Riktlinjer 01/2021

om exempel på anmälan av personuppgiftsincidenter

Antagna den 14 december 2021

Version 2.0

Translations proofread by EDPB Members.
This language version has not yet been proofread.

Versionshistorik

Version 2.0	14.12.2021	Antagande av riktlinjerna efter offentligt samråd
Version 1.0	14.1.2021	Antagande av riktlinjerna inför offentligt samråd

Innehållsförteckning

1 INLEDNING 5

2 UTPRESSNINGSATTACK 8

2.1 FALL nr 01: Utpressningsattack med ordentlig säkerhetskopiering och utan exfiltrering 8

2.1.1 FALL nr 01 – Tidigare åtgärder och riskbedömning 8

2.1.2 FALL nr 01 – Lindring och skyldigheter 9

2.2 FALL nr 02: Utpressningsattack utan ordentlig säkerhetskopiering 10

2.2.1 FALL nr 02 – Tidigare åtgärder och riskbedömning 10

2.2.2 FALL nr 02 – Lindring och skyldigheter 11

2.3 FALL nr 03: Utpressningsattack med säkerhetskopiering och utan exfiltrering på ett sjukhus 12

2.3.1 FALL nr 03 – Tidigare åtgärder och riskbedömning 12

2.3.2 FALL nr 03 – Lindring och skyldigheter 13

2.4 FALL nr 04: Utpressningsattack utan säkerhetskopiering och med exfiltrering 13

2.4.1 FALL nr 04 – Tidigare åtgärder och riskbedömning 13

2.4.2 FALL nr 04 – Lindring och skyldigheter 14

2.5 Organisatoriska och tekniska åtgärder för att förebygga/mildra effekterna av utpressningsattacker 14

3 DATAEXFILTRERINGSATTACKER 16

3.1 FALL nr 05: Exfiltrering av jobbansökningsuppgifter från en webbplats 16

3.1.1 FALL nr 05 – Tidigare åtgärder och riskbedömning 16

3.1.2 FALL nr 05 – Lindring och skyldigheter 17

3.2 FALL nr 06: Exfiltrering av ett hashat lösenord från en webbplats 17

3.2.1 FALL nr 06 – Tidigare åtgärder och riskbedömning 17

3.2.2 FALL nr 06 – Lindring och skyldigheter 18

3.3 FALL nr 07: Stulen inloggningsattack på en bankwebbplats 18

3.3.1 FALL nr 07 – Tidigare åtgärder och riskbedömning 19

3.3.2 FALL nr 07 – Lindring och skyldigheter 19

3.4 Organisatoriska och tekniska åtgärder för att förebygga/mildra effekterna av hackerattacker 20

4 INTERNA RISKER SOM ORSAKAS AV MÄNNISKOR 21

4.1 FALL nr 08: Exfiltrering av affärsuppgifter av en anställd 21

4.1.1 FALL nr 08 – Tidigare åtgärder och riskbedömning 21

4.1.2 FALL nr 08 – Lindring och skyldigheter 22

4.2 FALL nr 09: Oavsiktlig överföring av uppgifter till en betrodd tredje part 23

4.2.1 FALL nr 09 – Tidigare åtgärder och riskbedömning 23

4.2.2 FALL nr 09 – Lindring och skyldigheter 23

4.3 Organisatoriska och tekniska åtgärder för att förebygga/mildra effekterna av interna mänskliga riskkällor 23
5 BORTTAPPADE ELLER STULNA ENHETER OCH PAPPERSDOKUMENT 24
5.1 FALL nr 10: Stulet material med krypterade personuppgifter 25
5.1.1 FALL nr 10 – Tidigare åtgärder och riskbedömning 25
5.1.2 FALL nr 10 – Lindring och skyldigheter 25
5.2 FALL nr 11: Stulet material med okrypterade personuppgifter 26
5.2.1 FALL nr 11 – Tidigare åtgärder och riskbedömning 26
5.2.2 FALL nr 11 – Lindring och skyldigheter 26
5.3 FALL nr 12: Stulna pappersfiler med känsliga uppgifter 26
5.3.1 FALL nr 12 – Tidigare åtgärder och riskbedömning 27
5.3.2 FALL nr 12 – Lindring och skyldigheter 27
5.4 Organisatoriska och tekniska åtgärder för att förebygga/mildra effekterna av förlust eller stöld av enheter 27
6 FEL POST ELLER MEJL 28
6.1 FALL nr 13: Postfel 28
6.1.1 FALL nr 13 – Tidigare åtgärder och riskbedömning 28
6.1.2 FALL nr 13 – Lindring och skyldigheter 29
6.2 FALL nr 14: Mycket konfidentiella personuppgifter som av misstag skickas per e-post 29
6.2.1 FALL nr 14 – Tidigare åtgärder och riskbedömning 29
6.2.2 FALL nr 14 – Lindring och skyldigheter 29
6.3 FALL nr 15: Personuppgifter som av misstag skickas per e-post 29
6.3.1 FALL nr 15 – Tidigare åtgärder och riskbedömning 30
6.3.2 FALL nr 15 – Lindring och skyldigheter 30
6.4 FALL nr 16: Postfel 30
6.4.1 FALL nr 16 – Tidigare åtgärder och riskbedömning 31
6.4.2 FALL nr 16 – Lindring och skyldigheter 31
6.5 Organisatoriska och tekniska åtgärder för att förebygga/mildra effekterna av postfel 31
7 Andra fall – Social manipulering 32
7.1 FALL nr 17: Identitetsstöld 32
7.1.1 FALL nr 17 – Riskbedömning, lindring och skyldigheter 32
7.2 FALL nr 18: E-postexfiltrering 33
7.2.1 FALL nr 18 – Riskbedömning, lindring och skyldigheter 33

Europeiska dataskyddsstyrelsen har antagit följande riktlinjer

med beaktande av artikel 70.1 e i Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (*dataskyddsförordningen*),

med beaktande av EES-avtalet, särskilt bilaga XI och protokoll 37, ändrat genom gemensamma EES-kommitténs beslut nr 154/2018 av den 6 juli 2018[1],

med beaktande av artiklarna 12 och 22 i arbetsordningen,

med beaktande av meddelandet från kommissionen till Europaparlamentet och rådet *Dataskydd som en pelare för medborgarnas egenmakt och EU:s strategi för den digitala övergången – tillämpning av den allmänna dataskyddsförordningen under två års tid*[2].

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

1 INLEDNING

1. Genom dataskyddsförordningen införs i vissa fall ett krav på att en personuppgiftsincident ska anmälas till den behöriga nationella tillsynsmyndigheten och meddelas de personer vars personuppgifter har påverkats av incidenten (artiklarna 33 och 34).

2. Artikel 29-arbetsgruppen utarbetade redan i oktober 2017 *allmänna* riktlinjer om anmälan av uppgiftsincidenter och analyserade de relevanta avsnitten i dataskyddsförordningen (*Riktlinjer om anmälan av personuppgiftsincidenter enligt förordning (EU) 2016/679*, WP250) (*riktlinjerna WP250*[3]). På grund av riktlinjernas art och tidpunkt beskrev de dock inte alla praktiska frågor tillräckligt utförligt. Därför har det uppstått ett behov av *praktiskt inriktade, fallbaserade* riktlinjer som utnyttjar tillsynsmyndigheternas erfarenheter sedan dataskyddsförordningen började gälla.

3. Detta dokument ska komplettera riktlinjerna WP250 och återspeglar de gemensamma erfarenheterna för tillsynsmyndigheterna i EES sedan dataskyddsförordningen började tillämpas. Syftet är att göra det lättare för personuppgiftsansvariga att besluta om hur de ska hantera uppgiftsincidenter och vilka faktorer som ska beaktas under riskbedömningen.

[1] Hänvisningar till ”medlemsstater” i detta dokument bör förstås som hänvisningar till ”medlemsstater i EES”.

[2] COM(2020) 264 final av den 24 juni 2020.

[3] Artikel 29-arbetsgruppen, WP250 rev.1, 6.2.2018, *Riktlinjer om anmälan av personuppgiftsincidenter enligt förordning (EU) 2016/679* – godkända av Europeiska dataskyddsstyrelsen (EDPB), https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052.

4. För att hantera en incident måste den personuppgiftsansvarige och personuppgiftsbiträdet först kunna fastställa en incident. I dataskyddsförordningen definieras en personuppgiftsincident i artikel 4.12 som ”en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats”.

5. I sitt yttrande 3/2014 om personuppgiftsbrott[4] och i sina riktlinjer WP250 förklarade artikel 29-arbetsgruppen att incidenter kan kategoriseras utifrån följande tre välkända informationssäkerhetsprinciper:

- ”Konfidentialitetsbrott” – vid obehörigt eller oavsiktligt röjande av eller åtkomst till personuppgifter.
- ”Integritetsbrott” – vid obehörig eller oavsiktlig ändring av personuppgifter.
- ”Tillgänglighetsbrott” – vid obehörig eller oavsiktlig förlust av åtkomst till, eller förstöring av, personuppgifter[5].

6. En incident kan potentiellt få många olika allvarliga negativa effekter för enskilda personer och kan leda till fysisk, materiell eller immateriell skada. I dataskyddsförordningen förklaras att detta kan inbegripa förlust av kontrollen över de egna personuppgifterna eller till begränsning av deras rättigheter, diskriminering, identitetsstöld eller identitetsbedrägeri, ekonomisk förlust, obehörigt hävande av pseudonymisering, skadat anseende och förlust av konfidentialitet när det gäller personuppgifter som omfattas av tystnadsplikt. Dessa personer kan även drabbas av andra betydande ekonomiska eller sociala nackdelar. En av den personuppgiftsansvariges viktigaste skyldigheter är att utvärdera dessa risker för de registrerades rättigheter och friheter och vidta lämpliga tekniska och organisatoriska åtgärder för att bemöta dem.

7. Därför ska den personuppgiftsansvarige enligt dataskyddsförordningen

- dokumentera alla personuppgiftsincidenter, inbegripet omständigheterna kring personuppgiftsincidenten, dess effekter och de korrigerande åtgärder som vidtagits[6],
- anmäla personuppgiftsincidenten till tillsynsmyndigheten, såvida det inte är osannolikt att incidenten medför en risk för fysiska personers rättigheter och friheter[7],
- informera den registrerade om personuppgiftsincidenten, om incidenten sannolikt leder till en hög risk för fysiska personers rättigheter och friheter[8].

8. Uppgiftsincidenter är problem i sig själva, men kan också vara symtom på ett sårbart, eventuellt föråldrat datasäkerhetssystem. De kan också tyda på brister i systemet som måste åtgärdas. Det är i allmänhet alltid bättre att förhindra uppgiftsincidenter genom att förbereda sig i förväg, eftersom flera konsekvenser av

---

[4] Artikel 29-arbetsgruppen, WP213, *Opinion 03/2014 on Personal Data Breach* (inte översatt till svenska), 25.3.2014, s. 5, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm#maincontentSec4.

[5] Se riktlinjerna WP250, s. 8. – Det måste beaktas att en uppgiftsincident kan beröra antingen en kategori eller flera kategorier samtidigt eller tillsammans.

[6] Artikel 33.5 i dataskyddsförordningen.

[7] Artikel 33.1 i dataskyddsförordningen.

[8] Artikel 34.1 i dataskyddsförordningen.

dem till sin natur är oåterkalleliga. Innan en personuppgiftsansvarig *till fullo* kan bedöma den risk som uppstår till följd av en incident som orsakats av någon form av angrepp bör den grundläggande orsaken till problemet identifieras för att fastställa om eventuella sårbarheter som orsakade incidenten fortfarande föreligger och därför fortfarande kan utnyttjas. I många fall kan den personuppgiftsansvarige fastställa att incidenten sannolikt kommer att leda till en risk och därför ska anmälas. I andra fall behöver anmälan inte skjutas upp tills den risk och de konsekvenser som följer av incidenten har bedömts fullt ut, eftersom den fullständiga riskbedömningen kan ske parallellt med anmälan, och den information som erhålls på detta sätt kan lämnas till tillsynsmyndigheten i etapper utan onödigt ytterligare dröjsmål[9].

9. Incidenten bör anmälas när den personuppgiftsansvarige anser att den sannolikt kommer att medföra en risk för den registrerades rättigheter och friheter. Personuppgiftsansvariga bör göra denna bedömning när de får kännedom om incidenten. Personuppgiftsansvariga bör inte vänta på en detaljerad kriminalteknisk undersökning och (tidiga) mildrande åtgärder innan de bedömer om incidenten sannolikt kommer att leda till en risk och därför bör anmälas.

10. Om en personuppgiftsansvarig själv bedömer att risken är osannolik, men det visar sig att risken ändå uppstår, kan den behöriga tillsynsmyndigheten använda sina korrigerande befogenheter och besluta om påföljder.

