De 10 brud

10 typiske brud på persondatasikkerheden og gode råd til, hvordan de undgås

Senest opdateret januar 2024

DATATILSYNET

På baggrund af anmeldte brud på persondatasikkerheden har Datatilsynet identificeret 10 typiske brud. Her får du en række gode råd til, hvordan de kan undgås.

Hvad er brud på persondatasikkerheden?

Brud på persondatasikkerheden er ofte hændelser, hvor der enten hændeligt (noget sker utilsigtet eller ved en tilfældighed) eller tilsigtet (typisk ved hacking eller misbrug) sker noget med personoplysninger, som kan påvirke oplysningernes fortrolighed, f.eks. ved at data bliver tilgængelige for uvedkommende. Det kan også være hændelser, som kan medføre, at oplysningerne bliver utilgængelige for den dataansvarlige (tab af tilgængelighed), eller at oplysningerne ændres, så de er forkerte (tab af integritet).

Hvem er disse råd målrettet?

For hvert af de typiske brud beskrives en række konkrete tiltag, der kan overvejes for at nedbringe risikoen for, at det pågældende brud indtræder. Disse forslag er derfor især målrettet medarbejdere, der har mulighed for at udfærdige og/eller ændre på organisationens regler, procedurer, undervisning/awareness og tekniske opsætninger i it-miljøer for derigennem at beskytte organisationen imod disse typiske brud på persondatasikkerheden.

Ofte er det små tiltag, som skal til for at mindske risikoen for brud, og dermed ikke tiltag der kræver store investeringer, eller at den øverste ledelse nødvendigvis involveres. Hvis tiltag alligevel kræver, at den øverste ledelse involveres, kan disse råd være med til at illustrere, hvorfor det er nødvendigt eksempelvis at investere i eller på anden vis prioritere it-sikkerhed.

Sikkerhedsforanstaltninger skal være passende

Dataansvarlige og databehandlere skal gennemføre passende sikkerhedsforanstaltninger for at sikre et sikkerhedsniveau, der passer til risiciene ved behandlingen af personoplysninger. Det følger af databeskyttelsesforordningens artikel 32.

Bestemmelsen fastsætter ikke, hvilke præcise sikkerhedsforanstaltninger der skal træffes. Bestemmelsen fastslår imidlertid, at dataansvarlige og databehandlere er ansvarlige for at beskytte personoplysninger mod, at der sker brud på persondatasikkerheden. Det skyldes, at det

kan påføre de berørte personer skade, hvis oplysningernes fortrolighed, tilgængelighed eller integritet kompromitteres.

Dataansvarlige og databehandlere skal derfor afdække de risici, som behandlingen af personoplysninger indebærer for de berørte personer – de skal med andre ord lave en såkaldt risikovurdering. Her er det væsentligt at understrege, at der ikke er tale om risikoen for organisationens omsætning/indtjening, men om risikoen for de berørte personer, dvs. dem der behandles oplysninger om. På den baggrund skal dataansvarlige og databehandlere udvælge og fastsætte de sikkerhedsforanstaltninger, der i tilstrækkelig grad beskytter personoplysningerne.

Det indebærer, at hvad der er passende sikkerhedsforanstaltninger for én dataansvarlig/én databehandler, ikke nødvendigvis er passende sikkerhedsforanstaltninger for en anden.

Det betyder også, at de sikkerhedsforanstaltninger, der fremgår af denne samling af forslag ikke er udtømmende, ligesom ikke alle forslag vil være relevante eller tilstrækkelige for alle situationer, hvor organisationen behandler personoplysninger. Generelt kan det dog siges, at kravene til behandlingssikkerhed – og dermed også til sikkerhedsforanstaltninger – skærpes, jo højere risikoen er for de personer, hvis oplysninger organisationen har ansvaret for.

Hvis der sker brud på behandlingssikkerheden selvom organisationen har gennemført sikkerhedsforanstaltninger, skal dataansvarlige og databehandlere på ny vurdere, om der er behov for at tilpasse og eventuelt skærpe sikkerhedsforanstaltningerne for at undgå lignende brud i fremtiden.

