Indhold

Om kataloget

Kataloget beskriver tekniske og organisatoriske foranstaltninger, som er relevante at overveje i overensstemmelse med kravene i databeskyttelsesforordningens artikel 32 og dermed også for efterlevelse af flere af principperne i artikel 5.

Kommentar [F1]: Vi vil foreslå, at alene de foranstaltninger, som er relevante ift. rettighedsstyring medtages i vejledningen.

Hver foranstaltning kan læses individuelt. Eventuelle afhængigheder til andre foranstaltninger i kataloget er som regel angivet. Det skal dog bemærkes, at kataloget på ingen måde angiver alle foranstaltninger, som kan være relevante for at etablere et passende sikkerhedsniveau i behandlingen af personoplysninger. Kataloget dækker primært foranstaltninger som er relevante ift. emner behandlet i vejledninger udgivet af Datatilsynet. (fx "Rettighedsstyring" og "De ti brud"). Det er forventningen at kataloget jævnligt vil blive udvidet med nye foranstaltninger.

For hver foranstaltning angives risici, som foranstaltningen er rettet imod, samt implementeringsforslag. Endvidere er der en vejledning til vurdering af foranstaltningens relevans.

Foranstaltningerne i kataloget er i høj grad baseret på erfaringer fra tilsyn i private og offentlige virksomheder, it-sikkerhedskonsulenternes personlige erfaringer, brud på persondatasikkerheden anmeldt til Datatilsynet, EDBP's retningslinjer, samt ISO-standarderne 27001[1] og 27002. ISO-standarderne er internationale standarder for informationssikkerhed, som følges af de fleste offentlige myndigheder og mange private virksomheder, og er udtryk for et internationalt anerkendt niveau for sikkerheden ved anvendelse af informationsteknologi.

Foranstaltninger

Adgang koblet til viden

Dette er en forebyggende foranstaltning, som kan mindske sandsynligheden for fejlhåndtering af data, hvilket uforvarende resulterer i et sikkerhedsbrud.

Mange sikkerhedsbrud sker hos brugere, der anvender IT (informationsteknologi) til dagligt, hvorfor de føler, at de forstår teknologien, men begår alligevel fejl. Det skyldes i nogle tilfælde, at brugeres fokus ikke er på sikkerhed eller fordi sikker behandling af data kræver særlig forståelse for IT – en anden forståelse end den, der kræves for at udføre brugerens arbejdsopgaver. I nogle tilfælde skyldes sikkerhedsbrud direkte en manglende forståelse for forskellen mellem den fysiske verden og den elektroniske, fx at brugeren tror, at hvis data ikke umiddelbart er synlige (på skærmen), så er de der ikke.

Forslag til implementering

Ved godkendelse af adgange medfølger den nødvendige viden til brugeren om, hvordan sikkerhedsbrud undgås. Det handler om at undgå at give brugere et råderum (via adgangsrettigheder), som ligger uden for deres kompetencer og fokusområde/fagområde.

Følgende er ikke-udtømmende eksempler på, hvor viden kan tænkes sammen med brugeradgang.

- Adgang til at kunne offentliggøre data på et websted, gives kun til personer for hvem denne opgave er et hovedarbejdsområde, og kun efter brugeren har fået undervisning i, hvordan man finder/frasorterer personoplysninger gemt i fx metadata eller data bag en graf i regneark/præsentation.
- ~~Opgaver ang. offentliggørelse af anonymiserede data, lægges kun hos medarbejdere, som har fået værktøjer og viden, der gør dem i stand til fjerne data (ikke kun skjule dem), og som gør dem i stand til forstå, hvornår data er anonymiserede (når personoplysninger ikke længere med nogen midler kan knyttes til en fysisk person).~~

Kommentar [F2]: Adgang koblet til viden
Intentionen med denne er egentlig fin, men mere koblet til lederens instruktionsbeføjelse, end til egentlig adgangsstyring. Overvej om foranstaltningen kan udelades.

Kommentar [F3]: Da anonymiserede data ikke er personoplysninger, vil vi foreslå, at denne dot udgår. Alternativt at det tydeliggøres, at foranstaltningen ikke alene adresserer databeskyttelsesforordningens artikel 32.

[1] Dansk Standard DS/ISO/IEC 27001 – Krav til Informationsteknologi – sikkerhedsteknikker – Ledelsessystemer for informationssikkerhed (ISMS)

- Adgang til at kunne sende data med særligt beskyttelsesværdige personoplysninger ud af organisationen, gives kun til medarbejder, som er oplært i krypteringskrav, og har værktøjer, hvormed de nemt kan fortage forsendelsen sikkert.
- Adgangen til at anvende it-systemer til journalisering af dokumenter/breve, hvor der samtidig sker en automatisk offentliggørelse, gives kun til få personer, for hvem denne opgave er deres hovedarbejdsområde.
- Særlige adgangsrettigheder, fx muligheden for at slette data, som udgør en højere risiko eller er forbundet med særlige lovkrav, gives kun efter undervisning i disse risici/lovkrav, og adgangen gives kun til få personer, for hvem denne opgave er deres hovedarbejdsområde.

Grundlag for vurdering af nødvendighed

Det er primært en risikovurdering efter artikel 32, som skal vise, om denne foranstaltning er relevant, idet risici er meget afhængige af, om der i den konkrete organisation er funktioner/opgaver, hvor manglende viden kan udgøre en risiko.

Se foranstaltningen *Awareness* for at udvælge relevante informationer, der skal gives på ansættelsestidspunktet eller ved ændring af adgangsrettigheder.

Adgangsrettigheder efter behov

Dette er en forebyggende foranstaltning, som kan mindske konsekvensen ved utilsigtet eller ondsindet misbrug. En læseadgang giver fx mulighed for misbrug ift. datas fortrolighed, mens en trussel mod datas integritet kræver muligheden for at tilføje, ændre eller slette data. En bruger kan også uforvarende foretage handlinger, som brugeren ikke ville kunne, hvis adgangsrettighederne havde være mere begrænset.

Forslag til implementering

Adgangsrettigheder gives efter arbejdsbetinget behov, og begrænses i fx muligheden for at læse, tilføje, søge, ændre, udtrække eller slette data.

Hvis der anvendes RPA (Robotic Process Automation) eller lignende, og man i den forbindelse giver adgangsrettigheder til robot-brugere, skal man på samme måde begrænse deres adgang mest muligt. Økonomisk besparelse på robot-brugerlicenser kan friste til at give en robot så mange adgangsrettigheder som muligt. Men en robot, som har mange adgangsrettigheder, kan udgøre en højere risiko, hvis fx en hacker får mulighed for at opnå denne robots rettigheder.

Mulighederne for at begrænse adgangsrettigheder afhænger normalt af it-systemernes design, hvorfor disse aspekter skal være tænkt ind på tidspunktet for design eller indkøb af it-systemer.

Visse adgangsrettigheder kan være koblet til lovkrav, fx lov om offentlig forvaltning eller regnskabsloven, som specificerer, hvornår visse data må slettes. Denne foranstaltning hænger således sammen med foranstaltningen *Adgang koblet til viden*.

Grundlag for vurdering af nødvendighed

Artikel 5, stk. 1, litra f, handler om personoplysningers integritet og fortrolighed. Jo mindre den enkelte bruger kan gøre med de data, som brugeren har adgang til, desto mindre er den potentielle konsekvens, hvis nogle af disse brugere gør skade på data via utilsigtede eller ondsindede handlinger. Samtidig har dette også en beskyttende effekt ift. cybertrusler, idet hackere ofte opererer igennem adgangsrettigheder i kompromitterede bruger-konti, og færre rettigheder giver dermed hackerne færre muligheder. Man skal derfor begrænse adgangsrettigheder mest muligt.

Kommentar [F4]: Vi vil foreslå, at der i stedet står "Adgang til nødvendige it-systemer", så formuleringen bringes i overensstemmelse med art. 5, stk. 1, litra c.

Kommentar [F5]: En robot-bruger bør have et minimum af rettigheder for at sikre, at hvis der er fejl i koden/automatikken, så begrænses skaden ved et meget restriktivt rettighedssæt.

Artikel 25. Ved erhvervelse af nyt it-system eller udvikling/ændring i eksisterende it-system skal databeskyttelse være tænkt ind i design og standardindstillinger. En indbygget mulighed for at differentiere på adgangsrettigheder giver større mulighed for databeskyttelse ifm. brugeradministrering.

Awareness

Dette kan være både en forebyggende og opdagende foranstaltning. Når brugere ved, hvordan de skal spotte en phishing-mail der søger at få brugene til at afsløre login-oplysninger, er det en forebyggende foranstaltning. Når brugerne ved, at deres handlinger i it-systemer logges, kan det mindske sandsynligheden for bevidst misbrug af personoplysninger, hvilket indebærer en forebyggende foranstaltning. Hvis brugerne ved, hvad de skal gøre, for hurtigt at få spærret et tabt et adgangskort, kan det betegnes som en opdagende foranstaltning, som gør det muligt potentielt at standse en hændelse, inden den får en indvirkning på organisationens behandling af personoplysninger.

Følgende er en liste over foranstaltninger, hvorfra der kan plukkes, alt efter hvad der er relevant. fx skal en ny medarbejder typisk have flere informationer end en medarbejder, der blot skifter opgaver eller afdeling.

Hvis muligt bør punkterne implementeres teknisk, så brugerne ikke kan undgå at gøre det rigtige. For mange foranstaltninger implementeret via regler, som medarbejdere skal efterleve, øger byrden for brugerne, og det øger risikoen for uforvarende fejl.