11. Varje personuppgiftsansvarig och personuppgiftsbiträde bör ha planer och förfaranden för att hantera eventuella uppgiftsincidenter. Organisationer bör ha tydliga rapporteringsvägar och personer som ansvarar för olika aspekter av återställandeprocessen.

12. Utbildning och medvetenhet om dataskyddsfrågor för den personuppgiftsansvariges och personuppgiftsbiträdets personal, med fokus på hantering av personuppgiftsincidenter (identifiering av en personuppgiftsincident, ytterligare åtgärder som ska vidtas osv.), är också mycket viktigt för personuppgiftsansvariga och personuppgiftsbiträden. Utbildningen bör upprepas regelbundet, beroende på typen av behandling och storleken på den personuppgiftsansvariges personal, och inriktas på de senaste trenderna och varningarna om it-attacker eller andra säkerhetsincidenter.

13. Principerna om ansvarsskyldighet och inbyggt dataskydd skulle kunna inbegripa analys som fungerar som underlag för den personuppgiftsansvariges och personuppgiftsbiträdets egen handbok om hantering av personuppgiftsincidenter, som syftar till att beskriva varje del av behandlingen i varje större skede av processen. En sådan handbok som utarbetats i förväg skulle utgöra en mycket snabbare informationskälla och göra det möjligt för personuppgiftsansvariga och personuppgiftsbiträden att minska riskerna och fullgöra skyldigheterna utan onödigt dröjsmål. Om en personuppgiftsincident skulle inträffa skulle de i organisationen därmed veta vad de ska göra, och incidenten skulle med största sannolikhet hanteras snabbare än om det inte fanns några riskreducerande åtgärder eller planer.

14. Även om de fall som beskrivs nedan är fiktiva bygger de på typiska fall från tillsynsmyndighetens samlade erfarenheter av anmälningar av uppgiftsincidenter. De analyser som erbjuds gäller uttryckligen de granskade fallen, men målet är att hjälpa personuppgiftsansvariga att bedöma sina egna uppgiftsincidenter. Om omständigheterna ändras i de fall som beskrivs nedan kan det leda till andra eller högre risknivåer, vilket kräver andra eller ytterligare åtgärder. I dessa riktlinjer struktureras fallen efter vissa kategorier av incidenter (t.ex. utpressningsattacker). Vissa mildrande åtgärder behövs i varje enskilt fall när man hanterar en viss kategori av incidenter. Dessa åtgärder upprepas inte nödvändigtvis i varje fallanalys som hör till

[9] Artikel 33.4 i dataskyddsförordningen.

samma kategori av incidenter. För de fall som hör till samma kategori beskrivs endast skillnaderna. Läsaren bör därför studera alla fall som är relevanta för den relevanta incidentkategorin för att identifiera och särskilja alla rätta åtgärder som ska vidtas.

15. Intern dokumentation av en incident är en skyldighet som är oberoende av de risker som är förknippade med incidenten och måste tas fram i samtliga fall. I de fall som beskrivs nedan försöker vi sprida lite ljus över huruvida incidenten ska anmälas till tillsynsmyndigheten och meddelas de berörda registrerade.

2 UTPRESSNINGSATTACK

16. En vanlig orsak till en anmälan av en uppgiftsincident är en utpressningsattack som den personuppgiftsansvarige utsätts för. I dessa fall krypterar en skadlig kod personuppgifterna och angriparen kräver sedan den personuppgiftsansvarige på en lösensumma i utbyte mot dekrypteringskoden. Denna typ av attack kan vanligtvis klassificeras som ett tillgänglighetsbrott, men ofta kan även ett konfidentialitetsbrott ske.

2.1 FALL nr 01: Utpressningsattack med ordentlig säkerhetskopiering och utan exfiltrering

Ett litet tillverkningsföretags datorsystem utsätts för en utpressningsattack, och de uppgifter som lagras i dessa system krypteras. Den personuppgiftsansvarige har använt kryptering i vila, så alla uppgifter som utpressningsprogrammet hämtar lagras i krypterad form med hjälp av en modern krypteringsalgoritm. Dekrypteringsnyckeln äventyras inte i attacken, dvs. angriparen kan varken komma åt den eller använda den indirekt. Angriparen har därför endast tillgång till krypterade personuppgifter. Varken företagets e-postsystem eller några kundsystem som används för att få tillgång till det påverkas. Företaget använder sig av ett externt it-säkerhetsföretags expertis för att undersöka incidenten. Det finns loggar som spårar alla dataflöden som lämnar företaget (inklusive utgående e-post). Efter att ha analyserat loggarna och de uppgifter som samlats in av de detekteringssystem som företaget har använt fastställer en intern undersökning som stöds av det externa it-säkerhetsföretaget *med säkerhet* att angriparen endast krypterade uppgifterna, utan att exfiltrera dem. Loggarna visar inget utflöde av data under attacken. De personuppgifter som berörs av incidenten gäller företagets kunder och anställda – några tiotals personer totalt sett. Det finns en lättillgänglig säkerhetskopia och uppgifterna återskapas några timmar efter attacken. Incidenten leder inte till några konsekvenser för den personuppgiftsansvariges dagliga arbete. Lönerna till de anställda eller hanteringen av kundförfrågningar försenas inte.

17. I detta fall innebar följande att händelsen kunde betecknas som en personuppgiftsincident: Ett säkerhetsbrott ledde till olaglig ändring av och obehörig åtkomst till lagrade personuppgifter.

2.1.1 FALL nr 01 – Tidigare åtgärder och riskbedömning

18. Liksom med alla risker som externa aktörer utgör kan sannolikheten för att en utpressningsattack ska lyckas minskas drastiskt genom att säkerheten i den personuppgiftsansvariges miljö skärps. De flesta av dessa incidenter kan förhindras genom att man ser till att lämpliga organisatoriska, fysiska och tekniska säkerhetsåtgärder har vidtagits. Exempel på sådana åtgärder är korrekt hantering av programfixar och användning av ett lämpligt antivirusprogram. Ordentlig och separat säkerhetskopiering bidrar till att mildra konsekvenserna av en framgångsrik attack om en sådan inträffar. Dessutom kommer ett program för säkerhetsutbildning och säkerhetsmedvetenhet för anställda att bidra till att förebygga och identifiera denna typ av attack. (En förteckning över lämpliga åtgärder finns i avsnitt 2.5.) Bland dessa åtgärder är en av de viktigaste korrekt hantering av programfixar som säkerställer att systemen är uppdaterade och att

alla kända sårbarheter i de system som används har åtgärdats, eftersom de flesta utpressningsattacker utnyttjar välkända sårbarheter.

19. När den personuppgiftsansvarige bedömer riskerna bör den undersöka incidenten och identifiera typen av skadlig kod för att förstå de möjliga konsekvenserna av attacken. Bland de risker som ska bedömas finns risken för att uppgifter har exfiltrerats utan att lämna några spår i systemloggarna.

20. I detta exempel hade angriparen tillgång till personuppgifter, och konfidentialiteten i kryptotexten med personuppgifter i krypterad form äventyrades. Uppgifter som eventuellt exfiltrerades kunde dock inte läsas eller användas av angriparen, åtminstone inte för tillfället. Den krypteringsteknik som den personuppgiftsansvarige använde överensstämde med den senaste tekniken. Dekrypteringsnyckeln äventyrades inte och kunde förmodligen inte heller fastställas på annat sätt. Tack vare detta minskas sekretessriskerna för fysiska personers rättigheter och friheter till ett minimum, och kryptoanalytisk utveckling som gör de krypterade uppgifterna begripliga i framtiden förhindras.

21. Den personuppgiftsansvarige bör bedöma risken för enskilda personer på grund av incidenten[10]. I detta fall verkar riskerna för de registrerades rättigheter och friheter vara en följd av bristen på tillgänglighet till personuppgifterna, och personuppgifternas konfidentialitet äventyras inte[11]. I detta exempel mildrades de negativa effekterna av incidenten ganska snart efter att den hade inträffat. Att ha ett ordentligt system för säkerhetskopiering[12] gör effekterna av incidenten mindre allvarliga, och här kunde den personuppgiftsansvarige använda sig av systemet på ett effektivt sätt.

22. När det gäller hur allvarliga konsekvenserna är för de registrerade kunde endast mindre konsekvenser identifieras eftersom de berörda uppgifterna återskapades inom några timmar, incidenten inte ledde till några konsekvenser för den personuppgiftsansvariges dagliga arbete och den inte hade någon betydande inverkan på de registrerade (t.ex. lönerna till de anställda eller hanteringen av kundförfrågningar).

2.1.2 FALL nr 01 – Lindring och skyldigheter

23. Utan en säkerhetskopia kan den personuppgiftsansvarige inte göra mycket för att avhjälpa förlusten av personuppgifter, och uppgifterna måste samlas in igen. I detta särskilda fall kunde man dock begränsa effekterna av attacken genom att återställa alla komprometterade system till ett rent tillstånd som man vet

---

[10] För vägledning om ”sannolikt leder till en hög risk”, se artikel 29-arbetsgruppens *Riktlinjer om konsekvensbedömning avseende dataskydd och fastställande av huruvida behandlingen ”sannolikt leder till en hög risk” i den mening som avses i förordning 2016/679*, WP248 rev. 01 – godkända av EDPB, https://ec.europa.eu/newsroom/article29/items/611236, s. 9.

[11] Tekniskt sett kommer kryptering av uppgifter att innebära ”tillgång” till de ursprungliga uppgifterna, och när det gäller utpressningsattacker, radering av de ursprungliga uppgifterna. Uppgifterna måste hämtas genom utpressningsprogrammets kod för att de ska krypteras och för att de ursprungliga uppgifterna ska raderas. En angripare kan ta en kopia av de ursprungliga uppgifterna innan de raderas, men personuppgifter kommer inte alltid att extraheras. I takt med att den personuppgiftsansvariges utredning fortskrider kan ny information komma fram och ändra denna bedömning. Tillgång som leder till olaglig förstöring, förlust eller ändring eller till obehörig utlämning av personuppgifter eller till en säkerhetsrisk för en registrerad, även utan tolkning av uppgifterna, kan vara lika allvarlig som tillgång med tolkning av personuppgifterna.

[12] Förfarandena för säkerhetskopiering bör vara strukturerade, konsekventa och repeterbara. Exempel på förfaranden är 3-2-1-metoden och metoden farfar-far-son. Metoderna bör alltid testas med avseende på täckningseffektivitet och när uppgifter ska återskapas. Testningen bör också upprepas med jämna mellanrum och särskilt när det sker förändringar i behandlingen eller dess omständigheter för att säkerställa systemets integritet.

är fritt från skadlig kod, åtgärda sårbarheterna och återskapa de berörda uppgifterna strax efter attacken. Utan en säkerhetskopia går uppgifterna förlorade och allvarlighetsgraden kan öka eftersom riskerna eller konsekvenserna för enskilda också kan öka.

24. Att uppgifterna återskapas snabbt och effektivt från den lättillgängliga säkerhetskopian är en viktig variabel när incidenten analyseras. Att fastställa en lämplig tidsram för att återskapa de berörda uppgifterna beror på de unika omständigheterna kring incidenten i fråga. I dataskyddsförordningen anges att en personuppgiftsincident ska anmälas utan onödigt dröjsmål och, om möjligt, senast efter 72 timmar. Det kunde därför fastställas att det i vilket fall som helst är olämpligt att överskrida tidsfristen på 72 timmar, men när det rör sig om högriskfall kan det betraktas som otillfredsställande även när denna tidsfrist iakttas.

25. Efter en detaljerad konsekvensbedömning och incidenthantering konstaterade den personuppgiftsansvarige i detta fall att det var osannolikt att incidenten skulle leda till en risk för fysiska personers rättigheter och friheter, och att ingen information till de registrerade därför behövdes och att incidenten inte heller behövde anmälas till tillsynsmyndigheten. Precis som alla uppgiftsincidenter bör den dock dokumenteras i enlighet med artikel 33.5. Organisationen kan också behöva (eller senare åläggas av tillsynsmyndigheten) uppdatera och åtgärda sin organisatoriska och tekniska hantering av säkerheten för personuppgifter samt sina riskreducerande åtgärder och förfaranden. I samband med detta bör organisationen noggrant undersöka incidenten och identifiera orsakerna till den samt de metoder som användes av angriparen för att förhindra liknande händelser i framtiden.

Nödvändiga åtgärder på grundval av identifierade risker		
Intern dokumentation	Anmälan till tillsynsmyndigheten	Information till de registrerade
✓	X	X

2.2 FALL nr 02: Utpressningsattack utan ordentlig säkerhetskopiering

En av datorerna som används av ett jordbruksföretag utsätts för en utpressningsattack och dess data krypteras av angriparen. Företaget använder sig av ett externt it-säkerhetsföretags expertis för att övervaka sitt nätverk. Det finns loggar som spårar alla dataflöden som lämnar företaget (inklusive utgående e-post). Efter att ha analyserat loggarna och de uppgifter som samlats in av de andra detekteringssystemen fastställer en intern undersökning som stöds av det externa it-säkerhetsföretaget att angriparen endast krypterade uppgifterna, utan att exfiltrera dem. Loggarna visar inget utflöde av data under attacken. De personuppgifter som berörs av incidenten gäller företagets kunder och anställda – ett par dussin personer totalt sett. Inga särskilda uppgiftskategorier påverkas. Det finns ingen säkerhetskopia i elektroniskt format. De flesta uppgifterna återskapas utifrån papperskopior. Återskapandet av uppgifterna tar fem arbetsdagar och leder till mindre förseningar i orderleveranserna till kunderna.

