Styr på rettighedsstyring

Vejledning om adgangsrettigheder

December 2023

DATATILSYNET

Indhold

1. Introduktion

Hvad betyder rettighedsstyring i praksis? En analogi til flyrejser forklarer, hvad begrebet betyder i den fysiske verden.

For at forstå alle aspekterne i rettighedsstyring kan man lave en analogi til den fysiske verden. Sikkerheden ved at rejse med fly kan blive kompromitteret, hvis ikke det foregår efter strikse principper. Derfor skal en person, der ønsker at gå ombord, først autoriseres til dette gennem et boardingpas.

Et boardingpas giver en meget begrænset adgang for én specifik fysisk person til ét specifikt fly på én specifik afgang. Passageren har ikke adgang til hele flyet, men kun kabinen, og har dermed ikke mulighed for at styre flyet. Autorisationen (boardingpas) er desuden tidsbegrænset.

Beskyttelse af personoplysninger kræver, at der anvendes lignende strikse principper. Her beskrives et eksempel sammenholdt med anvendelse af boardingpas:

EN PASSAGERS ADGANG TIL ET FLY	EN MEDARBEJDERS ADGANG TIL PERSONDATA I ET IT-SYSTEM
Boardingpas kan udelukkende udstedes af det respektive flyselskab.	Autorisationer kan udelukkende udstedes af en autorisationsansvarlig, f.eks. medarbejderens nærmeste leder eller systemejeren.
Passageren får kun adgang til flyet, hvis vedkommende har et boardingpas.	Medarbejderen får kun adgang til data, hvis vedkommende er blevet autoriseret til adgangen.
Passageren får kun adgang til et specifikt fly på en specifik afgang, der opfylder et specifikt rejsebehov.	Medarbejderen får kun adgang til specifikke data, i et specifikt it-system, hvor adgangen er nødvendig for, at han/hun kan udføre sine arbejdsopgaver.
Passagerens adgang begrænses til kabinen, fordi det er nok til at opfylde rejsebehovet. Passageren får ikke en adgang, der giver mulighed for at styre flyet (cockpit).	Medarbejderen får kun adgang til at foretage den type behandling af data, som er nødvendig for at han/hun kan udføre sine arbejdsopgaver, f.eks. ved at medarbejderen kun får læseadgang, og dermed ikke kan redigere i data.
Adgang til cockpit gives ikke, fordi det indebærer særlige risici og kræver særlig viden og erfaring.	Autorisationer gives kun, når brugeren har den rette viden og erfaring til at undgå de særlige risici, som adgangen repræsenterer.
Passageren kan ikke komme tilbage ind i flyet, efter det er landet, fordi det specifikke rejsebehov er ophørt.	Medarbejderen adgang til data lukkes, når den ikke længere er nødvendig for at han/hun kan udføre sine arbejdsopgaver.
Når passageren har forladt flyet efter endt rejse, kan det udstedte boardingpas ikke genanvendes.	Når adgangen til data er lukket, kan autorisationen ikke genanvendes, hvilket sikrer, at adgangsbehov genvurderes ifm. ny autorisering.

2. Rettighedsstyring – hvem skal have adgang?

Dette kapitel beskriver, hvad rettighedsstyring er, hvorfor det er vigtigt, og hvordan et katalog med tekniske og organisatoriske foranstaltninger kan bruges til at håndtere de væsentligste risici.

2.1 Hvorfor er rettighedsstyring vigtigt?

Effektiv rettighedsstyring er afgørende for informationssikkerheden i din organisation. Ligesom du holder styr på, hvem der har nøgle til dit hjem, og hvem der skal have nøglen til dit arkivskab, skal du holde styr på, hvem der har adgang til dine systemer og til hvilke oplysninger – og du skal sikre, at de ved, hvordan oplysningerne skal behandles. Det er vigtigt for persondatasikkerheden for medarbejdere, kunder og for borgere, men det er også med til at beskytte din forretning.

I denne vejledning anvendes begrebet rettighedsstyring som et overordnet begreb, som omfatter det at styre, hvem der har adgang til organisationens it-systemer og lokaler, samt hvad de enkelte brugere kan anvende deres adgange til.

