Del 1 – Roller, ansvar och nuvarande situation

Acme Data Corp har ett tydligt upplägg för roller och ansvar, men i praktiken finns det vissa luckor som kan skapa risker. Finance ansvarar för ekonomiska dokument och ska endast ha åtkomst till det som verkligen behövs. HR hanterar personaldata och ser till att nya medarbetare får rätt åtkomst och att gamla konton stängs av när någon slutar. IT-administratörer sköter driften av system och säkerheten runt dem, medan managers godkänner åtkomst och ser till att teamen följer reglerna. Interns ska enbart använda de resurser som krävs för deras arbetsuppgifter och rapportera misstänkt aktivitet.

Företagets mest skyddsvärda resurser är ekonomiska dokument och dataarkiv, IT:s känsliga mappar samt själva IAM-systemet. Problemet är att åtkomst ibland inte matchar dessa principer. Till exempel finns Common-mappen där alla kan ändra filer, vilket ökar risken för oavsiktliga ändringar, borttagning av information eller spridning av skadlig kod.

Brister i RBAC- och PAM-designen påverkar hela miljön. Om roller inte är tydligt definierade eller om privilegier inte hanteras korrekt kan en användare som endast behöver läsa en fil plötsligt få rättigheten att ändra eller radera viktiga dokument. Exempelvis kan managers höja sina egna rättigheter på Finance-gruppen på grund av felaktig delegation, eller interns få Modify-rättigheter till filer de inte borde röra. Om PAM-lösningar inte används för att begränsa högprioriterade konton temporärt eller övervaka deras aktiviteter riskerar hela RBAC-strukturen att undergrävas.

Dessa brister gör det svårare att upprätthålla IAM-principerna Least Privilege, Separation of Duties och Need-to-Know, som både ISO 27001, NIST och CIS framhåller som grundläggande för säker identitetshantering. De största hoten kommer inifrån: anställda kan ha mer åtkomst än de behöver, interns kan råka ändra filer de inte borde, och tidigare anställda kan fortfarande logga in om offboarding inte hanteras korrekt. Dessutom är autentiseringen för vissa grupper otillräcklig, vilket kan öppna för attacker som lösenord gissning. Sammantaget visar detta att IAM-principer inte alltid efterlevs i praktiken, vilket skapar risk för både misstag och medvetna säkerhetsincidenter.

För att minska riskerna behöver företaget både förbättrade rutiner och ökad medvetenhet om hur RBAC och PAM fungerar.

Del 2 – Incidenter

Under den interna granskningen identifierades flera incidenter som tydligt visar brister i Acme Data Corps IAM-miljö.

1. Interns med Modify-rättigheter på Finance-Reports
Gruppen Interns hade av misstag Modify-rättigheter på Finance-Reports, vilket ledde till att en intern användare ändrade en ekonomisk fil. Rollen Interns borde normalt enbart ha Read-access eller tillgång till kopior för övning. Principerna om Least Privilege och Need-to-Know bröts tydligt. Incidenten uppstod eftersom felaktiga rättigheter delegerats av IT eller en manager, och den interna

användaren tillfälligt placerats i Finance utan korrekt auktorisation. Konsekvenserna kan inkludera dataförlust, korruption eller dataläckage samt potentiella brott mot GDPR. Relevanta loggar för utredning inkluderar ändringar av Interns-gruppen, användarens rolltilldelning och fil åtkomstloggar i Finance-Reports. Från ett IAM-perspektiv visar detta problem bristande kontroll över privilegier, vilket underminerar hela RBAC-modellen och bryter även mot andra kända principer såsom Least Common mechanism, Fail-safe defaults.

2. Tidigare HR-anställd som loggar in efter offboarding

Två veckor efter sin uppsägning loggade en tidigare HR-anställd in på sitt konto, trots att det borde ha inaktiverats vid offboarding. Kontot hade Read/Write-åtkomst till Common-mappen och läsrättigheter till Archive-resurser, vilket möjliggjorde åtkomst till känslig information. Incidenten involverade HR, IT och användarens manager och bröt mot principen om korrekt livscykelhantering och kontohantering, eftersom HR initierade offboarding men ifall som denna så bör HR manager initiera offboarding och IT genomför den tekniska avaktiveringen. Orsakerna kan vara glömd offboarding, bristande tekniskt stöd eller ineffektiv kommunikation. Konsekvenser inkluderar möjlig manipulation av data, sabotage, insiderbrott eller spridning av malware. Relevanta loggar är inloggningshistorik, filåtkomst och ändringar via kontot. Ur IAM-perspektiv visar detta att korrekt livscykelhantering är avgörande för att upprätthålla säkerhet och efterlevnad enligt ISO 27001 och GDPR.

