfaranden, tillfälliga webbplatser och liknande). För att säkerställa affärsverksamhetens kontinuitet kan man i vissa fall bli tvungen att inleda partiella återställningsåtgärder redan innan utredningen är färdig. För att minska risken för angrepp ska det temporära återställandet i mån av möjlighet genomföras med hjälp av isolerade underhållsförfaranden (koder, enheter och liknande) i en separat infrastruktur. Följ med och bedöm situationen samt uppdatera åtgärderna under hela incidenthanteringsprocessen.

Isolera de infekterade resurserna	Genom att isolera hotet försöker man hindra angreppet från att sprida sig samt skydda informationen i systemet.	Försök isolera den infekterade resursen genom att använda molnmiljöns hanteringsverktyg. Isolerande åtgärder kan i en molnmiljö innebära att man gör till exempel följande: • Stänger koden eller åtkomsttoken (access token). • Stoppar driften av applikationen. • Begränsar driften av applikationens gränssnitt och nättrafik. • Stänger integrationsgränssnittet. • Stoppar driften av den virtuella maskinen eller den containerbaserade tjänsten. Upprätthåll en händelselogg över de genomförda åtgärderna. Av loggen ska framgå vilken åtgärd som genomförts, tidsstämpeln för den och vem som utfört åtgärden.
Behöver du hjälp med att hantera incidenten? **Informera IT-tjänsteleverantören och be om hjälp**	I utredningen av en incident kan man behöva hjälp utifrån med till exempel de tekniska åtgärderna, hanteringen av incidenten eller organiseringen av åtgärderna. Om det inte finns tillräcklig kompetens internt eller direkt hos IT-tjänsteleverantörerna ska man överväga att anlita hjälp utifrån. Det kan krävas extern kompetens för till exempel insamling av identifieringsuppgifter och utredning av hotet utifrån dem. Den externa hjälpen kan även till exempel hjälpa till att kontrollera huruvida angriparen har kommit över data som är viktig för affärsverksamheten och i så fall vilka data.	Om du bedömer att du behöver extern hjälp med hanteringen av en incident ska du **kontakta en tjänsteleverantör** som är specialiserad på hantering av incidenter. I resurserna i fotnoten hittar du finländska tjänsteleverantörer[13].
Informera interna och externa intressenter om incidenten	Vid en incident är det viktigt att centrala beslutsfattare vet vad som händer. Informationssäkerhetsincidenten kan leda till risker eller problem med tillgången till tjänster för samarbetspartner, kunder och tjänsteleverantörer.	Agera i enlighet med din organisations incidenthanteringsplan samt se till att en incidenthanteringsgrupp har tillsatts och att informationen sprids inom gruppen. Hur mycket kommunikation som behövs beror i stor utsträckning på situationen: I synnerhet om man misstänker att situationen är allvarlig är det skäl att genast informera ledningen om situationen. Informera intressenternas kontaktpersoner vid krissituationer om incidenten om ni tror att den kan påverka tillgången till deras tjänster eller äventyra säkerheten i dem. Om det funnits anslutningar från servern till andra organisationer ska även dessa informeras. På så sätt kan de göra de koder, nycklar eller certifikat som använts på den infekterade servern ogiltiga. Det är också viktigt att de kontrollerar integriteten hos sina egna data.

[13] Finländska tjänsteleverantörer finns på följande webbplatser: https://dfir.fi/; https://www.fisc.fi/fi; https://www.hansel.fi/sv/upphandlingar/tiedonhallinnan-ja-digiturvallisuuden-asiantuntija/