Databeskyttelsesforordningen (GDPR) indeholder regler om behandlingssikkerhed samt databeskyttelse gennem design og standardindstillinger. Disse regler benytter en risikobaseret tilgang til sikkerhed, hvor et passende sikkerhedsniveau etableres ved hjælp af ”passende tekniske og organisatoriske foranstaltninger”.

Styring af brugeres adgange til data er en så basal del af informationssikkerhed – og dermed også behandlingssikkerhed inden for databeskyttelse – at det kan læses direkte ud af principperne i databeskyttelsesforordningens artikel 5, stk. 1, litra f.

Databeskyttelsesforordningens artikel 5, stk. 1, litra f.

Personoplysninger skal behandles på en måde, der sikrer tilstrækkelig sikkerhed for de pågældende personoplysninger, herunder beskyttelse mod uautoriseret eller ulovlig behandling og mod hændeligt tab, tilintetgørelse eller beskadigelse, under anvendelse af passende tekniske eller organisatoriske foranstaltninger (»integritet og fortrolighed«).

Når det er en så basal del af informationssikkerhed, betyder det, at god rettighedsstyring beskytter forretningsdata såvel som personoplysninger, og det kan beskytte datas fortrolighed, såvel som deres integritet og tilgængelighed. Det ses også af eksemplerne på virkelige sikkerhedsbrud beskrevet senere i vejledningen. Denne vejledning anviser dig muligheder for at undgå de situationer, der kan lede til sikkerhedsbrud.

2.2 Hvem skal have styr på rettighedsstyring?

Det korte svar er, at det skal alle, der anvender it-systemer, som indeholder personoplysninger. Databehandlere, som drifter it-systemer, skal også have styr på kravene og kan selvstændigt pådrage sig ansvar.

- **Ledelsen**. Det er ledelsens ansvar at sikre, at der arbejdes aktivt med rettighedsstyring – især autorisering og brugeradministrering – i organisationen gennem etablering af fornødne procedurer og tildeling af tilstrækkelige ressourcer til en effektiv opgaveløsning.

- **DPO (*Data Protection Officer*, databeskyttelsesrådgiver).** Som DPO skal du overvåge og rådgive om beskyttelsen af personoplysninger i din organisation, fx om der er etableret passende procedurer og tekniske foranstaltninger mod uautoriseret eller ulovlig adgang til personoplysninger[1].

- **Medarbejdere med ansvar for it-sikkerhed.** Det er en helt grundlæggende del af opgaven med it-sikkerhed at sikre, at der effektivt tages stilling til og løbende føres kontrol med, at adgangsrettigheder til it-systemer og personoplysninger passer til det arbejdsmæssige behov, og at rettighederne ikke skaber unødige muligheder for misbrug.

- **Medarbejder uden ansvar for it-sikkerhed.** Det er ikke enhver medarbejders overordnede ansvar, at der er styr på rettighedsstyringen i organisationen – men alle ansatte har et medansvar i forhold til deres egne rettigheder. Enhver bør være opmærksom på, om man har de rigtige rettigheder.

2.3 Katalog med relevante foranstaltninger

Denne vejledning suppleres af et katalog, der beskriver tekniske og organisatoriske foranstaltninger, som er relevante at overveje for at sikre en god og ansvarlig rettighedsstyring i overensstemmelse med princippet om at etablere et tilstrækkelig personoplysningssikkerhed, og tager særligt udgangspunkt i kravene efter databeskyttelsesforordningens artikel 32. Du finder kataloget her.

Databeskyttelsesforordningens artikel 32, stk. 1

Under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder gennemfører den dataansvarlige og databehandleren passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til disse risici, herunder bl.a. alt efter hvad der er relevant:

a) pseudonymisering og kryptering af personoplysninger
b) evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester
c) evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse
d) d) en procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed.

Kataloget fungerer som et opslagsværk. For hver foranstaltning er der angivet risici, som foranstaltningen er rettet imod, samt implementeringsforslag. Endvidere er der en vejledning til vurdering af foranstaltningens relevans. Foranstaltningerne i kataloget er bl.a. baseret på

[1] Databeskyttelsesforordningens artikel 39, stk. 1, litra b, samt artikel 5, stk. 1, litra f.