2.2.1 FALL nr 02 – Tidigare åtgärder och riskbedömning

26. Den personuppgiftsansvarige borde ha vidtagit samma tidigare åtgärder som anges i del 2.1 och avsnitt 2.9. Den största skillnaden jämfört med det förra fallet är bristen på en elektronisk säkerhetskopia och bristen på kryptering i vila. Detta leder till avgörande skillnader i följande steg.

27. När den personuppgiftsansvarige bedömer riskerna bör den undersöka infiltrationsmetoden och identifiera typen av skadlig kod för att förstå de möjliga konsekvenserna av attacken. I detta exempel krypterade utpressningsprogrammet personuppgifterna utan att exfiltrera dem. Därmed verkar riskerna för de registrerades rättigheter och friheter vara en följd av bristen på tillgänglighet till personuppgifterna, och personuppgifternas konfidentialitet äventyras inte. En grundlig undersökning av brandväggsloggarna och

dess följder är avgörande för att bedöma risken. Den personuppgiftsansvarige bör på begäran lägga fram de faktiska resultaten av dessa undersökningar.

28. Den personuppgiftsansvarige måste komma ihåg att om attacken är mer sofistikerad kan sabotageprogrammet redigera loggfiler och ta bort spåren. Eftersom loggarna inte vidarebefordras eller replikeras till en central loggserver kan den personuppgiftsansvarige – ens efter en grundlig undersökning som visar att personuppgifterna inte exfiltrerades av angriparen – inte uppge att avsaknaden av en loggpost bevisar att ingen exfiltrering har skett, och därför kan sannolikheten för ett konfidentialitetsbrott inte helt avfärdas.

29. Den personuppgiftsansvarige bör bedöma riskerna med denna incident[13] om angriparen fick tillgång till uppgifterna. Under riskbedömningen bör den personuppgiftsansvarige också ta hänsyn till arten, känsligheten, volymen och sammanhanget för de personuppgifter som påverkas av incidenten. I detta fall påverkas inga särskilda kategorier av personuppgifter, och mängden berörda uppgifter och antalet berörda registrerade är lågt.

30. Det är viktigt att samla in exakt information om obehörig åtkomst för att fastställa risknivån och förhindra en ny eller fortsatt attack. Om uppgifterna hade kopierats från databasen skulle det uppenbarligen ha varit en faktor som ökade risken. När det råder osäkerhet om detaljerna kring den orättmätiga åtkomsten bör det sämre scenariot beaktas och risken bedömas i enlighet med detta.

31. Avsaknaden av en databas med en säkerhetskopia kan betraktas som en riskförstärkande faktor beroende på hur allvarliga konsekvenserna är för de registrerade till följd av bristen på tillgänglighet till uppgifterna.

2.2.2 FALL nr 02 – Lindring och skyldigheter

32. Utan en säkerhetskopia kan den personuppgiftsansvarige inte göra mycket för att avhjälpa förlusten av personuppgifter, och uppgifterna måste samlas in igen, såvida det inte finns någon annan källa (t.ex. e-postmeddelanden med beställningsbekräftelser). Utan en säkerhetskopia kan uppgifter gå förlorade och allvarlighetsgraden beror på hur de enskilda personerna påverkas.

33. Att återskapa uppgifterna bör inte vara alltför svårt[14] om uppgifterna fortfarande finns tillgängliga på papper, men med tanke på avsaknaden av en elektronisk databas med en säkerhetskopia anses en anmälan till tillsynsmyndigheten vara nödvändig, eftersom återskapandet av uppgifterna tog ett tag och skulle kunna orsaka vissa förseningar i orderleveransen till kunderna, och en betydande mängd metadata (t.ex. loggar, tidsstämplar) kanske inte kan återvinnas.

34. Information till de registrerade om incidenten kan också bero på hur länge personuppgifterna är otillgängliga och de svårigheter det kan orsaka för den personuppgiftsansvariges arbete (t.ex. förseningar i överföringen av de anställdas löner). Eftersom dessa förseningar i löner och leveranser kan leda till ekonomiska förluster för de personer vars uppgifter har äventyrats kan man också hävda att incidenten sannolikt kommer att leda till en hög risk. Det kanske inte heller går att undvika att informera de registrerade om deras bidrag behövs för att återskapa de krypterade uppgifterna.

---

[13] För vägledning om ”sannolikt leder till en hög risk”, se fotnot 10.

[14] Detta kommer att bero på personuppgifternas komplexitet och struktur. I de mest komplexa scenarierna kan det krävas betydande resurser och insatser för att återställa dataintegriteten och överensstämmelsen med metadata, säkerställa korrekta förhållanden inom datastrukturer och kontrollera uppgifternas riktighet.

35. Det här fallet är ett exempel på en utpressningsattack som utgör en risk för de registrerades rättigheter och friheter, men inte leder till en hög risk. Den bör dokumenteras i enlighet med artikel 33.5 och anmälas till tillsynsmyndigheten i enlighet med artikel 33.1. Organisationen kan också behöva (eller åläggas av tillsynsmyndigheten) uppdatera och åtgärda sin organisatoriska och tekniska hantering av säkerheten för personuppgifter samt sina riskreducerande åtgärder och förfaranden.

Nödvändiga åtgärder på grundval av identifierade risker		
Intern dokumentation	Anmälan till tillsynsmyndigheten	Information till de registrerade
✓	✓	X

2.3 FALL nr 03: Utpressningsattack med säkerhetskopiering och utan exfiltrering på ett sjukhus

Ett sjukhus/en vårdcentrals informationssystem utsätts för en utpressningsattack och en stor del av dess data krypteras av angriparen. Företaget använder sig av ett externt it-säkerhetsföretags expertis för att övervaka sitt nätverk. Det finns loggar som spårar alla dataflöden som lämnar företaget (inklusive utgående e-post). Efter att ha analyserat loggarna och de uppgifter som samlats in av de andra detekteringssystem fastställer en intern undersökning som stöds av det externa it-säkerhetsföretaget att angriparen endast krypterade uppgifterna, utan att exfiltrera dem. Loggarna visar inget utflöde av data under attacken. De personuppgifter som berörs av incidenten gäller företagets anställda och patienter – flera tusen personer. Det finns säkerhetskopior i elektroniskt format. De flesta uppgifter återskapas, men detta tar två arbetsdagar och leder till stora förseningar i behandlingen av patienter och avbrutna/uppskjutna operationer samt till en sämre servicenivå eftersom systemen inte är tillgängliga.

2.3.1 FALL nr 03 – Tidigare åtgärder och riskbedömning

36. Den personuppgiftsansvarige borde ha vidtagit samma tidigare åtgärder som anges i del 2.1 och avsnitt 2.5. Den största skillnaden jämfört med det förra fallet är de allvarliga konsekvenserna för en betydande del av de registrerade[15].

37. Mängden berörda uppgifter och antalet berörda registrerade är stort, eftersom sjukhus vanligtvis behandlar stora mängder uppgifter. Att uppgifterna inte finns tillgängliga påverkar kraftigt en betydande del av de registrerade. Dessutom finns det en kvarstående, mycket allvarlig risk för patientuppgifternas konfidentialitet.

38. Det är viktigt med typen av incident samt arten, känsligheten och volymen av de personuppgifter som berörs. Även om det fanns en säkerhetskopia av uppgifterna och de kunde återskapas på några dagar finns det

[15] För vägledning om ”sannolikt leder till en hög risk”, se fotnot 10.

fortfarande en hög risk på grund av de allvarliga konsekvenserna för de registrerade till följd av bristen på tillgänglighet till uppgifterna vid tidpunkten för attacken och dagarna efteråt.

2.3.2 FALL nr 03 – Lindring och skyldigheter

39. En anmälan till tillsynsmyndigheten anses nödvändig, eftersom det rör sig om särskilda kategorier av personuppgifter och det kan ta lång tid att återskapa dem, vilket leder till stora förseningar i vården av patienter. Det är nödvändigt att underrätta de registrerade om incidenten på grund av påverkan på patienterna, även efter att de krypterade uppgifterna har återskapats. Uppgifter om alla patienter som behandlats på sjukhuset under de senaste åren har krypterats, men endast de patienter som skulle behandlas på sjukhuset under den tid som datasystemet låg nere påverkades. Den personuppgiftsansvarige bör underrätta dessa patienter direkt om uppgiftsincidenten. Direkt information till övriga patienter, varav vissa kanske inte har besökt sjukhuset på över 20 år, kanske inte behövs på grund av undantaget i artikel 34.3 c. I så fall ska i stället allmänheten informeras[16] eller en liknande åtgärd vidtas genom vilken de registrerade informeras på ett lika effektivt sätt. I det här fallet borde sjukhuset gå ut med utpressningsattacken och dess konsekvenser.

40. Detta fall är ett exempel på en utpressningsattack som utgör en hög risk för de registrerades rättigheter och friheter. Den bör dokumenteras i enlighet med artikel 33.5, anmälas till tillsynsmyndigheten i enlighet med artikel 33.1 och meddelas de registrerade i enlighet med artikel 34.1. Organisationen behöver också uppdatera och åtgärda sin organisatoriska och tekniska hantering av säkerheten för personuppgifter samt sina riskreducerande åtgärder och förfaranden.

Nödvändiga åtgärder på grundval av identifierade risker		
Intern dokumentation	Anmälan till tillsynsmyndigheten	Information till de registrerade
✓	✓	✓

2.4 FALL nr 04: Utpressningsattack utan säkerhetskopiering och med exfiltrering

Ett kollektivtrafikföretags server utsätts för en utpressningsattack och dess data krypteras av angriparen. Enligt resultaten från den interna undersökningen har angriparen inte bara krypterat uppgifterna, utan även exfiltrerat dem. Typen av berörda uppgifter är kunders och anställdas personuppgifter, och personuppgifter över flera tusen personer som använt företagets tjänster (t.ex. köpt biljetter online). Utöver grundläggande identitetsuppgifter berörs identitetskortsnummer och finansiella uppgifter såsom kreditkortsuppgifter av incidenten. Det finns en databas med en säkerhetskopia, men den har också krypterats av angriparen.

2.4.1 FALL nr 04 – Tidigare åtgärder och riskbedömning

41. Den personuppgiftsansvarige borde ha vidtagit samma tidigare åtgärder som anges i del 2.1 och avsnitt 2.5. Det fanns visserligen en säkerhetskopia, men den påverkades också av attacken. Enbart detta system väcker frågor om kvaliteten på den personuppgiftsansvariges tidigare it-säkerhetsåtgärder och bör granskas

[16] I skäl 86 i dataskyddsförordningen anges följande: ”De registrerade bör underrättas så snart detta rimligtvis är möjligt, i nära samarbete med tillsynsmyndigheten och i enlighet med den vägledning som lämnats av den eller av andra relevanta myndigheter, exempelvis brottsbekämpande myndigheter. Till exempel kräver behovet av att mildra en omedelbar skaderisk att de registrerade underrättas omedelbart, medan behovet av att vidta lämpliga åtgärder vid fortlöpande eller likartade personuppgiftsincidenter däremot kan motivera längre tid för underrättelsen.”

ytterligare under utredningen. I ett väl utformat system för säkerhetskopiering måste nämligen flera säkerhetskopior lagras på ett säkert sätt utan att kunna nås från huvudsystemet, annars kan de äventyras vid samma attack. Dessutom kan utpressningsattacker förbli oupptäckta under flera dagar och långsamt kryptera sällan använda uppgifter. Detta kan göra flera säkerhetskopior oanvändbara, så säkerhetskopior bör också göras med jämna mellanrum och vara isolerade. Detta skulle öka sannolikheten för att uppgifterna kan återskapas, om än med ökad dataförlust.

42. Denna incident handlar inte bara om tillgängligheten till uppgifter, utan även om konfidentialiteten, eftersom angriparen kan ha ändrat och/eller kopierat uppgifter från servern. Därför leder typen av incident till en hög risk[17].

43. Personuppgifternas art, känslighet och volym ökar riskerna ytterligare eftersom både antalet berörda personer är stort, liksom den totala mängden berörda personuppgifter. Utöver grundläggande identitetsuppgifter berörs också identitetskortsnummer och finansiella uppgifter såsom kreditkortsuppgifter. En uppgiftsincident som rör dessa typer av uppgifter utgör en hög risk i sig, och om uppgifterna behandlas tillsammans kan de bland annat användas för identitetsstöld eller bedrägeri.