- Alle oplyses om, hvor brugeres handlinger logges, formål med logningen, samt mulige sanktioner ved opdaget misbrug af adgangsrettigheder. Det kan omfatte logning i it-systemer, hvori der behandles personoplysninger, men kan også være logning af fysisk adgang til lokaler, tv-overvågning, mv.
- Brugere, autorisationsansvarlige og brugeradministratorer (se forklaring af titler i vejledning om rettighedsstyring) oplyses om, hvad de må med deres respektive adgangsrettigheder, fx:
    - at brugere ikke må anvende data til andet end arbejdsrelevante formål,
    - autorisationsansvarlige skal have fokus på begrænset adgang (ikke kun på brugernes mulighed for opgaveløsning), og
    - brugeradministratorer må ikke handle på egen hånd, og skal dokumentere alle autorisationer udsted af de autorisationsansvarlige.
- Vejledning til valg af adgangskoder, herunder at brugerne ikke må anvende koder, som også anvendes i privat regi, fordi disse kan være kompromitterede.
- Information om, at adgangskoder, tokens, adgangskort og andre adgangsgivende faktorer er strengt fortrolige og personlige og, at brugeren står til ansvar for alle handlinger udført under deres login – evt. med henvisning til logning og sanktioner. Instruktion i reaktion ved mistanke om, at uvedkommende har fået adgang/kendskab til adgangsgivende faktorer.
- Såfremt fysisk adgang er med til at begrænse/styre adgangen til personoplysninger, gives instruktion i reaktion ved mistanke om, at uvedkommende har fået adgang adgangsmedier, som nøgle, nøglebrik, adgangskort, mv. Dette kan være relevant, selv om der kun er elektronisk adgang til personoplysninger, fordi:
    - Den fysiske adgang kan være til it-udstyr, der indeholder personoplysninger, og dermed er det en del af rettighedsstyring til personoplysninger.
    - Elektronisk adgang kan være på forskellige sikkerhedsniveauer afhængigt af, hvor man befinder sig fysisk – fx indenfor eller udenfor en kontorbygning.
- Specifikt viden om, hvordan personoplysninger må anvendes ved test i forbindelse med udvikling af it-systemer.

Kommentar [F6]: Dette afsnit omfatter meget andet end rettighedsstyring og foreslås slettet.

- Informering om lovgivning der angår tavshedspligt og evt. krav om underskrevet tavshedserklæring, der angiver, at den også gælder efter ansættelsens/konsulentopgavens ophør. Bemærk, at dette er en foranstaltning, som skal gøre brugere mere opmærksomme på ansvar og regler, men som ikke kan forventes at forhindre hændelige fejl eller bevidst ondsindede handlinger.
- ~~Evt. krav om pletfri straffeattest eller sikkerhedsgodkendelse. Dette er ikke reelt en awareness-aktivitet, men det øger medarbejderes opmærksomhed på vigtigheden af korrekt adfærd.~~
- Generel viden om, hvordan personoplysninger må og skal behandles iht. databeskyttelsesforordningen og anden relevant lovgivning – kan angå opbevaring, anvendelse, videregivelse, sletning, transmission over usikre netværk, og andre behandlinger.
- Målrettet vejledning i anvendelsen af specifikke it-systemer, fx ang. journalisering, offentliggørelse, journalisering med automatiseret offentliggørelse, anonymisering, fjernelse af skjulte metadata, krav fra lovgivning, ... evt. kombineret med værktøjer, der gør dette nemmere at udføre handlingerne uden at begå fejl.
- Målrettet vejledning af brugeradministrator eller it-sikkerhedsansvarlig i at spotte forsøg på internet misbrug – fx kursus i at "spotte en insider".
- Målrettet vejledning af medarbejdere med adgang til organisationens bankkonti og økonomisystemer angående "CEO fraud". ~~Dette bør være kombineret med strikse procedurer for godkendelse af udbetalinger og valutaoverførsler.~~

Kommentar [F7]: Vi vil foreslå, at denne foranstaltning udgår, da den ikke har med awareness at gøre.

Kommentar [F8]: Vi vil foreslå, at denne foranstaltning udgår, da den ikke har med awareness at gøre.

Automatisk lukning af inaktive adgange

Dette er en forebyggende foranstaltning, som kan mindske sandsynligheden for misbrug af unødvendige adgange. Automatisk lukning af adgange kan baseres på brugers inaktivitet – altså at brugeren fx ikke har anvendt en it-systemadgang eller fysisk adgang i 40 dage.

Forslag til implementering

Hvis funktionen er indbygget, i de systemer der anvendes, kan den tilvælges. alternativt kan det gøres manuelt, men det vil næppe være rentabelt i en større organisation.

Kommentar [F9]: Bør komme fra centralt brugerstyringssystem, ikke i de enkelte fagsystemer. HR-systemet skal være autoritativt i forhold til, hvilke medarbejdere der er i organisationen, samt for deres fratrædelse.

Grundlag for vurdering af nødvendighed

Denne foranstaltning eliminerer ikke behovet for andre foranstaltninger, der angår lukning af unødvendige adgange, fordi en bruger kan vælge bevist at anvende en adgang med jævne mellemrum for at omgå den automatiske lukning.

Det er en risikovurdering efter artikel 32, som skal vise, om denne foranstaltning er relevant, idet den ikke i sig selv sikrer imod *bevidst* misbrug, og dens værdi afhænger meget af, hvilke andre foranstaltninger der implementeres, med henblik på hurtig lukning af unødvendige adgange.

Artikel 25. Ved erhvervelse af nyt it-system eller udvikling/ændring i eksisterende it-system skal databeskyttelse være tænkt ind i design og standardindstillinger. Automatisk lukning kræver, at funktionen er indbygget i it-systemet eller i det it-system, som styrer adgange til andre systemer.

Begrænsning af antal autorisationsansvarlige og brugeradministratorer

Dette er en forebyggende foranstaltning, som mindsker sandsynligheden for fejloprettelse af unødvendige adgange ved, at kun få personer kan udføre autorisere og styre brugeradgange, og disse personer har det som (én af) deres hovedopgave(r). Det mindsker endvidere sandsynligheden for internt misbrug.

Hvis det kun er brugeradministratorerne, som teknisk har mulighed for at give andre adgangsrettigheder, kan foranstaltningen også mindske risikoen i forbindelse med eksterne cyberangreb, fordi det er mindre sandsynligt, at kompromittering af én brugers log-in umiddelbart giver mulighed for at styre adgangsrettigheder til ét eller flere it-systemer.

Implementeringsforslag

Der udpeges færrest muligt autorisationsansvarlige, hvor den autorisationsansvarlige (typisk leder for nogle brugere) har et vist kendskab til brugernes adgangsbehov. De autorisationsansvarlige informeres om vigtigheden af, at begrænse brugernes adgange.

Idet brugeradgange, der anvendes ifm. brugeradministrering, normalt kan misbruges mere end normale brugeradgange, kan det evt. øge sikkerheden, hvis brugeradministratorer har to bruger-konti, så de kan begrænse anvendelsen af den konto, som giver større mulighed for misbrug (se foranstaltningen *Minimering af privilegerede adgangsrettigheder*). Det giver ikke nødvendigvis mening i små organisationer eller hvis den konkrete medarbejder udelukkende udfører brugeradministrering.

Kommentar [F10]: Dette bør forklares nærmere.

Den organisatoriske funktion, som står for brugeradministrering, begrænses til så få personer som muligt. Dette kan være svært, hvis brugeradministratorer er spredt ud i organisationen, hvorfor samtidig implementering af foranstaltningen *Centraliseret rettighedsstyring* vil styrke den samlede forebyggende effekt.

Grundlag for vurdering af nødvendighed

Artikel 5, stk. 1, litra f, og særligt udtrykket "ulovlig behandling" er i fokus her. Når foranstaltningen begrænser, hvem der kan give andre adgang til it-systemerne, begrænser den også muligheden og dermed sandsynligheden for, at sådanne rettigheder udnyttes til ulovlig behandling. Samtidig har dette også en beskyttende effekt ift. cybertrusler, idet hackere ofte opererer igennem adgangsrettigheder i kompromitterede bruger-konti, og færre rettigheder giver dermed hackerne færre muligheder.

Men den dataansvarliges risikovurdering efter artikel 32, kan vise, hvor meget denne foranstaltning reducerer sandsynligheden for den slags misbrug. Hvis der fx er tale om en tomandsvirksomhed, kan man argumentere, at begge skal kunne styre adgangsrettigheder, i tilfælde af at den ene er indisponibel, så reduktion af rettighederne vil tilføje andre risici (afhængighed af enkeltpersoner). Så der er tale om en afvejning.

Centraliseret rettighedsstyring

Dette er en forebyggende foranstaltning, som mindsker sandsynligheden for, at der sker fejl i styringen af adgange. Decentral rettighedsstyring indebærer nemlig ofte, at den der udfører det, ikke har det som sin hovedopgave, og det kan øge muligheden får fejl, grundet manglende erfaring, fokus og interesse for opgaven.

Foranstaltningen beskytter også imod, at autonomt udført rettighedsstyring bliver glemt ved ændringer i it-miljøer, med deraf følgende brud på persondatasikkerheden: Den slags kan evt. opdages inden ændring af it-systemet, men det kræver, at der er styr på en anden foranstaltning, nemlig *Ændringsstyring*.

Centraliseret rettighedsstyring vil normalt også gøre det nemmere at føre kontrol, og dermed at implementere foranstaltningen *Periodisk kontrol af adgangsrettigheders aktualitet*.

Forslag til implementering

Der sikres et overblik over alle brugeradgange, og en ensartet styring af disse. Opgaven samles organisatorisk hos personer, som får den nødvendige uddannelse til at håndtere netop denne opgave.

Via retningslinjer og evt. tekniske foranstaltninger forbydes/forhindres autonom brugeradministrering. Eksempelvis ved udelukkende medarbejdere i den centrale brugeradministrationsenhed kan styre adgangsrettigheder. Det kan fx omfatte en teknisk forhindring af, at medarbejdere generelt kan oprette mapper med adgangsbegrænsning på netværksdrev eller SharePoint.