Datatilsynets erfaringer fra tilsyn i private og offentlige virksomheder, brud på persondatasikkerheden anmeldt til Datatilsynet, EDBP's retningslinjer om artikel 25[2], samt ISO-standarderne 27001[3] og 27002. ISO-standarderne er internationale standarder for informationssikkerhed, som følges af de fleste offentlige myndigheder og mange private virksomheder, og som er udtryk for et internationalt anerkendt niveau for sikkerheden ved anvendelse af informationsteknologi.

[2] 4/2019 om artikel 25 – Databeskyttelse gennem design og databeskyttelse gennem standardindstillinger – Version 2.0

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

3. Skab overblik og vurdér risici ved din behandling af personoplysninger

En vigtig forudsætning for fyldestgørende rettighedsstyring er et fuldt overblik over it-miljøet.

Inden for it-sikkerhed handler rettighedsstyring typisk om foranstaltninger, der styrer *tildeling, ændring* og *fratagelse af* rettigheder i de it-systemer, man anvender i sin organisation. Databeskyttelsesforordningen vedrører dog også fysiske dokumenter/registre, som indeholder personoplysninger. Foranstaltninger har ofte form af interne politikker, procedurer og retningslinjer, men kan også være tekniske tiltag, der enten erstatter behovet for procedurer eller understøtter disse.

Når du skal vurdere, hvilke foranstaltninger det giver mening at implementere, og om det er din egen organisation eller en ekstern leverandør, der skal udføre det, er det en hjælp, hvis der er overblik over det samlede it-miljø. Hvis man ikke har helt styr på dette allerede, kan det være en proces, der skal igangsættes sideløbende med etablering af foranstaltninger vedrørende rettighedsstyring. Det kan tage lang tid at få det fulde overblik over it-miljøet.

Overblikket kan fx fortælle dig, hvad der skal til for at kunne lukke adgange hurtigt, når det er aktuelt, dvs. om der findes decentral rettighedsstyring udført af egne medarbejdere, eller om adgange skal lukkes via en ekstern databehandler. Risici ved decentral rettighedsstyring kan ses af nogle af eksemplerne på sikkerhedsbrud, som er beskrevet senere, og ved at læse om den afhjælpende foranstaltning "Centraliseret rettighedsstyring" i kataloget over foranstaltninger.

Både overblikket over it-miljøet og eksisterende foranstaltninger kan evt. allerede være afdækket gennem organisationens efterlevelse af reglen i databeskyttelsesforordningens artikel 30 angående "fortegnelse over behandlingsaktiviteter". Hvis organisationen skal efterleve it-sikkerhedsstandarden ISO 27001, så kan der allerede være etableret en oversigt over såkaldte ”aktiver”, herunder data, men en fortegnelse efter artikel 30 er dog mere konkret ift., hvad der skal fremgå angående behandlingen af personoplysninger. Det vil typisk være it-afdelingen, som fører fortegnelser over aktiver som led i deres efterlevelse af relevante it-sikkerhedsstandarder.

Visse tekniske og organisatoriske foranstaltninger kan blive implementeret via de værktøjer, der kan anvendes til brugeradministrering. Identity Access Management (IAM) og Privileged Access Management (PAM) er typer af systemer, som kan automatisere foranstaltninger angående rettighedsstyring.

Denne vejledning er en hjælp til at håndtere de mest gængse sikkerhedstrusler og problemstillinger i relation til rettighedsstyring i din organisation. Alle sikkerhedskrav efter databeskyttelsesforordningen forudsætter, at det er vurderet, hvilke trusler en behandling er udsat for, og hvilke risici dette udgør for personoplysningssikkerheden.

Databeskyttelsesforordningens artikel 32, stk. 2

Ved vurderingen af, hvilket sikkerhedsniveau der er passende, tages der navnlig hensyn til de risici, som behandling udgør, navnlig ved hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.

Vejledningen giver dig relevante input til din organisations risikovurdering med beskrivelser af relevante risikoscenarier og anbefalinger af mulige tekniske og organisatoriske foranstaltninger, som vil kunne mindske disse risici.

Vurderingen af, hvilket sikkerhedsniveau som kan anses for passende i netop din organisation, kræver dog en konkret risikovurdering efter databeskyttelsesforordningen, som ikke er temaet for denne vejledning.

