KPMG

Rapport

Ekstern undersøgelse af slettede emails i Sundhedsdatastyrelsen, Statens Seruminstitut og Sundhedsministeriets Koncern HR

Indholdsfortegnelse

Ledelsesresumé

Fredag d. 21. august 2020 blev indstillingerne for sletning af sendte emails i den emailløsning, som benyttes af Sundhedsdatastyrelsen (SDS), Statens Serum Institut (SSI) og Sundhedsministeriets Koncern HR (KHR), fejlagtigt ændret. Ændringen havde den konsekvens, at opbevaringsperioden gik fra ubegrænset til 30 dage. I praksis mistede brugerne således alle emails, de havde sendt i perioden frem til d. 22. juli 2020, og som de ikke havde arkiveret i en anden mappe end mappen "sendt post" eller journaliseret.

De ændrede indstillinger blev identificeret mandag d. 24. august og SDS gik derfor umiddelbart i gang med håndteringen af hændelsen. Først og fremmest blev den oprindelige slettepolitik gendannet, således at sendte emails igen blev opbevaret i en ubegrænset periode. Dernæst rettede SDS det løsningsmæssige fokus mod at gendanne de emails, der blev gjort utilgængelige i forbindelse med ændringen af slettepolitikken. Antagelsen var, at de utilgængelige mails ville blive gemt i en slags virtuel papirkurv i 30 dage, hvorefter de ville blive slettet permanent. De facto var perioden dog ikke *30 dage*, men kun *14 dage*, hvilket SDS først blev opmærksom på *efter* 14-dagesperiodens udløb.

Udover de praktiske udfordringer, som de slettede mails har medført for brugerne af de berørte konti, kan hændelsen få konsekvenser for organisationernes evne til at overholde reglerne i offentlighedsloven, forvaltningsloven og arkivloven i den udstrækning relevante mails ikke er journaliseret. Desuden giver hændelsen anledning til en mere generel opmærksomhed omkring informationssikkerhed og it-governance i SDS.

På den baggrund har Sundhedsministeriet bedt KPMG om at undersøge hændelsesforløbet med henblik på en uvildig redegørelse for selve hændelsen og håndteringen heraf. Undersøgelsen skal samtidig pege på væsentlige erfaringer og anbefalinger, som hændelsen måtte give anledning til.

KPMG's sammenfattende vurdering af hændelsesforløbet

KPMG's afdækning af hændelsesforløbet viser, at et bruger-ID (og dermed en specifik medarbejder), har opdateret en slettepolitik i email-systemet, hvilket medførte, at politikken for sendte mails blev ændret, så disse blev slettet efter 30 dage. Dette stemmer overens med SDS' egen undersøgelse af hændelsen.

Der er intet i KPMG's afdækning, der indikerer, at der er tale om en bevidst handling, eller at det pågældende bruger-ID er blevet kompromitteret eller hacket. Dette understøttes af, at der ved en bevidst handling kunne være foretaget betydeligt mere skadelige handlinger, herunder at også indbakker med modtagne mails kunne have været slettet på samme vis, og at sletningen kunne have været med umiddelbar og permanent effekt uden mulighed for genskabelse. Endvidere har det været muligt at genskabe en stor andel af de slettede mails (SDS skønner, at omkring 85-90 % af alle sendte mails siden 1. januar 2020 er genskabt). Det er således KPMG's vurdering, at sandsynligheden taler for, at der er tale om en utilsigtet, menneskelig fejl.

Imidlertid kan de eksakte omstændigheder omkring hændelsen ikke kortlægges på baggrund af den forhåndenværende information. Dette skyldes først og fremmest, at logdata vedrørende ændringer af systemindstillingerne kun opbevares i systemet i 90 dage. Dette gælder både hos SDS og hos systemleverandøren Microsoft. Idet undersøgelsen først blev igangsat mere end 90 dage efter hændelsestidspunktet, har KPMG således ikke kunnet gennemgå systemloggen for informationer om, hvad der præcist skete på hændelsestidspunktet eller i en periode op til tidspunktet. Det er efter KPMG's vurdering meget beklageligt, at disse logdata ikke er blevet sikret og gemt på anden vis, da de potentielt kunne have kastet lys over hændelsesforløbet.

På grundlag af den eksisterende dokumentation og de gennemførte interview, er det dog KPMG's vurdering, at hændelsesforløbet har været karakteriseret af flere alvorlige fejl. I den forbindelse skal særligt følgende fremhæves:

- KPMG finder det bekymrende, at det tilsyneladende har været relativt let at foretage så indgribende ændringer i systemets indstillinger, uden at dette er blevet bemærket af hverken den pågældende medarbejder eller den driftsorganisation, som er ansvarlig for systemet.
- KPMG finder det kritisabelt, at der ikke har været kendskab til eller kontrol af, hvor lang tid SDS reelt havde til rådighed til at genskabe de slettede mails. Havde SDS været bevidst om, at der reelt kun var 14 dage til rådighed, ville det have været muligt at tilrettelægge hændelseshåndteringen anderledes (herunder med tidligere og mere akut inddragelse af systemleverandøren), således at det havde været muligt at gendanne alle slettede mails.
- KPMG finder det særdeles uheldigt, at SDS ikke har været opmærksom på muligheden for at anvende "litigation hold" umiddelbart efter, at den ændrede slettepolitik blev konstateret. En anvendelse heraf ville have fastlåst indholdet i alle postkasser uagtet den aktuelle politik, så ingen af de sendte mails, som blev overflyttet til "slettet mail"-postkassen, ville være gået tabt.

KPMG bemærker i øvrigt, at hændelsen og dens håndtering naturligvis skal ses i lyset af den ekstraordinære situation, som SUM's koncern og herunder SDS har været i som følge af en usædvanligt stor arbejdsbyrde i relation til COVID-19. Således har organisationens fokus og ressourcer i høj grad været prioriteret til håndteringen af pandemien med afledt effekt på andre dele af den daglige drift og opgavevaretagelse.

Læring og anbefalinger

Hændelsesforløbet og håndteringen heraf giver anledning til en række observationer og anbefalinger, som kort opridses herunder. KPMG's fokus har været på læring og anbefalinger relateret til hændelsen, om end hændelsen naturligvis også skal forstås i kontekst af SDS' håndtering af IT- og informationssikkerhed i bredere forstand, herunder både teknisk, organisatorisk og ledelsesmæssigt.

Det skal bemærkes, at der i anbefalingerne ikke er taget stilling til konsekvenserne af den forestående transition af dele af IT-driften fra SDS til Statens IT. Nogle af de identificerede udfordringer vil således kunne forventes håndteret i forbindelse med transitionen, hvorfor prioriteringen af KPMG's anbefalinger naturligt vil skulle foretages i lyset af transitionen.

Anbefalinger til mulige tekniske tiltag	
Anbefaling #1. To konti til administratorer	Det anbefales, at SDS og SUM overvejer muligheden for at tildele administratorer to konti til administration af de centrale IT-systemer på ministerområder – en begrænset administrationskonto, som anvendes til den daglige drift og en konto, som alene anvendes, hvis særligt kritiske politikker eller lignende skal ændres.
Anbefaling #2. Etablering af back-up	Det anbefales, at SDS og SUM nøje overvejer hensigtsmæssigheden af at etablere en ekstern back-up af mail-systemet. Alternativt bør det overvejes at etablere et Vault-system til fremfinding og genskabelse af emails.
Anbefaling #3. Etablering af system til auditlog	Det anbefales, at SDS undersøger muligheden af at etablere et system til opbevaring af en auditlog for administratorhandlinger. Samtidig bør muligheden for, at systemet kan udsende advarsler ved bestemte hændelser, undersøges.
Anbefalinger til mulige organisatoriske og ledelsesmæssige tiltag	
Anbefaling #4. Analyse af og fremtidig strategi for IT-governance i SUM	Det anbefales, at SDS/SUM foretager en tilbundsgående analyse af varetagelsen af IT- og informationssikkerheds-governance på ministerområdet i dag og på den baggrund udarbejder en ny samlet strategi og vedvarende implementeringsplan for den fremadrettede varetagelse. I dette arbejde bør der tages højde for de ændrede governance-behov, som følger af at anvende cloud-baserede systemer, herunder det faktum at organisationen ikke har adgang til infrastruktur-laget, hvorfor mange sikkerhedsprocesser skal lægges væsentligt om.
Anbefaling #5. Risikovurdering af Microsoft 365	Det anbefales, at SDS gennemfører en risikovurdering af Microsoft 365 med henblik på at kortlægge risikobilledet og skabe et veldokumenteret grundlag for at planlægge og eksekvere mitigerende handlinger.
Anbefaling #6. Styrkelse af risikostyringen i SDS	Det anbefales, at SDS foretager et review af sin model for risikostyring og udarbejdelse af risikovurderinger med henblik på at sikre, at denne afspejler sundhedsvæsenets kritikalitet og de teknologiske udfordringer, som sundhedsvæsenet skal håndtere. På baggrund af reviewet bør der udarbejdes en handlingsplan for at optimere risikostyringen.
Anbefaling #7. Etablering af kode-repository med tilhørende governance	Det anbefales, at SDS overvejer etableringen af et kode-repository, hvor alle scripts til PowerShell skal opbevares, og at der indføres en klar governance omkring udarbejdelse, deling og anvendelse af scripts.
Anbefaling #8. Styrket systemforvaltning på kontorplatformen	Det anbefales, at SDS/SUM overvejer at styrke systemforvaltningen på kontorplatformen ved at etablere systemforvaltere med et indgående kendskab til brugernes anvendelse af systemerne.
Anbefaling #9. Efterprøvning af klassificeringer af hændelser på næsthøjeste niveau	Det anbefales, at SDS etablerer en standardmekanisme eller -proces, hvorved alle kritiske informationssikkerhedshændelser, som klassificeres til næsthøjeste niveau, indebærer at en gruppe af relevante ledere, medarbejdere og teknikere

	i samarbejde efterprøver forudsætningerne for, hvorfor klassificeringen ikke skal være som "major incident" på højeste niveau.
Anbefaling #10. Indførelse af en problem manager rolle	Det anbefales, at SDS overvejer at indføre en problem manager rolle, som vil have til opgave at sikre, at de rette, kritiske spørgsmål stilles i forbindelse med informationssikkerhedshændelser samt at sikre en langsigtet udbedring af eventuelle fejl.
Anbefaling #11. Styrkelse af læring og implementering af forbedringer på baggrund af hændelser	Det anbefales, at SDS foretager et review af, hvordan læring fra tidligere informationssikkerhedsmæssige hændelser opsamles og anvendes til at implementere forbedringer i den daglige drift. På baggrund af reviewet bør der udarbejdes handlingsplan for at sikre implementering af relevante resultater, herunder at SDS har en proces, der sikrer, at erfaringer bruges til kontinuerlige forbedringer.
Anbefaling #12. Styrkelse af læring og implementering af forbedringer på baggrund af hændelser	Det anbefales, at SDS overvejer at prioritere en fuld implementering og efterfølgende certificering af ISO 27001. Med henblik herpå bør der i givet fald udarbejdes en operationel handlingsplan for, hvordan SDS opnår dette.
Anbefaling #13. Konsolidering af systemporteføljen	Det anbefales, at SUM overvejer mulighederne for at konsolidere systemerne på kontorplatformen, således at den enkelte supportmedarbejder i højere grad kan specialisere sig i få løsninger.
Anbefaling #14. Konsolidering af IT-organiseringen	Det anbefales, at SUM overvejer at gennemføre et review af organiseringen af IT-kompetencer på tværs af koncernen, så det sikres, at opgaverne varetages mest hensigtsmæssigt.
Anbefaling #15. Analyse af fremadrettet ressourcebehov i koncern-IT	Det anbefales, at SUM gennemfører en grundig analyse af det fremadrettede ressource- og kompetencebehov på ministerområdet generelt og i SDS i særdeleshed med henblik på at sikre, at kvaliteten af den daglige IT-drift og informationssikkerhed afspejler sundhedsvæsenets samfundskritiske betydning.

1. Om undersøgelsen

1.1. Undersøgelsens baggrund

Fredag d. 21. august 2020 blev indstillingerne for sletning af sendte emails i den emailløsning, som benyttes af Sundhedsdatastyrelsen (SDS), Statens Serum Institut (SSI) og Sundhedsministeriets Koncern HR (KHR), fejlagtigt ændret. Ændringen havde den konsekvens, at opbevaringsperioden gik fra ubegrænset til 30 dage. Medarbejderne i de tre institutioner gik således fra at have adgang til alle deres tidligere sendte emails til kun at kunne tilgå de emails, som var sendt de seneste 30 dage, mens emails, der var ældre end 30 dage, blev slettet. I praksis mistede brugerne således alle emails, de havde sendt i perioden frem til d. 22. juli 2020, og som de ikke havde arkiveret i en anden mappe end mappen "sendt post" eller journaliseret.

De ændrede indstillinger blev identificeret mandag d. 24. august og SDS gik derfor umiddelbart i gang med håndteringen af hændelsen. Først og fremmest blev den oprindelige slettepolitik gendannet, således at sendte emails igen blev opbevaret i en ubegrænset periode. Dernæst rettede SDS det løsningsmæssige fokus mod at gendanne de emails, der blev gjort utilgængelige i forbindelse med ændringen af slettepolitikken. Antagelsen i det team, der arbejdede med gendannelse, var, at de utilgængelige mails ville blive gemt i en slags virtuel papirkurv i 30 dage, hvorefter de ville blive slettet permanent. Derfor blev hændelsen heller ikke klassificeret i den højeste kategori for kritikalitet, dvs. "major incident". De facto var perioden dog ikke *30 dage*, men kun *14 dage*, hvilket man i det pågældende team først blev opmærksom på *efter* 14-dagesperiodens udløb.

SDS har efterfølgende foretaget forskellige tiltag for at mindske de langsigtede konsekvenser af hændelsen, herunder først og fremmest gennem en indsats for at genskabe flest mulige af de slettede mails, *jf. boks 1*.

Boks 1. Hændelsens konsekvenser

- De ændrede indstillinger medførte sletning af ca. 500 fælles funktionspostkasser og ca. 2.200 individuelle brugerpostkasser i de berørte institutioner.
- SDS skønner, at i størrelsesordenen 750.000 sendte mails fra funktionspostkasser og 8,500.000 sendte mails fra brugerpostkasser blev slettet som følge af de ændrede indstillinger.
- Efterfølgende er det lykkedes at genskabe ca. 650.000 af de sendte mails fra funktionspostkasser (visse af disse postkasser var ikke konfigureret som funktionspostkasser, hvorfor de ikke indgik i den centraliserede indsats for genskabelse af funktionspostkasser).
- SDS skønner, at 85-90 % af de slettede mails fra brugerpostkasser genskabes via et script, som henter de sendte mails ud af modtagernes indbakker, *jf. rapportens afsnit 3*.
- Det er således SDS forventning, at andelen af de slettede mails, som er endegyldigt mistede, vil udgøre under 15 % af det samlede antal slettede mails.

Udover de praktiske udfordringer, som de slettede mails har medført for brugerne af de berørte konti, kan hændelsen få konsekvenser for organisationernes evne til at overholde reglerne i

offentlighedsloven, forvaltningsloven og arkivloven i den udstrækning relevante mails ikke er journaliseret. Desuden giver hændelsen anledning til en mere generel opmærksomhed omkring informationssikkerhed og it-governance i SDS.

1.2. Undersøgelsens formål

Som følge af hændelsen har Sundhedsministeriet (SUM) bedt KPMG foretage en undersøgelse af hændelsesforløbet med henblik på en uvildig redegørelse for dels selve hændelsen og håndteringen heraf og dels væsentlige erfaringer og anbefalinger, som hændelsen måtte give anledning til. Den konkrete undersøgelsesramme med de to undersøgelsesområder fastlagt af Departementet, er gengivet nedenfor, jf. boks 2.

Boks 2. SUMs opgavebeskrivelse for "Ekstern undersøgelse af slettede mails"

For det første skal undersøgelsen indeholde en redegørelse af hændelsesforløbet, som afklarer hvordan denne hændelse kunne finde sted. Redegørelsen skal særligt have fokus på:

- Ændring af indstilling for lagringstiden af sendte mails
- Den manglende indsigt i/bekræftelse af at standard-indstillingen på 30 dage for reetablering reelt var 14 dage.
- De iværksatte tiltag til gendannelse af sendte mails – reetableringen af de ca. 500 afdelings- og fællespostkasser samt vejledning til selv-reetablering
- Ledelsesmæssig og organisatorisk håndtering af hændelsen/-erne ifht. best practise for it-branchen

For det andet skal undersøgelsen pege fremad på læring og anbefalinger på baggrund af hændelsen. Herunder skal der særligt være fokus på:

- Mulige tekniske tiltag, der kan forhindre eller minimere konsekvenserne af tilsvarende hændelser, gerne med inddragelse af leverandøren (Microsoft Danmark)
- Organisatoriske og ledelsesmæssige tiltag, der kan forebygge tilsvarende hændelser eller minimere konsekvenserne samt forbedre håndteringen.

1.3. Undersøgelsesmetode og afgrænsninger

Undersøgelsen er gennemført i perioden november 2020 til februar 2021, og blev således først påbegyndt ca. tre måneder efter selve hændelsen fandt sted.

Som led i undersøgelsen har KPMG gennemført en lang række interviews med nøglepersoner i SDS, SSI, KHR samt virksomhederne Globeteam og Microsoft, som leverer system- og konsulentydelser til SDS i relation til mailløsningen Office 365. Endvidere er der gennemført interviews med vidanspersoner i Statens IT, hvortil en række ydelser, som i dag leveres af SDS, forventes transitioneret fra efteråret 2021, *jf. afsnit 2.3*.