Sikkerhedsforanstaltninger kan både være af teknisk og organisatorisk karakter

Sikkerhedsforanstaltningerne kan både være af teknisk og organisatorisk karakter, og i mange tilfælde er det relevant med begge dele.

Sikkerhedsbrud skyldes ofte menneskelige fejl. Derfor er det vigtigt, at alle medarbejdere forstår, hvordan de skal behandle personoplysninger. Det kan f.eks. ske ved at fastsætte retningslinjer og procedurer for håndtering af personoplysninger. Det gælder bl.a. i forhold til sikker intern og ekstern kommunikation, da størstedelen af de anmeldte brud angår utilsigtet deling af personoplysninger med forkerte modtagere. Den slags retningslinjer og procedurer skal løbende opdateres, ligesom det skal sikres, at medarbejderne rent faktisk har kendskab til dem. Det kan I som organisation f.eks. sikre ved at gennemføre uddannelse og awareness-kampagner for medarbejdere.

Retningslinjer og procedurer kan imidlertid blive misforstået, glemt eller ignoreret, og derfor kan det være nødvendigt også at gennemføre tekniske sikkerhedsforanstaltninger, som automatisk kan beskytte imod utilsigtet eller ulovlig behandling af personoplysninger. Hvis der findes en teknisk foranstaltning, som er let og uden stor omkostning kan implementeres, og som samtidigt yder en høj grad af beskyttelse mod et ofte forekommende risikoscenarie, så kan det følge af princippet om 'privacy by design' at sådan foranstaltning bør implementeres som supplement til eller i stedet for en organisatorisk foranstaltning.

Du kan finde beskrivelser af flere relevante sikkerhedsforanstaltninger i Datatilsynets foranstaltningskatalog, som løbende bliver udvidet.

1. Data til forkerte modtagere fordi forkert adressat flettes ind i udgående post

Sådanne brud kan berøre mange personer og personoplysninger, idet brevfletning ofte anvendes, når der skal sendes post til mange modtagere. Fejlen opstår typisk i en manuel proces, hvor en medarbejder fletter brevindhold med en forkert modtager. Fletningen kan foregå på forskellige måder, f.eks. fra et ESDH-system til en e-mail eller fra et regneark til breve skrevet i et tekstbehandlingsprogram (f.eks. Word eller Adobe Acrobat). Dette indebærer en risiko for, at indholdet og modtageren ikke passer sammen, og at e-mailen/brevet derfor bliver sendt til en forkert modtager. Det kan resultere i uautoriseret videregivelse af personoplysninger, som er et brud på persondatasikkerheden.

Tiltag der kan overvejes

- Indfør automatisk adressering med data fra en database over tilknyttede adressater. Sørg for at adressaterne i databasen er opdaterede og gennemgå dem jævnligt for fejl. Alternativt kan de opdateres automatisk fra en autoritativ kilde, f.eks. CPR.
- Minimer indholdet i brevet til det nødvendige, f.eks. ved ikke at angive privatadresser, hvis brevet sendes elektronisk. På den måde kan man i nogle tilfælde mindske konsekvensen af bruddet, hvis der sker fejl, når adressen flettes.
- Sørg for at have retningslinjer for intern og ekstern kommunikation, herunder at medarbejdere skal udvise påpasselighed for at sikre, at e-mails, breve mv. ikke sendes til forkerte modtagere.
- Hav faste procedurer for, at et ekstra sæt øjne i visse tilfælde tjekker forsendelsen, inden der trykkes på 'Send'.
- Indfør en teknisk forsinkelse på levering af e-mails. På den måde kan medarbejderen nå at afbryde leveringen, hvis vedkommende opdager en fejl eller får trykket på 'Send' for tidligt.
- Ved fordeling af forsendelser imellem Digital Post og fysisk post kan de breve, der skal sendes fysisk, muligvis stoppes i kuverteringsprocessen hos en postleverandør, afhængigt af leverandøren. I givet fald skal I have en procedure eller et kontaktpunkt parat til, når situationen opstår. Eventuelt kan det være en funktion i et it-system, som kan stoppe leveringen.
- Opsæt en automatisk advarsel i jeres ESDH- eller e-mailsystem om, at en e-mail f.eks. er ved at blive sendt 1) til en anden modtager end parten på sagen, 2) ud af organisationen/myndigheden eller 3) ud af afsenderens enhed/afdeling.
- Anvend værktøjer af typen DLP (Data Leak Prevention). Det er værktøjer, som kan screene for bestemte datatyper i dokumenter mv. og herefter advare eller forhindre, at mails bliver sendt uden yderligere verifikation