4. Centrale begreber

Her får du en kort forklaring af de begreber, der er mest væsentlige at kende til, når man arbejder med rettighedsstyring.

Registrerede: De fysiske personer, hvis personoplysninger er genstand for en behandling.

Autorisation: Fuldmagt, godkendelse – udstedt af en autoritet, fx en leder eller systemejer.

At autorisere: At bemyndige, godkende.

Uautoriseret adgang: En adgang, som ikke er autoriseret (godkendt). Det kan fx opstå, hvis:

- En autorisation udløber, uden at adgangen lukkes.
- Der ved en fejl gives adgang til alle ansatte i stedet for kun de ansatte, som er autoriserede.
- Der ved en fejl lægges data på internettet – hvorved reelt alle internetbrugere får uautoriseret adgang.
- En hacker misbruger svagheder i et it-system og derved opnår adgang til data.

Bemærk, at det er uafhængigt af, om adgangen er anvendt eller ej. En person kan altså have haft uautoriseret adgang til data uden at denne person nogensinde har tilgået de data, som der var adgang til.

Autorisationsansvarlig: En person, som er udpeget til at kunne autorisere og dermed godkende andres adgange til fx it-systemer og software. Dette kan fx være nærmeste leder, hvis vedkommende er den bedste til at vurdere, hvilke adgangsrettigheder medarbejderne har behov for. Men det kan også være personer med titlen "systemejer" (fagchefer), og disse kan have et mere sikkerhedsrettet fokus end nærmeste leder.

Brugeradministrator: En person, som er udpeget til at tildele andre personer adgang og rettigheder i ét eller flere it-systemer eller fysiske adgangsmedier, hvor denne tildeling sker på baggrund af en autorisation.

Brugeradministrering: Brugeradministrering er en proces, der ofte i vidt omfang består af organisatoriske foranstaltninger, som skal sikre, at kun de rigtige personer har en nøgle til døren, en adgangskode til it-systemet, osv. Men der kan også være tekniske foranstaltninger, der hjælper brugeradministratoren igennem processen, forhindrer fejl, samt dokumenterer, at opgaver er udført i henhold til anmodninger/godkendelser fra en autorisationsansvarlig.

Adgangsrettigheder: Personers adgange til fysiske og elektroniske aktiver (it-systemer, data, fysiske lokaler, mv.), og hvad brugerne kan med disse adgange (læse, ændres, slette, mv.).

Foranstaltning: Tiltag, der bevarer og/eller ændrer en risiko. En foranstaltning kan være forebyggende, opdagende, korrigerende eller en kombination af disse.

Tekniske foranstaltninger med relevans for rettighedsstyring er fx it-løsninger til brugeradministrering, automatisk kryptering/sletning, automatisk adgangskontrol (log-in), registrering af anvendelser af personoplysninger (logning), fysiske døre og låse.

Organisatoriske foranstaltninger med relevans for rettighedsstyring er fx sikkerhedspolitikker, procedure for jævnlig kontrol af adgangsrettigheder, procedure for inddragelse af adgangsrettigheder ved fritstilling og fratrædelse, opgavefordeling efter kompetencer, uddannelse i korrekt anvendelse af it-løsninger (altså kompetencer), vurdering og evaluering af effektiviteten af tekniske og organisatoriske foranstaltninger.

I standarder og lærebøger kan foranstaltninger være opdelt i yderligere kategorier, fx "fysiske", "personrelaterede" eller "adfærdsmæssige". Imidlertid beskriver databeskyttelsesforordningen

kun kategorierne "tekniske" og "organisatoriske", så eksemplerne herover dækker det hele. Når der står fx "fysiske låse" kan dette betegnes som en fysisk foranstaltning, men også som endnu en teknisk foranstaltning. Uddannelse kan betegnes som en personrelateret eller adfærdsmæssig foranstaltning, men også som endnu en organisatorisk foranstaltning.

5. Hvor galt kan det gå?

Her kan du læse nogle konkrete eksempler på, hvad konsekvensen af utilstrækkelig rettighedsstyring kan være.