Herudover har SDS på egen foranledning udleveret en række sagsakter (herunder en omfattende mailkorrespondance) og øvrige dokumenter, som af styrelsen selv er blevet vurderet til at bidrage til oplysning af hændelsen. Styrelsen har endvidere løbende i undersøgelsesprocessen på foranledning af KPMG overdraget en række øvrige dokumenter, som ligeledes har bidraget til oplysning af hændelsen. KPMG har i den forbindelse bl.a. efterspurgt logfiler, som kunne

dokumentere hændelsesforløbet, men idet mailløsningen alene giver adgang til logfiler for de seneste 90 dage, og idet SDS generelt ikke gemmer kopier af ældre logfiler, har SDS kun kunnet fremfinde en enkelt logfil fra hændelsestidspunktet. Dette har vanskeliggjort en entydig afdækning af, hvordan hændelsen præcist er forekommet, *jf. afsnit 3.*

I forbindelse med undersøgelsen har KPMG desuden bedt SDS være behjælpelig med at rekonstruere hændelsen i et testmiljø, hvilket har bidraget til et mere nuanceret billede af hændelsesforløbet.

Undersøgelsen har sigtet mod at tilvejebringe al væsentlig information med henblik på at give et retvisende billede af hændelsen i henhold til undersøgelsesrammen. KPMG's observationer, øvrige udsagn og konklusioner er alene baseret på det informationsgrundlag, der har været stillet til rådighed i forbindelse med afdækningen, og informationernes korrekthed og fuldstændighed er taget for pålydende.[1] KPMG's arbejde har således ikke haft til formål at stille enkeltpersoner til ansvar i forbindelse med hændelsen eller nogen form for afdækning af ansvarsaspekter i relation til omstændigheder eller forhold, som hændelsen kan henføres til.

1.4. Afrapporteringens struktur

Strukturen i nærværende afrapportering følger overordnet set strukturen i den fra SUM givne undersøgelsesramme. Indledningsvis gives i *afsnit 2* en introduktion til organiseringen af IT på SUMs ressortområde. I *afsnit 3* redegøres for hændelsesforløbet. Afsnittet indeholder indledningsvis en kronologisk gennemgang af hændelsesforløbet, og efterfølgende adresseres undersøgelsesområdets fire underliggende fokuspunkter, det vil sige *ændring af indstilling af lagringstid*, *fejlvurdering af reetableringsindstillinger*, *mailgendannelsesindsatsen*, samt *foretagne organisatoriske- og ledelsesmæssige tiltag*.

I *afsnit 4*, adresseres det andet primære undersøgelsesområde, dvs. læring og anbefalinger med afsæt i hændelsens omstændigheder. Afsnittet er overordnet struktureret efter de fem områder, som i henhold til Digitaliseringsstyrelsens vejledning om departementernes tilsyn med informationssikkerheden på ministerområderne[2] skal være i fokus i den løbende vurdering af informationssikkerheden i institutionerne på et ministerområde. Undersøgelsesområderne er *ledelsessystem, risikostyring, IT-sikkerhedspolitikker og -retningslinjer, IT-kontroller* samt *evaluering og opfølgning*.

[1] Det skal bemærkes, at KPMG som led i afdækningen ikke har foretaget revision, herunder IT-revision, eller review i henhold til internationale revisionsstandarder på de nævnte undersøgelsesområder, og KPMG udtrykker ikke nogen sikkerhed eller afgiver erklæring herom som led i afdækningen.

[2] Digitaliseringsstyrelsen: "Departementets tilsyn med informationssikkerheden på ministerområdet", 2015.

2. IT i Sundhedsministeriet

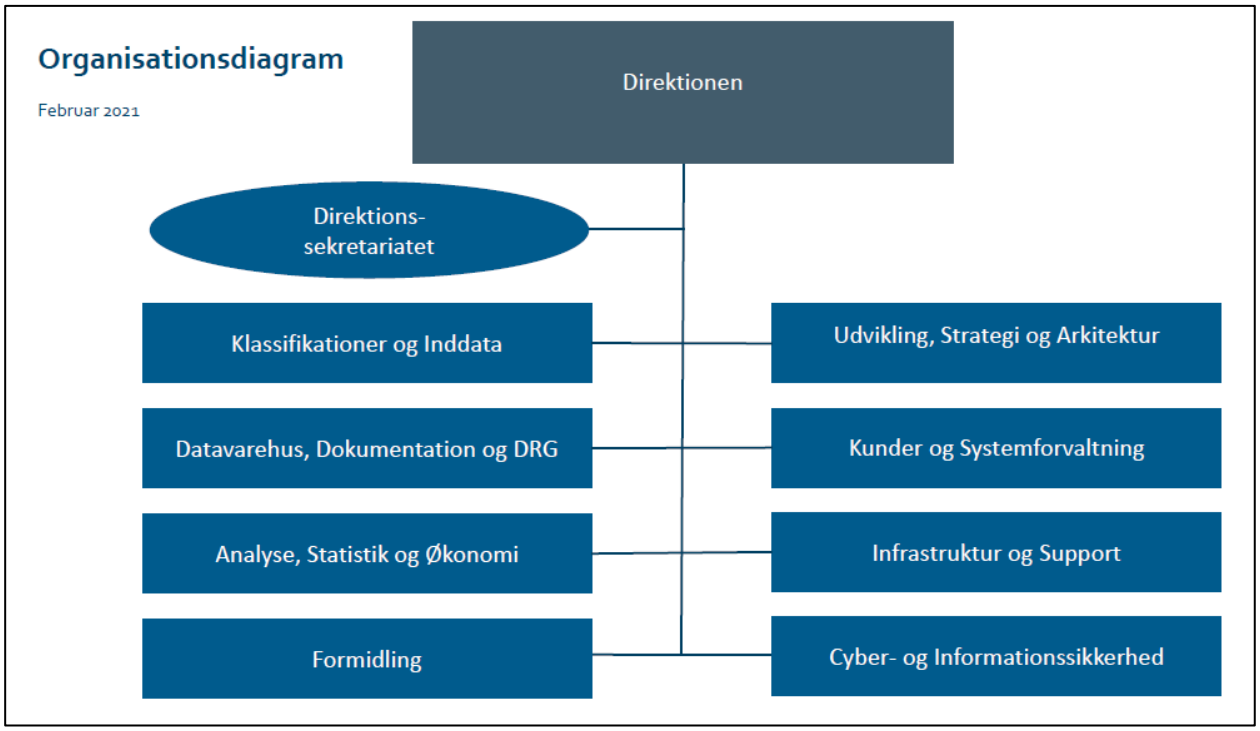
2.1. Sundhedsdatastyrelsens rolle som koncern IT-funktion i Sundhedsministeriet

SDS fungerer som den interne IT-driftsorganisation for SUM's koncern. I den sammenhæng har SDS ansvaret for at drifte og udvikle en række systemer, services og data på tværs af koncernen, herunder de enkelte institutioners mailsystemer.

SDS' kerneopgave er herudover at sikre sammenhængende sundhedsdata og digitale løsninger til gavn for patienter og klinikere samt forskningsmæssige og administrative formål i sundhedsvæsenet.

SDS er organiseret i 8 afdelinger, som varetager styrelsens hovedopgaver, samt et direktionssekretariat, der understøtter ledelsens arbejde og arbejder på tværs af styrelsens samlede opgaveportefølje, *jf. figur 1*.

Figur 1. Sundhedsdatastyrelsens organisation



Arbejdet som koncern IT-funktion for SUM's koncern varetages hovedsageligt af afdelingerne Cyber- og Informationssikkerhed (CIA), Infrastruktur og Support (IOS) samt Kunder og Systemforvaltning (KOS).

CIA har ansvaret for at facilitere og koordinere den fælles indsats for at styrke og øge kapabiliteten og kapaciteten indenfor cyber- og informationssikkerhed i SDS, i SUM's koncern og på tværs af

sundhedsvæsenet. CIA varetager endvidere et tilsynsansvar i relation til koncernens arbejde med informationssikkerhed på vegne af SUM's departement.

IOS har ansvaret for infrastruktur, sikker og stabil drift og support af brugere. Endvidere har IOS til opgave at implementere og videreudvikle de interne IT-service management processer samt at bidrage til forretningsmæssige IT-udviklingsprojekter. IOS varetager bl.a. systemejerskabet for Exchange Online.

KOS varetager det daglige samarbejde om behov for systemunderstøttelse, systemstrategier og roadmaps med forretningen i SUM's koncern og på tværs af sundhedsvæsenet. Det omfatter ansvaret for kundeaftaler, SLA'er, udbud, leverandørstyring og license management.

Desuden har direktionen og direktionssekretariatet et overordnet ansvar for at fremme professionel dataforvaltning og informationssikkerhed i SDS, SUM's koncern og sundheds-væsenet.

2.2. Anvendelsen af Microsoft 365 som emailløsning

SDS, SSSI og KHR har siden 2015 anvendt løsningen Microsoft 365 (tidligere "Office 365") til understøttelse af bl.a. emailområdet. Microsoft 365 består af en samling af abonnementstjenester, der indgår som en del af Microsoft Office-produktlinjen. Tjenesterne omfatter bl.a. Microsoft Office-softwarepakken, som inkluderer emailapplikationen Outlook. Nedenfor gennemgås nogle af de centrale konfigurationselementer i Microsoft med betydning for sletning af emails i Outlook.

2.2.1. Retention policy – opsætning af sletteregler for emails i Outlook

Slettepolitikker for emails sendt fra Outlook opsættes og administreres enten i Microsoft 365-applikationen Exchange eller i applikationen Windows PowerShell. Når Microsoft 365 implementeres i en organisation, defineres der altid en slettepolitik, som regulerer, hvor længe emails skal bevares. I Microsoft 365 betegnes slettepolitikken som "retention policy". Fastlæggelsen af retention policy'en sker med udgangspunkt i fx forretningsmæssige og juridiske overvejelser vedrørende organisationens virke, og policy'en sammensættes af en eller flere regler, som kaldes for "retention tags".

Et retention tag definerer, hvordan emails sletningsmæssigt skal håndteres med afsæt i hvilke attributter, der er knyttet til emailen. Et retention tag kan f.eks. foreskrive, at emails, som er sorteret til mappen "sendt post" (og dermed har en "sendt post"-attribut tilknyttet) efter 30 dage skal flyttes til mappen "slettet post", som det var tilfældet ved den aktuelle hændelse. Et andet retention tag kan foreskrive, at emails, der er sorteret til mappen "slettet post", skal slettes permanent efter 14 dage.

2.2.2. SUM's retention policy gældende for Microsoft 365

Almindeligvis vil defineringen af en retention policy tage udgangspunkt i en risikovurdering af den konkrete løsning. SDS har oplyst, at der i forbindelse med implementeringen af Microsoft 365 i

2015 ikke blev gennemført en egentlig risikovurdering af løsningen, men en overordnet gennemgang af, hvorvidt Datatilsynets anbefalinger om brug af Microsoft cloud-løsninger var opfyldt. Den retention policy, som SDS har benyttet siden implementeringen af løsningen, har således været en default policy, som ikke var baseret på en egentlig vurdering af den konkrete sikkerhedskontekst.

I forhold til undersøgelsen – og for at skabe størst mulig klarhed over hvordan hændelsen kunne opstå og eskalere til et punkt, hvor konsekvensen blev et varigt datatab af en betydelig størrelse – er det relevant at fokusere på, hvordan den benyttede retention policy regulerer dels *sendt post* og dels *slettet post*.

Med hensyn til *sendt post* blev der i SUM's retention policy ved implementeringen i 2015 *ikke* oprettet et retention tag, der definerede, at emails sorteret til "sendt post"-mappen skulle slettes efter en given periode. Når der ikke eksisterer et retention tag, regulerer retention policy'en som standard, at en sendt email bevares i "sendt post"-mappen i en ubegrænset periode, med mindre en bruger manuelt sletter den.

Med hensyn til *slettet post* har SUM's retention policy siden implementeringen i 2015 inkluderet et retention tag, der definerer, at emails, der er sorteret til "slettet post"-mappen, skulle slettes permanent efter 14 dage.

SDS har oplyst, at der ikke er foretaget f.eks. forretningsmæssige eller juridiske overvejelser, der har givet anledning til ændring af SUM's retention policy siden implementeringen. SDS har også oplyst, at retention policy'en vedrørende *sendt post* og *slettet* post var uændret fra 2015 og frem til, at hændelsen indtraf i 2020. Dette har dog ikke været muligt for KPMG at verificere teknisk, da der ikke er etableret logning af denne type oplysninger.

2.3. Transition af IT-drift til Statens IT

Det planlægges i øjeblikket at transitionere en del af IT-driften fra SDS til Statens IT (SIT), herunder emailservices. I forbindelse med transitionen skal der tages stilling til, hvad SUM som ny kunde hos SIT ønsker at aftage, ligesom det skal defineres hvilke behov, der bl.a. rent risikomæssigt er knyttet til disse ydelser.

Transitionen og de muligheder og udfordringer denne medfører har ikke været et selvstændigt genstandsområde for undersøgelsen, ligesom den SIT-analyse, der skal udgøre grundlaget for transitionen ikke er tilendebragt på tidspunktet for denne afrapportering. Det bemærkes dog, at transitionen til SIT under alle omstændigheder må forventes at ændre på en række grundlæggende forhold, herunder personalesituationen samt driftsprocesser og -procedurer, som er af grundlæggende betydning for IT-sikkerheden vedrørende bl.a. emails.

3. Redegørelse for hændelsesforløbet

I dette afsnit redegøres for det første undersøgelsesområde, dvs. selve hændelsesforløbet. Som led i redegørelsen gengives hændelsesforløbet indledningsvis i en kronologisk gennemgang. Efterfølgende adresseres hvert af de fire fokuspunkter, som der i henhold til Departementets undersøgelsesramme skal redegøres for, dvs. *ændring af indstilling af lagringstid*, *fejlvurdering af reetableringsindstillinger*, *mailgendannelsesindsatsen*, samt *foretagne organisatoriske- og ledelsesmæssige tiltag*.

3.1. Kronologisk gennemgang af hændelsesforløbet

Hændelsesforløbet er gengivet kronologisk i tabel 1 nedenfor. Informationen er indsamlet gennem interviews med medarbejdere i SDS, SSI og KHR samt virksomhederne Globeteam og Microsoft, som alle var involveret i forløbet, samt gennem skriftlig dokumentation, herunder f.eks. den incidentlog, der blev udarbejdet i forbindelse med hændelsen.

Tabel 1. Oversigt over hændelsesforløbet

Fredag d. 21. august	• Kort efter middag tilføjer en medarbejder i Sundhedsdatastyrelsen med administratorrettigheder et retention tag til SUM's retention policy. Det tilføjede retention tag'et definerer at emails sorteret til "sendt post"-mappen bevares i 30 dage, hvorefter de sorteres til mappen "slettet post". • Ændringen har den effekt, at alle emails som er sendt af medarbejdere i SDS, SSI og KHR fra personlige emailkonti og fra funktionsemailkonti mere end 30 dage tidligere overføres til mappen "slettet post". • SDS anslår, at det i alt drejer sig om ca. 8,5 millioner emails sendt fra personlige emailkonti og ca. 750.000 emails sendt fra funktionspostkasser.
Lørdag d. 22. august	• SDS' service desk modtager kl. 14:10 de første meldinger fra en bruger om, at sendte mails, der er ældre end 30 dage, ikke kan tilgås.
Mandag d. 24. august	• Som følge af en stor pukkel af supportsager visiteres førnævnte melding først et stykke op ad dagen, hvorefter service desken informerer det ansvarlige SDS-team (Driftsforvaltningsteamet) om problemet med sendte emails. • Driftsforvaltningsteamet igangsætter undersøgelse af problemet og konstaterer, at der er tilføjet et retention tag til retention policy'en, således at alle mails, der er sendt for mere end 30 dage siden sorteres til "slettet post".

	• Driftsforvaltningsteamet undersøger med SDS-afdelingen Cyber- og Informationssikkerhed, om indstillingen udgør officiel politik. Det konstateres med det samme, at dette ikke er tilfældet. • Da det er konstateret, at sendte emails ikke er fjernet som følge af en vedtaget politik, informeres der fra tekniker til sektionsledelsesniveau om hændelsen (kl. 14:06) • Kl. 15:00 er retention tag'et fjernet fra retention policy'en, således at sendte mails nu igen bevares i en ubegrænset periode. Ændringen af retention policy'en har dog kun fremadrettet virkning.
Tirsdag d. 25. august	• Driftsforvaltningsteamet igangsætter en indsats for at gendanne de slettede mails. Der udvikles et script til at gendanne emails, og det igangsættes kl. 9:30. • Der opereres i Driftsforvaltningsteamet på dette tidspunkt på basis af en antagelse om, at de emails, der er sorteret til brugeres og funktionspostkassers "slettet post"-mapper bevares i 30 dage. Antagelsen efterkontrolleres ikke, og der ageres i de efterfølgende knap to uger på basis af antagelsen, som viser sig at være fejlagtig. • Emails sendt fra funktionspostkasser skal af tekniske årsager gendannes fra centralt hold. Af kapacitetsmæssige årsager besluttes i første omgang at lade de enkelte brugere forestå gendannelsen af egne sendte mails, hvorved Driftsforvaltningsteamet kan koncentrere sig om gendannelsen af funktionspostkasser. • Ledelserne i SDS, SSI og KHR orienteres om problemet. • Der udarbejdes en vejledning til, hvordan ansatte selv kan gendanne sendte mails. Vejledningen lægges på koncernintranettet kl. 11:00. Det kan senere konstateres, at relativt få medarbejdere har benyttet adgangen til at gendanne egne mails.
Tirsdag d. 25. august – onsdag d. 26. august	• Indsatsen for at gendanne sendte mails fra funktionspostkasser igangsættes. I løbet af de første dages indsats konstateres det, at gendannelsen går relativt langsom, og at der kun gendannes mellem 2 og 4 mails i sekundet. • Hurtigt i gendannelsesforløbet konstateres desuden, at den tekniske gendannelsesløsning, som driftsforvaltningsteamet benytter sig af, afvikles ustabilt og ikke kører konstant, men kræver kontinuerlig overvågning og løbende genstart af en tekniker.
Torsdag d. 27. august	• Der rettes for første gang henvendelse til SDS' kontaktpunkt hos leverandøren Microsoft vedrørende sagen. • I første omgang går SDS' forespørgsel på, at Microsoft bistår med at få SDS' egen tekniske gendannelsesløsning til at køre hurtigere og mere stabilt ved at tillade flere forespørgsler fra løsningen ind imod det cloudmiljø, hvor Microsoft 365 er hostet.
Mandag d. 31. august	• En konsulent fra Microsoft tager kontakt til SDS og sagen drøftes yderligere.
Tirsdag d. 1. september	• Drøftelserne mellem Microsoft og SDS udmunder i, at Microsoft råder SDS til at oprette en sag vedrørende problemet.