Gör en anmälan till Cybersäkerhetscentret och andra myndigheter	Aktörer och tjänsteleverantörer, som är kritiska med tanke på försörjningsberedskapen och som omfattas av EU:s direktiv om säkerhet i nätverks- och informationssystem (det så kallade NIS-direktivet), ska anmäla informationssäkerhetsincidenter i nätverks- och informationssystem till myndigheterna[14]. Dessutom är det alltid bra att anmäla informationssäkerhetsincidenter till Cybersäkerhetscentret, som ger organisationer stöd och råd vid incidenter. Observera att en anmälan till Cybersäkerhetscentret i regel är konfidentiell och att information om den inte skickas vidare till exempelvis polisen. Om du misstänker brott är en brottsanmälan till polisen en separat process. <u>Säkerställ tillräcklig kommunikation och informationsdelning under incidentens hela livscykel</u> Incidenthantering kräver samordnad kommunikation såväl inom organisationen som till utomstående intressenter samt myndigheter. Kommunikationsansvaren ska vara överenskomna i förväg och finnas inskrivna i incidenthanteringsplanen.	Om din organisation är en kritisk aktör med tanke på försörjningsberedskapen ska du anmäla informationssäkerhetsincidenter till den myndighet som övervakar din bransch. Det är därtill värt att alltid anmäla informationssäkerhetsincidenter till Cybersäkerhetscentret i ett så tidigt skede som möjligt.[15] Cybersäkerhetscentret kan hjälpa organisationer med i synnerhet de första insatserna och genom att erbjuda tilläggsinformation om liknande fall i Finland och internationellt. Utse en roll/roller eller en person/personer som har till uppgift att dela lägesinformation till interna och externa intressenter (inklusive myndigheter) samt hålla dem uppdaterade under incidentens hela livscykel.

[14] https://www.kyberturvallisuuskeskus.fi/sv/vara-tjanster/rapportera-en-it-sakerhetsincident-nis-skyldighet
[15] Gör en anmälan till Cybersäkerhetscentret med webblanketten på https://www.kyberturvallisuuskeskus.fi/sv/anmal, per e-post (cert@traficom.fi) eller per telefon på numret 0295 345 630 (lna/msa). Telefontjänsten är öppen vardagar kl. 9–15

5.3 Utredning av incidenten

Stegets mål	Målet med utredningen av informationssäkerhetsincidenten är att ta reda på angreppets omfattning och inverkan i organisationen. Genom en grundlig utredning säkerställs att skadliga program och eventuella bakdörrar har avlägsnats ur miljön.