Danmark er et af de mest digitaliserede lande, og store dele af den offentlige forvaltning behandler næsten udelukkende oplysninger om borgerne digitalt. Det er effektivt og fleksibelt, men åbner for flere muligheder for fejlhåndtering og misbrug. Selv om fejl ikke kan undgås, kan risikoen nedbringes ved blandt andet at have styr på rettighedsstyring.

Rettighedsstyring handler ikke om, at medarbejdere er utroværdige og derfor skal begrænses mest muligt i deres adgange til it-systemer. Men mennesker begår fejl, og medarbejdere er bare mennesker. Eksemplerne herunder viser dog også, at man ikke kan se bort fra, at nogle mennesker bliver fristet til misbrug, alene ved at de får adgang til data, og at god rettighedsstyring samtidig er med til at beskytte mod eksterne trusler.

5.1 Manglende adgangsbegrænsning

Her påvirkes borgernes rettigheder direkte gennem manglende fortrolighed.

En medarbejder opsætter en mappe på et serverdrev og placerer nogle fortrolige kundedata eller HR-oplysninger, som kun skal kunne ses af særligt udvalgte HR-medarbejdere. Manglende viden om eller opmærksomhed på korrekt opsætning af adgangsrettigheder indebærer, at uautoriserede personer kan tilgå de fortrolige oplysninger.

Et andet eksempel er udskiftning af eller ændringer på en server uden sikring af, at den aktuelle adgangsbegrænsning aktivt videreføres ved ændringen, hvilket skaber uautoriseret adgang. Den manglende videreføring kan f.eks. skyldes manglende viden om den pågældende adgangsbegrænsning eller manglende test.

Mangler i adgangsbegrænsning kan ske på grund af fejl og manglende test, eller fordi ændringsbegrænsningen er lavet autonomt af en medarbejder eller enhed uden styring fra centralt hold. Konsekvensen er typisk, at mange eller alle medarbejdere via det interne netværk – eller hele verden via internettet – får uautoriseret adgang til beskyttelsesværdige personoplysninger.

Der går ofte meget lang tid, nogle gange flere år, inden denne type brud på persondatasikkerheden opdages, fordi de autoriserede brugere ikke bemærker, at andre end de relevante har adgang.

Relevante foranstaltninger

- Centraliseret rettighedsstyring
- Sammenhæng mellem brugerkompetencer, adgangsrettigheder og opgaver
- Ændringsstyring (Change Management)

5.2 Ransomware – når data holdes som gidsel

Her påvirkes borgernes rettigheder direkte gennem manglende tilgængelighed til personoplysninger og ofte også manglende fortrolighed.

Begrænsning af adgangsrettigheder kan evt. forhindre et succesfuldt ransomware-angreb, da hackere ofte har brug for at opnå særlige rettigheder i it-systemerne for at kunne udføre angrebet. Hvis angrebet alligevel er succesfuldt, kan begrænsede adgangsrettigheder mindske skaden ved angrebet, fordi angrebet derved kan nå færre it-systemer.

I de seneste år er flere og flere organisationer blevet ramt af ransomware. Der er tale om ondsindede angreb, hvor hackere udnytter sårbarheder i it-systemer eller snyder medarbejdere gennem phishing eller anden form for 'social engineering' for at opnå adgang til data på it-systemerne, kryptere data, og forlange løsepenge for at dekryptere dem. Ofte sker det først efter, at data er udtrukket af it-systemerne, og hvis løsesummen ikke betales, kan der i stedet afpresses under trussel om at offentliggøre data. Der ses også flere og flere eksempler på, at data sælges videre af hackerne og derefter anvendes til svindel og identitetsmisbrug til skade for de berørte personer – eller at personerne, hvis oplysninger er berørt, selv bliver udsat for afpresning.

Mange foranstaltninger er relevante for at opbygge et tilstrækkeligt forsvar mod ransomware-angreb – især backup af it-systemer/data og forsvar mod cyberangreb. Uanset om man har en god backup – og dermed er i stand til at reetablere sine it-systemer og data – så beskytter det ikke imod misbrug af de udtrukne data. Meget af udgiften ved et ransomware-angreb ligger desuden i reetableringen af it-systemerne via backup.

Det er dog vigtigt at bemærke, at foranstaltningerne beskrevet i denne vejledning ikke kan stå alene, når det angår beskyttelse mod ransomware. Se også vejledninger om ransomware fra Center for Cybersikkerhed[4].