Central rettighedsstyring indebærer også, at registrering af adgangsrettigheder kan centraliseres, hvilket igen gør det nemmere at føre kontrol med, om procedurer følges.

Centraliseringen kan inkludere en teknisk centralisering via anvendelse af Single Sign-On eller en Directory Service så som Active Directory i Windows.

Grundlag for vurdering af nødvendighed

Det er primært en risikovurdering efter artikel 32, som skal vise, om denne foranstaltning er relevant, idet risici og muligheder er meget afhængige af den konkrete organisation, og hvilke typer af it-systemer, der anvendes.

Artikel 25. Ved erhvervelse af nyt it-system eller udvikling/ændring i eksisterende it-system skal databeskyttelse være tænkt ind i design og standardindstillinger. Hvis it-systemer udvælges/designes efter at de kan indgå i en central rettighedsstyring, og evt. Single Sign-On, kan man undgå en decentral rettighedsstyring med de førnævnte risici.

Dataadgang efter behov

Dette er en forebyggende foranstaltning, som kan mindske sandsynligheden for utilsigtet eller ondsindet misbrug. En bred dataadgang øger muligheden for misbrug. Hvis der er stor sandsynlighed for at finde personer man kender (familie, naboer, kendte personer, datterens nye kæreste) i et it-system, så kan det også øge fristelsen til at misbruge adgangen til disse oplysninger.

Forslag til implementering

Adgange gives efter arbejdsbetinget behov, og kan begrænses på fx datas alder, datatype (fx om det er kundedata, HR-data, Whistleblowerdata), sagstype (fx "Vej & park" eller "familiesager"), osv.

Mulighederne afhænger normalt af it-systemernes design, hvorfor disse aspekter skal være tænkt ind på tidspunktet for design eller indkøb af it-systemer.

Hvis der anvendes RPA (Robotic Process Automation) eller lignende, og man i den forbindelse giver adgangsrettigheder til robot-brugere, skal man på samme måde begrænse deres adgang mest muligt. Økonomisk besparelse på robot-brugerlicenser kan friste til at give en robot så mange adgangsrettigheder som muligt. Men en robot, som har mange adgangsrettigheder, kan udgøre en højere risiko, hvis fx en hacker får mulighed for at opnå denne robots rettigheder.

Se også foranstaltningen *Pseudonymisering, anonymisering*, som ligeledes begrænser adgangen, men ved at fjerne eller separere data.

Grundlag for vurdering af nødvendighed

Artikel 5, stk. 1, litra f, handler om personoplysningers integritet og fortrolighed. Jo færre data der er adgang, desto mere mindskes sandsynligheden for, at nogle af disse brugere via utilsigtede eller ondsindede handlinger kan udgøre en trussel. Samtidig har dette også en beskyttende effekt ift. cybertrusler, idet hackere

Kommentar [F11]: Der bør ske kobling til autoritative systemer som HR-systemet samt en centraliseret rettighedstildeling via fx et IdM system.

Kommentar [F12]: Er der behov for at skelne mellem "Adgangsrettigheder efter behov" og "Dataadgang efter behov"?

Og vi vil foreslå, at overskriften ændres til "Nødvendig dataadgang" i stedet for "efter behov", så formuleringen bringes i overensstemmelse med art. 5, stk. 1, litra c.

Kommentar [F13]: Organisation er et vigtigt styringsredskab. Fx har en socialrådgiver i Social og Sundhed andre adgange end en socialrådgiver i Børn og Familie.

Kommentar [F14]: Se kommentar til brug af robotter under afsnittet om Adgangsrettigheder efter behov.

ofte opererer igennem adgangsrettigheder i kompromitterede bruger-konti, og færre rettigheder giver dermed hackerne færre muligheder. Man skal derfor begrænse adgangsrettigheder mest muligt.

Artikel 25. Ved erhvervelse af nyt it-system eller udvikling/ændring i eksisterende it-system skal databeskyttelse være tænkt ind i design og standardindstillinger. En indbygget mulighed for at minimere adgangsrettigheder giver større mulighed for databeskyttelse ifm. brugeradministrering. Standardindstillinger kan ligeledes minimere rettigheder som udgangspunkt, men det kan også handle om fx automatisk sletning af data efter deres alder, hvilket bidrager til minimering af dataadgang.

Dokumentation af autorisationer

Dette er en forebyggende foranstaltning, som kan mindske sandsynligheden for bevidst misbrug af de adgangsrettigheder, man har som brugeradministrator. Det kan også mindske sandsynligheden for hændelige fejl og bevidst misbrug fra den autorisationsansvarliges side. Det behøver ikke at være ondsindet. Det kan handle om en hverdag, hvor fokus er på at få de nødvendige adgange etableret hurtigt, så medarbejderne kan udføre deres arbejde, og hvor pression fra ledelsen kan friste til at udføre brugeradministrering i strid med de fastsatte procedurer.

Forslag til implementering

Procedurer og/eller teknik indrettes således, at brugeradministratorer dokumenterer, at de ikke har handlet på egen hånd ifm. udstedelse af adgangsrettigheder til andre.

Der er nedskrevne krav om, at autorisationer (autorisationsansvarliges godkendelser af adgangsrettigheder) dokumenteres af brugeradministrator. Autorisationer udarbejdes og lagres på en sådan måde, at de er beskyttet imod at blive ændret (manipuleret) af brugeradministrator. Dette beskytter både imod snyd fra brugeradministrators side, og imod at den brugeradministrator presses til at udstede adgangsrettigheder uden dokumenteret autorisation.

Grundlag for vurdering af nødvendighed

Det er primært en risikovurdering efter artikel 32, som skal vise, om denne foranstaltning er relevant, men den er sandsynligvis altid relevant, på grund af det menneskelige aspekt, som er beskrevet i indledningen til denne foranstaltning.

Artikel 5, stk. 1, litra f, siger bl.a., at personoplysninger skal behandles på en måde, der sikrer beskyttelse mod uautoriseret eller ulovlig behandling. Når autorisationer ikke er dokumenteret, kan det mindske ansvarsfølelsen hos både brugeradministrator og autorisationsansvarlig. Dermed kan det at *få dagligdagen til at fungere* blive prioriteret højere end at udføre rettighedsstyring korrekt.

Hvis adgangsrettigheder ender med at blive misbrugt, kan det være uklart, hvem der evt. ikke har gjort tilstrækkeligt for at udgå dette, og det kan resultere i interne konflikter.

[Følgende har ikke relevans for vejledningen om rettighedsstyring. Kataloget skal på denne måde kunne indeholde alle typer foranstaltninger. Det er indføjet som eksempel på noget, der kan anvendes i andre sammenhænge, fx afgørelser eller modenhedsmåling. Det kan også være et alternativ til en kort hjemmesidetekst. På samme måde kan eksisterende hjemmesidetekster måske beskrives som en foranstaltning, fx teksten om kryptering af e-mail, men dette skal ses i sammenhæng med en anden vejledning, som er på vej (DIS/ANC). CFCS har også skrevet en side om det her

Kommentar [F15]: Hvad menes der? Brugeradministrator har jo privilegeret adgang.

Kommentar [F16]: Definitionerne af autorisationsansvarlige og brugeradministratorer og deres respektive roller bør også fremgå af foranstaltningskataloget for, at dette afsnit bliver forståeligt.

https://www.cfcs.dk/globalassets/cfcs/dokumenter/vejledninger/-vejledning-passwordsikkerhed-2020.pdf, men det er ikke lige så fyldestgørende, til gengæld står det sammen med andre gode råd om passwords.]

Kommentar [F17]: Opbygningen – og brugen af dokumentet – kan med fordeles flyttes til indledningen af dokumentet.

Flere faktorer i login (også kendt som MFA, multi-faktor-login)

Dette er primært en forebyggende foranstaltning, idet den reducerer risici, ved at håndtere trusler som den enkelte faktor er udsat for.

Det evt. også betragtes som en opdagende foranstaltning: Forsøg på at opnå uautoriseret adgang ved en anden brugers login vil kræve flere trins, og det kan give øget mulighed for at opdage misbrugsforsøg, mens det foregår, og inden det ender i et succesfuldt uautoriseret login.

Forslag til implementering

MFA betyder, at brugeren skal afgive to eller flere *uafhængige* faktorer for at opnå adgang. To faktorer anses for uafhængige, såfremt det ikke er muligt at udlede én faktor ud fra viden om den anden faktor.

Faktorerne vælges fra *forskellige* kategorier af følgende:

A. Noget brugeren ved: Typisk en personlig adgangskode. Det skal være noget, som kun brugeren kender, og som brugeren kan nøjes med at have i hukommelsen. Derfor er det normalt også noget, som brugeren selv har valgt. Faktoren må ikke på noget tidspunkt have været tilgængelig eller blive tilgængelig for andre personer. Brugeren skal kunne udskifte denne faktor, hvis der er mistanke om, at andre har fået kendskab til den.
B. Noget brugeren har: Eksempelvis et personligt papkort med unikke engangskoder. Faktoren kan udgøres af et stykke unikt hardware som fx et elektronisk adgangskort. Faktoren kan også blive genereret af noget unikt software, som ligger i noget hardware, fx en engangskode genereret af en hardkey/nøgleviser. Det skal være noget, som brugeren kan have i sin fysiske besiddelse, og som brugeren kan holde helt for sig selv. Det må ikke være noget, som skal deles med andre. Brugeren skal kunne udskifte denne faktor, hvis der opstår mistanke om, at andre har mulighed for at bruge en kopi af hardwaren/softwaren.
C. Noget brugeren er: Typisk biometri, som fingeraftryk, irisscan, ansigtsgenkendelse, stemmegenkendelse, osv. Til sammenligning med kategori A og B, har kategori C en indbygget svaghed, nemlig at brugeren sjældent kan holde faktoren for sig selv eller udskifte den.