Onsdag d. 2. september	• SDS opretter en sag hos Microsoft. • Microsoft allokerer en tekniker, der skal bistå SDS med løsningshåndteringen. • Der igangsættes drøftelser mellem SDS og Microsoft. I første omgang ønsker SDS primært, at Microsoft kvalitetstjekker den tekniske gendannelsesløsning, som SDS benytter. • På baggrund af drøftelserne allokerer Microsoft mere båndbredde til SDS' gendannelsesløsning. Tiltaget resulterer dog ikke i den ønskede effekt, og gendannelseshastigheden vurderes af SDS stadig til at være utilstrækkelig.
Fredag d. 4. september	• Gendannelsen af mails sendt fra funktionspostkasser er gennemført. • Der igangsættes gendannelse af mails sendt fra de individuelle brugeres postkasser.
Lørdag d. 5. september-søndag d. 6. september	• Det konstateres, at gendannelsen af mails sendt fra de individuelle brugeres postkasser er stoppet
Mandag d. 7. september	• Der tages kontakt til Microsoft med henblik på afklaring af, hvorfor gendannelsen af mails er stoppet i løbet af weekenden. • Microsoft råder SDS til at anvende funktionen "litigation hold", som betyder, at alt data fra alle postkasser, inkl. slettede postkasser "fastfryses". • Det konstateres, at SDS' antagelse om, at retention policy'en definerede, at emails sorteret til "slettet post"-mappen skulle bevares, var fejlagtig, og at policy'en derimod definerede perioden til at være 14 dage. Policy'en regulerede dermed, at fredag d. 4. september var sidste dag for gendannelse. • SDS går i gang med at undersøge, om der er andre muligheder for at gendanne de slettede mails.
Torsdag d. 10. september	• Det konkluderes, at det ikke er muligt direkte at gendanne brugernes sendte mails fra papirkurv, back-up eller lignende. • Den nye situation drøftes på teknisk niveau med SSI.
Fredag d. 11. september	• Direktionen i SSI og KHR-chefen orienteres om situationen. • Der iværksættes en ny tilgang til gendannelse, hvor mails sendt fra ansatte i SDS, SSI og KHR til modtagere i SUM's koncern rekonstrueres ved teknisk at gennemsøge alle brugeres indbakker og "tilbageføre" mails, der kommer fra brugere fra de tre institutioner/organisationer i koncernen. Denne løsning kan dog ikke bidrage til at gendanne emails sendt fra en bruger i SDS, SSI eller KHR til en modtager uden for de tre institutioner/organisationer.
Fra fredag d. 11. september	• Der udvikles et script, som på tværs af SUM's koncern kan fremsøge alle modtagne mails fra brugere i SDS, SSI og KHR og gemme dem i såkaldte PST-filer.

	• SDS oplyser primo februar, at alle fremsøgte mails er gemt i PST-filer, og at disse snarligt vil kunne indlæse i de relevante medarbejderes postkasser for sendte mails. • Når indlæsningen er gennemført, skønner SDS, at 85-90 % af de slettede mails vil være genskabt.

3.2. Fokuspunkt 1: Ændring af indstilling for lagringstiden af sendte mails

I forbindelse med undersøgelsens redegørelse for hændelsesforløbet og afklaringen af, hvordan hændelsen kunne finde sted, er første fokuspunkt *ændringen af indstilling for lagringstiden af sendte mails*. Med henblik på at afdække forholdene omkring dette emne har KPMG gennemført en række interviews med medarbejdere fra bl.a. SDS's Driftsforvaltningsteam og Microsoft Danmark. Interviewene inkluderede bl.a. den exchange-administrator fra SDS, hvis bruger-ID ifølge logfiler blev anvendt ved de ændrede indstillinger og en field engineer fra Microsoft Danmark som bidrog som konsulent til implementeringen af Microsoft 365 i SDS, SSI og KHR i 2015 og leverede teknisk bistand til SDS i forbindelse med forløbet omkring hændelsen i august/september 2020.

3.2.1. Definering af retention policy for "sendt post".

Microsoft 365 blev implementeret i SDS, SSI og KHR i forbindelse med, at SDS blev etableret d. 1. november 2015 som en virksomhed i SUM's koncern. I forbindelse med implementeringen blev der i Microsoft 365 opsat en retention policy for bl.a. sendte emails.

Almindelig god praksis tilsiger, at defineringen af en eksplicit retention policy bør indgå som led i et velgennemført implementeringsforløb og skal foregå med afsæt i overvejelser om f.eks. forretningsmæssigt, juridisk og persondatabeskyttelsesmæssigt behov. Hvis der eksempelvis ikke er forretningsmæssige behov for, at emails bevares i mere end et år, kunne en overvejelse i defineringen af policy'en være, om emails, der er ældre end et år, automatisk bør slettes for at mitigere risikoen for kompromittering af personoplysninger.

KPMG har i forbindelse med undersøgelsen undersøgt hvilke overvejelser, der blev gjort i forbindelse med defineringen af sletteregler i 2015. I forbindelse med interviews har SDS-ansatte oplyst, at de ikke husker hvilke drøftelser, der mere konkret blev ført i 2015, hvorfor det ikke ad denne vej har været muligt at kaste lys over overvejelserne. SDS har heller ikke kunnet finde kunnet tilvejebringe skriftlig dokumentation vedrørende emnet.

3.2.2. Gennemgang af handlingsforløbet ved ændring af lagringstiden

Kortlægningen af handlingsforløbet har generelt været besværliggjort af, at SDS i forbindelse med hændelsen alene har sikret en enkelt log-fil fra hændelsestidspunktet. Denne fil giver ikke mulighed for at se, hvilke konkrete opsætningsændringer, der blev foretaget, eller hvordan disse blev foretaget. Af den gemte fil fremgår det alene, hvilket bruger-ID, der er anvendt til at foretage ændringerne, samt at der kl. 13:40:41 d. 21. august aktiveres et nyoprettet retention tag, og at

dette 21 sekunder senere knyttes til og anvendes i en aktiv retention policy. KPMG og SDS har i samarbejde med systemleverandøren Microsoft efterprøvet, om der kunne tilvejebringes logdata, hvilket viste sig ikke at være muligt.

Medarbejderen, hvis bruger-ID blev benyttet til at gennemføre ændringen i retention policy, har overfor KPMG bekræftet at vedkommende fredag d. 21. august 2020 var logget ind i Exchange på det tidspunkt, hvor ændringen ifølge logdata er gennemført. Medarbejderen har ca. 10 års erfaring som exchangeadministrator med on-premise exchangeløsninger, men har begrænset erfaring med med cloud-exchangeløsninger. Pågældende medarbejder har forklaret, at vedkommende var nyansat i SDS, og at formålet med arbejdet i Exchange på det pågældende tidspunkt var at gøre sig bekendt med den generelle parameteropsætning, som SDS benyttede i Microsoft 365. Medarbejderen forklarede også, at denne type sondering er standardpraksis for administratorer, når de skal sætte sig ind i en ny exchangeløsning.

I forbindelse med interviews har medarbejderen klart givet udtryk for, at vedkommende ikke kan genkalde sig at have ændret retention policy'en, men at det heller ikke kan afvises, at ændringen er forårsaget utilsigtet. Medarbejderen ser ikke grund til at betvivle de logdata, der viser, at vedkommendes bruger-ID blev anvendt til at foretage ændringen.

Ifølge forklaringer afgivet i forbindelse med interviews, blev der i perioden fra implementeringen af Microsoft 365 i 2015 og frem til d. 20. august 2020 ikke foretaget ændringer af retention policy'en for emails i "sendt post"-mappen. Alle sendte mails blev således gemt i en ubegrænset periode. Dette blev ændret d. 21. august 2020, da en medarbejder i SDS – som beskrevet i den kronologiske gennemgang af hændelsesforløbet ovenfor – tilføjede et retention tag til retention policy'en. Policy'en var nu defineret således, at emails i "sendt post"-mappen skulle bevares i 30 dage, hvorefter de blev overført til mappen "slettet post".

3.2.3. Gennemgang af den tekniske ændringsproces

I forbindelse med undersøgelsen har KPMG med bistand fra den SDS-medarbejder, der ifølge log-oplysningerne foretog ændringerne i retention policy'en, fået demonstreret systemet og dets opsætning, samt hvordan ændringer i sletteindstillinger foretages. Der er grundlæggende to måder, hvorpå indstillingerne kan ændres – én hvor der arbejdes i en grafisk brugergrænseflade, og én hvor der anvendes scripts i Windows PowerShell.3 Dette har systemleverandøren Microsoft bekræftet på møder med KPMG og SDS.

Den nævnte Exchange-administrator fra SDS har overfor KPMG givet udtryk for, at han den pågældende dag alene tilgik systemet via den grafiske brugergrænseflade. Dette skyldes, som tidligere nævnt, at formålet alene var at gøre sig bekendt med systemet og opsætningen. KPMG har derfor i samarbejde med vedkommende gennemgået hvilke skærmbilleder og trin, der skal gennemføres i den grafiske brugergrænseflade for at ændre retention policy'en, således at emails

[3] Windows PowerShell er en kommandolinjegrænseflade, som ved brug af scripts (et stykke kode som udfører en funktion) har til formål at automatisere og effektivisere administrationsopgaver i operativsystemer og server-applikationer.

i "sendt post"-mappen slettes efter 30 dage. Denne gennemgang har vist, at de pågældende ændringer umiddelbart forudsætter en række handlinger (fordelt over 7 trin).4 Endvidere har gennemgangen vist, at hændelsen potentielt kunne have haft endnu værre konsekvenser, end tilfældet er, idet det havde været muligt ikke kun at slette postkasserne med sendt mail men også alle indbakker, ligesom at det havde været muligt at slette alle mails umiddelbart og permanent i stedet for med de 30 dages opbevaringsperiode, som indstillingerne blev ændret til.

SDS-medarbejderen er overbevist om, at han ikke har foretaget den påkrævede række af handlinger i systemet. Det har derfor været drøftet, om nogle af de pågældende handlinger kunne have været foretaget på et andet tidspunkt og i en anden sammenhæng af andre medarbejdere, og at nogle allerede foretagne ændringer blot er blevet aktiveret d. 21. august. Microsoft har på møder med KPMG og SDS bekræftet, at dette er en praktisk mulighed, men som følge af fraværet af detaljerede log-filer både på hændelsestidspunktet og tilbage i tid er det ikke muligt hverken at be- eller afkræfte en sådan hypotese.

KPMG og SDS har på en række møder med Microsoft drøftet den tekniske ændringsproces med henblik på at tilstræbe en forståelse af, hvordan ændringen af indstillingerne kan være foregået. På baggrund af den gemte log-fil har Microsoft i den forbindelse vurderet, at den mest sandsynlige forklaring er, at den pågældende Exchange-administrator i SDS ved en fejl er kommet til at køre et tidligere udarbejdet script i PowerShell. Begrundelsen for denne vurdering er, at det forekommer særdeles usandsynligt, at administratoren uforvarende skulle have foretaget den række handlinger, som ændringerne forudsætter, ligesom det forekommer usandsynligt, at de påkrævede handlinger i den grafiske brugergrænseflade skulle være gennemført på de 21 sekunder, som log-filen viser, at der er gået mellem aktiveringen af det nye retention tag og tilknytningen til en aktiv retention policy.

SDS har på flere møder oplyst, at der i forbindelse med implementeringen af EU's persondataforordning (GDPR) i 2018 har været drøftelser om evt. at ændre politikken for opbevaring af sendte mails. SDS vurderer derfor, at det er muligt, at en tidligere medarbejder i den forbindelse kan have forberedt et script i PowerShell, som kunne anvendes i tilfælde af, at det blev besluttet at ændre politik. En sådan beslutning blev dog aldrig truffet.

3.2.4. Centrale observationer i relation til den ændrede indstilling for lagringstiden af sendte mails

Undersøgelsen viser, at de nærmere omstændigheder omkring hændelsen ikke lader sig kortlægge entydigt. Dette skyldes primært, at logdata vedrørende ændringer af systemindstillingerne kun gemmes i 90 dage, samtidig med at SDS kun sikrede en enkelt log-fil fra selve hændelsestidspunktet. Idet KPMG's undersøgelse først blev igangsat mere end 90 dage efter hændelsesdagen, har KPMG således ikke kunnet gennemgå systemloggen for

[4] En visualisering af trin og handlinger fremgår af rapportens bilag 1. Det skal understreges, at visualiseringens skærmbilleder af forsigtighedshensyn stammer fra et Exchange-demomiljø, men at KPMG har haft lejlighed til at se produktionsmiljøet og verificere, at miljøerne er funktionelt ens.

informationer om, hvad der skete på hændelsestidspunktet eller i en periode op til tidspunktet. Det er KPMG's vurdering, at sådanne logdata potentielt kunne have kastet lys over hændelsesforløbet.

På baggrund af undersøgelsen er KPMG's centrale observationer følgende:

- De begrænsede logdata, som blev sikret af SDS på selve undersøgelsestidspunktet, viser at et bruger-ID (og dermed en specifik medarbejder), har aktiveret et nyt 'retention tag' og en 'retention policy' d. 21. august 2020, hvilket medførte sletningen af sendte emails.
- Gennemgangen af processen for opdatering af en 'retention policy' i den grafiske brugergrænseflade viser, at der indgår så mange trin i processen, at det må vurderes som usandsynligt, at hændelsen skyldes, at den fulde proces er gennemført på hændelsesdagen ved en fejl.
- Microsoft vurderer, at den mest sandsynlige forklaring er, at ændringerne er foretaget ved, at den pågældende medarbejder ved en fejl har kørt et script i PowerShell, som evt. kan have været forberedt af en anden medarbejder på et andet tidspunkt og i en anden sammenhæng.
- Hændelsens konsekvenser kunne have været væsentligt værre, fordi det havde været muligt også at slette indbakker, og at gøre dette med øjeblikkelig virkning og uden mulighed for genskabelse.

Boks 3. KPMG's vurdering af ændringen i lagringstiden for sendte mails

Sammenfattende bemærkes det, at om end det på det forhåndenværende grundlag ikke er muligt at klarlægge, hvordan hændelsen præcis har fundet sted, er der intet i hverken de foreliggende tekniske informationer eller de gennemførte interviews som efter KPMG's vurdering indikerer, at hændelsen skulle skyldes en bevidst handling.

Det skal dog bemærkes, at det efter KPMG's vurdering er bekymrende, at der ikke har eksisteret – og fortsat ikke eksisterer tekniske foranstaltninger – der sikrer, at hændelsen ikke har kunnet finde sted, ligesom det er bekymrende, at hændelsen potentielt kunne have resulteret i et permanent tab af samtlige emails i SDS, SSI og KHR.

3.3. Fokuspunkt 2: Manglende indsigt i standardindstillingen for reetablering af emails

Andet fokuspunkt for redegørelsen for hændelsesforløbet og afklaringen af, hvordan hændelsen kunne finde sted, vedrører *den manglende indsigt i/bekræftelse af at standard-indstillingen på 30 dage for reetablering reelt var 14 dage*. Forholdene omkring dette emne er afdækket gennem interviews med ledere og medarbejdere i SDS, herunder særligt afdelingen Infrastruktur og Support (IOS) i SDS, hvor opgaven med reetablering var forankret, samt Microsoft Danmark.

3.3.1. Definering af retention policy for "sendt post".

Reetableringsperioden for emails, der slettes, fastsættes i forbindelse med oprettelse eller ændring af retention policy'en for den mappe, hvorfra de pågældende emails slettes. Således vælger administrator i forbindelse med oprettelsen af et retention tag den mappe, som tag'ets regler skal gælde for. I forbindelse med defineringen af tag'et angives det bl.a., om slettede mails skal kunne reetableres, og, hvis dette er tilfælde, hvor mange dage reetableringsperioden skal være.

Standardindstillingen i Exchange ved oprettelse af et retention tag er, at slettede emails skal kunne reetableres, men at de slettes permanent 14 dage, efter at de er flyttet til mappen "slettet post".