Steg	Syfte	Åtgärder
Identifiera skadlig aktivitet och samla in identifieringsuppgifter	Identifieringsuppgifter samlas in för att man ska kunna kartlägga i hur stor utsträckning enheterna har infekterats och på vilket sätt stulna behörigheter har utnyttjats. Efter att ha fått fotfäste kan angriparen använda olika angreppsmetoder. Därför ska identifieringsuppgifter samlas in i stor omfattning och tecken på att de använts undersökas noggrant, så att miljön kan rensas på ett tillförlitligt sätt. Först när angriparen har körts bort från miljöerna kan återhämtningen börja på ett säkert sätt.	Identifiera skadlig aktivitet och samla in identifieringsuppgifter i så omfattande utsträckning som möjligt. Identifieringsuppgifter som ska samlas in är bland annat tidpunkten för olika händelser, till exempel när man har loggat in på servern eller när ett visst kommando har körts på servern. Det skadliga programmet kommunicerar ofta med angriparens kommandoserver. Genom att kontrollera de infekterade enheternas nättrafik eller undersöka domännamnen (DNS-loggarna) kan de käll-IP-adresser eller domännamn som angriparen använder identifieras. När de skadliga filerna identifierats kan man ta reda på deras hashvärden MD5/SHA256), med hjälp av vilka de skadliga filerna kan identifieras även på övriga enheter. Utifrån identifieringshändelser som riktats mot de infekterade enheterna och de åtgärder som utförts med användarkonton i anknytning till dessa kan man fastställa vilka koder som använts för att sprida den skadliga programvaran. Den centraliserade övervakningen av enheterna inkluderar ofta funktioner för att samla in och använda ovannämnda identifieringsuppgifter. I annat fall ska åtgärderna utföras manuellt med hjälp av en centraliserad loggserver. Om inte heller detta alternativ är möjligt ska de enskilda servrarnas och enheternas loggar undersökas.
Identifiera och rensa infekterade resurser samt byt användarkoder	Med hjälp av de insamlade identifieringsuppgifterna kan man ta reda på i hur stor omfattning angriparen har tagit sig in i organisationen. Genom att samla in identifieringsuppgifter och söka efter dem i målsystemen kan man verifiera att alla infekterade enheter, koder, nycklar och certifikat hittas och åtgärdas. Med hjälp av identifieringsuppgifterna kan man söka efter infekterade enheter, till exempel genom att använda funktionerna i den centraliserade övervakningen av enheterna, vilka ofta erbjuder möjlighet att söka efter händelser på enheterna med hjälp av olika identifikationskoder. Om organisationen även har en centraliserad logghantering kan man med hjälp av den effektivt söka efter händelser i flera olika datorer samtidigt på basis av identifikationskoderna. Det finns en risk att angriparen, efter att ha tagit sig in i en enhet, har försökt dölja sina spår genom att koppla bort insamlingen av loggar. I sådana fall är det inte nödvändigtvis möjligt att hitta alla insamlade identifieringsuppgifter i enhetens loggar. Därför är det viktigt att försöka använda ett brett spektrum av olika slags identifieringsuppgifter och händelsekällor.	Använd identifieringsuppgifterna för att identifiera alla infekterade system och de koder, nycklar och certifikat som angriparen känner till. Använd till exempel information om övervakningen och logghanteringen av terminalutrustning. Om ingen av de ovanstående lösningarna är tillgängliga ska identifikationskoderna sökas efter separat på varje enhet. För det kan man dock ännu använda olika lösningar för fjärradministration, som ofta gör det möjligt att till exempel köra PowerShell-kommandon på flera servrar samtidigt. Rensa de infekterade systemen. Byt de koder, nycklar och certifikat som angriparen känner till.

Utred incidentens omfattning, inverkan och eventuella beroenden och samband	Ofta har molnresurser anslutningar till andra system. Sådana kan vara till exempel databasanslutningar eller olika API-förfrågningar, nycklar och certifikat. Integriteten hos kombinerade system och incidentens inverkan på affärsverksamheten ska säkerställas så fort som möjligt, så att man kan få en bild av hur allvarlig situationen är.	Om tjänsten har anslutningar till andra system ska uppgifternas integritet säkerställas genom granskningar av de kombinerade systemens loggar. I utredningen ska fokus ligga på de koder, certifikat eller åtkomsttoken (access token) som integrationerna har genomförts med.
Har kritiska eller personuppgifter äventyrats? **Följ anvisningen Dataintrång**	Som en del av utredningen ska man ta reda på huruvida angriparen har kommit över viktiga uppgifter om organisationen eller eventuellt personuppgifter för kunder eller anställda. Observera att angriparen kan ha ändrat data, även om hen inte skulle ha förstört eller stulit dem. Angriparen kan även ha stulit små, men viktiga data, såsom användarkoder. I situationer där molnleverantören är personuppgiftsbiträde och incidenten även kan vara en personuppgiftsincident är leverantören skyldig att hjälpa till med att utreda situationen och fylla i anmälan.	Ta reda på huruvida de koder, certifikat eller nycklar som använts i förbindelserna även använts för att logga in från något annat ställe än servern där de är avsedda att användas. Ta reda på huruvida angriparen har kommit över och stulit uppgifter genom att övervaka loggarna för informationstjänsterna och gränssnitten. Utifrån belastningen eller de sökningar som gjorts kan du avgöra om angriparen har försökt hämta eller ändra uppgifter. Om kritiska eller personuppgifter har äventyrats, **följ Cybersäkerhetscentrets anvisning Dataintrång[16].**
Misstänker du att ett brott har begåtts? **Gör en brottsanmälan till polisen**	Rapportera incidenten till myndigheterna. Organisationen kan enligt författningar eller villkoren i cyberförsäkringen vara skyldig att anmäla incidenten. Observera att en anmälan till Cybersäkerhetscentret i regel är konfidentiell och att information om den inte skickas vidare till exempelvis polisen. En brottsanmälan ska alltid göras separat.	Om du misstänker att ett brott har begåtts ska du **göra en brottsanmälan om händelsen till polisen[17].**
Spara loggfilerna och annat bevismaterial för senare undersökning	Syftet med att samla in och spara bevis är att säkerställa en högklassig utredning av incidenten i efterhand, så att grundorsakerna till den kan klarläggas. Bevisen kan behövas i samband med en brottsanmälan och för rättegångsförhandlingar. Om organisationen har en cyberförsäkring kan även försäkringsbolaget kräva närmare uppgifter om incidenten samt bevis för en utredning.	Spara de loggfiler som innehåller viktig information med tanke på undersökningen av incidenten på en hårddisk som är isolerad från nätverket. Samla även in eventuella skadliga e-postmeddelanden och övriga meddelanden. Sträva efter att förvara bevisen, såsom kompletta skivavbilder och minnesprover, så enhetliga som möjligt. Använd en hashfunktion för att säkerställa deras integritet. Sträva efter att spara bevis på de skadliga program som upptäckts. Stor försiktighet ska iakttas vid hanteringen. En säker hantering kräver ofta yrkeskompetens. Skicka proverna till Cybersäkerhetscentret[18].
Hjälpte åtgärderna och har hotet kunnat elimineras?	Innan återställandet inleds, säkerställ att de åtgärder som genomförts har hjälpt.	Om åtgärderna hjälpte, inled återställningsprocessen i de mest kritiska systemen och tjänsterna.