Relevante foranstaltninger

- Centraliseret rettighedsstyring
- Dataadgang efter behov
- Adgangsrettigheder efter behov
- Minimering af privilegerede adgangsrettigheder
- Automatisk lukning af inaktive adgange
- Håndtering af midlertidige brugerkonti
- Awareness
- Funktionsadskillelse
- Undgå kopiering af adgangsrettigheder uden aktiv stillingtagen
- Undgå genanvendelse af autorisation uden aktiv stillingtagen
- Periodisk kontrol af adgangsrettigheders aktualitet
- Pseudonymisering, anonymisering
- Tilpasning af adgangsrettigheder ved ændring af ansættelsesforholdet
- Backup

5.3 Når manglende instruktion eller it-kompetencer fører til fejl

Her påvirkes borgernes rettigheder direkte gennem manglende fortrolighed.

Pædagoger på en daginstitution får tildelt adgangsrettigheder til at arkivere breve med følsomme personoplysninger i kommunens ESDH-system. Betydningen af et "flueben" bliver misforstået og fører til, at breve utilsigtet bliver sat til automatisk offentliggørelse i en postliste på kommunens hjemmeside. Derved får uvedkommende uautoriseret adgang til indholdet i brevene. Problemet i denne type sikkerhedsbrud er, at der uddelegeres opgaver, uden at man forudgående sikrer sig sammenhæng mellem brugers kompetencer, tildelte adgangsrettigheder og opgaver. Forsøg på smidiggørelse af processer eller besparelse på administrative omkostninger sker på bekostning af persondatasikkerheden.

Da brugeren ikke selv har forudsætning for at opdage fejlen, kan der ved denne type brud på persondatasikkerheden gå lang tid, inden fejlen konstateres.

Relevante foranstaltninger

- Sammenhæng mellem brugerkompetencer, adgangsrettigheder og opgaver

[4] https://www.cfcs.dk/globalassets/cfcs/dokumenter/vejledninger/cfcs-ransomware-vejledning-.pdf
https://www.cfcs.dk/globalassets/cfcs/dokumenter/2021/varsel-om-forebyggelse-af-ransomware.pdf

- Awareness

5.4 Misbrug af superbrugerrettigheder

Her påvirkes borgernes rettigheder ikke direkte, men indirekte i kraft af afledte konsekvenser.

En offentlig styrelse bliver udsat for svindel i millionklassen gennem misbrug af tilskudsmidler. Svindlen var mulig pga. en enkelt medarbejders misbrug af tildelte "superbrugerrettigheder", der bl.a. gør det muligt at frakoble alarmer og gå ind i mange forskellige systemer og sætte godkendelsesprocedurer og andre foranstaltninger ud af kraft. Sagen kan fx have haft afledte menneskelige konsekvenser, hvis værdige modtagere gik glip af et offentligt tilskud. Sagen er et eksempel på, at tildeling af mange rettigheder uden effektive kontrolforanstaltninger kan udgøre en sårbarhed, der let kan udnyttes.

Relevante foranstaltninger

- Minimering af privilegerede adgangsrettigheder
- Funktionsadskillelse
- Centraliseret rettighedsstyring
- Adgangsrettigheder efter behov
- Logning af brugeradministrators handlinger

5.5 Manglende lukning af adgang ved off-boarding

Her påvirkes de registreredes rettigheder i den fysiske verden.

En kommune anvender vikarer til sundhedspleje, men disse vikarers adgang bliver ikke lukket, når deres arbejde for kommunen ophører. Adgangene forbliver derfor åbne, også efter de har forladt vikarbureauet. Adgangene kan anvendes uden adgang til kommunens interne netværk (direkte via internettet).

En tidligere vikar udnytter adgangen til at tilgå borgeres personoplysninger, bl.a. oplysninger om, hvilken medicin der bliver doseret til borgerne. Flere af de pågældende borgere får efterfølgende stjålet deres medicin af den tidligere vikar. Konsekvensen for de berørte borgere kan dermed være målrettet indbrud/tyveri og akut mangel på nødvendig medicin.