2. Beskyttet adresse eksponeres fejlagtigt efter ændring i it-system

Datatilsynet ser løbende brud på persondatasikkerheden, der opstår, fordi organisationen ikke har procedurer og regler, der sikrer opmærksomhed på, hvor personoplysningerne er hentet fra, hvad formålet med deres registrering er, eller begrænsninger i hvordan oplysningerne må anvendes. Det berører særligt beskyttede adresser og opholdssteder, der risikerer at blive eksponeret (dvs. afsløret) for den person, som er årsagen til, at der er valgt adressebeskyttelse.

Tiltag der kan overvejes

- Sørg for at have styring af ændringer i it-miljøet, da det kan mindske sandsynligheden for denne type af fejl. Se om Ændringsstyring (Change Management) i Datatilsynets foranstaltningskatalog, hvor der også henvises til en række eksempler fra praksis.

3. Fejludlevering af data ved sagsbehandling

Sådanne brud sker bl.a. ved, at dataansvarlige og databehandlere udleverer eller offentliggør dokumenter, som indeholder oplysninger, der ikke skulle være inkluderet. Det kan være, fordi dokumenterne er lagret på et forkert sted i et it-system (f.eks. journaliseret på en forkert sag) og derfor bliver udleveret i forbindelse med anmodninger om aktindsigt, indsigt eller lignende.

Det kan også ske ved, at et dokument ikke bliver tilstrækkeligt pseudonymiseret (bestemte personoplysninger bliver ikke fjernet/slettet), inden dokumentet bliver offentliggjort på internettet eller udleveret i forbindelse med f.eks. anmodninger om aktindsigt eller indsigt.

Fejludlevering af personoplysninger kan endvidere ske ved, at medarbejdere sender e-mails til forkerte modtagere, eller ved at e-mails til den rette modtager indeholder de forkerte personoplysninger. Se også nedenfor under brud nr. 5: Auto-complete medfører at e-mails bliver sendt til forkerte modtagere og Datatilsynets vejledende tekst om samme emne.

Tiltag der kan overvejes

- Sørg for at have retningslinjer for intern og ekstern kommunikation, som bl.a. understreger, at medarbejdere skal udvise påpasselighed for at sikre, at de ikke sender e-mails mv. til forkerte modtagere, og at de ikke sender forkerte dokumenter.
- Sørg for at have retningslinjer for at håndtere anmodninger om indsigt og aktindsigt, samt for processen hvor I offentliggør oplysninger på internettet. Retningslinjerne skal bl.a. indeholde en anvisning om, at medarbejdere skal gennemgå materialet manuelt med fokus på at slette/fjerne personoplysninger, inden materialet offentliggøres eller udleveres.
- Hav procedurer for, at et ekstra sæt øjne i visse tilfælde tjekker materialet, inden det sendes eller offentliggøres.
- Hav retningslinjer for, at fejlregistrering af oplysninger i ESDH- og CRM-systemer mv. skal rettes, så snart de opdages, for at undgå at fejlen senere leder til brud på persondatasikkerheden.
- Klassificer dokumenter for at markere de dokumenter, som ikke uden videre må sendes ud af organisationen. Det kan tydeliggøre over for medarbejdere og it-systemer, når der er ved at ske et brud på persondatasikkerheden.
- Anvend værktøjer af typen DLP (Data Leak Prevention). Det er værktøjer, som kan screene for bestemte datatyper i dokumenter mv. og herefter advare eller forhindre, at mails bliver sendt, at data overføres til USB-nøgler, at data uploades til hjemmesider mv.
- Anvend værktøjer til supplerende screening for bestemte typer af personoplysninger i offentliggjorte dokumenter og lignende med henblik på at opdage personoplysninger, der ikke skulle have været offentliggjort