[16] https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Tietomurto_SV.pdf
[17] https://poliisi.fi/sv/gor-en-brottsanmalan
[18] **https://www.kyberturvallisuuskeskus.fi/sv/aktuellt/formedla-e-post-och-prov-till-cybersakerhetscentret**

5.4 Återställande		
Stegets mål	I återställningsskedet försöker organisationen återställa affärsverksamheten till det normala så snabbt som möjligt efter att det kan göras på ett säkert sätt. Det är värt att inleda återställandet i de system som är mest kritiska med tanke på affärsverksamheten.	
Steg	**Syfte**	**Åtgärder**
Säkerställ att administratörskoderna är säkra och återställ dem	Se till att inloggningsuppgifterna för samtliga eventuellt infekterade användarkoder ändras, så att angriparen inte längre har tillträde till organisationens system med hjälp av koderna. Inloggningskraven för användarna skärps i mån av möjlighet.	Ändra lösenorden för de infekterade användarkoderna och återinför koderna. Gör på samma sätt med nycklar och certifikat. Ändra för säkerhets skull lösenorden för administratörskoderna och servicekoderna, utifall att angriparen skulle ha kommit över en del av dem. Informera användarna om de nya lösenorden antingen muntligt, per sms eller per telefon. Använd inte organisationens e-post eller snabbmeddelanden, eftersom angriparen fortfarande kan ha tillträde till dem. Säkerställ att flerfaktorsautentisering används för alla koder. Övervaka dock de koder som användes vid angreppet noggrannare efter återställandet, för den händelse att angriparen på nytt kommer över dem. Om det förblir oklart för organisationen hur angriparen kunde komma över vissa koder, överväg att skapa helt nya koder.
Skapa ersättande molnresurser	Skapa nya molnresurser genom att installera tjänsterna och applikationerna på nytt. Försök inte rensa ett infekterat system med automatiska verktyg eller antivirusprogram, eftersom de inte nödvändigtvis kan rensa systemet fullständigt.	En fördel med molnmiljöer är att återinstallationen av resurserna i allmänhet kan göras helt eller nästan helt automatiserat. Om DevOps-praxis dessutom följs kan även applikationerna och containrarna fördelas automatiskt. Det gör det betydligt snabbare att återställa arbetsbördorna, eftersom det inte finns något behov av att rensa och verifiera servrarna för återanvändning. Givetvis ska återställandet genomföras så att risken för att angreppet aktiveras på nytt är under kontroll. Det innebär bland annat att säkerställa att angriparen inte har exempelvis ändrat innehållet i containerregistret eller källkoden så att nya resurser innehåller till exempel en bakdörr.
Inled återställningsprocessen i de mest kritiska systemen	Man strävar efter att återställa data och systemen och återgå till normal verksamhet. Målet är att återställandet ska göras på ett så säkert sätt som möjligt, så att angriparen inte kan ta sig tillbaka in i systemen. Om man misstänker att angriparen har ändrat innehåll i databasen ska databasen återställas från en säkerhetskopia för att annullera angriparens ändringar, ifall det inte är möjligt att rensa data.	I molnmiljöer är det ofta så att det räcker med att återställa data, och infrastrukturtjänster, plattformar för körning av kod, containrar samt applikationskoder som körs i molnet kan installeras på nytt genom automation. Detta återställningssätt rekommenderas. Återställ vid behov även systemen såsom virtuella servrar från säkerhetskopior. Beakta även risken för att tidigare dagsspecifika (inkrementella) säkerhetskopior redan kan vara infekterade. När du återställer gamla säkerhetskopior ska du tänka på att säkerhetskopiorna kan innehålla sårbarheter som angriparen har utnyttjat vid angreppet.