44. På grund av bristfällig serverlogik eller bristfälliga organisatoriska kontroller påverkades säkerhetskopieringsfilerna av utpressningsprogrammet, vilket förhindrade återskapande av uppgifterna och ökade risken.

45. Denna uppgiftsincident utgör en stor risk för enskilda personers rättigheter och friheter, eftersom den sannolikt kan leda till både materiell (t.ex. ekonomisk förlust eftersom kreditkortsuppgifter påverkades) och immateriell skada (t.ex. identitetsstöld eller bedrägeri eftersom identitetskortsuppgifter påverkades).

2.4.2 FALL nr 04 – Lindring och skyldigheter

46. Det är viktigt att de registrerade underrättas så att de kan vidta nödvändiga åtgärder för att undvika materiell skada (t.ex. spärra sina bankkort).

47. Förutom att dokumentera incidenten i enlighet med artikel 33.5 är en anmälan till tillsynsmyndigheten också obligatorisk i detta fall (artikel 33.1), och den personuppgiftsansvarige är också skyldig att underrätta de registrerade om incidenten (artikel 34.1). Det senare kan göras personligen, men om kontaktuppgifter inte finns tillgängliga bör den personuppgiftsansvarige offentliggöra informationen, förutsatt att detta inte leder till ytterligare negativa konsekvenser för de registrerade, t.ex. genom ett meddelande på sin webbplats. I det senare fallet krävs exakt och tydlig information, på en tydlig plats på den personuppgiftsansvariges webbplats, med exakta hänvisningar till de relevanta bestämmelserna i dataskyddsförordningen. Organisationen kan också behöva uppdatera och åtgärda sin organisatoriska och tekniska hantering av säkerheten för personuppgifter samt sina riskreducerande åtgärder och förfaranden.

Nödvändiga åtgärder på grundval av identifierade risker		
Intern dokumentation	Anmälan till tillsynsmyndigheten	Information till de registrerade
✓	✓	✓

2.5 Organisatoriska och tekniska åtgärder för att förebygga/mildra effekterna av utpressningsattacker

[17] För vägledning om ”sannolikt leder till en hög risk”, se fotnot 10.

48. Det faktum att en utpressningsattack kunde ha ägt rum tyder ofta på en eller flera sårbarheter i den personuppgiftsansvariges system. Detta gäller även vid utpressningsattacker där personuppgifterna har krypterats men inte exfiltrerats. Oavsett resultatet och konsekvenserna av attacken kan man inte nog betona vikten av en heltäckande utvärdering av datasäkerhetssystemet – med särskild tonvikt på it-säkerheten. De identifierade svagheterna och säkerhetshålen ska dokumenteras och åtgärdas utan dröjsmål.

49. Lämpliga åtgärder:

(Förteckningen över följande åtgärder är inte på något sätt fullständig eller uttömmande. Målet är snarare att ge idéer till förebyggande och möjliga lösningar. Varje behandling är annorlunda, och därför bör den personuppgiftsansvarige fatta beslut om vilka åtgärder som bäst passar den givna situationen.)

- Hålla inbyggd programvara, operativsystem och tillämpningsprogram på servrar, klientdatorer, aktiva nätverkskomponenter och alla andra datorer på samma lokala nät (inklusive wifi-enheter) uppdaterade. Se till att lämpliga it-säkerhetsåtgärder vidtas och att de är effektiva och regelbundet uppdateras när behandlingen eller omständigheterna förändras eller utvecklas. Detta inbegriper att föra detaljerade loggar över vilka programfixar som tillämpas vid vilken tidpunkt.
- Utforma och organisera behandlingssystem och infrastruktur så att de segmenterar eller isolerar datasystem och nätverk för att undvika spridning av skadlig kod inom organisationen och till externa system.
- Ha en uppdaterad, säker och testad säkerhetskopieringsprocess. Media för säkerhetskopiering på medellång och lång sikt bör hållas åtskilda från lagringen av operativa uppgifter och utom räckhåll för tredje part, även vid en lyckad attack (t.ex. daglig inkrementell säkerhetskopiering och veckovis fullständig säkerhetskopiering).
- Ha/införskaffa ett lämpligt, uppdaterat, effektivt och integrerat antivirusprogram.
- Ha en lämplig, uppdaterad, effektiv och integrerad brandvägg samt system för upptäckt och förebyggande av intrång. Dirigera nätverkstrafiken genom brandväggen/intrångsdetektionen, även vid hemmakontor eller mobilt arbete (t.ex. genom att använda VPN-anslutningar till organisatoriska säkerhetsmekanismer när man går in på nätet).
- Utbilda anställda i metoder för att känna igen och förhindra it-attacker. Den personuppgiftsansvarige bör göra det möjligt att fastställa huruvida mejl och meddelanden som fås genom andra kommunikationsmedel är autentiska och tillförlitliga. De anställda bör utbildas i att förstå när en attack har skett, hur man tar bort slutpunkten från nätverket och om deras skyldighet att omedelbart rapportera attacken till den säkerhetsansvarige.
- Betona behovet av att identifiera typen av skadlig kod för att se konsekvenserna av attacken och kunna hitta rätt åtgärder för att minska risken. Om en utpressningsattack har lyckats och det inte finns någon säkerhetskopia kan verktyg som de som utvecklats genom projektet ”no more ransom” (nomoreransom.org) användas för att hämta uppgifter. Om det finns en säker säkerhetskopia rekommenderas det dock att återskapa uppgifterna från den.
- Vidarebefordra eller replikera alla loggar till en central loggserver (eventuellt med signering eller kryptografisk tidsstämpling av loggposter).
- Använda kraftfull kryptering och flerfaktorsautentisering, särskilt för administrativ åtkomst till it-system, samt lämplig nyckel- och lösenordshantering.
- Utföra regelbundna sårbarhets- och dataintrångstester.
- Upprätta ett it-incidentcentrum (CSIRT, *Computer Security Incident Response Team*) eller en it-incidenthanteringsorganisation (CERT, *Computer Emergency Response Team*) inom organisationen, eller gå med i ett gemensamt CSIRT/CERT. Skapa en incidenthanteringsplan, katastrofplan och en kontinuitetsplan och se till att dessa testas noggrant.
- Se över, testa och uppdatera riskanalysen vid bedömning av motåtgärder.

3 DATAEXFILTRERINGSATTACKER

50. Attacker som utnyttjar sårbarheter i tjänster som tillhandahålls av den personuppgiftsansvarige till tredje part via internet, t.ex. genom injektionsattacker (t.ex. SQL-injektion, sökvägstraversering), kompromettering av webbplatser och liknande metoder, kan likna utpressningsattacker på så sätt att risken härrör från en obehörig tredje parts agerande, men dessa attacker syftar vanligtvis till att kopiera, exfiltrera och missbruka personuppgifter för skadliga ändamål. Därför är de främst konfidentialitetsbrott och eventuellt även integritetsbrott. Samtidigt finns det, om den personuppgiftsansvarige känner till egenskaperna hos denna typ av incident, många åtgärder tillgängliga för den personuppgiftsansvarige som avsevärt kan minska risken för en framgångsrik attack.

3.1 FALL nr 05: Exfiltrering av jobbansökningsuppgifter från en webbplats

En arbetsförmedling utsätts för en cyberattack som placerar skadlig kod på dess webbplats. Denna skadliga kod gör personlig information som skickats in via jobbansökningsformulär på nätet och lagrats på webbservern tillgänglig för obehöriga. Eventuellt har 213 sådana formulär drabbats. Efter att man analyserat de berörda uppgifterna fastställs det att inga särskilda uppgiftskategorier har påverkats av incidenten. Det installerade virusprogrammet har funktioner som gör det möjligt för angriparen att radera eventuell exfiltreringshistorik och även övervaka behandling på servern och samla in personuppgifter. Programmet upptäcks först en månad efter att det har installerats.

3.1.1 FALL nr 05 – Tidigare åtgärder och riskbedömning

51. Säkerheten i den personuppgiftsansvariges miljö är extremt viktig, eftersom de flesta av dessa incidenter kan förhindras genom att säkerställa att alla system uppdateras kontinuerligt, känsliga uppgifter krypteras och program utvecklas enligt höga säkerhetsstandarder såsom kraftfull autentisering, åtgärder mot råstyrkeattacker, ”escaping” eller ”sanering”[18] av användarindata osv. Det krävs också regelbundna granskningar av it-säkerheten, sårbarhetsbedömningar och penetrationstester för att upptäcka dessa typer av sårbarheter i förväg och åtgärda dem. I detta särskilda fall skulle verktyg för övervakning av filintegritet i produktionsmiljön ha kunnat hjälpa till att identifiera kodinjektionen. (En förteckning över lämpliga åtgärder finns i avsnitt 3.7.)

52. Den personuppgiftsansvarige bör alltid börja utreda incidenten genom att identifiera typen av attack och dess metoder för att bedöma vilka åtgärder som ska vidtas. För att det ska gå snabbt och effektivt bör den personuppgiftsansvarige ha en incidenthanteringsplan där snabba och nödvändiga åtgärder för att ta kontroll över incidenten anges. I detta särskilda fall var typen av incident en riskförstärkande faktor, eftersom inte bara uppgifternas konfidentialitet inskränktes utan infiltratören även kunde göra förändringar i systemet. Därför kunde även dataintegriteten diskuteras.

53. De berörda personuppgifternas art, känslighet och volym bör bedömas för att fastställa i vilken utsträckning incidenten påverkade de registrerade. Även om inga särskilda kategorier av personuppgifter påverkades innehåller de uppgifter som hämtades omfattande information om personerna från onlineformulären, och

[18] ”Escaping” eller ”sanering” av användarindata är en form av indatavalidering som säkerställer att endast korrekt formaterade data matas in i ett informationssystem.

sådana uppgifter skulle kunna missbrukas på flera olika sätt (riktad oönskad reklam, identitetsstöld osv.), så konsekvensernas allvarlighetsgrad bör öka risken för de registrerades rättigheter och friheter[19].

3.1.2 FALL nr 05 – Lindring och skyldigheter

54. Efter att problemet har lösts bör databasen om möjligt jämföras med den som lagras i en säker säkerhetskopia. Erfarenheterna från incidenten bör användas för att uppdatera it-infrastrukturen. Den personuppgiftsansvarige bör återställa alla berörda it-system till ett känt rent tillstånd, åtgärda sårbarheten och genomföra nya säkerhetsåtgärder för att undvika liknande uppgiftsincidenter i framtiden, t.ex. filintegritetskontroller och säkerhetsgranskningar. Om personuppgifter inte bara exfiltrerades utan också raderades måste den personuppgiftsansvarige vidta systematiska åtgärder för att återskapa personuppgifterna till det tillstånd de befann sig i före incidenten. Det kan vara nödvändigt att lägga in fullständiga säkerhetskopior och inkrementella ändringar, och sedan eventuellt göra om behandlingen sedan den senaste inkrementella säkerhetskopieringen – vilket innebär att den personuppgiftsansvarige måste kunna replikera de ändringar som gjorts sedan den senaste säkerhetskopieringen. Detta kan innebära att den personuppgiftsansvarige måste utforma systemet så att de dagliga indatafilerna behålls om de behöver behandlas igen, och kräver en robust lagringsmetod och en lämplig lagringspolicy.

55. Mot bakgrund av ovanstående och eftersom incidenten sannolikt kommer att leda till en hög risk för fysiska personers rättigheter och friheter bör de registrerade definitivt underrättas om den (artikel 34.1), vilket naturligtvis även innebär att den bör anmälas till den eller de berörda tillsynsmyndigheterna. Det är obligatoriskt att dokumentera incidenten enligt artikel 33.5 i dataskyddsförordningen, och det gör det även lättare att bedöma situationen.

Nödvändiga åtgärder på grundval av identifierade risker		
Intern dokumentation	Anmälan till tillsynsmyndigheten	Information till de registrerade
✓	✓	✓

3.2 FALL nr 06: Exfiltrering av ett hashat lösenord från en webbplats

En SQL-injektionssårbarhet utnyttjas för att få åtkomst till en databas på servern för en matlagningswebbplats. Användarna har endast fått välja godtyckliga pseudonymer som användarnamn. De har avrådts från att använda e-postadresser för detta ändamål. Lösenord som lagras i databasen är hashade med en stark algoritm och saltet äventyras inte. De berörda uppgifterna utgörs av hashade lösenord för 1 200 användare. Av säkerhetsskäl informerar den personuppgiftsansvarige de registrerade om incidenten via e-post och uppmanar dem att byta

3.2.1 FALL nr 06 – Tidigare åtgärder och riskbedömning

56. I detta särskilda fall har uppgifternas konfidentialitet äventyrats, men lösenorden i databasen var hashade med en modern metod vilket minskar risken när det gäller personuppgifternas art, känslighet och volym. Detta fall innebär inga risker för de registrerades rättigheter och friheter.