Praksis

06-09-2022: Alvorlig kritik af Familieretshuset (journalnummer: 2021-432-0063)

25-04-2022: Alvorlig kritik af PrivatBo i sag om manglende behandlingssikkerhed (journalnummer: 2019-441-1480)

18-10-2021: Klage over sikkerhedsbrud hos Falkonergårdens Gymnasium og HF (journalnummer: 2021-32-2067)

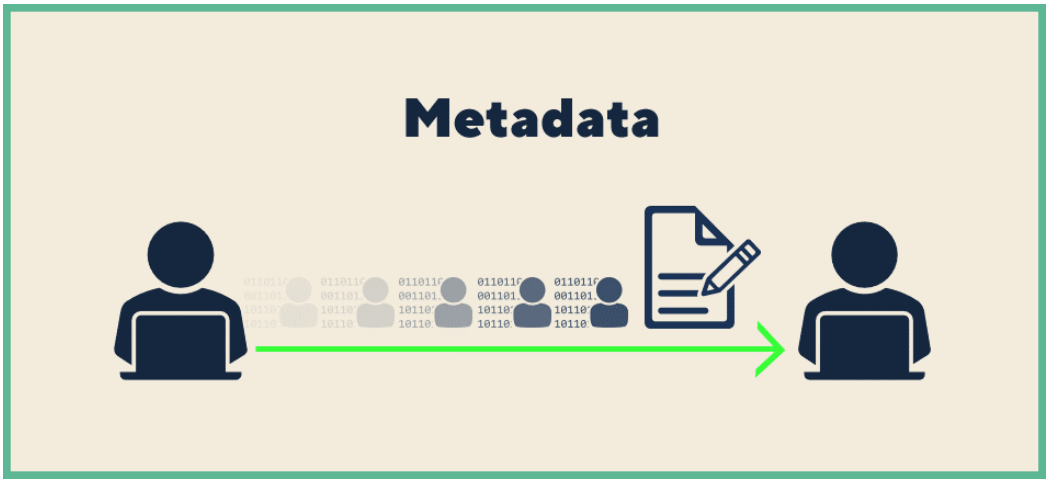
16-02-2021: Klage over offentliggørelse af personnummer på kommunal hjemmeside (journalnummer: 2020-32-1579)

15-04-2020: Brud på persondatasikkerheden hos Randers Kommune (journalnummer: 2019-442-4873)

17-09-2021: Region Syddanmark indstillet til bøde

4. Manglende sletning af data ved brug af digitale værktøjer

Hvis medarbejdere mangler kendskab til it-værktøjer, eller til det forhold at data kan være skjulte, kan det resultere i brud. Medarbejdere kan i så fald anvende værktøjer (i tekst-behandlingsprogrammer som f.eks. Word og Adobe Acrobat) til at fjerne oplysninger fra dokumenter i en fejlagtig tro på, at personoplysningerne er fjernet effektivt, men hvor oplysningerne blot er gjort ikke umiddelbart synlige – f.eks. ved at tekst dækkes af en "kasse", eller ved at tekstfarven ændres til hvid.



Brud kan også opstå, når personoplysninger er skjult i metadata, uden at medarbejdere er klar over det. Metadata er andre oplysninger end selve indholdet i et dokument. I et tekstdokument kan det f.eks. være oplysninger om, hvem der sidst har gemt filen, titler på brev-skabelon eller tidligere versioner af teksten.

Manglende forståelse for et værktøj kan også betyde, at personoplysninger videregives som metadata. Det kan være metadata i et skjult regneark, der er anvendt til at danne en graf i en præsentation, men fordi regnearket er en del af præsentationsfilen, kan personoplysninger i regnearket tilgås af alle, der får adgang til præsentationsfilen.

Tiltag der kan overvejes

- Sørg for, at medarbejdere har kendskab til de værktøjer, de anvender til at behandle personoplysninger.
- Anvend værktøjer, der kan sikre, at data bliver slettet effektivt.
- Hav retningslinjer for, hvilke værktøjer medarbejdere må anvende og procedurer for, hvordan medarbejdere sletter effektivt, når de anvender værktøjet.
- Læs også om foranstaltningen 'Sammenhæng mellem brugerkompetencer, adgangsrettigheder og opgaver' i Datatilsynets foranstaltningskatalog.

