

Identifiera informationssäkerhetsrisker – exempel och stöd

Om detta dokument

Det här dokumentet är ett stöd när ni genomför er riskanalys för informationssäkerhet. Syftet är att ge konkreta exempel på de typer av risker som ofta uppkommer för att underlätta diskussionen och minska risken för att viktiga riskområden missas.

Detta dokument ersätter inte er egen analys. Varje verksamhet har sina specifika förutsättningar och det är ni som bäst känner er miljö. Använd exemplen som utgångspunkt och inspiration, inte som en färdig checklista att kryssa av.

Hur ni använder dokumentet

- Gå igenom de risker som är relevant för er analys.
- Diskutera varje exempel: Kan detta hända oss? Har det hänt tidigare?
- Bedöm sannolikhet och konsekvens enligt den modellen som finns i metodstödet för riskhantering av information.
- Lägg till egna risker med hjälp av triggerfrågorna i slutet av dokumentet.
- Dokumentera riskerna och bedömningarna i riskanalysmallen.

Tre grundläggande skyddsaspekter

Informationssäkerhetsrisker kopplas till tre skyddsaspekter:

konfidentialitet, riktighet och tillgänglighet. Detta dokumentet är organiserat efter dessa aspekter.

Tillgänglighetsrisker

Risker som kan göra att information eller system inte är tillgängliga när de behövs.

Risk	Exempelscenario	Möjliga konsekvenser
Driftstopp i kritiska system	En server havererar eller ett strömbavbrott slår ut ett verksamhetskritiskt IT-system utan att backup-rutiner fungerar.	Verksamheten kan inte utföra sina uppdrag under avbrottstiden. Tjänster och ärenden fördröjs.
Ransomware angrepp	Skadlig kod krypterar filer och system. Verksamheten kan inte komma åt sin information förrän lösen betalas eller backuper används.	Verksamheten kan inte utföra sina uppdrag, potentiell dataförlust, höga återställningskostnader och allvarlig förtroendeskada.
Bristfälliga eller otestade backuper	Backuper tas men testas aldrig. Vid ett systemhaveri visar det sig att backuperna är korrupta eller ofullständiga.	Information kan inte återställas. Data från veckor eller månader kan gå förlorade permanent.
Nätverksstörningar	Internet- eller nätverksavbrott hos leverantör hindrar medarbetare från att nå molntjänster eller kommunicera digitalt.	Arbetsprocesser stannar upp. Tidskritiska uppgifter kan inte utföras.
Beroende av enstaka leverantör	En extern systemleverantör går i konkurs, har driftproblem eller säger upp avtalet med kort varsel.	Verksamheten förlorar tillgång till system och information utan möjlighet till snabb övergång.
Förlust av nyckelkompetens	En eller ett fåtal medarbetare sitter på kritisk kunskap om system och processer. Vid sjukdom eller avslut finns ingen som tar över.	Systemadministration, behörighetshantering eller processer kan inte upprätthållas.

Konfidentialitetsrisker

Risker där information kan nå obehöriga (oavsett om det sker avsiktligt eller av misstag).

Risk	Exempelscenario	Möjliga konsekvenser
Felskickade e-postmeddelanden	En medarbetare skickar ett e-postmeddelande med känsliga personuppgifter eller annan skyddsvärd information till fel mottagare.	Incident som måste anmälas till tillsynsmyndighet. Förtroendeskada, risk för juridiska konsekvenser.
Obehörig åtkomst via kvarglömda behörigheter	En tidigare anställd eller konsult har kvar sina inloggningsuppgifter månader efter att uppdraget avslutades.	Obehörig person kan komma åt känsliga uppgifter, göra ändringar eller ta ut information.
Nätfiske (phishing)	En medarbetare klickar på en länk i ett falskt e-postmeddelande och anger sina inloggningsuppgifter på en fejkad inloggningssida.	Angripare får tillgång till konton och system. Kan leda till dataintrång, spridning av skadlig kod eller ekonomiska konsekvenser.
Skugg-IT och otillåtna molntjänster	Medarbetare laddar upp arbetsrelaterade filer i privata molntjänster (t.ex. Dropbox, privat Google Drive) för att göra jobbet smidigare.	Känslig information lagras utanför kommunens kontroll utan rätt skyddsnivå eller avtal.
Osäker hantering av bärbara enheter	En bärbar dator eller ett USB-minne med känslig information försvinner eller stjäls utan att enheten är krypterad.	Obehöriga kan läsa all information på enheten. Incident som eventuellt behöver rapporteras till tillsynsmyndighet. Påverkan på liv och hälsa, verksamhet, förtroende.
Obehörig insyn i utskrifter och skärmar	Känsliga dokument hämtas inte omedelbart vid skrivaren eller skärmar med känslig information lämnas olästa i öppna miljöer.	Obehöriga personer kan se känslig information. Oavsiktlig exponering av personuppgifter eller verksamhetskritisk information.
Bristfällig åtkomstkontroll i system	Medarbetare har bredare behörigheter än vad arbetsuppgifterna kräver.	Ökad risk för obehörig åtkomst, missbruk och exponering.