	<u>Informera interna och externa intressenter om att incidenten är över</u> Meddela interna och externa intressenter (inklusive myndigheter) om att incidenten är över. Informera intressenterna (till exempel kunderna) om man varit tvungen att återställa uppgifterna till en äldre version från och med ett visst datum, så att vederbörande kan uppdatera sina uppgifter.	Man kan försöka undvika risken för ett nytt intrång under återställandet genom att återställa molntjänsterna och arbetsbördorna så att deras gränssnitt och internetanslutningar öppnas i begränsad utsträckning. Till exempel ett gränssnitt som tidigare varit öppet mot internet kan öppnas på nytt endast för att nå nödvändiga adresser eller nätverk. Använd dig av loggar för att ta reda på huruvida angriparen har ändrat poster. Om loggarna inte är tillräckligt exakta för att rensa ändringarna ska databasens uppgifter återställas från den senaste säkra säkerhetskopian. Om angriparen har stulit information ska alla lösenord i den stulna informationen ändras. Detta ska göras även om lösenorden skulle ha lagrats endast i form av lösenordshashar.
Hantera efterverkningarna av incidenten	När krisen är över och affärsfunktionerna normaliserat sig är det viktigt att börja hantera efterverkningarna av incidenten och lära sig av det inträffade för framtiden.	Hantera efterverkningarna av incidenten, identifiera nödvändiga åtgärder och uppdatera incidenthanteringsplanen.

6 Efterverkningar av incidenten

När krisen är över och affärsfunktionerna normaliserat sig är det viktigt att börja hantera efterverkningarna av angreppet och lära sig av det inträffade för framtiden. Samtidigt är det skäl att uppdatera krishanteringsplanerna utifrån de observationer som gjorts. Det är möjligt att organisationen på nytt faller offer för ett liknande angrepp om grundorsakerna till det inträffade inte kommer fram och man inte tar lärdom av händelsen.