Brugernavn, kundenummer, personnummer (CPR-nr.), mv. betragtes ikke som en faktor, fordi det typisk ikke er noget, som udelukkende brugeren kender eller har adgang til.

MFA har sin styrke i, at det kan minimere konkrete risici. Derfor er der først sket en afdækning af alle de risici, som et konkret login er udsat for, og derefter er faktorerne valgt ud fra en vurdering af, om de i tilstrækkelig grad påvirker de konkrete risici. Eksempel:

1. Der er afdækket risici ved anvendelsen af adgangskoder indtastet via pc/smartphone. Dette kan blive udført af medarbejderen på offentlige steder. Adgangskoden er derfor udsat for at blive opsnappet af ondsindet software eller hackere, som har kompromitteret denne pc/smartphone, og de er udsat for at blive opsnappet ved kik over skulderen eller via overvågningskameraer på et offentligt sted.
2. Hvis den anden faktor er engangskoder fra en elektronisk kodeviser, så kan disse også blive opsnappet af malware/kamera. Men hvis koden vist på kodeviseren kun kan anvendes én gang og indenfor meget kort tid – og brugeren antageligt vil gøre det straks – er denne faktor ikke i samme grad udsat for at blive misbrugt via samme risici.
3. Kodeviseren er udsat for risici som fysisk tyveri, men det er adgangskoden ikke, idet den er i hovedet på brugeren. Brugeren må derfor ikke skrive koden på en papirlap, der kan blive stjålet sammen med

kodeviseren. Derfor suppleres med en organisatorisk foranstaltning i form at retningslinjer til brugerne om håndtering af adgangskoden og hurtig rapportering af tyveri, med henblik på spærring af kodeviser og evt. login.

Hvis man fx har et login som kræver et elektronisk adgangskort kombineret med fingeraftryk, så er kortet udsat for tyveri/tab, og med stor sandsynlighed sidder den anden faktor på kortet, og dermed ar begge faktorer berørt af samme risiko, selv om de er fra to forskellige kategorier (nogen man *har* og nogen man *er*). Om det er et problem, afhænger af andre forhold, fx om kortet kan nå at blive spærret før nogen for "løftet" fingeraftrykket af og lavet en kopi. Det kan også være, at dette adgangsmedie primært er etableret for at beskytte imod tyveri fra en bygning, mens adgangen til personoplysninger kræver endnu et login, som ikke er blevet kompromitteret ved tyveriet af kortet.

Endeligt sikres det, at der ikke er omveje til login, som reelt eliminerer kravet om MFA. Det kunne fx være en løsning til, når brugeren har glemt sin adgangskode, som reelt giver mulighed for login med kun én faktor.

Grundlag for vurdering af nødvendighed

Det er primært en risikovurdering efter artikel 32, som skal vise, om denne foranstaltning er relevant, idet risici og muligheder er meget afhængige af de konkrete forhold. Bemærk dog artikel 5, stk. 1, litra f, som angiver, at personoplysninger skal behandles på en måde, der sikrer beskyttelse mod uautoriseret eller ulovlig behandling, og ved adgang til særligt beskyttelsesværdige personoplysninger via internettet, kan det være umuligt at beskytte dette tilstrækkeligt gennem en-faktor-login.

Praksis: Datatilsynet har XXXX

Forhindring af anonym adgang

Dette er en forebyggende foranstaltning, som kan mindske sandsynligheden for misbrug, idet anonyme adgange til it-systemer kan friste til misbrug. Endvidere vil foranstaltninger, der angår logning, have mindre eller ingen præventiv effekt imod misbrug, når brugere kan skjule sig bag et anonymt login.

Anonym adgang betyder, at der er brugerkonti, som kan anvendes, uden at handlingerne kan henføres til en enkelt fysisk person. Det kan handle om fælles-login eller fx testbrugerkonti, som anvendes af forskellige udviklere på skift, uden at det er klart, hvem der har anvendt login, og hvornår. Det er dog ikke en hjælp at anvende personlige brugerkonti, hvis brugerne er klar over, at deres handlinger ikke logges, så det skal ses i sammenhæng med foranstaltninger som *Logning af brugernes anvendelser af personoplysninger*.

Fordelen begrænser sig dog ikke til *bevidst* misbrug. Når flere deles om en systemadgang, så deles de reelt set også om ansvaret for, de behandlinger af personoplysninger, der sker via systemadgangen, og når flere deles om et ansvar, så føler den enkelte ofte mindre eller intet ansvar.

Endeligt kan anonyme adgange øge sandsynligheden for, at de adgangsgivende faktorer (fx adgangskode) ikke håndteres forsvarligt – af flere årsager:

- Adgangskoder kan blive delt mellem personer, der ikke nødvendigvis er blevet autoriseret. Den enkelte bruger føler ikke stort ansvar for at beskytte adgangskoden.
- Adgangskoderne skiftes måske ikke, når personer udtræder af brugergruppen og dermed ikke længere er autoriseret til adgangen.
- Adgangskoder, som man ikke selv har valgt, er ofte sværere at huske og nedskrives derfor.

Forslag til implementering

Kommentar [F18]: Overvej gerne en mere umiddelbart forståelig benævnelse.

Kommentar [F19]: Der kan være situationer, hvor fællesbrugere har et praktisk formål, typisk på udstyr i undersøgelsesrum (Sundhedscentre), hvor flere faggrupper er sammen med en patient samtidigt, og med et større flow pr. time af borgere.

It-systemer og procedurer indrettes således, at anonym adgang så vidt muligt forhindres. Det indebærer, at adgangsgivende faktorer (fx adgangskoder) er personlige og kun kendes af den enkelte bruger.

Eventuelle servicekonti, hvis login er indkodet i software, beskyttes imod misbrug.

Hvis bruger-id'er genanvendes (videregives til en anden person), så registreres det, hvornår det er sket, så man altid ved, hvem der på et hvert givent tidspunkt har anvendt den bruger-id. Typisk aktuelt ved brugerkonti der anvendes til test eller midlertidige ansættelser (eksterne konsulenter, vikarer, elever).

Hvis man ikke kan undgå deling af adgangsgivende faktorer mellem flere personer, så minimeres adgangen, og så snart der sker ændring i brugergruppen, ændres den adgangsgivende faktor, så kun den aktuelle brugergruppe kan foretage login.

Det suppleres med awareness til brugerne ang. hvordan adgangsgivende faktorer skal håndteres og beskyttes, så brugeren er klar over, at de stadig står til ansvar for handlinger udført under login.

Det suppleres med, at det skal være nemt, sikkert at logge på hurtigt, fx ved brug af biometri-læsninger eller ved scanning af kort kombineret med en kode.

Grundlag for vurdering af nødvendighed

Det er primært en risikovurdering efter artikel 32, som skal vise, om denne foranstaltning er relevant, idet risici og muligheder er meget afhængige af de konkrete forhold. Bemærk dog artikel 5, stk. 1, litra f, som angiver, at personoplysninger skal behandles på en måde, der sikrer beskyttelse mod uautoriseret eller ulovlig behandling. Som det ses af ovenstående, kan anvendelsen af anonym adgang øge sandsynligheden for bevidst misbrug, manglende ansvarsfølelse og andet, der resulterer i uautoriseret/ulovlig behandling af data.

Forlods angivelse af adgangslukning

Dette er en forebyggende foranstaltning, som kan mindske sandsynligheden for misbrug af unødvendige adgange.

Forslag til implementering

Hvis it-systemerne gør det muligt, kan man allerede ved etableringen af en adgang sætte en udløbsdato på. Det kan fx være ifm. ansættelse af eksterne konsulenter knyttet til et projekt med en klar tidshorisont. Alternativt kan det foregå manuelt med påmindelser i en kalenderfunktion.

Foranstaltning kan også hjælpe på den ophobning af opgaver vedr. ansættelse og fratrædelse, som kan ske ved månedsskifte eller blot en tilfældig ophobning af opgaver, som gør, at der ikke er tid til at lukke alle adgange præcist, når en ansættelse stopper. Hvis it-systemerne gør det muligt, kan lukning af adgange planlægges til at ske automatisk, så snart det registreres (fx i HR-systemet), at en ansættelse ophører.

Grundlag for vurdering af nødvendighed

Det er en risikovurdering efter artikel 32, som skal vise, om denne foranstaltning er relevant. Hvis man fx har få ansatte eller der sjældent sker ansættelser eller fratrædelser, kan skriftlige procedurer være tilstrækkeligt, og denne foranstaltning vil i så fald ikke bidrage væsentligt til sikkerheden.

Artikel 25. Ved erhvervelse af nyt it-system eller udvikling/ændring i eksisterende it-system skal databeskyttelse være tænkt ind i design og standardindstillinger. Automatisering af denne foranstaltning kræver, at funktionen er indbygget i et it-system.

Kommentar [F20]: Overvej gerne en mere umiddelbart forståelig benævnelse, fx "Sæt slutdato for brugeradgang ved oprettelse."

Kommentar [F21]: Giver kun mening, hvis brugerstyring ikke er styret af et centralt brugerstyringssystem, der fodres fra et HR-system.

Kommentar [F22]: Centraliseret brugerstyring vil kunne løse den udfordring.

Funktionsadskillelse

Dette er en forebyggende foranstaltning, som mindsker sandsynligheden for, at en person misbruger adgangsrettigheder, hvor opgaver udført med én rettighed gør personen inhabil ift. opgaver, som kan udføres med en anden rettighed. Eksempelvis berigtigelse *og* godkendelse af faktura for eget indkøb, eller bestilling *og* autorisering af egen adgang til et it-system.

Implementeringsforslag

Funktionsadskillelse kendes fra økonomisystemer, hvor det sikrer imod, at én medarbejder alene kan stjæle penge fra arbejdsgiveren. Implementeringsforslaget her fokuserer dog på funktionsadskillelse indenfor rettighedsstyring.