Riktighetsrisker

Risker som hotar att information är korrekt och tillförlitlig. Ofta svårare att upptäcka och kan ha stor påverkan på t.ex. beslutsfattande.

Risk	Exempelscenario	Möjliga konsekvenser
Felaktig manuell inmatning	Medarbetare för in uppgifter manuellt i ett system utan automatisk validering. Fel sprids vidare i processer.	Felaktiga beslut fattas baserat på felaktiga data. Kan leda till ekonomiska förluster, felbehandling eller rättsliga problem.
Manipulation av information	En intern eller extern aktör ändrar uppgifter i ett system avsiktligt eller av misstag utan att ändringen loggas eller märks.	Verksamheten fattar beslut på en falsk grund. Svårt att i efterhand identifiera vad som är korrekt.
Felaktig synkronisering mellan system	Två system som delar information synkroniseras felaktigt, t.ex. vid en uppdatering eller integration, vilket skapar motstridiga uppgifter.	Olika delar av verksamheten arbetar med olika versioner av sanningen. Fel i rapporter och ärendehantering.
Bristfällig versionshantering av dokument	Medarbetare arbetar i olika versioner av samma dokument utan tydlig märkning. Gamla eller felaktiga versioner används av misstag.	Felaktiga beslut, inkonsekventa rutiner, risk för att gammal eller felaktig information sprids externt.
Otillräcklig loggning och spårbarhet	Systemet loggar inte vem som gjort vad och när. Det går inte att i efterhand utreda vad som hänt vid ett fel eller incident.	Incidenter kan inte utredas korrekt. Svårt att uppfylla rättsliga krav på spårbarhet.

Triggerfrågor

Följande frågor är till för att ni ska hitta risker som inte finns med i katalogen ovan. Diskutera dem i grupp och dokumentera alla potentiella risker i mallen.

1. Vilken information hanteras i systemet/processen och hur känslig är den? Vad händer om den röjs för obehöriga?
2. Vad händer om informationen är felaktig eller inaktuell. Vilka beslut eller åtgärder kan gå fel till följd av det?
3. Vad händer om systemet inte går att nå under en dag eller en vecka, kan verksamheten ändå genomföra sitt uppdrag?
4. Finns det information som inte får försvinna, ändras eller vara otillgänglig utan att det märks?
5. Är systemet eller processen beroende av att information från ett annat system är korrekt och uppdaterad?
6. Vilka externa parter har tillgång till eller påverkar informationen?
7. Finns det moment där medarbetare hanterar information manuellt och vad händer om de gör fel?
8. Vet alla som hanterar systemet eller processen vad de får och inte får göra med informationen?

Viktigt att komma ihåg!

- Riskkatalogen är ett stöd, inte en checklista. Syftet är att väcka tankar och diskussion.
- Det är bättre att identifiera för många risker och sedan prioritera bort de minst allvarliga än att missa viktiga risker.
- Det finns inga självklara svar. Samma risk kan vara stor i en verksamhet och liten i en annan. Det är ni som känner er miljö bäst.
- Riskbilden förändras. Nya system, processer eller omvärldsförändringar kan skapa nya risker. Se över er analys minst en gång per år.