3.3.2. Gennemgang af handlingsforløbet - reetablering

Med afsæt i hvordan indstillingen for reetablering af emails håndteres i Exchange-brugergrænsefladen, ses i det nedenstående på de faktiske omstændigheder omkring den manglende indsigt i standardindstillingen for reetablering af emails.

Som nævnt tidligere blev der i perioden fra implementeringen af Microsoft 365 i 2015 og indtil d. 20. august 2020 ikke foretaget ændringer af retention policy'en for emails i "sendt post"-mappen. Alle sendte emails blev således gemt i en ubegrænset periode. En ny retention policy blev som redegjort for aktiveret d. 21. august 2020. Den nye policy, hvormed sendte mails skulle overføres til "slettet post"-mappen, når de var 30 dage gamle og slettes permanent efter yderligere 14 dage, gjaldt indtil den oprindelige retention policy blev genetableret d. 24. august 2020.

SDS igangsatte d. 24. august 2020 håndteringen af hændelsen med afsæt i SDS' incident management proces. Hændelsen blev vurderet som "kritisk", bl.a. idet den berørte flere men ikke alle institutioner i SUM. På denne baggrund tildeltes den en prioritet 2 på en skala fra 1 til 5, hvor 1 udgør højeste prioritet og indikerer, at der er tale om et såkaldt "major incident", som i henhold til SDS' retningslinjer skal håndteres med afsæt i særskilte retningslinjer.

De personer, der er interviewet i forbindelse med KPMG's undersøgelse, forklarer samstemmende, at den højeste prioritet ikke blev tildelt hændelsen, fordi man på tidspunktet for hændelsen var overbevist om, at a) man havde forstået hændelsen og b) man vidste, hvordan de slettede emails kunne genskabes. De interviewede personer giver udtryk for, at man på dette tidspunkt antog, at slettede emails først slettes permanent 30 dage efter, at de er flyttet til slettet post. Antagelsen viste sig dog at være fejlagtig, idet den aktive retention policy som nævnt faktisk definerede, at emails ville blive slettet permanent, allerede 14 dage efter at de var flyttet til "slettet post"-mappen".

Som årsag til at misforståelsen af reetableringsperioden opstod, har flere af de interviewede nævnt, at Microsoft 365's "standardperiode" for, hvor længe slettede emails opbevares, tidligere har været 30 dage. Adspurgt om dette har Microsoft dog oplyst, at 14 dage er og altid har været standardindstillingen, og at en længere periode på f.eks. 30 dage skal konfigureres af brugeren.

3.3.3. Centrale observationer i relation til den manglende indsigt i standardindstillingen for reetablering af emails

I forhold til den manglende indsigt i standardindstillingen for reetablering kan KPMG sammenfattende konstatere følgende:

- Standardindstillingen for opbevaring af mails sorteret til mappen "slettet post" har altid været 14 dage.
- Der har i SDS været et manglende overblik over indstillingerne, og ydermere har man undladt at kontrollere, om den fælles antagelse om en 30 dages opbevaring var korrekt.
- Der har endvidere tilsyneladende ikke været tilstrækkelig indsigt i en hensigtsmæssig incident håndtering til at sikre en grundig afdækning af risikobilledet, hvilket fik den beklagelige konsekvens, at hændelsen ikke blev taget tilstrækkeligt alvorligt.

Boks 4. KPMG's vurdering af manglende indsigt i standardindstillingen for reetablering af emails

Det manglende overblik over og den manglende kontrol af indstillingerne er efter KPMG's vurdering en alvorlig fejl i håndteringen, idet de sendte mails, som var blevet sorteret til "slettet post", efter de 14 dage ikke længere kunne gendannes. Såfremt SDS havde været opmærksom på eller kontrolleret indstillingen, kunne reetableringsprocessen have været tilrettelagt anderledes, så det muligvis havde været muligt at genskabe alle de slettede mails.

3.4. Fokuspunkt 3: Tiltag til gendannelse af sendte mails

Det tredje fokuspunkt i undersøgelsens redegørelse for hændelsesforløbets er de iværksatte tiltag til gendannelse af sendte mails, herunder reetableringen af de ca. 500 afdelings- og fællespostkasser samt vejledning til selv-reetablering. KPMG's undersøgelse i relation til dette emne er baseret på interviews med en række medarbejdere og ledere i både SDS og SSI. Tiltagene havde til formål at sikre gendannelse af datatabet.

3.4.1. Den centrale gendannelsesindsats i retentionperioden på 14 dage

Som nævnt ovenfor blev der i SDS i de første 14 dage efter sletningen ageret med afsæt i en antagelse om, at man havde 30 dage til at gendanne de slettede emails. Antagelsen var altså, at man havde indtil *d. 20. september* til at gendanne de slettede emails, mens gendannelsesvinduet de facto kun var på 14 dage, dvs. indtil fredag *d. 4. september*.

Gendannelsen er i sig selv en relativt ukompliceret operation, og den umiddelbare vurdering i SDS var, at 30-dages-vinduet derfor gav tilstrækkeligt tid til at genskabe data. Følgelig blev sletningen betragtet som en forretningsmæssigt ærgerlig hændelse, men også som en hændelse, som måtte forventes at resultere i få eller ingen varige konsekvenser for forretningen. Af denne grund - og fordi hændelsen ikke berørte brugerne i hele ministerområdet - betragtedes

hændelsen ikke som et 'major incident', der i henhold til incident management-processen er den højest prioriterede hændelsestype.

Som det fremgår af den kronologiske gennemgang af hændelsesforløbet, konstateredes det mandag d. 24. august, at retention policy'en var blevet ændret. Efter drøftelser i SDS besluttedes det at iværksætte en plan, hvormed gendannelse af emails sendt fra funktionspostkasser håndteredes fra centralt hold, mens individuelle brugere i første omgang selv skulle gendanne emails ved akut behov. Prioriteringen bundde primært i, at brugerne af funktionspostkasser ikke har rettigheder til at foretage gendannelse på egen hånd, hvorfor der ville være behov for assistance fra en administrator, ligesom det også vurderedes, at en stor del af de emails, der sendes via funktionspostkasser, under normale omstændigheder skal journaliseres, og at sikring af disse derfor var vigtig. Endvidere er det teknisk svært at håndtere gendannelse af emails slettet fra funktionspostkasser og individuelle brugerkonti simultant.

Indsatsen for at gendanne sendte mails fra funktionspostkasser blev igangsat onsdag d. 26. august. Løsningen indebar, at der foretoges kald fra SDS' Microsoft 365-løsning op imod Microsofts cloudmiljø, hvilket kan give udfordringer med båndbredde, når der – som i dette tilfælde – skal gendannes meget store mængder emails. I løbet af de første dages indsats konstateredes det, at fremdriften på gendannelse var under det ventede og ønskede niveau. Gendannelse skete således med en frekvens på mellem 2 og 4 emails i sekundet. Endvidere blev gendannelsesløsningen afviklet ustabilt og krævede kontinuerlig fysisk overvågning og løbende genstart af SDS' tekniker.

Med henblik på at øge gendannelseshastigheden rettede SDS torsdag d. 27. august henvendelse til sit kontaktpunkt hos leverandøren Microsoft vedrørende sagen. SDS' forespørgsel gik i første omgang på at bede Microsoft bistå med at få SDS' egen tekniske gendannelsesløsning til at køre hurtigere og mere stabilt ved at tillade flere forespørgsler fra løsningen op imod Microsofts cloudmiljø. Mandag d. 31. august kontaktede en tekniker fra Microsoft den tekniske lead på gendannelsesløsningen i SDS' for at drøfte, hvordan hændelsen skulle håndteres. Drøftelserne førte dagen efter, tirsdag d. 1. september, til at Microsoft anbefalede, at SDS oprettede en supportsag vedrørende hændelsen. SDS oprettede sagen næste dag, hvilket umiddelbart efter resulterede i, at der blev allokeret mere båndbredde til SDS' gendannelsesløsning. Over de følgende par dage kørte SDS' gendannelsesløsning, men konstateringen hos SDS var, at hastigheden fortsat var utilstrækkelig.

Fredag d. 4. september var gendannelsen af alle emails sendt fra funktionspostkasser gennemført, og SDS igangsatte med det samme løsningen til gendannelse af emails sendt fra individuelle brugerkonti. Samme dag var retentionperioden på de 14 dage dog gået. Dette betød, at resterende emails overført til "slettet post"-mappen var slettet permanent, og derfor ikke længere kunne gendannes.

3.4.2. Brugernes egen gendannelsesindsats i retentionperioden på 14 dage

Som beskrevet ovenfor blev det besluttet i første omgang at lade brugerne selv forestå gendannelsen af emails sendt fra individelle brugerkonti, mens den centrale gendannelsesindsats blev fokuseret på funktionspostkasser.

Til individuelle brugere med akut behov for at gendanne sendte emails, blev der udarbejdet en vejledning til, hvordan de på egen hånd kunne forestå gendannelsen. Selve proceduren for gendannelse er teknisk set ukompliceret og tidsmæssigt ikke særligt krævende. SDS vurderede således, at en medarbejder – afhængigt af hvor mange emails vedkommende skulle gendanne – ville skulle bruge mellem 5 og 15 minutter på at gennemføre gendannelsesproceduren.

Vejledningen til gendannelse blev publiceret på SDS' intranet tirsdag d. 25. august kl. 11:00 og efterfølgende på hhv. SSI's og KHR's intranet. Af meddelelsen, der blev publiceret på intranettet sammen med vejledningen, fremgik, at de brugere, der måtte vælge ikke at benytte sig af løsningen, ville få gendannet deres emails gennem den centrale løsning. Således var det antageligvis primært brugere med et akut behov for at tilgå sendte emails, der ville benytte sig af løsningen.

I Driftsforvaltningen i SDS blev det drøftet, om vejledningen i tillæg til publicering på intranettet skulle sendes til brugerne pr. email, men det blev besluttet ikke at gøre dette pga. forventningen om, at den centrale løsning snarligt ville blive anvendt til gendannelse af emails sendt fra individuelle brugerkonti. Samtidig blev det lagt til grund, at medarbejdere, der var fraværende pga. f.eks. ferie, orlov eller sygdom ikke vil benytte sig af vejledningen, hvorfor det under alle omstændigheder ville være nødvendigt at gøre centrale foranstaltninger til gendannelse.

SDS kan ikke give et autoritativt estimat på hvor mange medarbejdere, der på egen hånd har forestået gendannelse, men vurderer, at det drejer sig om relativt få medarbejdere, da kommunikationen omkring hændelsen netop gav indtryk af, at gendannelsesopgaven ville blive løftet centralt.

3.4.3. Gendannelsesindsatsen efter retentionperioden på 14 dage

Den faktiske gendannelsesperiode udløb fredag d. 4. september, og alle ikke-gendannede emails er efter denne dag slettet permanent. I weekenden lørdag d. 5. - søndag d. 6. september blev det konstateret, at den centrale gendannelsesløsning, som blev sat i gang med at gendanne emails fra individuelle brugerkonti fredag d. 4. september, ikke leverede det forventede output.

Om mandagen, d. 7. september, kontaktede SDS derfor Microsoft med henblik på at få afklaret, hvorfor gendannelsen af mails var stoppet. Microsoft rådgav SDS til at benytte funktionaliteten "litigation hold", som kan oversættes til "juridisk opbevaring". Funktionaliteten tillader, at en administrator kan "fastfryse" samtlige emails, der opbevares i en organisations postkasser, uagtet om de pågældende emails måtte være blevet underlagt en politik om at skulle slettes permanent efter en given periode. I det konkrete tilfælde ville aktiveringen af litigation hold betyde, at medarbejderne i SDS, SSI og KHR ikke længere selv ville være i stand til at slette emails, og at emails i "slettet post"-mappen ikke ville blive slettet efter udløb af retention-perioden. SDS aktiverede litigation hold-funktionaliteten samme dag, men det blev umiddelbart

efter konstateret, at retentionperioden faktisk var på 14 dage og ikke de antagne 30 dage, og at emails følgeligt allerede var slettet permanent.

SDS gik på baggrund af denne konstatering sammen med Microsoft i gang med at undersøge, om der fandtes alternative måder, hvorpå de slettede emails kunne gendannes. Onsdag d. 9. september bekræftede Microsoft efter forskellige overvejelser, at de ikke kunne gøre yderligere for at gendanne de slettede emails. Microsofts udmelding betød, at SDS torsdag d. 11. september – efter at have orienteret direktionerne i både SDS og SSI om situationen – iværksatte en ny tilgang til gendannelse. Tilgangen – som kun ville muliggøre en delvis gendannelse – indebar, at emails sendt fra ansatte i SDS, SSI og KHR til modtagere i SUM's koncern (hvad enten modtageren var den primære modtager eller blot sat i cc) skulle rekonstrueres ved at bruge Microsoft 365 funktionaliteten eDiscovery til at gennemsøge alle brugeres indbakker og i processen udfinde alle emails med en afsender fra en af de tre virksomheder. De pågældende emails, ville herefter kunne trækkes ud i form af en såkaldt PST-fil som efterfølgende ville kunne indlæses i den oprindelige afsenders "sendt post"-mappe. Emails som alene er blevet sendt til modtagere udenfor SUM's koncern måtte dog betragtes som værende tabt.

SDS har siden medio september arbejdet på at raffinere det script, der skal køres i eDiscovery med henblik på at udføre tilbageførslen af emails fra indbakkerne i institutionerne inden for SUM's koncern. I en periode på ca. 14 dage i oktober blev første gendannelsesforløb gennemført på 100 højt prioriterede brugerkonti og funktionspostkasser i SSI. Gendannelsen af de 100 postkasser var færdig d. 23. oktober, og i SSI bad man de pågældende brugere kontrollere, om de havde modtaget de forventede mails, samt om de mod forventning skulle have modtaget emails, som de ikke selv havde sendt. Kontrollen viste, at seks ud af de 100 brugere fejlagtigt havde fået gendannet emails, som de ikke selv havde sendt. Denne information blev delt med SSI's informationssikkerhedsansvarlige, som bad om at arbejdet blev stoppet og hændelsen indrapporteret til Datatilsynet. KPMG er i interview med SDS og KHR blevet oplyst om, at lignende problemstillinger ikke gør sig gældende i de to organisationer, idet test-gendannelsen – af hensyn til corona-indsatsen – alene omfattede brugere i SSI. SDS har efterfølgende udviklet et nyt og bedre script, og i skrivende stund oplyser SDS, at alle PST-filer er dannet og klar til snarlig indlæsning i brugernes "sendt mail"-postkasser. Det er SDS' vurdering, at i størrelsesordenen 85-90 % af alle mails sendt efter 1. januar 2020 hermed vil være genskabt.

3.4.4. Centrale observationer i relation til tiltag til gendannelse af sendte mails

I forhold til SDS' tiltag til gendannelse af de sendte mails, som var blevet slettet, kan KPMG sammenfattende konstatere følgende:

- I forlængelse af at de ændrede sletteindstillinger var konstateret, iværksatte SDS d. 26. august et arbejde med at genskabe de slettede mails.
- Det blev antaget, at det var muligt at gendanne mails i 30 dage, selvom der reelt kun var 14 dage til rådighed.
- Driftsforvaltningsteamet prioriterede i første omgang gendannelse af funktionspostkasser fra centralt hold, mens individuelle brugere via en besked på de berørte institutioners intranet blev instrueret i, hvordan de selv kunne genskabe deres egne mails.

- Som følge af at gendannelsen af funktionspostkasserne forløb i et utilfredsstillende tempo, blev Microsoft kontaktet for bistand d. 27. august, men først d. 2. september allokeredes der mere båndbredde til gendannelsesløsningen.
- Fredag d. 4. september var alle funktionspostkasser gendannet, men samtidig var retentionperioden på 14 dage gået, hvorfor de resterende mails fra alle de individuelle brugere ikke længere kunne gendannes.
- Mandag d. 7. september anbefalede Microsoft, at SDS straks benyttede funktionen "litigation hold", som fastlåser indholdet i alle postkasser uagtet den aktuelle politik.
- Medio september iværksatte SDS en ny tilgang, hvorved alle brugere i SUM's koncern fik deres indbakker gennemsøgt med henblik på at finde og udtrække alle mails modtaget fra afsendere i SDS, SSI og KHR, således at disse mails kunne indlæses i afsendernes "sendt mail"-postkasser. Denne proces er nu gennemført, og alene indlæsningen i afsendernes postkasser udestår. SDS vurderer, at ca. 85-90 % af de slettede mails siden 1. januar 2020 herved er genskabt.

Boks 5. KPMG's vurdering af tiltagene til gendannelse af sendte mails

Der er efter KPMG's vurdering begået flere væsentlige fejl i gendannelsesprocessen. Ud over den manglende indsigt i og kontrol af, hvor lang tid en fuldstændig gendannelse var mulig, finder KPMG det også uheldigt, at Microsoft først blev inddraget aktivt i gendannelsesbestræbelserne mere end en uge efter, at disse var påbegyndt.

Ligeledes er det kritisabelt, at SDS ikke var opmærksom på muligheden for at anvende "litigation hold", før Microsoft foreslår dette mere end to uger efter, at de ændrede indstillinger har ført til sletningen af de sendte mails. Såfremt SDS umiddelbart efter, at de ændrede indstillinger blev konstateret, havde anvendt "litigation hold" ville det have været muligt at sikre, at ingen af de sendte mails, som blev overflyttet til "slettet mail"-postkassen, ville være gået tabt.