Der bør altid være funktionsadskillelse mellem dem som er brugere (dem som anvender adgange), de autorisationsansvarlige (dem som kan godkende adgange) og brugeradministratorer (dem som kan styre adgange). Der kan også være et fjerde led, hvis man fx har en it-driftsmedarbejder, der i praksis styrer adgangen på vegne af brugeradministratoren.

Der laves en skarp adskillelse i arbejdsopgaver og adgangsrettigheder, hvor ovennævnte personers opgaver/adgange så vidt muligt ikke overlapper. Fx må en brugeradministrator ikke godkende sin egen adgang til et it-system, og hvis det ikke kan forhindres teknisk, skal der være en godkendelsesprocedure, som gør det umuligt for brugeradministrator at forfalske den autorisationsansvarliges godkendelse. Ved manuelle blanketbasserede procedurer, kan det således være nødvendigt at udforme autorisationsblanketten, så der ikke kan rettes i den, efter den autorisationsansvarlige sat sin underskrift.

Der er regler imod eller en teknisk forhindring af, at en autorisationsansvarlig kan godkende sin egen adgang.

Hvis muligheden er til stede i it-systemet kan brugeradministrators adgang begrænses til kun at kunne give mulighed for *rettighedsstyring* i it-systemet, uden at det giver brugeradministratoren mulighed for at *tilgå* data i samme it-system. Altså der er en adgang, som ikke giver adgang til data, men som kun giver mulighed for at styre andres adgange til data.

Ved tildeling af nye adgange ifm. nyansættelse eller omrokering i organisationen, er der procedurer eller beskrivelser, som sikrer, at der ikke kan opstå en situation, hvor en medarbejder får adgange på tværs af den ønskede funktionsadskillelse. Det kan evt. sikres gennem den formular, som anvendes ved tildeling af adgangsrettigheder.

Det sikres, at adgange, der kun har et it-driftsmæssigt formål, udelukkende gives til it-driftspersonale med rette uddannelse, og hvis muligt også tidsbegrænset.

Funktionsadskillelse er ikke kun relevant mellem mennesker, men også mellem robotter. Hvis der anvendes RPA (Robotic Process Automation) eller lignende, og man i den forbindelse giver adgangsrettigheder til robot-brugere, kan det fremstå som om manglede funktionsadskillelse ikke indebærer samme risici, som hvis samme rettigheder var samlet hos én fysisk person. Økonomisk besparelse på robot-brugerlicenser kan friste til at give en robot så mange adgangsrettigheder som muligt. Men det kan udgøre en højere risiko, hvis fx en hacker eller softwareudvikler får mulighed for at misbruge denne robots rettigheder.

Grundlag for vurdering af nødvendighed

Kommentar [F23]: I kommunalt regi vil det typisk være systemejerne (fagchefer), der tager stilling til, hvilke rettigheder og adgange de enkelte brugere skal have. Dette sker automatisk via digitale templates. Herefter opretter en it-medarbejder (brugeradminstrator) brugerne i de relevante systemer.

Kommentar [F24]: Dette sker typisk digitalt i kommunerne.

Artikel 5, stk. 1, litra f, handler om personoplysningers integritet og fortrolighed, og det er normalt ikke sikret godt nok, uden en vis grad af funktionsadskillelse. Men den dataansvarliges risikovurdering efter artikel 32, kan dog indikere, at funktionsadskillelse ikke er nødvendig ift. konkrete behandlinger.

Muligheden for at implementere denne foranstaltning kan endvidere begrænses af organisationens størrelse, og dermed kan man ikke forvente funktionsadskillelse i fx en tomandsvirksomhed.

Kontrolleret/forhindret dublering af adgangsrettigheder

Dette er en forebyggende foranstaltning, som kan mindske sandsynligheden for, at en bruger får flere adgangsrettigheder end nødvendigt, og derigennem mindskes også sandsynligheden for ulovlig behandling.

Når man dublerer adgangsrettigheder fra én bruger (der allerede har disse rettigheder) til en anden bruger, kan det medføre følgende risici:

- Hvis der er fejl i de adgangsrettigheder, som dubleres, fx adgange som burde være lukket tidligere, så vil fejlen blive duplikeret til endnu en bruger.
- Den autorisationsansvarlige er muligvis ikke klar over, hvad der bliver dubleret, og tager dermed ikke aktiv stilling til, om det *er* nødvendigt at dublere *alle* adgangsrettigheder.
- Adgangsrettigheder for den eksisterende bruger kan nå at blive ændret mellem tidspunktet for den autorisationsansvarliges godkendelse og tidspunktet for dublering af adgange, og dermed kan der opstå tvivl om, hvad der blev godkendt. Der kan således opstå tvivl om, hvorvidt burgeradministrator har behandlet opgaven korrekt, eller hvilke adgange den autorisationsansvarlige rent faktisk har godkendt til at blive duplikeret.
- Idet den autorisationsansvarlige ikke specifikt angiver, hvilke adgange der skal tildeles, er det uklart, hvad den autorisationsansvarlige efterfølgende kan stilles til ansvar for, såfremt der bliver tildelt flere adgange end nødvendigt, og disse bliver misbrugt.

Forslag til implementering

Procedurer eller teknik kan bruges til at forbyde/forhindre dublering af adgangsrettigheder, eller de kan sikre, at det sker forsvarligt, og dermed at man undgår de ovenfor nævnte risici. Mulighederne for implementering afhænger af, hvordan brugeradministreringen udføres.

Grundlag for vurdering af nødvendighed

Artikel 5, stk. 1, litra f, handler om personoplysningers integritet og fortrolighed. Jo færre der har adgang, desto mere mindskes sandsynligheden for, at nogle af disse brugere via utilsigtede eller ondsindede handlinger kan udgøre en trussel. Jo mindre den enkelte bruger har adgang til, desto mindre er den potentielle konsekvens, hvis nogle af disse brugere gør skade på data via utilsigtede eller ondsindede handlinger. Samtidig har dette også en beskyttende effekt ift. cybertrusler, idet hackere ofte opererer igennem adgangsrettigheder i kompromitterede bruger-konti, og færre rettigheder giver dermed hackerne færre muligheder. Man skal derfor begrænse adgangsrettigheder mest muligt.

Kontrolleret/forhindret genanvendelse af autorisation

Dette er en forebyggende foranstaltning, som kan mindske sandsynligheden for, at en bruger får flere adgangsrettigheder end nødvendigt, og derigennem mindskes også sandsynligheden for ulovlig behandling.

Forslag til implementering

Kommentar [F25]: Svært forståelig benævnelse. Kan evt. omdøbes til "Undlad at kopiere adgangsrettigheder".

Kommentar [F26]: Et andet forslag kan være, at man ikke må kopiere brugere ved ny-oprettelse. Brugerne skal altid opbygges fra grunden.

Kommentar [F27]: Denne foranstaltning minder meget om ovennævnte foranstaltning. Måske kan foranstaltningerne slås sammen?

Genbrug af en tidligere afgivet autorisation betyder, at der ikke på ny bliver taget stilling til, om adgangsrettighederne stadig er nødvendige for denne bruger, og det kan give brugeren unødvendige rettigheder. Beskyttelsen kan ske via procedurer, it-systemer eller blanketter, som anvendes ifm. brugeradministreringen.

Grundlag for vurdering af nødvendighed

Artikel 5, stk. 1, litra f, handler om personoplysningers integritet og fortrolighed. Jo færre der har adgang, desto mere mindskes sandsynligheden for, at nogle af disse brugere via utilsigtede eller ondsindede handlinger kan udgøre en trussel. Jo mindre den enkelte bruger har adgang til, desto mindre er den potentielle konsekvens, hvis nogle af disse brugere gør skade på data via utilsigtede eller ondsindede handlinger. Samtidig har dette også en beskyttende effekt ift. cybertrusler, idet hackere ofte opererer igennem adgangsrettigheder i kompromitterede bruger-konti, og færre rettigheder giver dermed hackerne færre muligheder. Man skal derfor begrænse adgangsrettigheder mest muligt.

Logning af brugernes anvendelser af personoplysninger

Hvis brugernes anvendelser af data i et it-system registreres (logges), så kan man undersøge for misbrug. Det udgør dog udelukkende en *opdagende* foranstaltning, i og med at det kan blive opdaget, at der på et tidligere tidspunkt er sket misbrug af en autoriseret adgang til et it-system. Som sådan vil det ikke nødvendigvis kunne mindske risikoen for de registrerede, idet skaden allerede er sket, og loggen kan blot anvendes til (måske) at finde den skyldige – den som har misbrugt en autoriseret adgang. Denne type log vil dermed ikke nødvendigvis kunne påvirke risici ved behandlingen af personoplysninger.

Hvis loggen også skal have en præventiv effekt og dermed være en *forebyggende* foranstaltning, forudsætter det, at brugerne er blevet gjort bekendt med, at misbrug kan blive opdaget (via logs) og sanktioneret. Det forudsætter, at alle handlinger kan spores til en enkelt fysisk person. Derfor hænger denne foranstaltning sammen med foranstaltningen *Forhindring af anonym adgang*.

Implementeringsforslag

It-systemer udvikles og opsættes så de logger alle anvendelser af personoplysninger foretaget af brugere, herunder læsning, tilføjelse, søgning (evt. søgekriterium), ændring, udtræk og sletning – uanset hvordan anvendelsen af personoplysninger udføres af brugeren. Relevante it-systemer udvikles/tilrettes så der er mulighed for denne logning, og logning er som udgangspunkt aktiveret.

It-systemerne udvikles til at kunne gemme logdata i et specifikt tidsrum, fx de sidste x måneder, og ældre logs slettes automatisk, med mindre de gemmes manuelt af hensyn til efterforskning af en konkret hændelse eller mistanke om misbrug.