[19] För vägledning om ”sannolikt leder till en hög risk”, se fotnot 10.

57. Inte heller några kontaktuppgifter (t.ex. e-postadresser eller telefonnummer) äventyrades för de registrerade, vilket innebär att det inte finns någon betydande risk för att de registrerade ska utsättas för bedrägeriförsök (t.ex. nätfiske via e-post eller bedrägliga sms och telefonsamtal). Inga särskilda kategorier av personuppgifter påverkades.

58. Vissa användarnamn skulle kunna betraktas som personuppgifter, men webbplatsens innehåll har inga negativa konnotationer. Det måste dock noteras att riskbedömningen kan förändras[20] om typen av webbplats och de uppgifter som hämtades kan avslöja särskilda kategorier av personuppgifter (t.ex. ett politiskt partis eller en fackförenings webbplats). De negativa effekterna av incidenten kan mildras genom att använda modern kryptering. Genom att se till att antalet inloggningsförsök är begränsat kommer framgångsrika råstyrkeattacker att förhindras, vilket kraftigt minskar riskerna med angripare som redan känner till användarnamnen.

3.2.2 FALL nr 06 – Lindring och skyldigheter

59. Att underrätta de registrerade kan i vissa fall betraktas som en mildrande faktor, eftersom de registrerade också kan vidta nödvändiga åtgärder för att undvika ytterligare skador till följd av incidenten, till exempel byta lösenord. I detta fall var det inte obligatoriskt att anmäla incidenten, men det kan i många fall betraktas som god praxis.

60. Den personuppgiftsansvarige bör åtgärda sårbarheten och genomföra nya säkerhetsåtgärder för att undvika liknande uppgiftsincidenter i framtiden, till exempel systematiska säkerhetsgranskningar av webbplatsen.

61. Incidenten bör dokumenteras i enlighet med artikel 33.5, men ingen anmälan eller underrättelse behövs.

62. Det rekommenderas i samtliga fall kraftigt att informera de registrerade om incidenter som rör lösenord, även när lösenorden lagras genom en saltad hash med en modern algoritm. Det är lämpligt att använda autentiseringsmetoder som innebär att lösenord inte behöver behandlas på serversidan. De registrerade bör kunna välja att vidta lämpliga åtgärder när det gäller deras egna lösenord.

Nödvändiga åtgärder på grundval av identifierade risker		
Intern dokumentation	Anmälan till tillsynsmyndigheten	Information till de registrerade
✓	X	X

3.3 FALL nr 07: Stulen inloggningsattack på en bankwebbplats

[20] För vägledning om ”sannolikt leder till en hög risk”, se fotnot 10.

En bank drabbas av en cyberattack mot en av sina webbplatser. Attacken syftar till att lista alla möjliga inloggnings-id:n med ett fast trivialt lösenord. Lösenorden består av åtta siffror. På grund av en sårbarhet på webbplatsen läcker i vissa fall uppgifter om registrerade (namn, efternamn, kön, födelsedatum och födelseort, personnummer, användaridentifieringskoder) ut till angriparen, även om det lösenord som användes inte stämde eller bankkontot inte längre var aktivt. Detta påverkar runt 100 000 registrerade. Av dessa lyckas angriparen logga in på cirka 2 000 konton som använder det triviala lösenord som angriparen provade. Efter händelsen kunde den personuppgiftsansvarige identifiera alla misstänkta inloggningsförsök. Den personuppgiftsansvarige kunde bekräfta att inga transaktioner hade utförts av dessa konton under attacken, enligt bedrägerikontroller. Banken känner till uppgiftsincidenten eftersom dess säkerhetscentral upptäckte ett stort antal inloggningsförfrågningar mot webbplatsen. Som svar på händelsen inaktiverar den personuppgiftsansvarige möjligheten att logga in på webbplatsen genom att tillfälligt stänga ned den och tvinga de angripna kontona att återställa sina lösenord. Den personuppgiftsansvarige underrättar endast användarna med de angripna kontona om incidenten, dvs. de användare vars lösenord hade äventyrats eller vars uppgifter hade röjts.

3.3.1 FALL nr 07 – Tidigare åtgärder och riskbedömning

63. Det är viktigt att nämna att personuppgiftsansvariga som hanterar uppgifter av mycket personlig natur[21] har ett större ansvar när det gäller att tillhandahålla tillräcklig datasäkerhet, till exempel att ha ett säkerhetscenter och andra åtgärder för att förebygga, upptäcka och hantera incidenter. Om dessa högre standarder inte uppfylls kommer det helt klart att leda till allvarligare åtgärder under tillsynsmyndighetens undersökning.

64. Incidenten gäller finansiella uppgifter utöver identitetsuppgifter och uppgifter om användar-id, vilket gör den särskilt allvarlig. Antalet drabbade personer är stort.

65. Det faktum att en incident kunde inträffa i en så känslig miljö pekar på betydande datasäkerhetsbrister i den personuppgiftsansvariges system och kan vara ett tecken på att översyn och uppdatering av de berörda åtgärderna är ”nödvändig” i enlighet med artiklarna 24.1, 25.1 och 32.1 i dataskyddsförordningen. De berörda uppgifterna gör det möjligt att identifiera registrerade och innehåller annan information om dem (inklusive kön, födelsedatum och födelseort). Dessutom kan angriparen använda uppgifterna för att gissa kundernas lösenord eller för att genomföra en nätfiskekampanj riktad mot bankens kunder.

66. Av dessa skäl ansågs det sannolikt att uppgiftsincidenten skulle leda till en hög risk för alla berörda registrerades rättigheter och friheter[22]. Därför är materiell (t.ex. ekonomisk förlust) och immateriell skada (t.ex. identitetsstöld eller bedrägeri) ett tänkbart resultat.

3.3.2 FALL nr 07 – Lindring och skyldigheter

67. Den personuppgiftsansvariges åtgärder som nämns i fallbeskrivningen är lämpliga. I kölvattnet av incidenten åtgärdade den personuppgiftsansvarige också sårbarheten på webbplatsen och vidtog andra åtgärder för att

[21] Till exempel uppgifter om de registrerade som rör betalningsmetoder såsom kortnummer, bankkonton, onlinebetalning, löner, bankutdrag, ekonomiska undersökningar eller annan information som kan avslöja ekonomisk information om de registrerade.

[22] För vägledning om ”sannolikt leder till en hög risk”, se fotnot 10.

förhindra liknande framtida uppgiftsincidenter, såsom att lägga till tvåfaktorsautentisering på den berörda webbplatsen och övergå till kraftfull kundautentisering.

68. Det är i detta scenario obligatoriskt att dokumentera incidenten enligt artikel 33.5 i dataskyddsförordningen och underrätta tillsynsmyndigheten. Dessutom bör den personuppgiftsansvarige underrätta alla 100 000 registrerade (inklusive de registrerade vars konton inte äventyrades) i enlighet med artikel 34 i dataskyddsförordningen.

Nödvändiga åtgärder på grundval av identifierade risker		
Intern dokumentation	Anmälan till tillsynsmyndigheten	Information till de registrerade
✓	✓	✓

3.4 Organisatoriska och tekniska åtgärder för att förebygga/mildra effekterna av hackerattacker

69. Precis som vid utpressningsattacker är det obligatoriskt för personuppgiftsansvariga att se över it-säkerheten i liknande fall, oavsett resultatet och konsekvenserna av attacken.

70. Lämpliga åtgärder[23]:

(Förteckningen över följande åtgärder är inte på något sätt fullständig eller uttömmande. Målet är snarare att ge idéer till förebyggande och möjliga lösningar. Varje behandling är annorlunda, och därför bör den personuppgiftsansvarige fatta beslut om vilka åtgärder som bäst passar den givna situationen.)

- Använda modern kryptering och nyckelhantering, särskilt när lösenord och känsliga eller finansiella uppgifter behandlas. Kryptografisk hashning och saltning för hemlig information (lösenord) är alltid att föredra framför kryptering av lösenord. Användning av autentiseringsmetoder som innebär att lösenord inte behöver behandlas på serversidan är att föredra.
- Hålla systemet uppdaterat (programvara och inbyggd programvara). Se till att alla it-säkerhetsåtgärder vidtas och att de är effektiva och regelbundet uppdateras när behandlingen eller omständigheterna förändras eller utvecklas. För att kunna visa överensstämmelse med artikel 5.1 f i enlighet med artikel 5.2 i dataskyddsförordningen bör den personuppgiftsansvarige föra register över alla uppdateringar som utförs, inklusive den tidpunkt då de tillämpades.
- Använda kraftfulla autentiseringsmetoder såsom tvåfaktorsautentisering och autentiseringsservrar, som kompletteras med en uppdaterad lösenordspolicy.
- Använda säkra utvecklingsstandarder, inklusive filtrering av användarindata (med användning av godkännandelistor i den mån det är praktiskt möjligt), escaping av användarindata och åtgärder för att förhindra råstyrkeattacker (såsom att begränsa det maximala antalet försök). Brandväggar för webbaserade program kan bidra till en effektiv användning av denna teknik.
- Införa starka användarrättigheter och principer för hantering av åtkomstkontroll.
- Använda en lämplig, uppdaterad, effektiv och integrerad brandvägg samt intrångsupptäckssystem och andra system för perimeterförsvar.
- Utföra systematiska it-säkerhetsgranskningar och sårbarhetsbedömningar (penetrationstester).
- Utföra regelbundna granskningar och tester för att säkerställa att säkerhetskopior kan användas för att återskapa uppgifter vars integritet eller tillgänglighet har påverkats.
- Undvika sessions-ID i URL i oformaterad text.

[23] För säker utveckling av webbprogram, se även https://www.owasp.org/index.php/Main_Page.

4 INTERNA RISKER SOM ORSAKAS AV MÄNNISKOR

71. Den mänskliga faktorn vid personuppgiftsincidenter måste lyftas fram eftersom den är så vanlig. Eftersom dessa typer av incidenter kan vara både avsiktliga och oavsiktliga är det mycket svårt för de personuppgiftsansvariga att identifiera sårbarheterna och vidta åtgärder för att undvika dem. Den internationella konferensen för ombudsmän för dataskydds- och integritetsfrågor erkände vikten av att ta upp sådana mänskliga faktorer och antog en resolution för att behandla den roll som den mänskliga faktorn spelar vid personuppgiftsincidenter i oktober 2019[24]. I denna resolution betonas att lämpliga skyddsåtgärder bör vidtas för att förhindra mänskliga fel, och en icke uttömmande förteckning över sådana skyddsåtgärder och metoder tillhandahålls.

4.1 FALL nr 08: Exfiltrering av affärsuppgifter av en anställd

Under sin uppsägningstid kopierar en anställd vid ett företag affärsuppgifter från företagets databas. Den anställde får endast ta del av uppgifterna för att utföra sina arbetsuppgifter. Flera månader senare, efter att ha slutat jobbet, använder han de uppgifter han fått på detta sätt (grundläggande kontaktuppgifter) för en ny databehandling för vilken han är personuppgiftsansvarig för att kontakta företagets kunder och locka dem till sitt nya företag.

4.1.1 FALL nr 08 – Tidigare åtgärder och riskbedömning

72. I detta särskilda fall vidtogs inga tidigare åtgärder för att hindra den anställde från att kopiera kontaktuppgifter för företagets kunder, eftersom han behövde – och hade – rättmätig tillgång till denna information för sina arbetsuppgifter. Eftersom personalen behöver någon form av åtkomst till personuppgifter för att kunna utföra arbeten som rör kundrelationer kan dessa uppgiftsincidenter vara de svåraste att förhindra. Begränsningar av åtkomsten kan begränsa det arbete som den anställde kan utföra. En välgenomtänkt åtkomstpolicy och konstant kontroll kan dock bidra till att förhindra sådana incidenter.

73. Som vanligt ska hänsyn tas till typen av incident och de berörda personuppgifternas art, känslighet och volym vid riskbedömningen. Denna typ av incident utgör vanligtvis ett konfidentialitetsbrott, eftersom databasen oftast lämnas intakt och dess innehåll ”bara” kopieras för vidare användning. Mängden uppgifter som påverkas är vanligtvis också liten eller medelstor. I detta särskilda fall påverkades inga särskilda kategorier av personuppgifter. Den anställde behövde bara kundernas kontaktuppgifter för att kunna kontakta dem efter att han hade lämnat företaget. De berörda uppgifterna är därför inte känsliga.

74. Även om det enda målet för den tidigare anställde som uppsåtligen kopierade uppgifterna kan begränsas till att få kontaktuppgifter för företagets kunder för sina egna kommersiella syften kan den personuppgiftsansvarige inte betrakta risken för de berörda registrerade som låg, eftersom den personuppgiftsansvarige inte känner till den anställdes avsikter. Konsekvenserna av incidenten kan därför begränsas till exponering för oönskad marknadsföring av den tidigare anställde, men man kan inte utesluta ytterligare och allvarligare missbruk av de stulna uppgifterna, beroende på syftet med den behandling som den tidigare anställde utför[25].