3.5. Fokuspunkt 4: Ledelsesmæssig og organisatorisk håndtering af hændelsen

Fjerde fokuspunkt for redegørelsen for hændelsesforløbet og afklaringen af, hvordan hændelsen kunne finde sted, vedrører den ledelsesmæssige og organisatoriske håndtering af hændelsen/-erne ifht. best practice for it-branchen. I undersøgelsen af dette fokuspunkt har KPMG gennemført en række interviews med ledere og medarbejdere i SDS, SSI og KHR. Interviewene er blevet suppleret med forskellig skriftlig dokumentation, herunder ikke mindst en omfattende mail-korrespondance. I afdækningen har KPMG primært lagt vægten på håndteringen af hændelsen af direktionen i SDS.

3.5.1. Gennemgang af handlingsforløbet – ledelsesmæssig og organisatorisk håndtering

I forbindelse med de gennemførte interviews, har KPMG fået oplyst, at direktionen første gang blev gjort opmærksom på hændelsen, da medarbejdere i direktionssekretariatet spurgte, hvorfor det var besluttet at ændre slettepolitik for sendte mails. På den baggrund rettedes henvendelse til styrelsens afdeling for Infrastruktur og Support (IOS). Afdelingen bekræftede, at retention policy for sendte mails var blevet ændret, men at dette skyldtes en menneskelig fejl og ikke en bevidst ændring af politikken. Samtidig oplyste IOS, at retention policy var tilbageført til de oprindelige indstillinger.

Direktionen orienteredes endvidere om, at der var tale om en kritisk hændelse ("incident"), men ikke en hændelse af højeste kritikalitet ("major incident"). Begrundelsen herfor var, at driftsforvaltningsteamet kunne genetablere de slettede mails, og at tiltag til genetablering allerede var iværksat. Disse forklaringer underbygges af den omfattende interne mailkorrespondance, som KPMG har haft adgang til. Således fremgår det af en mail til direktionen og direktionssekretariatet d. 25. august, at de sendte mails "p.t. er utilgængelige", men at "det er vigtigt at påpege, at mails ikke er gået tabt". Senere samme dag modtog direktionen og direktionssekretariatet endnu en mail, hvoraf følgende fremgår: "Vi er i fuld gang med at restore alle postkasser. Vi starter med fællespostkasserne og derefter brugernes postkasser. Desuden er der på IT nyheden lagt en vejledning til, hvordan man selv kan restore sine sendte mails både via outlook og webmail. Vi betragter dette incident som tæt ved løst".

Det er KPMG's forståelse, at direktionen på den baggrund vurderede, at situationen var under kontrol, og at det var mest hensigtsmæssigt at lade teknikerne i driftsforvaltningsteamet koncentrere sig om genetableringen uden unødig forstyrrelse.

Da driftsforvaltningsteamet i weekenden d. 5.-6. september konstaterede, at der ikke længere blev gendannet mails, blev problemet i første omgang anset for teknisk, og der blev derfor arbejdet på at finde en teknisk løsning. Efter KPMG's oplysninger blev direktionen ikke orienteret herom. Først d. 10. september konstateredes det i samarbejde med Microsoft, at det ikke længere var muligt at genskabe de slettede mails, og direktionen blev orienteret samme eftermiddag. Om morgenen d. 11. tog direktionen kontakt til ledelserne i SSI og KHR og orienterede dem om situationen.

Det fremgår af den tilgængelige mailkorrespondance, at direktionen fra dette tidspunkt var tæt involveret i den interne håndtering af hændelsen i SUM's koncern såvel som den eksterne håndtering, herunder særligt forberedelse af intern og ekstern kommunikation. Samtidig fulgte direktionen de tekniske tiltag med gendannelse via løbende statusopdateringer.

3.5.2. Centrale observationer i relation til den ledelsesmæssige og organisatoriske håndtering af hændelsen

I forhold til den ledelsesmæssige og organisatoriske håndtering af hændelsen, kan KPMG sammenfattende konstatere følgende:

- SDS' direktion blev orienteret umiddelbart efter, at de ændrede sletteindstillinger var konstateret, men blev oplyst om, at situationen var under kontrol, og at alt kunne gendannes.

- Først d. 10. september, hvor det ikke længere lod sig gøre at genskabe de slettede mails, blev direktionen og direktionssekretariatet igen involveret direkte i hændelsen.
- D. 11. september kontaktede SDS' direktion ledelserne i SSI og KHR for at orientere om situationen, og fra dette tidspunkt var direktionen og direktionssekretariatet tæt involveret i hændelseshåndteringen.

Boks 6. KPMG's vurdering af den ledelsesmæssige og organisatoriske håndtering af hændelsen

Efter KPMG's vurdering skal SDS' direktions håndtering af hændelsen ses i lyset af den fejlagtigt betryggende orientering, den har modtaget. KPMG vurderer således, at SDS' direktion vanskeligt kan kritiseres for ikke at involvere sig i højere grad, på baggrund af oplysningerne om, at situationen var under kontrol. Direktionens håndtering af og reaktion på de modtagne oplysninger skal ydermere ses i sammenhæng med den helt særlige kontekst, som styrelsens arbejde har været udført under i relation til corona-indsatsen.

Generelt er det dog KPMG's vurdering, at SDS' organisation og ledelse er karakteriseret ved en udstrakt grad af delegering og tillid, og det kan ikke udelukkes, at dette har været medvirkende til, at oplysningerne fra driftsorganisationen ikke er blevet udfordret i ønskeligt omfang.

3.6. KPMG's sammenfattende vurdering af hændelsesforløbet

KPMG's afdækning af hændelsesforløbet viser, at et bruger-ID (og dermed en specifik medarbejder), har opdateret et 'retention tag' og en 'retention policy', hvilket medførte, at politikken for sendte mails blev ændret, så disse blev slettet efter 30 dage. Dette stemmer overens med SDS' egen undersøgelse af hændelsen.

Der er intet i KPMG's afdækning, der indikerer, at der er tale om en bevidst handling, eller at det pågældende bruger-ID er blevet kompromitteret eller hacket. Dette understøttes af, at der kunne være foretaget betydeligt mere skadelige handlinger, herunder at også indbakker med modtagne mails kunne have været slettet på samme vis, og at sletningen kunne have været med umiddelbar og permanent effekt uden mulighed for genskabelse. Endvidere har det været muligt at genskabe en stor andel af de slettede mails (SDS skønner, at omkring 85-90 % af alle sendte mails siden 1. januar 2020 er genskabt). Det er således KPMG's vurdering, at sandsynligheden taler for, at der er tale om en utilsigtet, menneskelig fejl.

Imidlertid kan de eksakte omstændigheder omkring hændelsen ikke kortlægges på baggrund af den forhåndenværende information. Dette skyldes først og fremmest, at logdata vedrørende ændringer af systemindstillingerne kun opbevares i systemet i 90 dage. Dette gælder både hos SDS og hos systemleverandøren Microsoft. Idet undersøgelsen først blev igangsat mere end 90 dage efter hændelsestidspunktet, har KPMG således ikke kunnet gennemgå systemloggen for informationer om, hvad der præcist skete på hændelsestidspunktet eller i en periode op til

tidspunktet. Det er efter KPMG's vurdering meget beklageligt, at disse logdata ikke er blevet sikret og gemt på anden vis, da de potentielt kunne have kastet lys over hændelsesforløbet.

På grundlag af den eksisterende dokumentation og de gennemførte interview, er det dog KPMG's vurdering, at hændelsesforløbet har været karakteriseret af flere alvorlige fejl. I den forbindelse skal særligt følgende fremhæves:

- KPMG finder det bekymrende, at det tilsyneladende har været relativt let at foretage så indgribende ændringer i systemets indstillinger, uden at dette er blevet bemærket af hverken den pågældende medarbejder eller den driftsorganisation, som er ansvarlig for systemet.
- KPMG finder det kritisabelt, at der ikke har været kendskab til eller kontrol af, hvor lang tid SDS reelt havde til rådighed til at genskabe de slettede mails. Havde SDS været bevidst om, at der reelt kun var 14 dage til rådighed, ville det have været muligt at tilrettelægge hændelseshåndteringen anderledes (herunder med tidligere og mere akut inddragelse af systemleverandøren), således at det havde været muligt at gendanne alle slettede mails.
- KPMG finder det særdeles uheldigt, at SDS ikke har været opmærksom på muligheden for at anvende "litigation hold" umiddelbart efter, at den ændrede slettepolitik blev konstateret. En anvendelse heraf ville have fastlåst indholdet i alle postkasser uagtet den aktuelle politik, så ingen af de sendte mails, som blev overflyttet til "slettet mail"-postkassen, ville være gået tabt.

4. Læring og anbefalinger

I dette afsnit adresseres undersøgelsens andet primære fokus, dvs. læring og anbefalinger på baggrund af hændelsen. Som det fremgår af undersøgelsesrammen, har denne del af undersøgelsen særligt haft fokus på *mulige tekniske tiltag, der kan forhindre eller minimere konsekvenserne af tilsvarende hændelser* samt *organisatoriske og ledelsesmæssige tiltag, der kan forebygge tilsvarende hændelser eller minimere konsekvenserne samt forbedre håndteringen*.

Med udgangspunkt i opdragets ordlyd skal hændelsen naturligvis forstås i kontekst af SDS' håndtering af IT- og informationssikkerhed i bredere forstand, herunder både teknisk, organisatorisk og ledelsesmæssigt. Det skal dog bemærkes, at KPMG's fokus har været på læring og anbefalinger relateret til hændelsen. Det følgende er således ikke baseret på en systematisk og tilbundsgående analyse af SUM's IT-organisering og -governance, men har karakter af generelle observationer i tilknytning til hændelsen.

Samtidig bør hændelsen og dens håndtering ses i lyset af den ekstraordinære situation, som SUM's koncern og herunder SDS har været i som følge af en usædvanligt stor arbejdsbyrde i relation til COVID-19. Således har organisationens fokus og ressourcer i høj grad været prioriteret til håndteringen af pandemien med afledt effekt på andre dele af den daglige drift og opgavevaretagelse.

Endelig skal det bemærkes, at der i nedenstående anbefalinger ikke er taget stilling til konsekvenserne af den forestående transition af dele af IT-driften fra SDS til Statens IT. Nogle af de identificerede udfordringer vil således kunne forventes håndteret i forbindelse med transitionen, hvorfor prioriteringen af KPMG's anbefalinger naturligt vil skulle foretages i lyset af transitionen.

Undersøgelsens observationer og anbefalinger er i det følgende struktureret efter opdragets ordlyd, således at tekniske tiltag henholdsvis organisatoriske og ledelsesmæssige tiltag er beskrevet separat. I praksis vil de mulige tiltag dog ofte skulle implementeres i sammenhæng, og til tider vil tekniske og organisatoriske tiltag være hinandens forudsætninger. Endelig afrundes afsnittet med en kort redegørelse for øvrige væsentlige observationer, som KPMG har gjort i forbindelse med undersøgelsen.

4.1. Mulige tekniske tiltag

De mulige tekniske tiltag kan, som det fremgår af undersøgelsens opdrag, groft inddeles i tiltag til at forhindre lignende hændelser fremadrettet og tiltag til at begrænse konsekvenserne, hvis lignende hændelser alligevel måtte indtræffe.

4.1.1. Tekniske tiltag til at forhindre tilsvarende hændelser

Som beskrevet i afsnit 3.2 har KPMG i samarbejde med SDS og Microsoft kortlagt de nødvendige trin i forbindelse med en ændring af retention policy i den grafiske brugergrænseflade i Exchange. Denne kortlægning har vist, at ændringer i retention policy forudsætter en længere kæde af handlinger og trin, før ændringerne aktiveres. Som beskrevet forekommer det usandsynligt, at en administrator gennemgår alle de pågældende handlinger og trin – og dermed ændrer retention policy – ved et uheld. Det er således KPMG's vurdering, at de mange trin i den grafiske brugergrænseflade – i sammenhæng med dialogbokse, hvor administratoren både skal trykke "gem" og "ok" til ændringer ad to omgange – i sig selv burde være tilstrækkeligt til at forhindre utilsigtede ændringer i retention policy. Såfremt det alligevel måtte ønskes at indsætte yderligere tekniske begrænsninger, kan det dog overvejes at integrere endnu klarere advarsler i systemet ved ændringer af SDS' grundlæggende slettepolitikker. Dette vil dog formodentlig forudsætte en særskilt tilpasning til SDS med en tilhørende omkostning.

Dialogen med systemleverandøren Microsoft har som beskrevet givet anledning til at formode, at den ændrede retention policy snarere skyldes, at der er blevet eksekveret en kommando (et script) i PowerShell. Det vil rent teknisk forudsætte, at en administrator koder den specifikke kommando til ændring af retention policy, og dette forudsætter igen en væsentlig forståelse for kommandoer i PowerShell. Derfor forekommer det også særdeles usandsynligt, at en administrator ved en fejl har udarbejdet en fejlagtig kode, hvorfor tekniske tiltag i PowerShell efter KPMG's vurdering ikke vil udgøre en praktisk løsning. Som det fremgår af afsnit 3.2, er den mest plausible forklaring således, at der er tale om, at et allerede forberedt script ved en fejl er blevet kørt i PowerShell. En beskyttelse mod en sådan hændelse vil snarere være organisatorisk end teknisk, jf. afsnit 4.2. nedenfor.

I forhold til tekniske tiltag for at forhindre lignende hændelser finder KPMG det derimod væsentligt at overveje, om det er muligt at give administratorer adgang til systemerne, uden at der er risiko for, at de kan foretage ændringer af væsentlige politikker. Det kunne være i form af en begrænset administrativ adgang til brug i den daglige drift, hvor det er muligt at foretage almindelige administrative opgaver såsom oprettelse af nye brugere mv., men hvor særligt kritiske ændringer ikke kan foretages. Administratoren ville derudover kunne tildeles en ekstra konto (login), som kun ville skulle anvendes, når eksempelvis retention policy eller andre væsentlige og kritiske indstillinger skal ændres. Derved ville risikoen for utilsigtede ændringer som den aktuelle være kraftigt reduceret.

Anbefaling #1. To konti til administratorer

Det anbefales, at SDS og SUM overvejer muligheden for at tildele administratorer to konti til administration af de centrale IT-systemer på ministerområder – en begrænset administrationskonto, som anvendes til den daglige drift og en konto, som alene anvendes, hvis særligt kritiske politikker eller lignende skal ændres.

4.1.2. Tekniske tiltag til at minimere konsekvenserne af tilsvarende hændelser

Uagtet de tiltag, som SDS måtte foretage, vil der aldrig være en garanti for, at tilsvarende hændelser ikke kan ske i fremtiden. Som redegørelsen for hændelsesforløbet i afsnit 3 har dokumenteret, har håndteringen af hændelsen og dens konsekvenser dog ikke været optimale. Således er der tidligere truffet tekniske valg, som har forværret konsekvenserne.

I forbindelse med implementeringen af Microsoft 365 i 2015 fravalgte SDS, SSI og KHR at etablere en back-up for mailløsningen. KPMG er ikke bekendt med, i hvilken udstrækning der har været tale om et oplyst valg, men det er erfaringen, at back-up ved traditionelle on-premise systemer som oftest fravælges ud fra en vurdering af risikoen for uheld – brand, oversvømmelse eller lignende – i det rum, hvor serveren opbevares, og den risiko der herved ville være for, at data kunne gå tabt. De gennemførte interview har som nævnt ikke afdækket de konkrete overvejelser bag fravælgelsen af back-up i 2015. Imidlertid har flere medarbejdere i interview givet udtryk for, at det på daværende tidspunkt formentlig har været antaget, at der ikke har været behov for en back-up, da der ikke var et fysisk serverrum, hvor der kunne ske uheld, idet mails blev opbevaret i Microsofts cloud-løsning, og da Microsoft naturligvis ikke sletter kundernes mails. Som hændelsen har demonstreret, tager en sådan tilgang dog ikke højde for, at SDS selv utilsigtet kunne komme til at ændre indstillingerne for opbevaring af sendte mails. Havde SDS haft en back-up af mail-systemet, ville konsekvenserne af den ændrede retention policy imidlertid alene været ulejlighed i form af behov for genindlæsning af back-up'en.

I organisationer, hvor emails er en central del af sagsbehandlings- og beslutningsprocesser, er det almindeligt, at der anvendes en såkaldt Vault-løsning. Dette er en database, hvor alle emails – både interne og eksterne – gemmes. Databasen tillader ikke sletning, hvilket betyder, at forsvundne mails altid kan genskabes. Der er ikke tale om et egentligt backup-system, men om en samlet log over alle afsendte og modtagende emails, som med gode søge- og eksportmuligheder gør det muligt at genskabe mails uanset årsagen til, at de ikke længere er tilgængelige for brugeren – eller hvis brugeren er ophørt.

Anbefaling #2. Etablering af back-up

Det anbefales, at SDS og SUM nøje overvejer hensigtsmæssigheden af at etablere en ekstern back-up af mail-systemet. Alternativt bør det overvejes at etablere et Vault-system til fremfinding og genskabelse af emails.

4.1.3. Øvrige mulige tekniske tiltag

Undersøgelsen af hændelsen har været besværliggjort af, at SDS ikke har kunnet stille mere end en enkelt logfil til rådighed for KPMG. Som beskrevet i afsnit 3 giver SDS' mailløsning kun adgang til logfiler for de seneste 90 dage, og hverken SDS eller systemleverandøren Microsoft gemmer kopier af ældre logfiler. Ud over at dette har vanskeliggjort afdækningen af, hvad der teknisk er sket i den konkrete hændelse, leder manglende logfiler også til mere generelle udfordringer i

forhold til læring og forbedringer for at undgå og håndtere tilsvarende hændelser fremadrettet. Det burde imidlertid være simpelt at etablere en auditlog for administratorhandlinger, som ville give mulighed for læring, når der fremadrettet måtte ske fejl, ligesom auditlogs ville kunne bidrage til i højere grad at klargøre roller og ansvar i den daglige drift. Endvidere ville et logningssystem eventuelt kunne søges etableret med muligheden for at udsende advarsler ved konkrete hændelser som f.eks. ændringer af retention policy.