Relevante foranstaltninger

- Automatisk lukning af inaktive adgange
- Centraliseret rettighedsstyring
- Håndtering af midlertidige brugerkonti
- Periodisk kontrol af adgangsrettigheders aktualitet
- Tilpasning af adgangsrettigheder ved ændring af ansættelsesforholdet

Undgå svage led – brug en kombination af foranstaltninger

Eksemplerne tager udgangspunkt i konkrete sikkerhedsbrud og angår både utilsigtede fejl og ondsindede handlinger. I begge tilfælde er de beskrevne foranstaltninger i denne vejledning relevante at forholde sig til.

Fælles for mange af de brud på persondatasikkerheden, som Datatilsynet tager stilling til, er, at de kun kan undgås gennem en kombination af flere foranstaltninger, som tilsammen etablerer et passende sikkerhedsniveau, fordi der ellers kan være et svagt led i "sikkerhedskæden", som kan udnyttes.

6. Gruppering af foranstaltninger efter opgaver i organisationen

Her finder du en oversigt over, hvilke foranstaltninger der kan være relevante i forskellige situationer på arbejdspladsen.

I nogle arbejdsmæssige situationer er det særligt relevant at skærpe opmærksomheden på autorisering og brugeradministrering for at etablere eller opretholde de foranstaltninger, der skal sikre god rettighedsstyring.

Nedenfor grupperes en række foranstaltninger i forhold til, *hvilken opgave* der skal udføres i organisationen.

Nogle gange bliver dele af opgaven med rettighedsstyring udført hos en leverandør (typisk en databehandler). Her kan organisationen ikke direkte styre, hvilke foranstaltninger der implementeres eller hvordan. I den situation kan de beskrevne foranstaltninger i stedet beskrives i en databehandleraftale, eller den dataansvarlige må på anden vis sikre sig, at god rettighedsstyring opretholdes. Se fx Datatilsynets vejledning om tilsyn med databehandlere[5].

6.1 Etablering af brugeradministration

På det tidspunkt, hvor organisationen etablerer en enhed, som får til opgave at styre adgangsrettigheder, dannes fundamentet for de principper, hvorefter man vil styre adgangsrettigheder. Derfor skal der på dette tidspunkt være gjort overvejelser om, hvilke procedurer, værktøjer, rollefordelinger osv. der skal anvendes for at sikre god rettighedsstyring.

Relevante foranstaltninger

- Funktionsadskillelse
- Minimering af antal autorisationsansvarlige og brugeradministratorer
- Centraliseret rettighedsstyring
- Rollebaserede adgangsrettigheder
- Undgå kopiering af adgangsrettigheder uden aktiv stillingtagen
- Undgå genanvendelse af autorisation uden aktiv stillingtagen
- Undgå unødvendig anvendelse af flerbrugerkonti
- Styring af fysiske adgange
- Awareness
- Dokumentation af autorisationer
- Automatisk lukning af inaktive adgange
- Håndtering af midlertidige brugerkonti

6.2 Personalemæssige ændringer i en organisation

6.2.1 Ny afdeling eller nye opgaver

Når medarbejdere skifter afdeling eller får nye arbejdsopgaver, og når nye medarbejdere onboardes, er der særlig grund til at være opmærksom på, om adgangsrettigheder skal ændres. Dette forudsætter, at man ikke kun har fokus på oprettelse af nye adgangsrettigheder, men også nedlæggelse af de eksisterende.

[5] https://www.datatilsynet.dk/Media/637710957381234368/Datatilsynet_Vejledning%20om%20tilsyn%20med%20databehandlere_oktober-2021.pdf

Relevante foranstaltninger

- Funktionsadskillelse
- Styring af fysiske adgange
- Tilpasning af adgangsrettigheder ved ændring af ansættelsesforholdet
- Dataadgang efter behov
- Adgangsrettigheder efter behov
- Sammenhæng mellem brugerkompetencer, adgangsrettigheder og opgaver
- Minimering af privilegerede adgangsrettigheder
- Awareness

6.2.2 Off-boarding

Ved off-boarding af medarbejdere i forbindelse med fratrædelse eller afskedigelse – herunder evt. fritstilling – skal der ske en lang række ting for at sikre inddragelse af adgangsrettigheder, og hurtig inddragelse kræver normalt, at man er forberedt.