Vid hanteringen av efterverkningarna (eng. Post-Incident Review) granskas verksamheten i krissituationen: vilka åtgärder genomfördes väl, var fanns det utrymme för förbättringar samt hur kan säkerhetsnivån och -planerna förbättras? Det är skäl att utarbeta en rapport om hanteringen av efterverkningarna som, förutom händelseförloppet, även inkluderar svar på åtminstone följande frågor:

- Grundorsaker till incidenten:
  - Vilka tekniska eller funktionsmässiga svagheter ledde till situationen?
- Det egna skyddets effektivitet:
  - Var de kontroller som användes för att upptäcka angrepp tillräckliga?
  - Orsakade angriparens handlingar några larm?
  - Hur reagerade man på larmen? Fick rätt ansvariga personer information om larmen?
- Agerande i krissituationen:
  - Följde man krisplanen? Hur användbar var den?
  - Fördelades krisgruppens ansvar mellan rätt personer?
  - Hur väl lyckades man begränsa angreppet och driva bort angriparen?
  - Hur väl lyckades krisgruppens kommunikation? Hur beaktades intressenterna?
- Återställande:
  - Hur väl lyckades man återställa kritiska uppgifter och tjänster?
- Efterverkningar:
  - Har händelseförloppet och utredningsarbetet dokumenterats?
  - Var den tekniska utredningen av incidenten tillräcklig? Har man kunnat förse till exempel myndigheterna med tillräckligt med material om angreppet?
  - Utvärdera tjänsteleverantörernas verksamhet. Var svarstiden och de avtalade tjänsterna tillräckliga för att utreda incidenten?

Efter incidenten ska organisationen uppdatera sin incidenthanteringsplan och sina mer detaljerade anvisningar för bekämpning av olika typer av avvikelser. Det rekommenderas även att organisationerna med jämna mellanrum övar på olika scenarier, så att nyttan med dem kan garanteras vid en krissituation.

Cybersäkerhetscentret önskar att företag och organisationer skulle dela med sig av de viktigaste lärdomarna som de dragit av incidenter. Med hjälp av fallrapporter kan Cybersäkerhetscentret hjälpa andra organisationer i Finland och utomlands vid utredningen av liknande fall. De lärdomar som återställandet ger bidrar till att utveckla beredskapen för alla organisationer.

Bilagor

Bilaga 1

Datainnehållet i diagrammet i bild 1 i tabellform (tillgänglig version).

Tabell 22. Typisk ansvarsfördelning i tabellform

Typ av molntjänst	Ansvarsfördelning
IaaS (Infrastructure-as-a-Service)	Kunden (engl. Customer / Tenant) är vanligtvis ansvarig för: Gränssnitt (Interface), Applikation (Application), Mjukvarustapel (Stack) och Operativsystem (Operating System) Tjänsteleverantör (engl. Provider) är vanligtvis ansvarig för: Virtualisering (Virtualisation), Kalkylering och lagring (Compute & Storage), Datornät (Networking) och Datorhall (Facility)
PaaS (Platform-as-a-Service)	Kunden (engl. Customer / Tenant) är vanligtvis ansvarig för: Gränssnitt (Interface) och Applikation (Application) Tjänsteleverantör (engl. Provider) är vanligtvis ansvarig för: Mjukvarustapel (Stack), Operativsystem (Operating System), Virtualisering (Virtualisation), Kalkylering och lagring (Compute & Storage), Datornät (Networking) och Datorhall (Facility)
SaaS (Software-as-a-Service)	Kunden (engl. Customer / Tenant) är vanligtvis ansvarig för: Gränssnitt (Interface) Tjänsteleverantör (engl. Provider) är vanligtvis ansvarig för: Applikation (Application), Mjukvarustapel (Stack), Operativsystem (Operating System), Virtualisering (Virtualisation), Kalkylering och lagring (Compute & Storage), Datornät (Networking) och Datorhall (Facility)

Bilaga 2

Datainnehållet i diagrammet i bild 2 i tabellform (tillgänglig version).