Anbefaling #3. Etablering af system til auditlog

Det anbefales, at SDS undersøger muligheden af at etablere et system til opbevaring af en auditlog for administratorhandlinger. Samtidig bør muligheden for, at systemet kan udsende advarsler ved bestemte hændelser, undersøges.

4.2. Mulige organisatoriske og ledelsesmæssige tiltag

Afdækningen af hændelsesforløbet har givet anledning til en række observationer i relation til organisatoriske og ledelsesmæssige tiltag til forebyggelse af tilsvarende hændelser såvel som til en bedre håndtering af eventuelle hændelser. Disses observationer og tilknyttede anbefalinger præsenteres i det følgende.

4.2.1. Styrket IT-governance

Som tidligere nævnt har KPMG ikke foretaget en systematisk og tilbundsgående analyse af IT-governance i SDS og inden for SUM's koncern. Alligevel har både hændelsen i sig selv og den efterfølgende håndtering indikeret, at IT-governance på ministerområdet på en række punkter kan styrkes. Samtidig kræver cloud-governance et større fokus på systemforvaltningen og mindre på infrastrukturen, end tilfældet er ved on-premise governance, hvilket også forudsætter nogle andre kompetencer. Neden for nævnes en række konkrete observationer og anbefalinger til overvejelse i den henseende, men samtidig tilsiger disse også, at der kan være behov for et mere generelt eftersyn af SDS' og SUM's IT- og informationssikkerheds-governance.

Således har afdækningen af hændelsesforløbet vist, at der tilsyneladende på intet tidspunkt har været enkeltpersoner eller enheder, som har haft et overblik over den samlede hændelseskæde, før længe efter selve hændelsen. Upåagtet at den konkrete hændelse sandsynligvis ikke gentages, er mulighedsrummet for uhensigtsmæssige hændelser blevet markant større de seneste år, idet kompleksiteten af den digitale understøttelse har været kraftigt stigende. Herved er risikoen for (små) fejl, som kan vokse sig kritiske, øget markant. I SUM's koncern – som på alle ministerområder – betyder den stærkt stigende kompleksitet, at ministeriet skal have styr på, hvordan selv marginale ændringer i f.eks. en konfiguration i et administrativt IT-system i sidste ende kan føre til, at forretningskritiske systemer eller data bliver påvirket af ændringen. Det er KPMG's vurdering, at dette mest effektivt gøres ved at skabe rammerne for kontinuerlig udvikling af den samlede modenhed, hvormed der arbejdes med cyber- og informationssikkerhed. Dette

gøres typisk med udgangspunkt i et direktionsforankret dokument, som behandler de retningslinjer, tiltag og standarder, som bør efterleves for at ministerområdet bedst muligt kan forudse, imødegå og håndtere IT- og informationssikkerhedsmæssige udfordringer. Blandt de standarder, som KPMG vil forvente som minimum inddrages, er, ISO2700X (herunder med særligt fokus på ISO27001/27002 om ledelsessystemet og dets kontroller og ISO27005 om risikostyring), ISO27701, ISO22301 (om forretningskontinuitet), BS11200 (om krisestyring) og ISO27031 (om ICT-parathed til forretningskontinuitet). Hertil vil KPMG normalt anbefale, at der udarbejdes konkrete planer, herunder en implementeringsplan, samt en samlet overordnet forretningsgang eller procedure for de mere konkrete anvisninger ift. den koncernforbundne efterlevelse af den samlede IT- og informationssikkerhedsmæssige tilgang.

Anbefaling #4. Analyse af og fremtidig strategi for IT-governance i SUM

Det anbefales, at SDS/SUM foretager en tilbundsgående analyse af varetagelsen af IT- og informationssikkerheds-governance på ministerområdet i dag og på den baggrund udarbejder en ny samlet strategi og vedvarende implementeringsplan for den fremadrettede varetagelse. I dette arbejde bør der tages højde for de ændrede governance-behov, som følger af at anvende cloud-baserede systemer, herunder det faktum at organisationen ikke har adgang til infrastruktur-laget, hvorfor mange sikkerhedsprocesser skal lægges væsentligt om.

4.2.2. Risikostyring

En afgørende forudsætning for en robust IT-governance og hensigtsmæssig informationssikkerhed er, at der løbende samt i forbindelse med væsentlige ændringer foretages grundige risikovurderinger. Selve risikobegrebet er komplekst og har mange delelementer, herunder:

- Risikovillighed – hvilke risici er den strategiske ledelse villig til at acceptere?
- Risikoniveauer – hvornår er noget en risiko, og hvad er "høj" risiko?
- Trusselsbilledet – hvor truede er vi, og hvem vil os det dårligt?
- Beskyttelsesværdige aktiver – hvad er organisationens mest væsentlige aktiver / systemer / processer / personer?
- Sårbarhedsvurdering – hvilke systemer har hvilke sårbarheder, som er i fare for udnyttelse eller fejl?
- Modenhedsanalyse – med hvilken modenhed (erfaring / viden / indsigt) udfører vi alle de trin, som skal efterleves (strategisk, taktisk og operativt)?

En forudsætning for en helhedsorienteret risikostyring er, at der er en klar "rød tråd" fra den strategiske ledelses beslutninger til implementering på det operative niveau og den modsatte vej. Risikostyringen og -vurderingen samler alle de ovenstående elementer og gør det muligt at prioritere, hvad der skal nyde fremme, og hvad der kan ignoreres eller accepteres.

Strategisk risikostyring er desuden præget af, hvordan risici kvantificeres og kvalificeres – samt om risici lader sig identificere. En ofte overset risiko er de forhold, som antages at være irrelevante, men som viser at have stor kausal betydning for såvel systemer som data. Den aktuelle hændelse forekommer at være et eksempel på, at SDS ikke har haft en tilstrækkelig forståelse for risici i forbindelse med implementering af Microsoft 365.

Risikovurdering af en løsning som Microsoft 365 gennemføres med henblik på at skabe et klart billede af, hvad der kan gå galt i anvendelsen af systemet, hvilken effekt dette kan have, samt hvad der kan og bør iværksættes af modforanstaltninger. En email-løsning tjener i næsten alle tilfælde en central funktion i en organisation – både i forhold til den interne og i forhold til den eksterne kommunikation. Som sådan er der tale om, at der med email leveres en essentiel funktionalitet, som det bør være naturligt at prioritere risikovurdering og -styring af.

Som led i afdækningen af hændelsen om den ændrede retention policy for sendte mails er KPMG blevet oplyst om, at der ikke blev foretaget en egentlig risikovurdering i forbindelse med hverken beslutningen om at implementere Microsoft 365 eller den efterfølgende implementering af løsningen. Ifølge det oplyste blev der således kun foretaget en vurdering af løsningen med afsæt i et sæt af krav, som Datatilsynet stiller til løsninger, der skal behandle persondata.[5] Ifølge flere af de interviewede medarbejdere har risikovurderinger i SDS da også historisk primært handlet om beskyttelse af de følsomme persondata, som sundhedsvæsenet behandler, og i langt mindre grad om sikring af sikker og stabil drift.

KPMG er i øvrigt ikke i forbindelse med undersøgelsen blevet nærmere oplyst om, hvordan processen omkring vurderingen af risici for persondatabehandlingen ved anvendelse af Microsoft 365 er foregået, herunder om den f.eks. er gennemført af én medarbejder, eller om der har været tale om en mere inkluderende proces, hvor eksempelvis repræsentanter for de omfattede institutioner, teknikere fra SDS' driftsafdeling og leverandøren har været inddraget. Det er dog oplyst, at der ikke siden er foretaget yderligere vurderinger af løsningen, herunder heller ikke i forbindelse med implementeringen af GDPR i 2018.

KPMG vurderer, at SDS/SUM bør gennemføre en udtømmende risikovurdering af Microsoft 365. En sådan risikovurdering, inklusive en plan for mitigerende handlinger, må antages at forbedre forståelsen af risici forbundet med Microsoft 365 i relevante dele af SDS og dermed forbedre evnen til at styre og navigere i disse.

Anbefaling #5. Risikovurdering af Microsoft 365

Det anbefales, at SDS gennemfører en risikovurdering af Microsoft 365 med henblik på at kortlægge risikobilledet og skabe et veldokumenteret grundlag for at planlægge og eksekvere mitigerende handlinger.

[5] Sundhedsdatastyrelsen: "Sikkerhedskrav ved anvendelse af Office 365 og andre løsninger i cloud", 17. februar 2016.

I et bredere perspektiv giver observationerne i relation til risikostyringen af Microsoft 365 også anledning til at fokusere på den generelle risikostyring i SDS og SUM's koncern.

Anbefaling #6. Styrkelse af risikostyringen i SDS

Det anbefales, at SDS foretager et review af sin model for risikostyring og udarbejdelse af risikovurderinger med henblik på at sikre, at denne afspejler sundhedsvæsenets kritikalitet og de teknologiske udfordringer, som sundhedsvæsenet skal håndtere. På baggrund af reviewet bør der udarbejdes en handlingsplan for at optimere risikostyringen.

4.2.3. Governance vedrørende udarbejdelse og opbevaring af scripts til PowerShell

Som redegørelsen for hændelsesforløbet beskriver, er det plausibelt, at den ændrede retention policy skyldes, at et tidligere forberedt script utilsigtet er blevet eksekveret i PowerShell. I forbindelse med nogle af de gennemførte interviews har KPMG fået oplyst, at scripts og kodestumper i dag opbevares og deles på en række forskellige måder i IOS, herunder på desktops, i fileshare-løsninger, i notepad og i mails. Der er derfor ikke noget samlet overblik over, hvor scripts og kodestumper opbevares. Samtidig er det blevet oplyst, at disse scripts kan være kodet som eksekverbare filer, som ikke forudsætter, at en medarbejder nødvendigvis er inde i PowerShells for at sætte en kommando i gang. Dette indebærer naturligvis en risiko for, at et scripts eksekveres utilsigtet. En mitigerende løsning kunne være oprettelsen af et kode-repository med alle udarbejdede scripts, inkl. versionsstyring, kodeforklaring mv. Der ville samtidig skulle etableres en klar governance-struktur omkring et sådant repository. Dette ville sikre et samlet overblik over alle SDS' scripts, og at mindske risikoen for, at en administrator utilsigtet eksekvere et script. Samtidig vil etableringen af et respository formentlig i sig selv anspore til en højere grad af opmærksomheden omkring anvendelsen af scripts og de risici, der bør håndteres i den forbindelse. Dette kan i øvrigt med fordel gøres i sammenhæng med anbefaling #1 om indførelse af en begrænset administrativ adgang til brug i den daglige drift, idet dette ville styrke overholdelsen af governance-processer omkring script-afvikling.

Anbefaling #7. Etablering af kode-repository med tilhørende governance

Det anbefales, at SDS overvejer etableringen af et kode-repository, hvor alle scripts til PowerShell skal opbevares, og at der indføres en klar governance omkring udarbejdelse, deling og anvendelse af scripts.

4.2.4. Systemforvaltning på kontorplatformen

Som det er fremgået af redegørelsen for hændelsesforløbet, blev den ændrede retention policy konstateret og ændret tilbage efter få dage. Samtidig iværksatte SDS straks en proces til genskabelse af de slettede mails. Imidlertid forløb håndteringen af hændelsen utilfredsstillende. Dette skyldes først og fremmest den manglende indsigt i eller kontrol af indstillingen af reetableringsperioden til 14 dage, men formentlig også i bredere forstand en utilstrækkelig detailforståelse for systemet og dets kritikalitet hos brugerne i de berørte institutioner.

I forbindelse med undersøgelsen har flere af de interviewede peget på, at der i dag mangler egentlige systemforvaltere på SDS' kontorplatform, som har tilstrækkeligt kendskab til brugernes anvendelse af systemerne. Således er systemforvalteransvaret formelt placeret hos en sektionsleder i IOS, som dermed har ansvaret for ca. 25 forskellige systemer. Det betyder, at det i praksis ikke er muligt at kende systemerne og deres anvendelse, og dermed at systemforvaltningen ikke varetages i fornødent omfang.

En løsning herpå kunne være at etablere egentlige systemforvalterroller – eventuelt decentralt hos SDS' kunder. Sådanne systemforvaltere ville have et detailkendskab til og forståelse for, hvem der bruger en given service, hvordan den bruges, hvad de forretningsmæssige konsekvenser af konkrete handlinger ville være etc. De bliver dermed centrale, når det kommer til at opdage og forebygge fejl eller brud på informationssikkerheden, fordi de kan se udfordringerne i praksis. I forbindelse med den konkrete hændelse ville sådanne systemforvaltere kunne have forbedret håndteringen, herunder muligvis have sikret, at den reelle reetableringsperiode var kendt eller blev kontrolleret.

Anbefaling #8. Styrket systemforvaltning på kontorplatformen

Det anbefales, at SDS/SUM overvejer at styrke systemforvaltningen på kontorplatformen ved at etablere systemforvaltere med et indgående kendskab til brugernes anvendelse af systemerne.

4.2.5. Incident-håndtering

Afdækningen af hændelsesforløbet har vist, at den utilstrækkelige håndtering af hændelsen var kritisk for de langsigtede konsekvenser i mindst ligeså høj grad som ændringen af retention policy'en i sig selv. Havde SDS været opmærksom på den begrænsede reetableringsperiode eller muligheden for at aktivere "litigation hold", ville det sandsynligvis være lykkedes at genskabe alle de slettede mails. At dette ikke var tilfældet skyldes, at der er blevet stillet for få kritiske spørgsmål i processen.

I praksis blev hændelsen vurderet som kritisk på det næsthøjeste niveau men ikke som en "major incident" på højeste niveau af kritikalitet. Det er KPMG's vurdering, at denne klassificering af hændelsen muligvis ikke var forkert, idet konsekvenserne som beskrevet kunne have været

mitigeret. Imidlertid er det også KPMG's vurdering, at en mekanisme eller proces, som sikrede en mere systematisk vurdering af forudsætningerne for, hvorfor hændelsen skulle klassificeres på næsthøjeste og ikke højeste niveau, ville have kunnet bidrage til at både den reelle reetableringsperiode og muligheden for at aktivere "litigation hold" blev identificeret.

Da en hændelse på næsthøjeste niveau i sig selv er kritisk, og da et fravalg af klassificering på højeste niveau har væsentlig betydning, finder KPMG, at det kunne have været ønskeligt at forudsætningerne for klassificeringen i højere grad var blevet trykprøvet. Dette kunne have været gjort ved at prioritere tid til, at en gruppe af udvalgte ledere, teknikere og medarbejdere fra IOS, KOS og CIA såvel som fra de faglige dele af de berørte institutioner, sammen gennemgik disse forudsætninger og fik stillet de rigtige, kritiske spørgsmål.

Anbefaling #9. Efterprøvning af klassificeringer af hændelser på næsthøjeste niveau

Det anbefales, at SDS etablerer en standardmekanisme eller -proces, hvorved alle kritiske informationssikkerhedshændelser, som klassificeres til næsthøjeste niveau, indebærer at en gruppe af relevante ledere, medarbejdere og teknikere i samarbejde efterprøver forudsætningerne for, hvorfor klassificeringen ikke skal være som "major incident" på højeste niveau.

KPMG har i forbindelse med undersøgelsen endvidere fået oplyst, at SDS har udpeget en incident manager, men at der i dag ikke findes en rolle som problem manager. Forskellen mellem disse to roller er ifølge ITIL, at incident manageren har til opgave at minimere negative hændelsers konsekvenser ved at genoprette normal drift hurtigst muligt, mens en problem manager i højere grad vil have til opgave at stille kritiske spørgsmål – både til håndteringen af den konkrete hændelse men også i forhold til den mere langsigtede udbedring af fejl. En problem manager med en vis teknisk indsigt ville derfor ved håndteringen af de slettede mails have haft som eksplicit opgave at trykprøve de forudsætninger, som lå til grund for hændelseshåndteringen. Dermed ville en problem manager, som udfyldte sin rolle korrekt, også have sikret, at eksempelvis antagelsen om reetableringsperioden var blevet be- eller afkræftet.

Anbefaling #10. Indførelse af en problem manager rolle

Det anbefales, at SDS overvejer at indføre en problem manager rolle, som vil have til opgave at sikre, at de rette, kritiske spørgsmål stilles i forbindelse med informationssikkerheds-hændelser samt at sikre en langsigtet udbedring af eventuelle fejl.

4.2.6. Evaluering, læring og opfølgning

Et afgørende element i styrkelse af en organisations it- og informationssikkerheds-governance er, at informationssikkerhedsmæssige fejl og hændelser anvendes aktivt gennem evaluering og implementering af forbedringer. KPMG har fået oplyst, at SDS i dag ved større hændelser udarbejder root cause analyser for at sikre, at hændelserne evalueres. Imidlertid er det KPMG's forståelse, at der mangler en klar proces for, hvordan resultaterne af disse analyser omsættes til konkrete forbedringer, samt hvordan de formidles i organisationen, således at forbedringer implementeres i den daglige drift. Dette er blevet bekræftet i flere af de gennemførte interview.

Som beskrevet ovenfor giver SDS' mailløsning kun adgang til logfiler for de seneste 90 dage, og SDS gemmer ikke kopier af ældre logfiler. Dette betyder, at væsentlige informationer til at undgå og håndtere gentagne fejl ikke kan anvendes til fremadrettet læring og forbedringer.