[24] http://globalprivacyassembly.org/wp-content/uploads/2019/10/AOIC-Resolution-FINAL-ADOPTED.pdf.

[25] För vägledning om ”sannolikt leder till en hög risk”, se fotnot 10.

4.1.2 FALL nr 08 – Lindring och skyldigheter

75. Det är svårt att mildra de negativa effekterna av incidenten i det ovannämnda fallet. Det kan bli nödvändigt att vidta omedelbara rättsliga åtgärder för att förhindra att den tidigare anställde missbrukar och sprider uppgifterna ytterligare. Som ett nästa steg bör målet vara att undvika liknande situationer i framtiden. Den personuppgiftsansvarige kan försöka beordra den tidigare anställde att sluta använda uppgifterna, men det är i bästa fall tveksamt om detta lyckas. Lämpliga tekniska åtgärder, till exempel att det inte går att kopiera eller ladda ned uppgifter till flyttbara enheter, kan hjälpa.

76. Det finns ingen lösning som passar alla dessa typer av fall, men ett systematiskt tillvägagångssätt kan bidra till att förhindra dem. Företaget kan till exempel överväga att om möjligt återkalla vissa former av åtkomst för anställda som har tillkännagett att de tänker säga upp sig eller införa åtkomstloggar så att oönskad åtkomst kan loggas och flaggas. Anställningsavtalet bör innehålla klausuler som förbjuder sådana handlingar.

77. På det hela taget räcker det med en anmälan till tillsynsmyndigheten, eftersom incidenten inte kommer att leda till en hög risk för fysiska personers rättigheter och friheter. Det kan dock gynna den personuppgiftsansvarige att underrätta de registrerade, eftersom det kan vara bättre att de hör talas om uppgiftsläckan från företaget än från den tidigare anställde som försöker kontakta dem. Det är en rättslig skyldighet att dokumentera uppgiftsincidenter i enlighet med artikel 33.5.

Nödvändiga åtgärder på grundval av identifierade risker		
Intern dokumentation	Anmälan till tillsynsmyndigheten	Information till de registrerade
✓	✓	X

4.2 FALL nr 09: Oavsiktlig överföring av uppgifter till en betrodd tredje part

En försäkringsagent noterar – vilket möjliggörs av de felaktiga inställningarna i en Excel-fil som mottas per e-post – att han kan få tillgång till information om ett tjugotal kunder som inte hör till hans område. Han har tystnadsplikt och är den ende som får mejlet. Enligt avtalet mellan den personuppgiftsansvarige och försäkringsagenten ska agenten utan onödigt dröjsmål underrätta den personuppgiftsansvarige om en personuppgiftsincident inträffar. Därför underrättar agenten omedelbart den personuppgiftsansvarige om misstaget, som korrigerar filen och skickar ut den igen, och ber agenten att radera det tidigare mejlet. Enligt ovannämnda avtal måste agenten bekräfta raderingen i en skriftlig förklaring, vilket han gör. Den information som erhölls omfattade inga särskilda kategorier av personuppgifter, endast kontaktuppgifter och uppgifter om själva försäkringen (försäkringstyp, belopp). Efter att ha analyserat de personuppgifter som berördes av incidenten identifierade den personuppgiftsansvarige inte några särskilda egenskaper vad gäller de enskilda personerna eller den personuppgiftsansvarige som kan påverka incidentens inverkan.

4.2.1 FALL nr 09 – Tidigare åtgärder och riskbedömning

78. Här beror incidenten inte på en anställds avsiktliga handling, utan på ett oavsiktligt mänskligt fel orsakat av ouppmärksamhet. Denna typ av incident kan undvikas eller minskas genom att a) genomföra program för utbildning och medvetandegörande där de anställda får en bättre förståelse för vikten av skydd av personuppgifter, b) minska filutbytet via e-post och i stället använda särskilda system för behandling av kunduppgifter, c) dubbelkolla filer innan de skickas, d) skapa och skicka filer separat.

79. Denna uppgiftsincident gäller endast uppgifternas konfidentialitet, och uppgifternas integritet och tillgänglighet lämnas intakt. Uppgiftsincidenten berörde endast ett tjugotal kunder, vilket innebär att den berörda mängden uppgifter kan anses vara liten. Dessutom innehåller de berörda personuppgifterna inga känsliga uppgifter. Det faktum att personuppgiftsbiträdet omedelbart kontaktade den personuppgiftsansvarige efter att ha blivit varse om incidenten kan betraktas som en riskreducerande faktor. (Möjligheten att uppgifter har skickats till andra försäkringsagenter bör också undersökas och lämpliga åtgärder bör vidtas om detta bekräftas vara fallet.) På grund av de lämpliga åtgärder som vidtogs efter uppgiftsincidenten kommer den sannolikt inte att påverka de registrerades rättigheter och friheter.

80. Kombinationen av det låga antalet berörda personer, det faktum att incidenten upptäcktes omedelbart och de åtgärder som vidtogs för att minimera dess effekter innebär att detta fall inte utgör någon risk.

4.2.2 FALL nr 09 – Lindring och skyldigheter

81. Andra riskreducerande omständigheter spelar också in: agenten har tystnadsplikt, han rapporterade själv problemet till den personuppgiftsansvarige och han tog bort filen på begäran. Att öka medvetenheten och eventuellt inbegripa ytterligare åtgärder för att kontrollera dokument som innehåller personuppgifter kommer troligen att bidra till att undvika liknande fall i framtiden.

82. Utöver att dokumentera incidenten i enlighet med artikel 33.5 behövs ingen annan åtgärd.

Nödvändiga åtgärder på grundval av identifierade risker		
Intern dokumentation	Anmälan till tillsynsmyndigheten	Information till de registrerade
✓	X	X

4.3 Organisatoriska och tekniska åtgärder för att förebygga/mildra effekterna av interna mänskliga riskkällor

83. En kombination av nedanstående åtgärder – som tillämpas beroende på hur fallet ser ut – bör bidra till att minska risken för att en liknande incident sker igen.

84. Lämpliga åtgärder:

(Förteckningen över följande åtgärder är inte på något sätt fullständig eller uttömmande. Målet är snarare att ge idéer till förebyggande och möjliga lösningar. Varje behandling är annorlunda, och därför bör den personuppgiftsansvarige fatta beslut om vilka åtgärder som bäst passar den givna situationen.)

- Regelbundet genomföra program för utbildning och medvetandegörande för anställda om deras integritets- och säkerhetsskyldigheter samt upptäckt och rapportering av hot mot säkerheten för personuppgifter[26]. Utveckla ett informationsprogram för att påminna de anställda om de vanligaste felen som leder till personuppgiftsincidenter och hur de kan undvikas.
- Inrätta robusta och effektiva rutiner, förfaranden och system för dataskydd och integritet[27].
- Utvärdera rutiner, förfaranden och system för integritet för att säkerställa fortsatt ändamålsenlighet[28].
- Skapa lämpliga principer för åtkomstkontroll och tvinga användarna att följa reglerna.
- Införa metoder för att kräva användarautentisering när känsliga personuppgifter tillhandahålls.
- Inaktivera användarens företagsrelaterade konto så fort personen slutar på företaget.
- Kontrollera ovanliga dataflöden mellan filservern och de anställdas arbetsstationer.
- Ställa in gränssnittssäkerhet för I/O i BIOS eller genom att använda programvara som kontrollerar användningen av datorgränssnitt (t.ex. USB/CD/DVD).
- Se över åtkomstpolicyn för anställda (t.ex. logga åtkomst till känsliga uppgifter och kräva att användaren anger ett affärsmässigt skäl, så att detta är tillgängligt vid granskningar).
- Koppla bort öppna molntjänster.
- Förbjuda och förhindra tillgång till kända öppna e-posttjänster.
- Koppla bort funktionen för att ta skärmbilder i operativsystemet.
- Tillämpa en så kallad *clean desk policy*.
- Låsa alla datorer automatiskt efter en viss tid av inaktivitet.
- Använda mekanismer (t.ex. en (trådlös) token för att logga in på eller öppna låsta konton) för snabba användarbyten i gemensamma miljöer.
- Använda särskilda system för hantering av personuppgifter som har lämpliga mekanismer för åtkomstkontroll och förhindrar mänskliga misstag, såsom att meddelanden skickas till fel person. Det är inte lämpligt att använda kalkylblad och andra kontorsdokument för att hantera kunduppgifter.

5 BORTTAPPADE ELLER STULNA ENHETER OCH PAPPERSDOKUMENT

85. Ett vanligt förekommande fall är förlust eller stöld av bärbara enheter. I dessa fall måste den personuppgiftsansvarige ta hänsyn till omständigheterna kring behandlingen, såsom typen av uppgifter som lagras på enheten samt stödtillgångarna, och de åtgärder som vidtagits före incidenten för att säkerställa en

[26] Underavsnitt i i avsnitt 2 i resolutionen för att behandla den roll som den mänskliga faktorn spelar vid personuppgiftsincidenter.

[27] Underavsnitt ii i avsnitt 2 i resolutionen för att behandla den roll som den mänskliga faktorn spelar vid personuppgiftsincidenter.

[28] Underavsnitt iii i avsnitt 2 i resolutionen för att behandla den roll som den mänskliga faktorn spelar vid personuppgiftsincidenter.

lämplig säkerhetsnivå. Allt detta påverkar de potentiella effekterna av uppgiftsincidenten. Riskbedömningen kan vara svår eftersom enheten inte längre är tillgänglig.

86. Denna typ av incident kan alltid klassificeras som konfidentialitetsbrott. Men om det inte finns någon säkerhetskopia av den stulna databasen kan det också vara ett tillgänglighetsbrott och ett integritetsbrott.

87. Scenarierna nedan visar hur de ovan nämnda omständigheterna påverkar uppgiftsincidentens sannolikhet och allvarlighetsgrad.

5.1 FALL nr 10: Stulet material med krypterade personuppgifter

Vid ett inbrott på en förskola stjäls två datorplattor. På plattorna finns en app med personuppgifter för barnen som går på förskolan. Det gäller namn, födelsedatum och personuppgifter om barnens utbildning. Båda de krypterade plattorna är avstängda vid inbrottet och appen skyddas av ett starkt lösenord. Säkerhetskopierade uppgifter finns faktiskt och lätt tillgängliga för den personuppgiftsansvarige. Efter att ha blivit varse om inbrottet kör förskolan ett fjärrkommando för att rensa plattorna kort efter att inbrottet upptäcks.

5.1.1 FALL nr 10 – Tidigare åtgärder och riskbedömning

88. I detta särskilda fall vidtog den personuppgiftsansvarige lämpliga åtgärder för att förhindra och mildra effekterna av en potentiell uppgiftsincident genom att använda enhetskryptering, införa lämpligt lösenordsskydd och se till att uppgifter som lagras på datorplattorna säkerhetskopieras. (En förteckning över lämpliga åtgärder finns i avsnitt 5.7.)

89. Efter att ha blivit varse om en incident bör den personuppgiftsansvarige bedöma riskkällan, de system som används vid uppgiftsbehandlingen, vilken typ av personuppgifter som berörs och uppgiftsincidentens potentiella effekter på de berörda personerna. Den personuppgiftsincident som beskrivs ovan skulle ha kunnat utgöra brott mot uppgifternas konfidentialitet, tillgänglighet och integritet, men på grund av den personuppgiftsansvariges lämpliga åtgärder före och efter uppgiftsincidenten uppstod inget av dessa.

5.1.2 FALL nr 10 – Lindring och skyldigheter

90. Konfidentialiteten hos personuppgifterna på enheterna äventyrades inte på grund av det starka lösenordsskyddet på både datorplattorna och apparna. Plattorna hade konfigurerats på ett sådant sätt att uppgifterna på enheten krypteras när ett lösenord ställs in. Detta förstärktes ytterligare av den personuppgiftsansvariges försök att fjärrensa allt från de stulna enheterna.

91. På grund av de åtgärder som vidtogs bevarades även uppgifternas konfidentialitet. Dessutom säkerställde säkerhetskopieringen att personuppgifterna var fortsatt tillgängliga, och därför kunde ingen potentiell negativ inverkan ha inträffat.

92. På grund av dessa omständigheter var det osannolikt att den ovan beskrivna uppgiftsincidenten skulle leda till en risk för de registrerades rättigheter och friheter, och därför var det inte nödvändigt med någon anmälan till tillsynsmyndigheten eller information till de berörda registrerade. Incidenten måste dock dokumenteras i enlighet med artikel 33.5.