Tabell 33. Arbetsflödet för incidenthantering i en molnmiljö i tabellform

Steg	Ytterligare information eller alternativt processflöde
Omedelbara åtgärder	
Incident upptäcks i en tjänst	
Administrerar din organisation själv tjänsten?	Om inte, anmäl incidenten till molnleverantören. Tjänsteleverantören ansvarar för de tekniska åtgärderna. Följ dock aktivt utredningen av händelsen samt informera interna och externa intressenter (inklusive myndigheter) om situationen. Gå till steg "Isolera de infekterade resurserna". Om ja, gå till steg "Gör en preliminär analys".
Gör en preliminär analys. Handlar det om en incident?	Om inte, överför observationen till rätt tjänsteprocess och hantera den enligt den. Hanteringen av incidenten avslutas. Om ja, gå till steg "Isolera de infekterade resurserna".
Isolera de infekterade resurserna	För en händelselogg över de genomförda åtgärderna (inklusive genomförd åtgärd, tidsstämpel och vem som genomfört åtgärden).
Behöver du hjälp med att hantera incidenten?	Om ja, informera IT-tjänsteleverantören och be om hjälp. Om nej, gå till steg "Informera...".
Informera interna och externa intressenter om incidenten	
Gör en anmälan till Cybersäkerhetscentret och andra myndigheter.	Säkerställ tillräcklig kommunikation och informationsdelning med interna och externa intressenter (inklusive myndigheter) under incidentens hela livscykel.
Utredning av incidenten	
Identifiera skadlig aktivitet och samla in identifieringsuppgifter	
Identifiera och rensa infekterade resurser samt byt användarkoder	
Utred incidentens omfattning, inverkan och eventuella beroenden och samband	
Har kritiska eller personuppgifter äventyrats?	Om ja, följ anvisningen Dataintrång. Om inte, gå till steg "Misstänker du att ett brott har begåtts?"
Misstänker du att ett brott har begåtts?	Om ja, gör en brottsanmälan till polisen. Om inte, gå till steg "Spara loggfilerna...".
Spara loggfilerna och annat bevismaterial för senare undersökning	
Hjälpte åtgärderna och har hotet kunnat elimineras?	Om inte, gå tillbaka till steg "Identifiera och rensa infekterade resurser samt byt användarkoder". Om ja, gå till steg "Säkerställ att administratörskoderna är säkra och återställ dem".
Återställande	
Säkerställ att administratörskoderna är säkra och återställ dem	
Skapa ersättande molnresurser	
Inled återställningsprocessen i de mest kritiska systemen	Informera interna och externa intressenter om att incidenten är över.
Hantera efterverkningarna av incidenten	
(Processen avslutas)	

Bilaga 3

Datainnehållet i inforutorna i guiden i tabellform (tillgänglig version).