Loggens opbevaringstid sættes efter formålet, så hvis en log skal kunne anvendes til at spore misbrug, kan det være passende at sætte opbevaringstiden efter, hvor ofte der foretages kontrol af adgangsrettigheder (se *Periodisk kontrol af adgangsrettigheders aktualitet*). Fund af fejl i disse rettigheder kan afstedkomme et behov for at gennemgå logs i minimum den periode, som er gået siden foregående kontrol, fordi det vil være en den periode, hvor de forkerte rettigheder eksisterede og dermed kunne misbruges. Behov for at kunne undersøge for cyberangreb kan dog fordre længere opbevaringstid.

Logs lagres et sted, hvor de er beskyttet ift. både fortrolighed, integritet og tilgængelighed.

Det sikres, at det bliver muligt for den dataansvarlige at få logs udleveret uden større besvær eller udgifter – fx fra en databehandler.

Kommentar [F28]: Kan dette forslag evt. gøres mere konkret?

Der laves en vejledning i hvordan log tolkes. Det testes, at loggen kan tolkes korrekt ved brug af vejledningen – helst ved blindtest, altså hvor en person udfører/dokumenterer handlinger og en anden anvender vejledningen til at tolke loggen, og derefter sammenholdes de to personers opfattelse af, hvad der er sket.

Logning aktiveres ved idriftsættelse af it-systemet.

Det testes, at alle anvendelser af personoplysninger logges. Hvis fx brugeren kan anvende flere metoder til at få vist dada, så er det testet, at det logges, uanset hvilken metode brugeren anvender.

Ang. informering af medarbejdere om logning og mulige sanktioner: Se foranstaltningen *Awareness*.

Der bør være kontrol af, om der til stadighed logges som forventet og, at logdata gemmes længe nok, og kan tolkes med den aktuelle vejledning eller et dertilhørende it-system. Det er altså en afprøvning af en etableret foranstaltning, og dermed omfattet af databeskyttelsesforordningens artikel 32, stk. 1 litra d. Det bør især ske ved systemændringer, men også løbende, hvis der går lang tid imellem systemændringerne.

Hvis der er direkte fysisk adgang til personoplysninger, så er loggen i et fysisk adgangssystem også omfattet af ovenstående tiltag.

Alarmer fra logs bør være automatiserede/regelbaserede for at sikre, at mængden af logningsdata ikke er en barriere for at gennemgå loggen.

Kommentar [F29]: Forslag til tilføjelse.

Grundlag for vurdering af nødvendighed

Det er primært en risikovurdering efter databeskyttelsesforordningens artikel 32, som skal vise, om denne foranstaltning er relevant, idet risici er meget afhængige af, hvilke behandlinger af personoplysninger der sker i forskellige it-systemer, samt hvilken præventiv effekt man kan forvente af, at brugerne evt. ved deres handlinger logges.

Generelt kan det siges, at it-systemer, der indeholder mange personers oplysninger, øger fristen for misbrug fordi det øger muligheden for misbrug, samt muligheden for at finde personer i systemet, som man kender. Men risikovurderingen skal se på både fortrolighed, integritet og tilgængelighed, så andre aspekter kan også gøre logning til en passende foranstaltning.

Kommentar [F30]: Hvad menes der?

Artikel 25. Ved erhvervelse af nyt it-system eller udvikling/ændring i eksisterende it-system skal databeskyttelse være tænkt ind i design og standardindstillinger. For at kunne implementere foranstaltningen her, skal muligheden for at logge anvendelser af personoplysninger være indbygget i it-systemet. Det inkluderer muligheden for at lagre loggen et sikkert sted, hvor brugerne ikke kan tilgå/manipulere den.

Logning af brugeradministrators handlinger

Denne foranstaltning har reelt samme formål som foranstaltningen *Logning af brugernes anvendelser af personoplysninger*. Men indholdet i loggen kan være anderledes, fordi fokus skal være på at kunne spotte misbrug af brugeradministrators adgangsrettigheder.

Forslag til implementering

Med ovenstående i mente, kan man følge beskrivelsen af foranstaltningen *Logning af brugernes anvendelser af personoplysninger*.

Grundlag for vurdering af nødvendighed

Samme som foranstaltningen *Logning af brugernes anvendelser af personoplysninger*. Idet brugeradministratoren typisk kan give andre og evt. sig selv adgang til flere it-systemer, er der ofte en relativt højere risiko ved denne persons handlinger – med risiko ift. databeskyttelsesforordningens artikel 32 menes her særligt risiko for misbrug af personoplysninger der behandles i de it-systemer, som brugeradministratoren styrer adgangen til.

Artikel 25. Ved erhvervelse af nyt it-system eller udvikling/ændring i eksisterende it-system skal databeskyttelse være tænkt ind i design og standardindstillinger. For at kunne implementere foranstaltningen her, skal muligheden for logning af brugeradministrator handlinger være indbygget i it-systemet, som anvendes til brugeradministrering. Det inkluderer muligheden for at lagre loggen et sikkert sted, hvor brugeradministratoren ikke kan tilgå/slette den.

Minimering af privilegerede adgangsrettigheder

Dette er en forebyggende foranstaltning, som kan mindske konsekvensen ved en kompromitteret brugeradgang. Et typisk hackerangreb inkluderer ofte en eller anden form for eskalering af adgangsrettigheder til administratorniveau, fordi det giver flere muligheder end en almindelig brugers adgangsrettigheder. Derfor skal anvendelse af privilegerede adgange minimeres.

Forslag til implementering

Udfordringen er, at der altid er nogen, som skal have privilegerede adgangsrettigheder, så ud over at begrænse hvem der har disse rettigheder, kan man også give samme bruger to brugerkonti – én almindelig med almindelige adgangsrettigheder, og én med flere rettigheder. Ved kun at anvende den privilegerede brugerkonto, når det er absolut nødvendigt, begrænses dens eksponering – dog ikke, hvis medarbejderen skal anvende den privilegerede brugerkonto det meste af tiden. Opsplitningen kan også have den positive effekt, at brugeren er mere opmærksom på, hvornår han/hun arbejder med adgangsrettigheder, der kan gøre større skade (hvis der begås fejl).

Direkte adgang til en database, fx en såkaldt "SQL-adgang" kan indebære mulighed for direkte manipulation af databasen – dvs. udenom enhver adgangsbegrænsning og sikkerhedsfunktioner, der normalt findes i applikationer, som ligger mellem brugeren og databasen. Denne type adgang er meget risikabel og bør så vidt muligt ske under følgende forhold:

- Gives kun, når det er absolut nødvendigt (tidsbegrænset).
- Gives kun til personer med it-driftsopgaver og rette kompetencer.
- Gives kun efter en form for sikkerhedsgodkendelse og evt. under forudsætning af ren straffeattest.
- Anvendelsen logges og loggen gemmes et sted, hvor den ikke kan tilgås af dem, der anvender adgangen.

Grundlag for vurdering af nødvendighed

Det er primært en risikovurdering efter artikel 32, som skal vise, om denne foranstaltning er relevant, idet risici er meget afhængige af, hvilken skade man kan gøre med privilegerede adgangsrettigheder. Samtidig har dette også en beskyttende effekt ift. cybertrusler, idet hackere ofte opererer igennem adgangsrettigheder i kompromitterede bruger-konti, og færre rettigheder giver dermed hackerne færre muligheder.

Periodisk kontrol af adgangsrettigheders aktualitet

Dette er en opdagende foranstaltning der mindsker sandsynligheden for misbrug eller fejl fra brugernes side, ved at fjerne unødvendige adgangsrettigheder.

Forslag til implementering

En kontrol kan omfatte én eller flere af følgende undersøgelser:

1. Om de faktisk etablerede adgange er omfattet af en gældende autorisation.
2. Om adgange skulle være lukket tidligere grundet en tidsbegrænset/udløbet autorisation, fratrædelse, orlov eller andet.
3. Om autorisationerne er aktuelle – altså om alle godkendelser af adgange er nødvendige og bunder i et arbejdsbetinget behov.
4. Om der er er adgange som ikke længere benyttes af den retmæssige bruger ("ghost accounts"), som burde være lukket.

Mulighederne og hvad der er nemmest afhænger af de it-systemer, der anvendes. Man skal fx vælge en autoritativ kilde at holde adgangsrettighederne op imod – en kilde, som man kan stole på er opdateret. Typisk er der et HR-system, som viser, hvem der aktuelt er ansat, og hvilken stilling de har. Har man *rollebaserede adgangsrettigheder*, kan registreringen i HR-systemet meget præcist angive, hvem der skal have adgang til hvad, og hvilke adgange der burde være lukket.

Når der udføres kontroller skal man være opmærksom på "kontrollantens" fokus. Hvis man beder en leder om at kontrollere adgange for egne medarbejdere, kan denne leder have mere fokus på, om de nødvendige adgange er etableret, end om nogle brugere har for mange adgange. Fokus kan også være på at spare penge på brugerlicenser, hvilket kan fjerne unødvendige adgange, men det er stadig ikke et fokus på, om adgange er nødvendige for at opfylde et *arbejdsbetinget behov*.

Kommentar [F31]: Her er det i særdeleshed vigtigt, at der udstedes rettigheder efter anvisninger fra systemejer, der står inde for de arbejdsmæssige processer og dataopsamlinger, der sker i systemet.

"Kontrollanter" med forskellige roller (daglig leder, sikkerhedsansvarlig, systemejer, osv.) har forskellige interesser, og man skal være opmærksom på dette, når kontrolopgaven placeres og forklares for kontrollanten.

Hyppigheden af de ovenfor nævnte kontroller kan justeres alt efter, hvad man finder af problemer i ifm. kontrol. Hvis kontroller viser, at der sjældent er fejl, kan man evt. sænke hyppigheden af disse kontroller. Hvis kontroller derimod viser mange fejl, skal hyppigheden måske øges. Mange fejl kan imidlertid antyde, at nogle af de andre foranstaltninger ikke fungerer optimalt, så i stedet for at øge hyppigheden af kontrollen, kan den mest korrekte reaktion være at forsøge at rette op på, hvordan den daglige styring af adgangsrettigheder foregår.