Nödvändiga åtgärder på grundval av identifierade risker		
Intern dokumentation	Anmälan till tillsynsmyndigheten	Information till de registrerade
✓	X	X

5.2 FALL nr 11: Stulet material med okrypterade personuppgifter

En elektronisk bärbar dator tillhörande en anställd vid ett tjänsteleverantörsföretag stjäls. Den stulna datorn innehåller namn, efternamn, kön, adress och födelsedatum för mer än 100 000 kunder. Eftersom den stulna enheten inte är tillgänglig går det inte att identifiera om andra kategorier av personuppgifter också berörs. Åtkomsten till datorns hårddisk skyddas inte av något lösenord. Personuppgifter kan återskapas från dagliga säkerhetskopieringar som finns tillgängliga.

5.2.1 FALL nr 11 – Tidigare åtgärder och riskbedömning

93. Den personuppgiftsansvarige vidtog inga tidigare säkerhetsåtgärder, och därför var de personuppgifter som lagrades på den stulna datorn lätta att komma åt för tjuven eller någon annan som därefter kom över enheten.

94. Denna uppgiftsincident gäller konfidentialiteten hos de uppgifter som lagras på den stulna enheten.

95. Den dator som innehöll personuppgifterna var sårbar i det här fallet eftersom den inte hade något lösenordsskydd eller någon kryptering. Avsaknaden av grundläggande säkerhetsåtgärder ökar risken för de berörda registrerade. Dessutom är det svårt att identifiera de berörda registrerade, vilket också ökar incidentens allvar. Det stora antalet berörda personer ökar risken, men inga särskilda kategorier av personuppgifter berördes av uppgiftsincidenten.

96. Under riskbedömningen[29] bör den personuppgiftsansvarige beakta de potentiella konsekvenserna och de negativa effekterna av konfidentialitetsbrottet. Till följd av incidenten kan de berörda registrerade utsättas för identitetsbedrägeri som bygger på uppgifterna på den stulna enheten, och risken anses därför vara hög.

5.2.2 FALL nr 11 – Lindring och skyldigheter

97. Att aktivera enhetskryptering och använda ett starkt lösenordsskydd för den lagrade databasen kunde ha förhindrat att uppgiftsincidenten ledde till en risk för de registrerades rättigheter och friheter.

98. På grund av dessa omständigheter måste en anmälan göras till tillsynsmyndigheten och de berörda registrerade måste underrättas.

Nödvändiga åtgärder på grundval av identifierade risker		
Intern dokumentation	Anmälan till tillsynsmyndigheten	Information till de registrerade
✓	✓	✓

5.3 FALL nr 12: Stulna pappersfiler med känsliga uppgifter

[29] För vägledning om ”sannolikt leder till en hög risk”, se fotnot 10.

En loggbok i papper stjäls från ett behandlingshem för narkotikamissbruk. Boken innehåller grundläggande identitets- och hälsouppgifter för patienter som är inlagda på behandlingshemmet. Uppgifterna lagras endast på papper och det finns ingen säkerhetskopia för de läkare som behandlar patienterna. Boken förvarades inte i en låst låda eller ett låst rum, och den personuppgiftsansvarige hade varken ett system för åtkomstkontroll eller någon annan skyddsåtgärd för

5.3.1 FALL nr 12 – Tidigare åtgärder och riskbedömning

99. Den personuppgiftsansvarige vidtog inga säkerhetsåtgärder i förväg, och därför var de personuppgifter som lagrades i boken lätta att komma åt för den som hittade den. Dessutom innebär arten av de personuppgifter som lagras i boken att bristen på säkerhetskopierade uppgifter är en mycket allvarlig riskfaktor.

100. Det här fallet fungerar som ett exempel på en uppgiftsincident med hög risk. På grund av underlåtenheten att vidta lämpliga säkerhetsåtgärder gick känsliga hälsouppgifter i enlighet med artikel 9.1 i dataskyddsförordningen förlorade. Eftersom det i detta fall rörde sig om en särskild kategori av personuppgifter ökade de potentiella riskerna för de berörda registrerade, vilket också bör beaktas av den personuppgiftsansvarige vid riskbedömningen[30].

101. Denna incident gäller de berörda personuppgifternas konfidentialitet, tillgänglighet och integritet. Till följd av incidenten bryts den medicinska sekretessen och obehöriga tredje parter kan få tillgång till patienternas privata medicinska information, vilket kan få allvarliga konsekvenser för patientens privatliv. Tillgänglighetsbrottet kan också störa kontinuiteten i patientens behandling. Eftersom ändring/radering av delar av bokens innehåll inte kan uteslutas äventyras även personuppgifternas integritet.

5.3.2 FALL nr 12 – Lindring och skyldigheter

102. Vid bedömningen av skyddsåtgärder bör även typen av stödtillgång beaktas. Eftersom patientloggboken var ett fysiskt dokument borde den ha skyddats annorlunda än en elektronisk enhet. Pseudonymisering av patienternas namn, förvaring av boken i en skyddad lokal och i en låst låda eller ett låst rum samt ordentlig åtkomstkontroll med autentisering när boken tas fram kunde ha förhindrat uppgiftsincidenten.

103. Den ovan beskrivna incidenten kan allvarligt påverka de berörda registrerade. Det är därför obligatoriskt att göra en anmälan till tillsynsmyndigheten och underrätta de berörda registrerade.

Nödvändiga åtgärder på grundval av identifierade risker		
Intern dokumentation	Anmälan till tillsynsmyndigheten	Information till de registrerade
✓	✓	✓

5.4 Organisatoriska och tekniska åtgärder för att förebygga/mildra effekterna av förlust eller stöld av enheter

104. En kombination av nedanstående åtgärder – som tillämpas beroende på hur fallet ser ut – bör bidra till att minska risken för att en liknande incident sker igen.

105. Lämpliga åtgärder:

(Förteckningen över följande åtgärder är inte på något sätt fullständig eller uttömmande. Målet är snarare att ge idéer till förebyggande och möjliga lösningar. Varje behandling är annorlunda, och därför bör den personuppgiftsansvarige fatta beslut om vilka åtgärder som bäst passar den givna situationen.)

[30] För vägledning om ”sannolikt leder till en hög risk”, se fotnot 10.

- Aktivera enhetskryptering (t.ex. Bitlocker, Veracrypt eller DM-Crypt).
- Använda lösenkod/lösenord på alla enheter. Kryptera alla mobila elektroniska enheter så att ett komplext lösenord krävs för dekryptering.
- Använda flerfaktorsautentisering.
- Slå på de funktioner hos mycket mobila enheter som gör att de kan lokaliseras om de förloras eller förläggs.
- Använda en programvara/app för MDM (*Mobile Device Management*) och lokalisering. Använda sekretessfilter för skärmen. Stänga av alla enheter som lämnas obevakade.
- Undvika att spara personuppgifter på mobila enheter utan i stället göra det på en central backend-server, om det är möjligt och lämpligt för databehandlingen i fråga.
- Göra en automatisk säkerhetskopiering av arbetsmapparna om det är oundvikligt att personuppgifter lagras där (om arbetsstationen är ansluten till företagets lokala nät).
- Använda en säker VPN (som till exempel kräver en separat tvåfaktorsautentiseringsnyckel för att upprätta en säker anslutning) för att ansluta mobila enheter till backend-servrar.
- Ge de anställda fysiska lås så att de kan säkra sina mobila enheter fysiskt när de lämnas obevakade.
- Reglera användningen av enheter utanför företagets lokaler på lämpligt sätt.
- Reglera användningen av enheter i företagets lokaler på lämpligt sätt.
- Använda en programvara/app för MDM (*Mobile Device Management*) och aktivera funktionen för fjärrensning.
- Använda centraliserad enhetshantering med minimirättigheter för slutanvändarna att installera programvara.
- Installera fysiska åtkomstkontroller.
- Undvika att lagra känslig information på mobila enheter eller hårddiskar. Om någon behöver komma åt företagets interna system bör säkra kanaler användas, såsom tidigare angetts.

6 FEL POST ELLER MEJL

106. Riskkällan är även i detta fall ett internt mänskligt fel, men här har ingen fientlig handling lett till incidenten. Den beror på ouppmärksamhet. Den personuppgiftsansvarige kan inte göra så mycket efter det att incidenten inträffat, så förebyggande är ännu viktigare i dessa fall än vid andra typer av incidenter.

6.1 FALL nr 13: Postfel

Två beställningar av skor packas av ett detaljhandelsföretag. På grund av den mänskliga faktorn blandas två följesedlar ihop, vilket resulterar i att både produkterna och de relevanta följesedlarna skickas till fel person. Detta innebär att de två kunderna får varandras beställningar, inklusive följesedlarna med personuppgifter. Efter att ha blivit varse om incidenten återkallar den personuppgiftsansvarige beställningarna och skickar dem till rätt mottagare.

6.1.1 FALL nr 13 – Tidigare åtgärder och riskbedömning

107. Följesedlarna innehöll de personuppgifter som krävdes för leveransen (namn och adress, plus den inköpta varan och dess pris). Det är viktigt att identifiera hur det mänskliga felet kunde ha inträffat från början, och om det på något sätt hade kunnat förhindras. I detta särskilda fall beskrivs risken som låg eftersom det inte rör sig om några särskilda kategorier av personuppgifter eller andra uppgifter vars missbruk kan leda till betydande negativa effekter, incidenten inte beror på ett systemfel från den personuppgiftsansvariges sida och endast två personer berörs. Det gick inte att identifiera några negativa effekter på de enskilda personerna.

6.1.2 FALL nr 13 – Lindring och skyldigheter

108. Den personuppgiftsansvarige bör erbjuda gratis retur av varorna och tillhörande följesedlar, och även begära att de felaktiga mottagarna förstör/raderar alla eventuella kopior av följesedlarna med den andra personens personuppgifter.

109. Även om incidenten i sig inte utgör en stor risk för de berörda personernas rättigheter och friheter, och det därför inte föreskrivs att de registrerade ska informeras enligt artikel 34 i dataskyddsförordningen, går det inte att undvika att informera dem om incidenten eftersom deras samarbete behövs för att risken ska lindras.

Nödvändiga åtgärder på grundval av identifierade risker		
Intern dokumentation	Anmälan till tillsynsmyndigheten	Information till de registrerade
✓	X	X

6.2 FALL nr 14: Mycket konfidentiella personuppgifter som av misstag skickas per e-post

Rekryteringsavdelningen vid en offentlig myndighet skickar ett mejl om kommande kurser till de som är registrerade som arbetssökande i dess system. Av misstag bifogas ett dokument med alla dessa arbetssökandes personuppgifter (namn, e-postadress, postadress, personnummer) till mejlet. Antalet berörda personer är över 60 000. Efter detta kontaktar avdelningen alla mottagare och ber dem att radera föregående mejl och inte använda informationen i det.

6.2.1 FALL nr 14 – Tidigare åtgärder och riskbedömning

110. Strängare regler borde ha införts för att skicka sådana mejl. Införandet av ytterligare kontrollmekanismer måste övervägas.

111. Antalet berörda personer är betydande, och det faktum att deras personnummer är med tillsammans med andra mer grundläggande personuppgifter ökar ytterligare risken, som kan identifieras som hög[31]. Den personuppgiftsansvarige kan inte hindra någon av mottagarna från att sprida uppgifterna.

6.2.2 FALL nr 14 – Lindring och skyldigheter

112. Som nämnts tidigare är medlen för att effektivt minska riskerna för en liknande incident begränsade. Även om den personuppgiftsansvarige begärde att mejlet skulle raderas kan den inte tvinga mottagarna att göra det, och följaktligen kan den inte heller vara säker på att de respekterar begäran.

113. Det bör vara en självklarhet att alla tre åtgärder som anges nedan vidtas i ett fall som detta.

Nödvändiga åtgärder på grundval av identifierade risker		
Intern dokumentation	Anmälan till tillsynsmyndigheten	Information till de registrerade
✓	✓	✓

6.3 FALL nr 15: Personuppgifter som av misstag skickas per e-post

[31] För vägledning om ”sannolikt leder till en hög risk”, se fotnot 10.

En lista över deltagare på en kurs i juridisk engelska som äger rum på ett hotell i fem dagar skickas av misstag till 15 tidigare kursdeltagare i stället för till hotellet. Listan innehåller namn, e-postadresser och matpreferenser för de 15 deltagarna. Endast två deltagare har fyllt i sina matpreferenser och uppgett att de är laktosintoleranta. Ingen av deltagarna har skyddad identitet. Den personuppgiftsansvarige upptäcker felet omedelbart efter att ha skickat listan och informerar mottagarna om felet och ber dem radera listan.

6.3.1 FALL nr 15 – Tidigare åtgärder och riskbedömning

114. Stränga regler borde ha införts för att skicka mejl som innehåller personuppgifter. Införandet av ytterligare kontrollmekanismer måste övervägas.