Tabell 4 Datainnehållet i inforutorna i guiden i tabellform

Sida	Inforutorna
Sida 3	Obs! Denna anvisning utarbetades 2023. Molntjänsternas egenskaper utvecklas i snabb takt och en del av de tekniker eller rutiner som nämns i denna anvisning är inte nödvändigtvis aktuella när du läser den. Den senaste informationen om till exempel säkerhetsegenskaperna hos en viss molnplattform finns i anvisningarna för den aktuella tjänsten. Du kan även kontrollera om det finns en nyare version av denna anvisning bland Cybersäkerhetscentrets samlade anvisningar på https://www.kyberturvallisuuskeskus.fi.
Sida 7	I molnmiljöer används ofta cloud security posture management (CSPM)-produkter, som är lösningar för hantering av moln-resursernas informationssäkerhetskonfigurationer som skräddarsytts för molnplattformen. Produkterna kan inkludera även observation av sårbarheter i och hot mot molnets arbetsbördor. Till exempel Azure Defender for Cloud och AWS Security Hub är sådana avgiftsbelagda produkter. Kunden i molnet kan välja att istället för dessa delvis utnyttja produkter som licensierats för datacentermiljön, till exempel sårbarhetsskannrar och EDR-produkter. Det är viktigt att känna till att när det handlar om IaaS- och PaaS-plattformar är det kunden som ansvarar för anskaffningen och ibruktagandet av samt hanteringen av observationer i dessa.
Sida 8	Vid aktivitet i exempelvis molntjänsten Azure skapas loggar av typen resource log över åtgärder på administrationsnivå. Av loggarna framgår de åtgärder som anknyter till tjänsternas livscykel, såsom skapande och konfigurationsändringar. Över den egentliga användningen av resurser, till exempel användning av databasen, lagringstjänsten eller Azure Key vault-hemligheter, skapas däremot inga loggar av typen activity log automatiskt, utan det är kunden som ansvarar för att ta dem i bruk och hantera deras livscykel.
Sida 11	Molntjänsternas egenskaper utvidgas och blir mångsidigare hela tiden. I allmänhet försämrar inte tjänsteproducenterna egenskaperna ur informationssäkerhetsperspektiv. Ibland kan det oväntat bli så. Å andra sidan kan tjänsternas informationssäkerhetsmöjligheter även förbättras med tiden. Därför är det viktigt att säkerställa att en kompetent personal följer tjänsternas utveckling och kan bedöma hur föränderliga egenskaper kan utnyttjas effektivt och säkert.
Sida 12	Se till att dokumentation som eventuellt behövs vid en incident finns tillgänglig även i situationer där dokumentationens primära lagringsplats, såsom en webbtjänst, inte är tillgänglig.
Sida 13	Kapitlet behandlar de tekniska åtgärderna på en övergripande nivå. Eftersom det finns olika slags molntjänster, är det viktigt att du beträffande alla tekniska åtgärder tar del av molnleverantörens egna anvisningar i ämnet för att få aktuell information.
Sida 14	Ett ovarsamt ibruktagande av lagringstjänster i molnet (till exempel AWS S3 eller Azure storage account) genom att göra standardinställningarna mindre strikta kan leda till en situation, där en angripare kan hitta alla lagrade data på en webbadress på internet. En sådan incident skulle kunna inträffa till exempel om man följer en färdig mall eller anvisning på nätet utan att helt och fullt förstå alla instruktioner och inställningar som den innehåller.
Sida 16	Se även till att de testkonton och resurstester som gjorts i molnmiljön är korrekt skyddade. Användningen av en resurs avsedd för försök eller övning kan utvidgas med tiden, så att den blir en etablerad del av organisationens IT-helhet. Om informations-säkerheten inte har beaktats när resursen skapas finns det en risk för att resursens skydd är bristfälliga. I molnmiljöer är det bra att ta i bruk standardiserade riktlinjer (eng. policy) och modeller (eng. template), med hjälp av vilka man kan styra de standardiserade inställningarna för organisationens molnresurser och säkerställa att de uppfyller organisationens krav.
Sida 17	Koder avsedda för nödanvändning ska alltid omfattas av automatiserad övervakning så att användningen av dem ger företagets nyckelpersoner ett larm.
Sida 19	Till exempel en mikrotjänstmiljö som baserar sig på containrar är ofta utspridd så att övervakningen av viktiga händelser avseende informationssäkerheten förutsätter noggrann planering. I sådana fall ska man säkerställa enhetlig loggningspraxis och automatiserad logghantering för att upptäcka händelser som avviker från det normala.

Sida 24	Obs! Beträffande samtliga ovanstående larm och informations-säkerhetsteknologier är det viktigt att säkerställa att man i organisationen har kommit överens om vilket team eller vilken roll som ansvarar för att följa upp larm och reagera på dem. Inte ens det bästa verktyget är till hjälp vid en incident om man inte reagerar på larm som kräver manuellt arbete.

Transport- och kommunikationsverket Traficom
Cybersäkerhetscentret
PB 320, 00059 TRAFICOM
tfn 029 534 5000

kyberturvallisuuskeskus.fi

ISBN 978-952-311-879-9
ISSN 2669-8757 (e-publikation)

FÖRSÖRJNINGS-
BEREDSKAPCENTRALEN

TRAFICOM
Transport- och kommunikationsverket
Cybersäkerhetscentret