Grundlag for vurdering af nødvendighed

Datatilsynet har udtalt, at det er tilsynets opfattelse, at kravet om passende sikkerhed i artikel 32, stk. 1 normalt vil indebære, at den dataansvarlige løbende kontrollerer om brugeradgange til systemer er begrænset til de personoplysninger, som er nødvendige og relevante for den pågældende brugers arbejdsbetingede behov.

Det skyldes, at uanset hvor stringent man styrer brugerrettigheder, kan det gå galt mange steder i en sådan proces, der ofte involverer mange mennesker, og der vil derfor med al sandsynlighed være fejl, som kun opdages ved periodiske kontroller.

Pseudonymisering, anonymisering

Dette er en forebyggede foranstaltning, som mindsker sandsynligheden for misbrug ved at gøre det sværere eller umuligt, at henføre data til fysiske personer. Reelt set er det dataminimering.

Pseudonymiserede personoplysninger, er personoplysninger, der kun kan henføres til en fysisk person ved brug af yderligere oplysninger, hvor adgangen til disse yderligere oplysninger er stærkt begrænset. Pseudonymisering kan anvendes, hvis nogle brugere skal anvende data, uden de behøver at kunne identificere individer. De yderligere oplysninger, som gør det muligt at identificere individerne, findes fx i et andet it-system, hvor de samme brugere ikke har adgang.

Anonymisering er en proces der sikrer, at data aldrig mere kan knyttes til en fysisk person. Hvis blot én person har adgang til oplysninger, som gør det muligt at henføre data til en fysisk person, er der ikke tale om anonyme data, men derimod personoplysninger. Anonyme data er ikke længere personoplysninger, og behandlingen af dem er ikke omfattet af databeskyttelsesreglerne.

Forslag til implementering

Der gives ikke forslag til implementering, idet mulighederne afhænger af it-systemer og arbejdsopgaver i den konkrete organisation.

Grundlag for vurdering af nødvendighed

Det er primært en risikovurdering efter artikel 32, som skal vise, om denne foranstaltning er relevant, og samme artikel nævner også pseudonymisering som en potentiel relevant foranstaltning, dog med den bemærkning, at både pseudonymisering og anonymisering er tiltag, der giver dataminimering, hvilket er et generelt princip efter artikel 5, stk. 1, litra c. ~~Fravalg af foranstaltningen skal derfor kunne begrundes.~~

Artikel 25. Ved erhvervelse af nyt it-system eller udvikling/ændring i eksisterende it-system skal databeskyttelse være tænkt ind i design og standardindstillinger. Muligheden for at pseudonymisere/anonymisere kræver, at det er tænkt i designet af it-systemet og, at det fungerer med de arbejdsopgaver, som er i organisationen. Standardindstillinger kan fx handle om at pseudonymisering/anonymisering sker automatisk når data når en vis alder.

Rollebaserede adgangsrettigheder

Dette er en forebyggende foranstaltning, som kan mindske sandsynligheden for fejl i tildeling af adgangsrettigheder.

Forslag til implementering

Med mange it-systemer og forskellige adgangsniveauer i hvert system giver det mening at simplificere rettighedstildeling ved at benytte grupperede adgangsrettigheder, som er knyttet til brugernes roller/opgaver, fx: HR-medarbejder, bogholder, kundesupporter, osv. Dette kan ligeledes anvendes til at definere adgange på tværs af it-systemer.

Rollebaseret adgangstildeling gør det også nemmere for den autorisationsansvarlige af vurdere og godkende anmodninger om adgange, fordi det ikke kræver forståelse for adgangsbehov i det enkelte it-system, men blot viden om brugernes roller/opgaver. Dette letter opgaven for alle involverede parter, og mindsker derved risikoen for fejl.

Grundlag for vurdering af nødvendighed

Kommentar [F32]: Denne foranstaltning har ikke med rettighedsstyring at gøre og foreslås derfor slettet.

Kommentar [F33]: Vi mener ikke, at der gælder et decideret begrundelseskrav.

Behovet afhænger af, hvor komplekst ens it-miljø er. Behovet øges med sandsynligheden for fejl grundet kompleksitet. Derfor er det en risikovurdering efter artikel 32, som skal vise, om denne foranstaltning er relevant.

Artikel 25. Ved erhvervelse af nyt it-system eller udvikling/ændring i eksisterende it-system skal databeskyttelse være tænkt ind i design og standardindstillinger. Muligheden for at simplificere rettighedstildeling, kan afhænge af it-systemernes design.

Stikprøver i log over brugernes anvendelser af personoplysninger

Stikprøver i logs kan øge loggens præventive (forebyggende) effekt, ved at brugerne bliver mere opmærksomme på, at misbrug af adgange kan blive opdaget.

Forslag til implementering

Der etableres en fast rutine, for stikprøver i logs, dog ikke på en sådan måde, at tidspunkterne er forudsigelige for brugerne, så en ondsindet bruger kan vælge, kun at foretage misbrug uden for disse tidspunkter.

Brugerne bør være informeret på forhånd om dette (behandling af oplysninger om dem), som en del af opfyldelsen af oplysningspligten efter databeskyttelsesforordningens artikel 13 og 14. Formålet er jo at undgå misbrug og ikke at "fange" medarbejdere i at begå fejl/misbrug.

Hvis man vælger at konfrontere brugerne med indhold fra loggen, bør det ske kort tid efter, at de loggede handlinger er udført, så man med rimelighed kan forvente, at brugeren kan huske og dermed begrunde sine handlinger.

Stikprøverne kan anvendes som en kontrol af, om der til stadighed logges som forventet og, at logdata gemmes længe nok, og kan tolkes med den aktuelle vejledning. Det er altså en afprøvning af en etableret foranstaltning, og dermed omfattet af databeskyttelsesforordningens artikel 32, stk. 1 litra d. Se foranstaltningen *Logning af brugernes anvendelser af personoplysninger*.

Grundlag for vurdering af nødvendighed

Det er primært en risikovurdering efter databeskyttelsesforordningens artikel 32, som skal vise, om denne foranstaltning er relevant, idet risici er meget afhængige af, hvilke behandlinger af personoplysninger der sker i forskellige it-systemer.

[Datatilsynets praksis: Under den tidligere persondatalovgivning blev der etableret en praksis, hvor brede adgange – dvs. mange personers adgang til mange særligt beskyttelsesværdige personoplysninger om mange individer – skulle logges og der skulle foretages stikprøve i disse. Det gjaldt fx i borgerservicecentre og i sundhedssektoren, hvor der er brede adgange, og derfor var det svært at undgå at mange havde adgang til mange data, de normalt ikke har brug for. Kravet om stikprøver var en delvis kompensering for dette.]

Stikprøver i log over brugeradministrators handlinger

Med det i mente, at fokus skal være på misbrug af brugeradministrators adgangsrettigheder: Se foranstaltningen *Stikprøver i log over brugernes anvendelser af personoplysninger*.

Kommentar [F34]: Som tidligere kommenteret bør kontrollen i videst muligt omfang generere alarmer på baggrund af regler, da omfanget af logningsdata oftest er omfangsrigt.

Kommentar [F35]: Vil derfor mest hensigtsmæssigt kunne ske via automatikker.

Kommentar [F36]: Det bør tydeliggøres, at der ikke længere gælder et krav om logning – men at det blot kan være hensigtsmæssigt.

Styring af fysiske adgange

Dette er en forebyggende foranstaltning, som mindsker sandsynligheden for misbrug, ved at besværliggøre fysisk adgang til dokumenter, it-systemer og computernetværk. Det skal dog være afstemt med andre mulige foranstaltninger, mod omgåelse af fysiske adgangsbegrænsninger, fx vagter, forstærkede døre, indbrudsalarmer, bevægelsessensorer, alarm ved manglende dørlukning, personsluser, m.v.

Kravene til at opnå adgang til et it-system er ofte mindre inden for en fysisk ramme (fx en kontorbygning), end udenfor. Et login er derfor ofte mere kompliceret, når adgangen skal etableres fra en fjernarbejdsplads end når man foretager login fra en kontorarbejdsplads. Alternativt kan fjernadgangen være mere begrænset.

Der kan endvidere være elektroniske adgange, som af sikkerhedsmæssige årsager kun er mulige at opnå inden for en bestemt fysisk ramme. Derfor kan fysiske adgangsrettigheder være en vigtig del af beskyttelsen af personoplysninger – både dem der opbevares elektronisk og dem på papir.

Forslag til implementering

Central brugeradministration koblet til et HR-system samt rollebaserede adgange er den afgørende implementering her.

Følgende angår som udgangspunkt beskyttelse af datas fortrolighed. Beskyttelse af integritet eller tilgængelighed kan kræve væsentlig anderledes foranstaltninger.

Personalet i en reception kan stoppe uvedkommende og receptionister er instrueret i, hvordan der reageres på personer, som ikke normalt har adgang (folk der påstår at have et ærinde, som håndværkere, it-supportere, mv.), i hvilken grad personerne skal identificeres, om de fx skal have ledsaget indgang, mv. Gæsters adgang gennem en reception registreres.

Hvis ikke receptionspersonalet kan forventes at kende alle medarbejdere er det antageligt mere sikkert at anvende personlige adgangsmedier, så som elektronisk adgangskort kombineret med personlig kode, hvor kort og kode tildeles, registreres og spærres efter samme principper, som bruger-id og adgangskode til et login på et it-system.

Hvis man har lokaler med fysisk adgang til et it-miljø (krydsfelter og maskinstuer), indebærer denne adgang ofte muligheden for at omgå den elektroniske adgangsbegrænsning og dermed den elektroniske rettighedsstyring. Sådanne lokaler skal have en særlig fysisk begrænsning, og der skal overvejes indbrudssikrede døre, automatisk dørlukker med alarm ved manglende lukning, sikre nøglesystemer (dirkesikre, kopibeskyttede), alarmer, bevægelsessensorer, seismiske detektorer, mv.