Anbefaling #11. Styrkelse af læring og implementering af forbedringer på baggrund af hændelser
Det anbefales, at SDS foretager et review af, hvordan læring fra tidligere informationssikkerhedsmæssige hændelser opsamles og anvendes til at implementere forbedringer i den daglige drift. På baggrund af reviewet bør der udarbejdes handlingsplan for at sikre implementering af relevante resultater, herunder at SDS har en proces, der sikrer, at erfaringer bruges til kontinuerlige forbedringer.

4.2.7. ISO 27001

Siden 2016 har alle statslige myndigheder været underlagt krav om at implementere og efterleve informationssikkerhedsstandarden ISO 27001. Således skal myndighederne følge principperne i standarden og foretage en vurdering af behovet for certificering. I henhold til *National strategi for cyber- og informationssikkerhed 2018-2021* skal de myndigheder, der ikke er i mål med implementeringen, "forelægge en handleplan for regeringen med henblik på at sikre fuld implementering af standarden". Kravet indbefatter som sådan ikke, at myndighederne skal dokumentere efterlevelse gennem eksempelvis certificering foretaget af en ekstern part. I stedet skal myndighederne egen-vurdere deres modenhed, hvilket gøres ved besvarelse af et spørgeskema, som dækker de væsentligste områder af ISO-standarden.

Sundhedsområdet berører alle danskere, og sundhedsvæsenet er en hjørnesten i den danske velfærdsstat. I den nationale strategi for cyber- og informationssikkerhed er sundhedssektoren udpeget som én af seks samfundskritiske sektorer, for hvilke der skal udarbejdes specifikke strategier for cyber- og informationssikkerhed.

Der er således et stort og kontinuerligt behov for at opretholde den højeste grad af offentlig tillid til kvaliteten i den daglige IT-drift. En sådan tillid skal baseres på et højt fagligt niveau samt god og transparent dokumentation for dette. På trods af at sundhedsdata og de systemer, der benyttes til databehandling i og forretningsunderstøttelse af sundhedssektoren, således må

betragtes som særdeles informationssikkerhedsmæssigt følsomme, er SDS i dag ikke ISO 27001-certificeret. SDS får årligt udarbejdet en ISAE 3000 revisorerklæring, men som det er forelagt for KPMG, fokuserer denne udelukkende på overholdelse af GDPR og ikke på den bredere håndtering af informationssikkerhed.

En fuld implementering af ISO 27001 og efterfølgende certificering vil først og fremmest kræve, at SDS fagligt er i stand til at efterleve de relevante elementer i standarden og samtidig give SDS' ledelse nogle klare styringsparametre i denne sammenhæng. Certificeringen ville dokumentere efterlevelse af de internationale standarder og bevirke en løbende ekstern validering af, at standarderne overholdes. Dermed ville SUM's koncern generelt have en højere grad af sikkerhed for, at ledelsessystemet fungerer efter hensigten, og at sikkerhedsmæssige fejl og hændelser begrænses. Samtidig ville certificeringen udgøre en væsentlig dokumentation og et bidrag i forhold til den eksterne kommunikation om hvilke standarder, der efterleves i arbejdet med informationssikkerheden. Endelig ville en fuld ISO 27001-implementering og -certificering understøtte en række af de øvrige anbefalinger ovenfor.

Anbefaling #12. ISO 27001-implementering og certificering

Det anbefales, at SDS overvejer at prioritere en fuld implementering og efterfølgende certificering af ISO 27001. Med henblik herpå bør der i givet fald udarbejdes en operationel handlingsplan for, hvordan SDS opnår dette.

4.2.8. Konsolidering af systemportefølje og IT-organisering

Da SDS blev etableret 1. november 2015 var et af styrelsens hovedformål at fungere som koncern-IT på vegne af SUM's koncern. SDS overtog derved ansvaret for at drifte og supportere de forskellige administrative systemer på tværs af de daværende institutioner på ministerområdet, og for de institutioner der er kommet til siden.

Institutionerne på ministerområdet anvender i dag en række forskellige administrative IT-løsninger. Det betyder, at SDS – og i særdeleshed IOS – i dag varetager administrationen af et meget komplekst systemlandskab. Flere af de interviewede medarbejdere har adresseret denne kompleksitet, og at "der er tale om sammenbragte børn, hvilket indebærer et kludetæppe af systemer, hvor gamle løsninger ikke lukkes". Eksempelvis drifter IOS fem forskellige løsninger til fildeling og tre forskellige telefoniløsninger, *jf. figur 2*.

Figur 2. Administrative systemer og supportmodel for SUM's institutioner

	DKSUND domænet	Exchange Online	Exchange On-Prem	Exchange Hybrid	Lync	Teams	Skype for Business	DPG sikkermail	Fusemail Sikkermail	Bluewhale	Strålefors	Lasernet	sFTP	Sharefile
SDS	X	X			X	X		X					X	X
SSI	X	X			X	X		X					X	
SST	X		X			(X)			X			X		
DEPT			X			(X)			X					
STPK	X			X		(X)	X		X	X	X	X		
STPS	X		X				X		X	X				
NGC			X			X			X					
DKEtik	X	X			X				X					
E-boks integration	(X)	(X)	(X)					X	X	X	X	X		

Styrelser migreret til centralt domæne | Hvilket Exchange-setup mails er knyttet til | Den anvendte telefoniløsning | Hvilken type sikkermail er knyttet til insitutionen | Teknologier til fildeling med andre institutioner

Systemkomplekset betyder, at hver af koncernens institutioner har sin egen supportmodel baseret på de anvendte systemer. Det betyder, at IOS' medarbejderressourcer fordeles meget tyndt på løsningerne, og at der kan være udfordringer med at sikre tilstrækkelig indsigt i de enkelte systemer og de tilhørende politikker/retningslinjer. Samtidig giver det udfordringer i forhold til en optimal udnyttelse af medarbejderressourcerne, hvor det i interviews er blevet tilkendegivet, at nogle gange sættes eksperter til at løse simple opgaver, mens generalister andre gange sættes til at løse komplekse sager. Det komplekse systemlandskab betyder, at IOS har vanskeligt ved at levere en specialiseret support. Specifikt i relation til administrationen af Exchange-løsningen i Microsoft 365, har KPMG i forbindelse med interviews fået oplyst, at SDS desuden har haft vanskeligt ved at rekruttere specialiserede medarbejderressourcer, så i perioder har administrationen af Exchange været varetaget af eksterne konsulenter. En konsolidering af systemporteføljen ville lette SDS' ressourcebelastning og muliggøre en mere professionel og dedikeret administration og support af de enkelte systemer.

Anbefaling #13. Konsolidering af systemporteføljen

Det anbefales, at SUM overvejer mulighederne for at konsolidere systemerne på kontorplatformen, således at den enkelte supportmedarbejder i højere grad kan specialisere sig i få løsninger.

En beslægtet problemstilling er, at institutionerne i koncernen også har deres egne it-afdelinger, som tager sig af en del af den daglige drift og hver har samarbejde med forskellige eksterne IT-leverandører. Der vil naturligvis altid være behov for decentrale IT-kompetencer, hvor den enkelte institution har særlige lokale systemmæssige behov, men dette indebærer også en risiko for, at der opstår selvstændige initiativer lokalt, som kan være i modstrid med den sammenhængende drift af systemunderstøttelsen på tværs af koncernen. KPMG vurderer derfor, at det i forbindelse

med en konsolidering af systemporteføljen vil være naturligt også at overveje, om snittet mellem SDS i rollen som koncern-IT og de decentrale IT-enheder i de enkelte institutioner er hensigtsmæssig.

Anbefaling #14. Konsolidering af IT-organiseringen

Det anbefales, at SUM overvejer at gennemføre et review af organiseringen af IT-kompetencer på tværs af koncernen, så det sikres, at opgaverne varetages mest hensigtsmæssigt.

4.2.9. Analyse af ressourcer og kompetencer

En række af de ovennævnte anbefalinger vil forudsætte en vis ressourceindsats. Samtidig har det på flere af de gennemførte interview været fremført, at den daglige IT-drift i SDS generelt er udfordret af en ubalance mellem opgaver, krav og behov på den ene side og de tilgængelige ressourcer på den anden side.

Det har ikke været en del af KPMG's opdrag at vurdere balancen mellem opgaver og ressourcer i SDS, hvorfor KPMG ikke på baggrund af nærværende undersøgelse kan udtale sig om et eventuelt behov for ressourcetilførsel. Det er dog KPMG's vurdering, at systemunderstøttelsen, IT-driften og informationssikkerheden i sundhedsvæsenet er af samfundskritisk betydning – som det også understreges i den nationale strategi for cyber- og informationssikkerhed – og at det derfor er afgørende at sikre, at der afsættes de tilstrækkelige ressourcer hertil.

Anbefaling #15. Analyse af fremadrettet ressourcebehov i koncern-IT

Det anbefales, at SUM gennemfører en grundig analyse af det fremadrettede ressource- og kompetencebehov på ministerområdet generelt og i SDS i særdeleshed med henblik på at sikre, at kvaliteten af den daglige IT-drift og informationssikkerhed afspejler sundhedsvæsenets samfundskritiske betydning.

Bilag 1 – Teknisk ændrings-proces ved anvendelse af grafisk brugergrænseflade

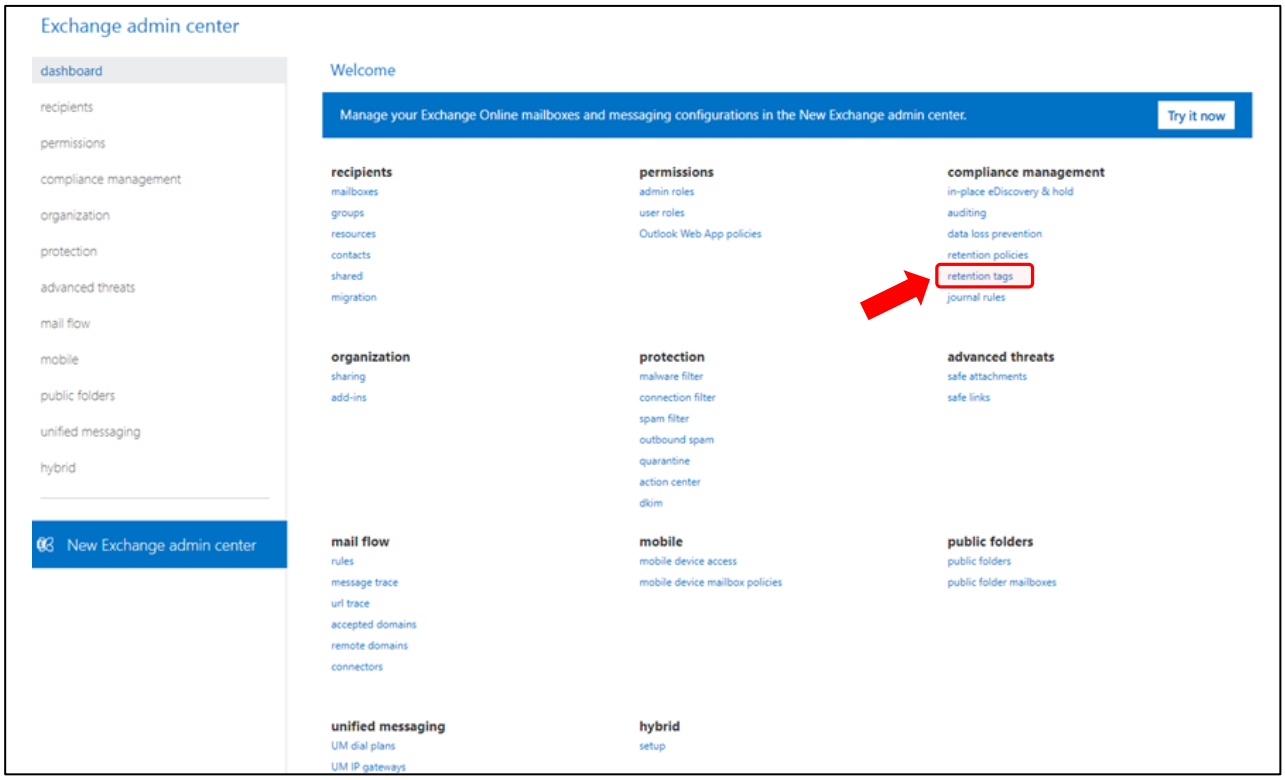
I forbindelse med undersøgelsen har KPMG med teknikerbistand fra Microsoft og den SDS-medarbejder, der foretog ændringerne i retention policy'en, gennemgået hvilke trin, der fra start til slut kræves for at ændre retention policy'en, således at emails i "sendt post"-mappen slettes efter 30 dage.

Der er nedenfor redegjort for trinnene i denne proces, og de enkelte trin er visualiseret i form af skærmbilleder. Det bemærkes, at skærmbillederne stammer fra et Exchange-demomiljø, idet der ville være risici forbundet med at demonstrere processen i produktionsmiljøet. KPMG har dog haft lejlighed til at se produktionsmiljøet og ved selvsyn konstatere, at det funktionelt er identisk med demomiljøet.

Det bemærkes, at der ikke er tale om en rekonstruktion af medarbejderens handlinger foretaget d. 21. august 2020. Medarbejderen giver udtryk for, at vedkommende den pågældende dag foretog en løs sondering og at de enkelte trin, der blev foretaget bl.a. derfor ikke står klart i hukommelsen.

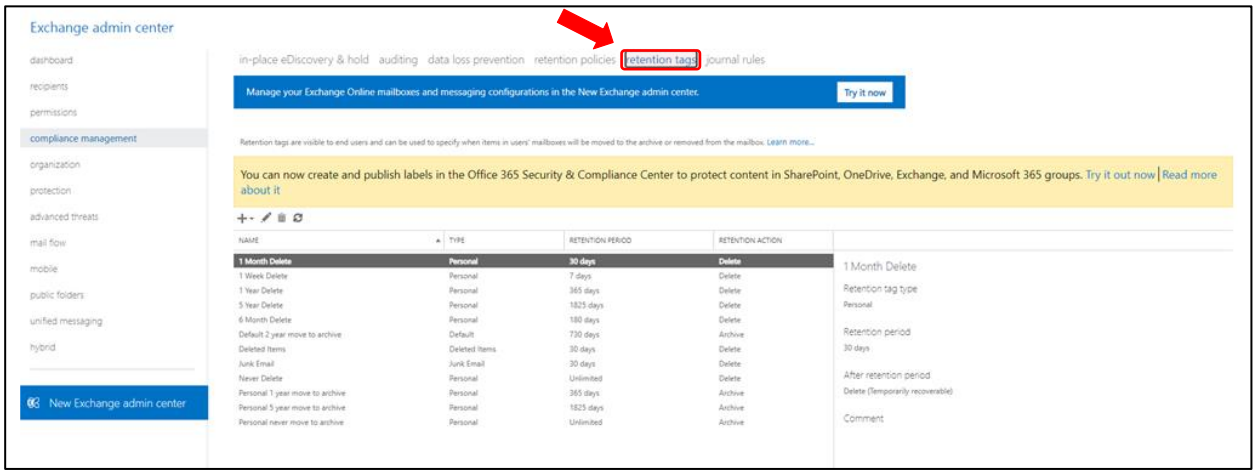
Trin 1

I trin 1 logger administratoren ind i Microsoft Exchange. Skærmbilledet viser hovedmenuen "Exchange admin center". Under menuen "compliance management" klikkes på menuemnet "retention tags".



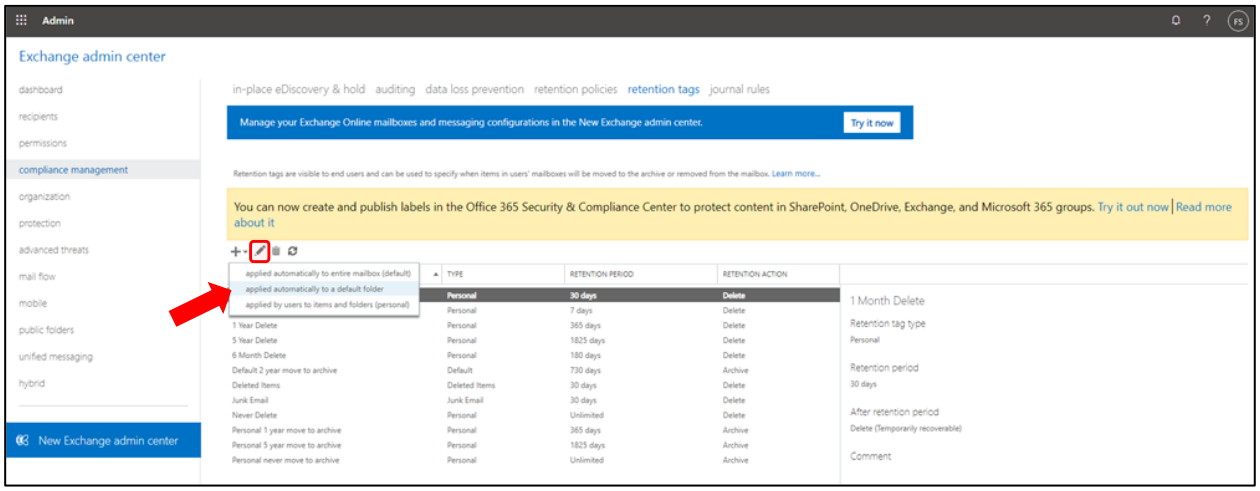
Trin 2

I trin 2 står administrator på siden "retention tags". Der ses en oversigt med en række forskellige retention tags, der hver især definerer en sletteregel.