Relevante foranstaltninger

- Styring af fysiske adgange
- Tilpasning af adgangsrettigheder ved ændring af ansættelsesforholdet

6.2.3 Andre former for permanent eller midlertidig fratrædelse

Orlov, barsel, sygemelding, fritstilling mv. er situationer, der i samme grad som fratrædelse skal ske med opmærksomhed på, hvilke adgangsrettigheder der bør inddrages eller midlertidigt deaktiveres.

Relevante foranstaltninger

- Styring af fysiske adgange
- Tilpasning af adgangsrettigheder ved ændring af ansættelsesforholdet

6.2.4 Midlertidig arbejdskraft

Ved engagering af ekstern/midlertidig arbejdskraft, fx konsulenter til softwareudvikling, vikarer mv. er der særlige forhold, som gør sig gældende, om end det meste kan foregå efter de samme principper som ved ansættelse:

Relevante foranstaltninger

- Håndtering af midlertidige brugerkonti
- Funktionsadskillelse
- Styring af fysiske adgange
- Tilpasning af adgangsrettigheder ved ændring af ansættelsesforholdet
- Dataadgang efter behov
- Adgangsrettigheder efter behov
- Sammenhæng mellem brugerkompetencer, adgangsrettigheder og opgaver
- Minimering af privilegerede adgangsrettigheder
- Awareness

6.3 Udvikling eller erhvervelse af nyt it-system eller udvikling/ændring i eksisterende it-system

Nyudvikling og erhvervelse af nye it-systemer eller væsentlige ændringer i eksisterende systemer med nye eller ændrede funktioner kræver, at der helt fra start fokuseres på rettighedsstyring. Følgende foranstaltninger bør overvejes implementeret i it-systemet.

Relevante foranstaltninger

- Funktionsadskillelse
- Centraliseret rettighedsstyring
- Rollebaserede adgangsrettigheder
- Undgå unødvendig anvendelse af flerbrugerkonti
- Styring af fysiske adgange

- Dataadgang efter behov
- Adgangsrettigheder efter behov
- Logning af brugernes anvendelser af personoplysninger
- Logning af brugeradministrators handlinger
- Pseudonymisering og anonymisering
- Automatisk lukning af inaktive adgange
- Ændringsstyring (Change Management)

6.4 Outsourcing af behandling af personoplysninger til databehandler eller aftale med ny databehandler

Hvis du overlader det til en databehandler at administrere dine it-systemer, så kan alle foranstaltningerne i kataloget potentielt være relevante. Det afhænger af, hvilke opgaver databehandleren udfører for din organisation. Krav til styring af adgangsrettigheder vil altid være relevante, og derfor er det relevant at overveje, hvilke foranstaltninger der skal kræves via databehandleraftaler eller andre kontrakter. Dette gælder særligt, hvis databehandleren skal styre adgangsrettigheder på it-systemer med personoplysninger, hvor din organisation er dataansvarlig for behandlingen af disse oplysninger.

Hvis du lader en databehandler styre adgangsrettigheder på dine vegne, har du stadig pligt til at sikre dig, at databehandleren lever op til kravene om passende sikkerhed, og dermed at rettighedsstyringen er tilstrækkelig. Du kan læse mere om dine forpligtelser om at føre tilsyn med databehandlere i Datatilsynets vejledning herom.

6.5 Overvågning af rettighedsstyring

Der skal løbende følges på rettighedsstyring. Der kan let ske fejl i en travl hverdag, og det kan modvirkes af, at du med jævne mellemrum kontrollerer, at de foranstaltninger, der støtter op om din rettighedsstyring, fungerer efter hensigten.

Relevante foranstaltninger

- Stikprøver i log over brugernes anvendelser af personoplysninger
- Periodisk kontrol af adgangsrettigheders aktualitet
- Awareness

Styr på rettighedsstyring

Udgivet af:
Datatilsynet
Carl Jacobsens Vej 35
2500 Valby
T 33 19 32 00
dt@datatilsynet.dk
datatilsynet.dk

Datatilsynet
Carl Jacobsens Vej 35
2500 Valby
T 33 19 32 00
dt@datatilsynet.dk
datatilsynet.dk