Adgang til fysiske dokumenter på fx kontorer kan begrænses ved sikringsskabe fæstnet til fast bygningsdel. Nøgle/koder til skabet administreres efter samme principper som den elektroniske rettighedsstyring. Dog skal indbrudstiden i et skab være afpasset til hvor lang tid, der kan gå før en alarm/vagt afbryder tyven i sit arbejde. Printere placeres, hvor der kun er adgang for medarbejdere, og der kan i tilgift til dette anvendes løsninger, som kun printer, når rette bruger står ved printeren.

Grundlag for vurdering af nødvendighed

Det er primært en risikovurdering efter artikel 32, som skal vise, om denne foranstaltning er relevant, idet risici og muligheder er meget afhængige af de konkrete forhold.

Det er i høj grad et samspil mellem foranstaltninger, som danner et tilstrækkeligt sikkerhedsniveau. Hvis fx adgang til it-systemer fra kontoret sker på samme måde og med samme høje sikkerhedsniveau, som når medarbejderen arbejder hjemmefra, så er databeskyttelse ikke umiddelbart et argument for særlig fysisk

Kommentar [F37]: Indsat forslag til tekst.

Kommentar [F38]: Handler foranstaltningen ikke netop om at hindre tilgængeligheden?

sikkerhed på kontoret. Andre foranstaltninger kan også drastisk mindske behovet for fysisk sikkerhed, fx kryptering af datamedier.

Artikel 25. Ved erhvervelse af nyt it-system eller udvikling/ændring i eksisterende it-system skal databeskyttelse være tænkt ind i design og standardindstillinger. Systemer til fx adgangskort skal dermed også udvælges efter, om de kan minimere adgang til personoplysninger, fx ved at kunne differentiere mellem adgang til serverum, kontor, kundebetjeningsområde, printerrum, mv.

Tilpasning af adgangsrettigheder ved ændring af ansættelse

Dette er en forebyggende foranstaltning, som kan mindske sandsynligheden for den retmæssige brugers og andres misbrug af adgangsrettigheder.

Forslag til implementering

Central brugeradministration koblet til et HR-system, samt rollebaserede adgange er den afgørende implementering her.

Via procedurer eller teknik kan organisationen påtvinges en reaktion, når der sker ændringer i ansættelsesmæssige forhold, så som ansættelse, ændrede arbejdsopgaver, orlov, fratrædelse, langtidssygdom og død. Ændringer i ansættelsesforhold kan "hejse et flag" fx via et HR-system, men alternativt, skal der være en fast procedure, der påbegynder nedlæggelsen af unødvendige brugerrettigheder. Processen skal sikre samme høje fokus på nedlæggelse af eksisterende rettigheder, som på oprettelse af nye.

Nogle ændringer i ansættelsesforhold kræver, at der på forhånd er sat et tidspunkt for, hvornår der skal "hejses et flag" og en særlig proces startes – det gælder fx hvis en sikkerhedsgodkendelse automatisk udløber efter x år, med deraf følgende manglende godkendelse til at tilgå visse særligt klassificerede data.

Ved intern rokering, kan arbejdsopgaver ændres gradvist. I denne situation, er der en procedure eller automatik, som sikrer, at man ikke glemmer at lukke adgange, når de ikke længere er nødvendige.

Endeligt kan det være nødvendigt med særlige procedurer for perifere/eksterne systemer, der ikke kan lukkes gennem en centraliseret brugeradministration.

En bruger-konto, der ikke længere anvendes af den retmæssige bruger, kaldes også for "ghost account", og selv om den retmæssige bruger forhindres i at anvende den, fx ved spærring af brugeren i Active Directory, så kan adgangen måske stadig misbruges. Nedlæggelse af sådanne bruger-konti reducerer angrebsfladen idet hackere, som har opnået en vis adgang på netværk/it-systemer, forhindres i at anvende en "ghost account" til at udvide deres adgang. Endvidere kan misbrug af "ghost accounts" muligvis foregå i længere tid, uden at det opdages, end de konti, som stadig anvendes af den retmæssige bruger.

Når adgangsrettigheder skal fjernes, skal følgende overvejes:

- Medarbejderen skal evt. selv lukke adgange i eksterne it-systemer, som det ellers vil være sværere for andre at lukke efter fratrædelse eller overgang til anden stilling.
- Medarbejdere med administrative rettigheder, masterkoder og lignende skal evt. selv overdrage disse til en anden medarbejder.
- Sletning af data på pc/smartphone inden aflevering og evt. nulstilling eller udlevering af kode så udstyr kan genanvendes.

Kommentar [F39]: Hvad menes der?

Kommentar [F40]: Indsat forslag til tekst.

Kommentar [F41]: Hvad er det?

- Oprydning på e-mailkonto, netværksdrev og især på steder, hvor kun denne medarbejder havde adgang, eller oprydning i private data, så kontoens indhold kan gøres tilgængelig for andre efter fratrædelsen.
- Lukning af adgange på it-systemer, funktionspostkasser, eksterne it-systemer.
- Inddragelse af id-kort, nøglebrik, nøgler til døre/postkasser/racks/..., adgangsgivende tokens, pc, smartphone, tastatur, skærm, mus, stol, bord, fysiske dokumenter, mv.
- Ændring af koder som er delt mellem flere brugere (fælles-login).
- Spærring af adgange via nøglebrikker, adgangskort fysiske adgangs-/alarmpaneler, sikringsskabe/pengeskabe.
- Udskiftning/omkodning af låsecylindre (hvis ikke nøgle er kopibeskyttet).
- Spærring af fjernadgang til it-systemer.
- Spærring af certifikater (NemID, MitID, certifikater knyttet til hardware, ...).
- Ophævelse af telefonabonnement, internetabonnement og medlemsskaber gennem virksomheden.
- Sletning af data om medarbejder, der ikke længere er nødvendige, fx foto brugt til id-kort eller telefonbogsoplysninger på intranettet.
- Interne kontaktlister opdateres og eksterne samarbejdspartner informeres om ændring i kontaktpunkter (kunder, vagtselskab, håndværkere, ...), især hvis medarbejder fortsat kan anvende telefonnummer efter fratrædelse.
- Revision af beredskabsorganisation, hvis medarbejderen var med i denne.
- Det overvejes, om der opstår afhængighed af enkeltpersoner, grundet at færre nu har de adgange som denne bruger havde.

Kommentar [F42]: Disse kan/skal vel ikke spærres?

Grundlag for vurdering af nødvendighed

Artikel 5, stk. 1, litra f, især "uautoriseret og ulovlig behandling". Lukning af adgange mindsker muligheden for ulovlig behandling, hvilket kan være særligt vigtigt i situationer, hvor en medarbejder afskediges. En risikovurdering kan dog vise at foranstaltningen ikke er nødvendig, hvis brugeradgange fx kun er til offentligt tilgængelige personoplysninger, og misbrug i form af ændring/sletning af disse oplysninger ikke kan skade de registrerede.

Ændringsstyring (Change Management)

Kommentar [F43]: Denne foranstaltning har ikke med rettighedsstyring at gøre og foreslås derfor slettet.

Dette er en foranstaltning, som kan hjælpe på mange udfordringer omkring it-sikkerhed. Det handler om, at ændringer i it-miljøer, software, organisationen, forretningsprocesser, mv. skal styres efter fastlagte principper.

Forslag til implementering

Foranstaltningen skal minimere sandsynligheden for fejl ved overgangen til et nyt it-system, ny organisation, mv. Hvis fejl opstår, skal der være en plan for at håndtere konsekvenserne.

Decentral rettighedsstyring kan foregå indenfor en meget lille gruppe personer, og være ukendt af resten af organisationen. Om det foregår, skal derfor afdækkes, inden man begynder at ændre i it-systemet.

Hvis der anvendes RPA (Robotic Process Automation) eller lignende, kan ændringsstyring sikre at robot-brugerens adgangsrettigheder stadig er aktuelle, eller om de skal begrænses.

Ændringsstyringen omfatter kontroller af, om eksisterende foranstaltninger videreføres ved systemændring. Fx:

- Det kontrolleres om der foregår logning i it-systemet (som skal ændres). Hvis der gør testes det umiddelbart efter ændringen, at der stadig logges som forventet og, at logdata gemmes længe nok, og kan tolkes med den aktuelle vejledning eller et dertilhørende it-system. Ellers kan en systemændringen underminere foranstaltninger som *Logning af brugernes anvendelser af personoplysninger* og *Logning af brugeradministrators handlinger*.
- Det kontrolleres om it-systemet (som skal ændres) omfatter områder med begrænset adgang. Hvis det gør, sikres der videreføring, nedlæggelse eller centralisering af rettighedsstyringen. Hvis det videreføres, bliver det testet umiddelbart efter ændringen, om adgangsbegrænsningen stadig fungerer efter hensigten.
- Ved integration mellem it-systemer, og særligt udveksling af data, er det afdækket, om
    - opdateringsfrekvensen er tilstrækkelig,
    - om der overføres tilstrækkeligt med data,
    - om data anvendes til formål, som passer til, hvor data hentes fra (anvendelse er afpasset formålet med registreringen),
    - osv.,

  og det ses i forhold til, hvad der skal til, for at undgå, at ændringer i integrationen medfører ændringer i adgangsrettigheder.

Grundlag for vurdering af nødvendighed

Ændringsstyring er altid relevant. Hvad den bør indeholde er en konkret vurdering i din organisation.

Artikel 25. Ved erhvervelse af nyt it-system eller udvikling/ændring i eksisterende it-system skal databeskyttelse være tænkt ind i design og standardindstillinger. Ændringsstyring kan netop sikre, at dette sker.