Trin 3

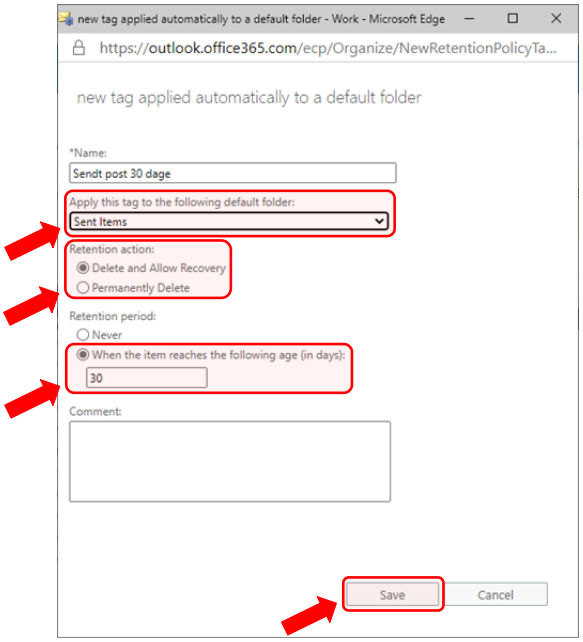
I trin tre markeres retention tag'et "1 Month Delete". Fra symbolmenuen over listen over retention tags vælges redigeringssymbolet (blyanten), og i menuen der fremkommer vælges muligheden "applied automatically to a default folder".

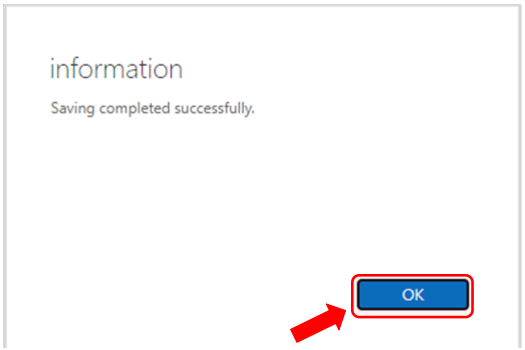


Trin 4

I trin 4 er administratoren blevet præsenteret for et pop-up-vindue, hvori retention tag'et kan redigeres, hvormed den sletteregel, som tag'et definerer, kan ændres.

I vinduet vælges først den mappe, som tag'et skal tilknyttes. Dette gøres ved at vælge en mappe fra rullemenuen under overskriften "Apply this tag to the following default folder". I det pågældende tilfælde vælges fra rullemenuen mappen "sent items".





Under punktet "Retention action" specificeres hvordan emails omfattet af retention tag'et skal håndteres. Der er mulighed for at vælge enten "Delete and Allow Recovery" – altså at emails

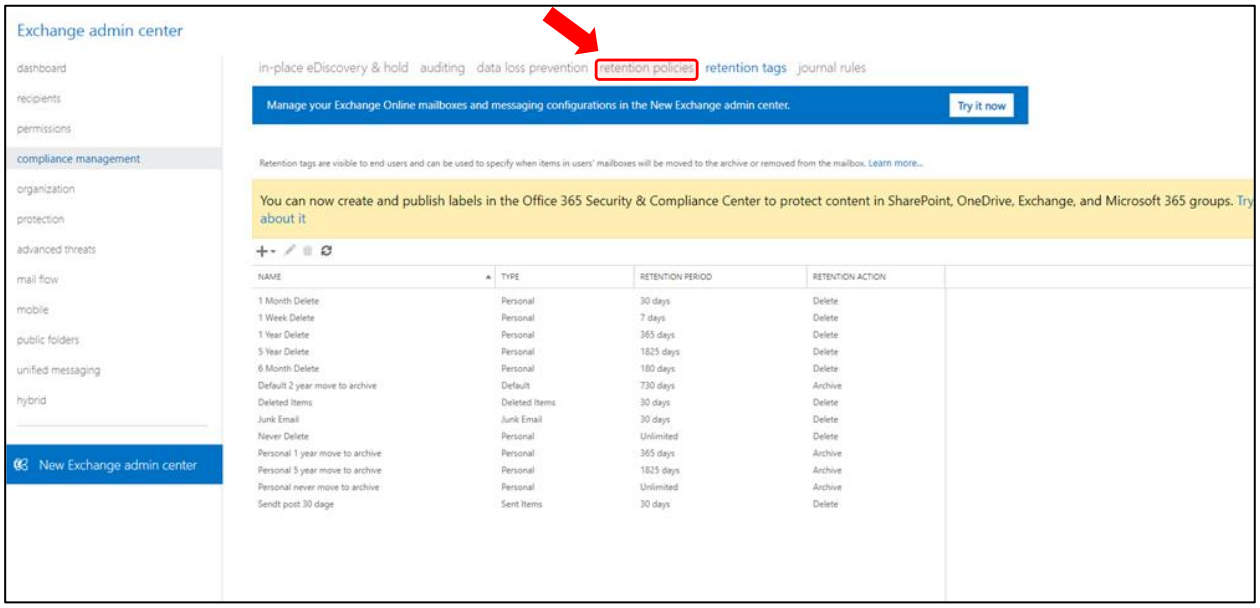
skal kunne genskabes efter sletning - eller "Permanently Delete" – altså at emails slettes permanent. I dette tilfælde vælges første mulighed.

Efterfølgende under punktet "Retention period" specificeres hvornår emails skal omfattes af den "retention action", der blev defineret i forrige punkt. Her kan vælges mellem "Never" – altså at emails aldrig skal omfattes og dermed aldrig slettes - og "When the item reaches the following age (in days)", hvor der kan angives et valgfrit antal dage, hvorefter den valgte retention action effektueres. I den konkrete situation vælges anden mulighed, hvor det specificeres at emails skal slettes, når de bliver 30 dage gamle.

Herefter klikkes "save", og administratoren bliver præsenteret for en bekræftelsesbesked, hvoraf det fremgår, at informationen tilføjet retention tag'et er gemt. Der klikkes "OK" i bekræftelsesbeskeden.

Trin 5

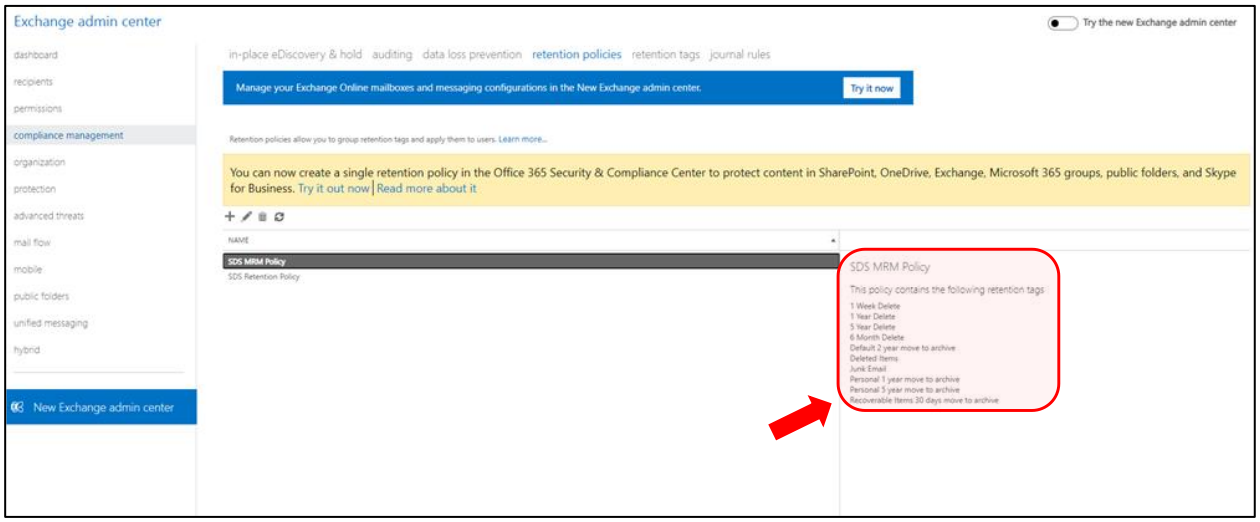
I trin 5 vælges muligheden "retention policies" fra menuen over den blå bjælke.



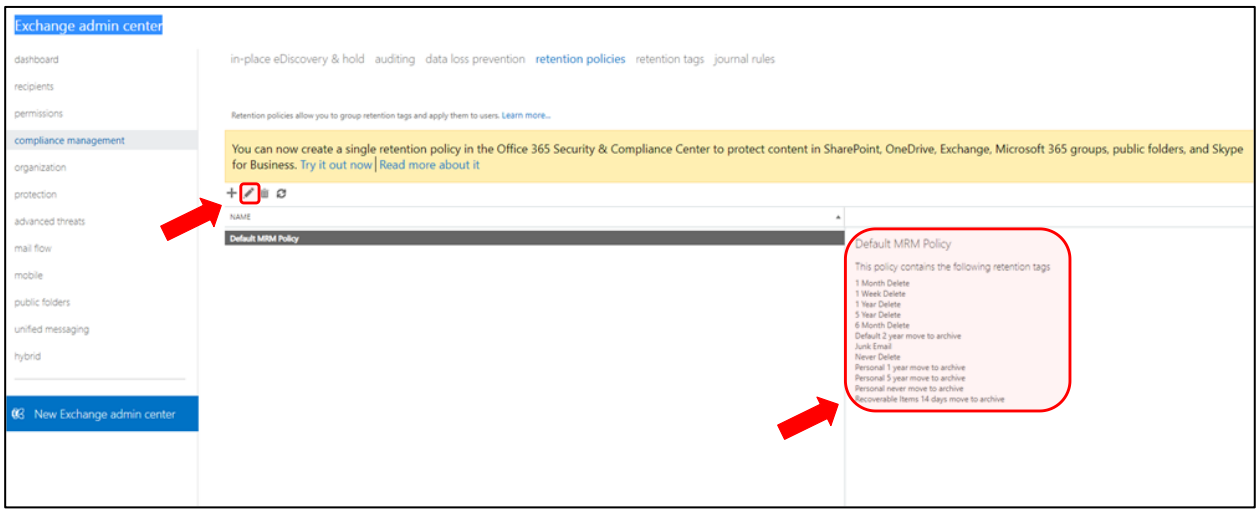
Trin 6

I trin 6 står administrator på den side, hvor organisationens retention policies ses. Skærmbilledet er fra SUM's produktionsmiljø og viser de tags, der er knyttet til SUM-politikken "SDS MRM Policy", som er den globale slettepolitik for SDS, SSI og KHR.

Det bemærkes, at der, som det ses af skærmbilledet, eksisterer endnu en retention policy ved navn "SDS Retention Policy". SDS oplyser, at denne politik ikke anvendes til emailkonti.

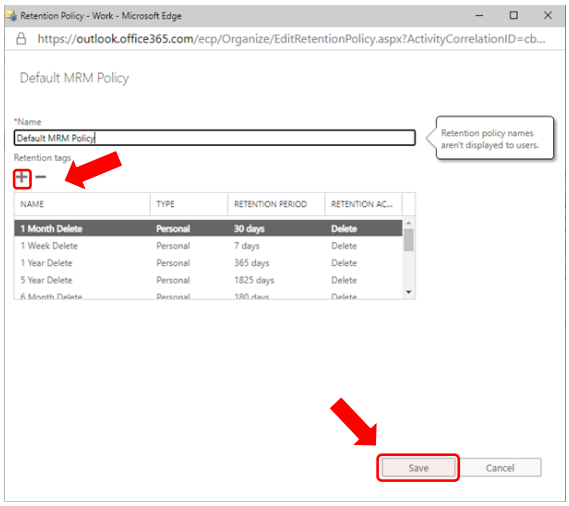


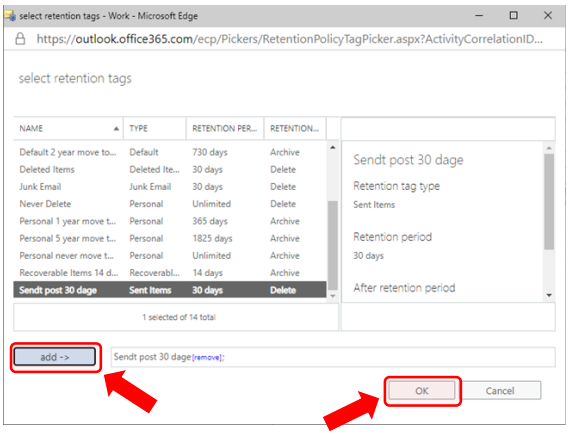
I nedenstående skærmbillede vises en oversigt over de retention tags, der er tilføjet retention policy'en for testmiljøet. For at tilføje et retention tag til retention policy'en skal sidstnævnte redigeres. For at gøre dette klikkes på redigeringssymbolet (blyanten).



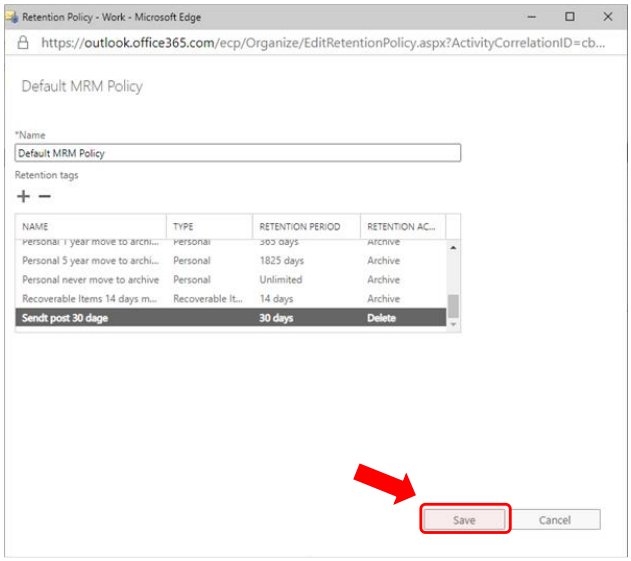
Trin 7

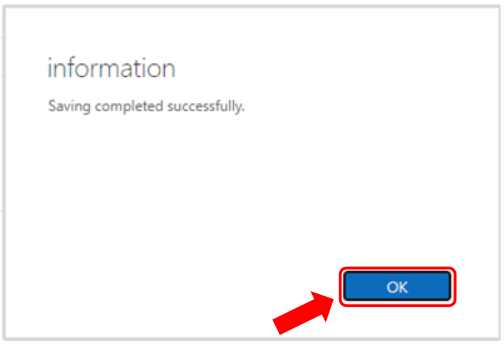
I trin 7 redigerer administrator retention policy'en. På skærmbilledet til venstre ses en rullemenu med de retention tags, der er knyttet til den aktuelle retention policy. Der klikkes på "+", og administrator præsenteres nu for muligheden for at tilknytte nye tags til policyen. Det netop oprettede tag "Sendt post 30 dage" markeres, og der klikkes på knappen "add ->".



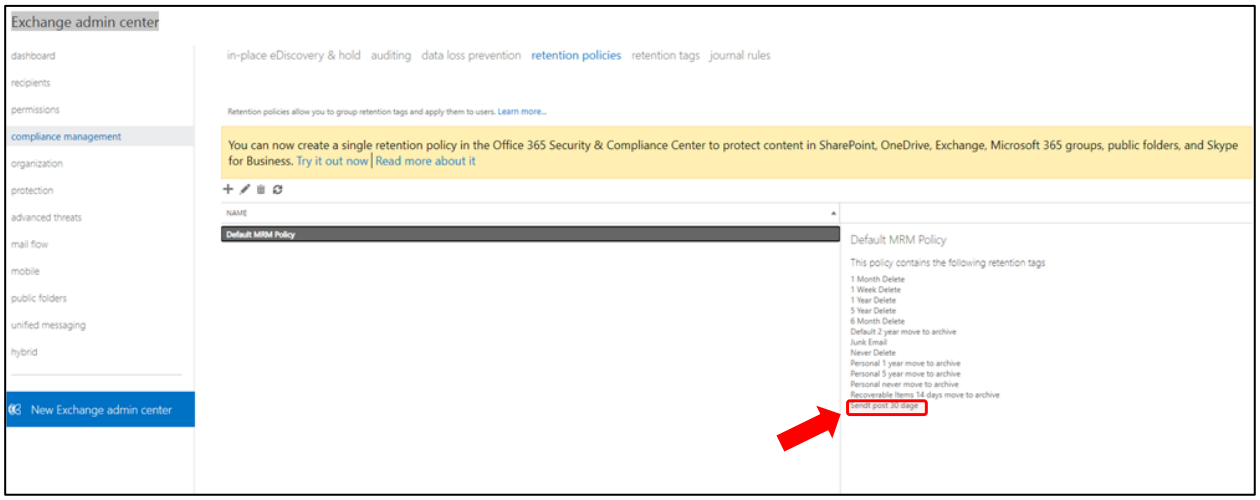


Det nye tag ligger nu parat i listen over retention tags. Før tag'et knyttes til retention policyen skal administratoren dog først gemme ved at klikke på knappen "save". Herefter modtages en notifikation "saving completed successfully" fremgår – altså bekræftes at tag'et er gemt som en del af policy'en.





Sidstnævnte ses også ved, at tag'et nu er tilføjet til listen over tag's, der er en del af retention policy'en. I modsætning til tidligere viste skærmbilleder, inkluderer nedenstående skærmbillede tag'et "Sendt post 30 dage".



KPMG P/S
Dampfærgevej 28
2100 København Ø
www.kpmg.dk