3. Brute force mot Finance-konto

Ett Finance-konto utsattes för 72 misslyckade inloggningsförsök mellan 02:00 och 03:00, vilket indikerar ett brute force-angrepp. Kontot är attraktivt eftersom det har åtkomst till finansiella dokument och Common-mappen. Bristen på konto spärrar, svag lösenordspolicy och frånvaro av obligatorisk MFA underlättade attacken. Finanskonton borde inte ha access utanför arbetstid och enligt Complete mediation principen bör alla åtkomstförsök kontrolleras. Konsekvenserna inkluderar risk för kompromettering av känsliga dokument om kontot tas över. Event Viewer och Active Directory-loggar är viktiga för att verifiera aktivitet och upptäcka eventuella ändringar. Ur IAM-perspektiv visar detta att bristande autentisering utsätter hela miljön för allvarliga risker.

4. IT-Admin loggar in från annat land under semester

En IT-Admin med hög privilegie nivå loggade in från ett annat land trots att personen var på semester. Incidenten bröt mot principerna Need-to-Know och Strong Authentication. Orsaken var avsaknad av geografiska restriktioner på inloggning och larm för ovanlig aktivitet. Konsekvenserna inkluderar risk för obehörig åtkomst, manipulation av kritiska system. För utredning krävs granskning av inloggningsloggar, sessionstiden och geografisk plats. Ur IAM-perspektiv visar detta behovet av striktare autentiseringskontroller och övervakning för hög privilegierade konton.

5. Excel-fil med kund- och personuppgifter i Common-mappen

En Excel-fil med känsliga kunduppgifter placerades i Common-mappen, där alla anställda har Modify-rättigheter. Detta innebar att interns, managers och andra som normalt inte ska hantera data kunde läsa, ändra eller radera filen. Filen hamnade där troligen av misstag från Finance eller HR. Incidenten bröt mot Need-to-know och Least Privilege, samt strider mot GDPR, ISO 27001 och NIST:s riktlinjer. Loggar över filåtkomst och ändringar kan visa vilka användare som har interagerat med filen. Ur IAM-perspektiv illustrerar detta brister i RBAC- och PAM-kontroller som ökar risken för dataläckage och oavsiktliga fel.

6. Manager höjer sina egna rättigheter

Vid revisionen upptäcktes att en manager kunde lägga till sig själv i Finance-gruppen på grund av felaktig delegation i AD, vilket gav full åtkomst till Finance-Docs. Managers ska normalt enbart ha Read-access, så detta bröt mot principerna Least Privilege, Need-to-Know och Separation of Duties. Loggar visar grupp ändringen och efterföljande filåtkomst. Orsaken var bristande kontroll över delegation och RBAC-design. Incidenten underminerar hela IAM-strukturen genom att tillåta obehörig privilegiehöjning, vilket kan leda till dataläckage eller insiderbrott.

Del 3 – Riskanalys

Analysen av de identifierade incidenterna visar att Acme Data Corps IAM-miljö har flera övergripande brister som skapar betydande risker för organisationen. För det första framgår att privilegie-kontrollen inte alltid fungerar som avsett. Felaktig RBAC- och PAM-design gör att användare kan få åtkomst till resurser de inte behöver, vilket ökar risken för oavsiktlig manipulation, dataläckage eller insider-attacker. Principerna om *Least Privilege* och *Separation of Duties* följs inte konsekvent, vilket särskilt framgår i situationer där managers kan höja sina egna privilegier eller interns får Modify-rättigheter till känsliga filer.

Livscykelhanteringen är en annan tydlig riskfaktor. Offboarding-processen är inte tillräckligt automatiserad eller strikt kontrollerad, vilket innebär att tidigare anställda kan behålla åtkomst till kritiska system och data. Bristande kommunikation mellan HR och IT förstärker denna sårbarhet och skapar möjligheter för obehörig åtkomst, vilket kan utnyttjas både av interna och externa aktörer.