115. Riskerna som följer av personuppgifternas art, känslighet, volym och sammanhang är låga. Personuppgifterna omfattar känsliga uppgifter om matpreferenser för två av deltagarna. Även om informationen att någon är laktosintolerant är en hälsouppgift bör risken för att dessa uppgifter används på ett skadligt sätt anses vara relativt låg. När det gäller hälsouppgifter antas det vanligtvis att incidenten sannolikt kommer att leda till en hög risk för den registrerade[32], men samtidigt kan ingen risk i detta särskilda fall identifieras för att incidenten kommer att leda till fysisk, materiell eller immateriell skada för den registrerade på grund av otillåtet utlämnande av information om laktosintolerans. Till skillnad från vissa andra matpreferenser kan laktosintolerans normalt inte kopplas till någon religiös eller filosofisk övertygelse. Mängden berörda uppgifter och antalet berörda registrerade är också mycket lågt.

6.3.2 FALL nr 15 – Lindring och skyldigheter

116. Sammanfattningsvis kan det konstateras att incidenten inte hade någon betydande inverkan på de registrerade. Det faktum att den personuppgiftsansvarige omedelbart kontaktade mottagarna efter att ha blivit varse om misstaget kan betraktas som en riskreducerande faktor.

117. Om ett mejl skickas till fel mottagare eller till en obehörig mottagare rekommenderas det att den personuppgiftsansvarige skickar ett uppföljningsmejl i form av en dold kopia (BCC) till de icke avsedda mottagarna och ber om ursäkt, uppmanar dem att radera det felaktiga mejlet och informerar dem om att de inte har rätt att använda de e-postadresser som identifierats för dem.

118. På grund av dessa omständigheter var det osannolikt att denna uppgiftsincident skulle leda till en risk för de registrerades rättigheter och friheter, och därför var det inte nödvändigt med någon anmälan till tillsynsmyndigheten eller information till de berörda registrerade. Incidenten måste dock dokumenteras i enlighet med artikel 33.5.

Nödvändiga åtgärder på grundval av identifierade risker		
Intern dokumentation	Anmälan till tillsynsmyndigheten	Information till de registrerade
✓	X	X

6.4 FALL nr 16: Postfel

[32] Se riktlinjerna WP250, s. 23.

Ett försäkringsbolag erbjuder bilförsäkringar. För att göra detta skickar bolaget ut regelbundet justerade försäkringsbrev per post. Utöver försäkringstagarens namn och adress innehåller brevet fordonets registreringsnummer utan dolda siffror, försäkringskostnaderna för innevarande och nästa försäkringsår, den ungefärliga årliga körsträckan och försäkringstagarens födelsedatum. Inga hälsouppgifter enligt artikel 9 i dataskyddsförordningen, betalningsuppgifter (bankuppgifter) eller ekonomiska och finansiella uppgifter ingår.

Breven förpackas med automatiska kuverteringsmaskiner. På grund av ett mekaniskt fel läggs två brev till olika försäkringstagare i ett och samma kuvert och skickas till en försäkringstagare per post. Försäkringstagaren öppnar brevet hemma och tittar både på det korrekt skickade brevet och på det felaktigt skickade brevet till den andra försäkringstagaren.

6.4.1 FALL nr 16 – Tidigare åtgärder och riskbedömning

119. Det felaktigt skickade brevet innehåller namn, adress, födelsedatum, icke dolt registreringsnummer och klassificering av försäkringskostnaden för innevarande och nästa år. Effekterna på den berörda personen ska betraktas som medelhöga, eftersom information som inte är allmänt tillgänglig, såsom födelsedatum och icke dolt registreringsnummer, och uppgifter om ökningen av försäkringskostnaden lämnas ut till en obehörig mottagare. Sannolikheten för att dessa uppgifter ska missbrukas bedöms vara låg till medelhög. Även om många mottagare förmodligen kommer att slänga det felaktigt mottagna brevet kan det i enskilda fall inte helt uteslutas att brevet läggs upp på sociala medier eller att försäkringstagaren kontaktas.

6.4.2 FALL nr 16 – Lindring och skyldigheter

120. Den personuppgiftsansvarige bör få tillbaka originaldokumentet på egen bekostnad. Den felaktiga mottagaren bör också informeras om att den lästa informationen inte får missbrukas.

121. Det kommer förmodligen aldrig att gå att helt förhindra att post delas ut till fel person vid massutskick med helautomatiserade maskiner. Om frekvensen ökar måste man dock kontrollera om kuverteringsmaskinerna är rätt inställda och underhålls ordentligt, eller om något annat systemproblem leder till sådana incidenter.

Nödvändiga åtgärder på grundval av identifierade risker		
Intern dokumentation	Anmälan till tillsynsmyndigheten	Information till de registrerade
✓	✓	X

6.5 Organisatoriska och tekniska åtgärder för att förebygga/mildra effekterna av postfel

122. En kombination av nedanstående åtgärder – som tillämpas beroende på hur fallet ser ut – bör bidra till att minska risken för att en liknande incident sker igen.

123. Lämpliga åtgärder:

(Förteckningen över följande åtgärder är inte på något sätt fullständig eller uttömmande. Målet är snarare att ge idéer till förebyggande och möjliga lösningar. Varje behandling är annorlunda, och därför bör den personuppgiftsansvarige fatta beslut om vilka åtgärder som bäst passar den givna situationen.)

- Fastställa exakta standarder – utan något utrymme för tolkning – för att skicka brev/mejl.
- Ordna lämplig utbildning för personalen i hur man skickar brev/mejl.
- Se till att när mejl skickas till flera mottagare visas de som standard i BCC-fältet (dold kopia).
- Kräva extra bekräftelse när mejl skickas till flera mottagare och de inte visas i BCC-fältet.
- Tillämpa fyra ögon-principen.
- Använda automatisk adressering i stället för manuell, med automatisk hämtning av uppgifter från en tillgänglig och uppdaterad databas. Systemet för automatisk adressering bör granskas regelbundet för att kontrollera om det finns dolda fel eller felaktiga inställningar.

- Tillämpa meddelandefördröjning (t.ex. att mejl kan raderas/redigeras inom en viss tid efter att de har skickats).
- /Koppla bort funktionen för textförslag när e-postadresser skrivs in.
- Ordna informationsmöten om de vanligaste misstagen som leder till personuppgiftsincidenter.
- Ordna utbildning och ta fram handböcker om hur man hanterar händelser som leder till personuppgiftsincidenter och vem som ska informeras (involvera dataskyddsombudet).

7 ANDRA FALL – SOCIAL MANIPULERING

7.1 FALL nr 17: Identitetsstöld

Ett telekommunikationsföretags kontaktcentrum får ett telefonsamtal från en person som utger sig för att vara en kund. Den påstådda kunden kräver att företaget ändrar den e-postadress till vilken faktureringsinformationen ska skickas. Personen på kontaktcentrumet validerar kundens identitet genom att be om vissa personuppgifter, i enlighet med företagets rutiner. Den uppringande parten anger korrekt kundens personnummer och adress (eftersom han hade tillgång till dessa). Efter valideringen gör operatören den begärda ändringen och från och med då skickas faktureringsinformationen till den nya e-postadressen. I enlighet med förfarandet skickas inget meddelande till den förra e-postadressen. Månaden därpå kontaktar den riktiga kunden företaget och frågar varför han inte fått någon faktura till sin e-postadress, och nekar till alla samtal från honom om att e-postadressen ska ändras. Senare inser företaget att informationen har skickats till en illegitim användare och ångrar ändringen.

7.1.1 FALL nr 17 – Riskbedömning, lindring och skyldigheter

124. Det här fallet fungerar som ett exempel på vikten av tidigare åtgärder. Utifrån en riskaspekt utgör incidenten en hög risk[33], eftersom faktureringsuppgifter kan ge information om den registrerades privatliv (t.ex. vanor, kontakter) och leda till materiella skador (t.ex. stalkning, risk för personens fysiska integritet). De personuppgifter som erhölls under denna attack kan också användas för att underlätta kontokapning i denna organisation eller för att utnyttja ytterligare autentiseringsmetoder i andra organisationer. Med tanke på dessa risker bör den ”lämpliga” autentiseringsmetoden uppnå en hög nivå, beroende på vilka personuppgifter som kan behandlas till följd av autentisering.

125. Därför krävs både en anmälan till tillsynsmyndigheten och information till den registrerade från den personuppgiftsansvarige.

126. Mot bakgrund av detta fall är det uppenbart att den föregående processen för kundvalidering måste förfinas. De metoder som användes för autentisering var inte tillräckliga. Den fientliga parten kunde låtsas vara den avsedda användaren genom att använda offentligt tillgänglig information och information som parten hade tillgång till på annat sätt.

[33] För vägledning om ”sannolikt leder till en hög risk”, se fotnot 10.

127. Det rekommenderas inte att använda denna typ av statisk kunskapsbaserad autentisering (där svaret inte ändras och där informationen inte är ”hemlig”, i motsats till ett lösenord).

128. I stället bör organisationen använda en form av autentisering som leder till stort förtroende för att den autentiserade användaren är den avsedda personen, och inte någon annan. Införandet av en metod för flerfaktorsautentisering utanför bandet skulle lösa problemet, till exempel att verifiera begäran om ändring genom att skicka ett bekräftelsemeddelande till den tidigare e-postadressen eller ställa ytterligare frågor och kräva information som endast syns på de tidigare fakturorna. Det är den personuppgiftsansvariges ansvar att besluta om vilka åtgärder som ska införas, eftersom denne bäst känner till detaljerna och kraven för sin interna verksamhet.

Nödvändiga åtgärder på grundval av identifierade risker		
Intern dokumentation	Anmälan till tillsynsmyndigheten	Information till de registrerade
✓	✓	✓

7.2 FALL nr 18: E-postexfiltrering

En stormarknadskedja upptäcker tre månader efter konfigurationen att vissa e-postkonton har ändrats och regler skapats så att varje mejl som innehåller vissa uttryck (t.ex. ”faktura”, ”betalning”, ”banköverföring”, ”autentisering av kreditkort”, ”bankkontouppgifter”) flyttas till en oanvänd mapp och även vidarebefordras till en extern e-postadress. Vid den tidpunkten har dessutom en social manipuleringsattack redan genomförts, dvs. angriparen, som utgett sig för att vara en leverantör, har fått den riktiga leverantörens bankkontouppgifter ändrade till sina egna. Samtidigt har flera falska fakturor skickats med de nya bankkontouppgifterna. E-postplattformens övervakningssystem varnar till sist om mapparna. Företaget kan inte identifiera hur angriparen kunde få åtkomst till e-postkontona från början, men antar att det var ett infekterat mejl som hade gett åtkomst till den grupp av användare som ansvarade för betalningarna.

Via den nyckelordsbaserade vidarebefordran av mejl har angriparen fått följande information om 99 anställda: namn och lön för en viss månad avseende 89 registrerade samt namn, civilstånd, antal barn, lön, arbetstid och övriga uppgifter i lönespecifikationen för 10 anställda vars anställningsavtal hade upphört att gälla. Den personuppgiftsansvarige underrättar endast de sistnämnda 10 anställda.

7.2.1 FALL nr 18 – Riskbedömning, lindring och skyldigheter

129. Även om angriparen troligen inte tänkte samla in personuppgifter kommer personuppgiftsincidenten sannolikt att leda till en hög risk för fysiska personers rättigheter och friheter, eftersom incidenten skulle kunna leda till både materiell skada (t.ex. ekonomisk förlust) och immateriell skada (t.ex. identitetsstöld eller bedrägeri), eller eftersom uppgifterna skulle kunna användas för att underlätta andra angrepp (t.ex. nätfiske). Alla 99 anställda bör därför informeras om incidenten, och inte bara de 10 anställda vars löneinformation läckte ut.

130. Efter att ha blivit varse om incidenten tvingade den personuppgiftsansvarige igenom en lösenordsändring för de angripna kontona, gjorde det omöjligt att mejla angriparens e-postkonto, underrättade leverantören av den e-posttjänst som angriparen använde om attacken, tog bort de regler som angriparen hade angett och förfinade varningarna från övervakningssystemet så att det varnar så fort en automatisk regel skapas. Som ett alternativ skulle den personuppgiftsansvarige kunna ta bort rätten för användare att ange vidarebefordringsregler, vilket skulle innebära att it-servicegruppen endast kan göra det på begäran. Den personuppgiftsansvarige skulle även kunna införa en policy om att användare som hanterar finansiella uppgifter bör kontrollera och rapportera om reglerna för deras konton minst en gång i veckan.

131. Det faktum att en incident kunde inträffa och inte upptäcktes på så lång tid och det faktum att social manipulation under en längre tid kunde ha använts för att ändra fler uppgifter åskådliggjorde stora problem i den personuppgiftsansvariges it-säkerhetssystem. Dessa bör åtgärdas utan dröjsmål, till exempel genom att betona automatiseringsgranskningar, ändringskontroller, incidentdetektering och motåtgärder. Personuppgiftsansvariga som hanterar känsliga uppgifter, finansiell information osv. har ett större ansvar när det gäller att skapa tillräcklig datasäkerhet.

Nödvändiga åtgärder på grundval av identifierade risker		
Intern dokumentation	Anmälan till tillsynsmyndigheten	Information till de registrerade
✓	✓	✓