Säkerheten kring autentisering är också otillräcklig. Nuvarande system för inloggning bygger på lösenord som inte alltid är starka, och MFA är inte obligatoriskt för alla användare. Avsaknaden av konto låsningar efter upprepade felaktiga inloggningsförsök gör organisationen sårbar för brute force-attacker och konto kapningar, särskilt mot hög privilegierade konton med tillgång till ekonomiska och känsliga filer.

Vidare har organisationen brister i dataskydd och åtkomstkontroll. Känslig information, såsom kunddata, placeras i gemensamma mappar där alla anställda har Modify-rättigheter. Brist på tekniska restriktioner och tydlig dataklassificering medför risk för oavsiktlig åtkomst, felaktig ändring eller radering av information och potentiella brott mot GDPR. Bristen på aktiv övervakning och loggning förstärker dessa risker, eftersom det försvårar upptäckt av ovanlig aktivitet eller otillåten åtkomst vilket innebär att incidenter bara upptäcks i efterhand.

Slutligen visar incidenterna att interna hot och mänskliga fel utgör en betydande risk. Organisationen är utsatt för både misstag och medvetna handlingar från användare som har för mycket åtkomst, och bristande övervakning av privilegierade konton gör det möjligt att utföra handlingar som kan påverka företagets ekonomi, data eller rykte negativt. Sammantaget visar analysen att IAM-miljön har höga risknivåer för kritiska system och känslig information, vilket understryker behovet av en övergripande förbättring av processer, tekniska kontroller och organisatoriska rutiner.

Del 4 – Förbättringar och strategisk uppföljning

För att stärka IAM-säkerheten hos Acme Data Corp är det viktigt att se förbättringarna i ett övergripande strategiskt sammanhang. Åtgärderna bör inte bara lösa enskilda problem utan ingå i en långsiktig plan där IAM-processer kontinuerligt följs upp och utvärderas. Regelbunden översyn av privilegier, autentisering, livscykelhantering och loggning säkerställer att systemet anpassas till förändringar i verksamheten och att brister upptäcks innan de leder till incidenter.

Rättigheterna till känsliga mappar, som Finance-Reports, bör begränsas enligt need to know så att endast dem som verkligen behöver åtkomst kan ändra filer. Interns kan exempelvis få en kopia av filerna eller enbart läsa dem, vilket förhindrar oavsiktliga ändringar. Managers som behöver åtkomst kan ges temporär, tidsbegränsad rättighet som automatiskt tas bort. Känsliga filer, som kunduppgifter, bör flyttas från gemensamma mappar till skyddade mappar med tydligt definierad åtkomst för att skydda data enligt regelverk som GDPR.

För en stark autentisering, bör man implementera tvåstegsverifiering för alla anställda, samt automatiska blockeringar och meddelanden vid ovanliga inloggningar. Lösenordspolicyn kan förbättras med längre, mer komplexa lösenord och konto låsning vid flera felaktiga försök, vilket förhindrar brute force-attacker. Enligt principen least Privilege bör en IT-administratör som är på semester inte ha åtkomst till systemet då personen inte har arbetsuppgifter under semestern. I linje med PAM bör systemet automatiskt flagga inloggningar från okända IP-adresser eller ovanliga geografiska platser. Hög privilegierad åtkomst bör dessutom godkännas av en oberoende person och begränsas till en viss tidsperiod istället för att vara permanent. Denna lösning skulle ha förhindrat inloggningen från ett annat land, minskat risken för felaktig användning av hög privilegierade konton och stärkt skyddet mot lateral movement om någon skulle få tillgång till adminkontot.

Offboarding måste automatiseras så att konton stängs samma dag som anställningen avslutas, med automatisk signalering från HR till IT och påminnelser vid avvikelser. Loggning och övervakning bör förbättras så att ovanliga aktiviteter genererar automatiskt larm till IT eller säkerhetsteam.

Ytterligare säkerhetsprinciper som är applicerbara för Acme Data Corp skulle kunna vara Fail-safe defaults som innebär inga privilegier som standard, detta omfattar tillgång till arkivet för alla anställda och Modify rights till common foldern

Genom att kombinera dessa åtgärder blir IAM-processerna tydliga, automatiserade och mer säkra, vilket kraftigt minskar riskerna för dataläckage, insider threat och oavsiktliga fel.