Praksis

21-04-2022: Datatilsynet udtaler alvorlig kritik af Finanstilsynets behandling af person-oplysninger (journalnummer: 2020-442-8099)

Region 20Syddanmark indstillet til bøde

5. Auto-complete medfører, at e-mails bliver sendt til forkerte modtagere

I mange e-mailprogrammer er det en standardindstilling, at funktionen auto-complete er slået til. Funktionen virker ved, at e-mailprogrammer gemmer navne og e-mailadresser på modtagere af e-mails, som en bruger tidligere har sendt. På baggrund af de gemte oplysninger oplistes forslag til modtagere, når brugeren begynder at skrive i et af modtagerfelterne.

Det vil ofte være tidsbesparende at anvende denne funktion, og den kan også understøtte, at e-mails bliver sendt til rette modtager. I nogle tilfælde sker det imidlertid, at man kommer til at vælge en forkert modtager med den følge, at e-mailen bliver sendt til uvedkommende. Hvis e-mailen indeholder personoplysninger, vil der være sket et brud på persondatasikkerheden.

Læs også Datatilsynets vejledende tekst om auto-complete af e-mailadresser.

Tiltag der kan overvejes

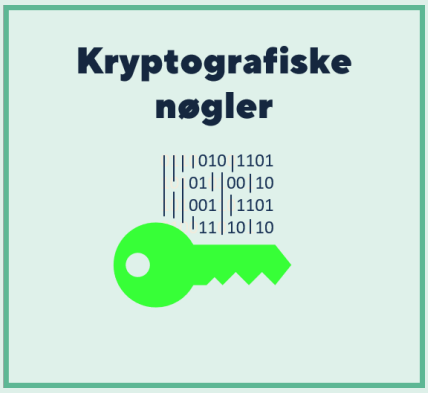
- Hav retningslinjer for intern og ekstern kommunikation, herunder at medarbejdere skal udvise påpasselighed for at sikre, at de ikke sender e-mails til forkerte modtagere.
- Hav faste procedurer for, at et ekstra sæt øjne (f.eks. en betroet kollega) kontrollerer e-mailen, inden du trykker ”send”, hvis der f.eks. er tale om en e-mail med mange personoplysninger.
- Hav retningslinjer for, at man ikke må indtaste e-mailadresser (manuelt eller ved anvendelse af auto-complete), når man sender e-mails til eksterne modtagere. I stedet skal e-mailadresserne kopieres fra f.eks. et CRM-system, hvor de allerede er registreret og bekræftet som værende korrekte.
- Sørg for jævnlig (automatisk) sletning af gemte e-mailadresser, der ikke er benyttet for nylig.
- Indfør teknisk forsinkelse på levering af e-mails. På den måde kan medarbejderen nå at afbryde leveringen, hvis vedkommende opdager en fejl eller får trykket på ’send-knappen’ for tidligt.
- Opsæt en automatisk advarsel i e-mailsystemet om, at en e-mail f.eks. er ved at blive sendt 1) til en anden modtager end parten på sagen, 2) ud af organisationen/myndigheden eller 3) ud af afsenderens enhed/afdeling.
- Anvend værktøjer af typen DLP (Data Leak Prevention). Det er værktøjer, som kan screene for bestemte datatyper i dokumenter mv. og herefter advare eller forhindre, at mails bliver sendt. Sådanne værktøjer kan både medvirke til at forhindre brud, og formindske risikoen for alvorligere brud og dermed konsekvenserne af et brud, der kan ske ved anvendelse af auto-complete-funktionen.
- Slå auto-complete-funktionen fra.

6. Tab/tyveri af transportable enheder med ukrypteret data

USB-pinde, bærbare computere, mobiltelefoner, tablets og eksterne harddiske, der indeholder ikke-krypterede personoplysninger, kan mistes som følge af f.eks. tab eller tyveri. Det kan ske under transport, postforsendelse, anvendelse uden for kontoret, herunder på rejse, eller ved at de bliver stjålet fra biler, private hjem mv. I sådanne tilfælde kan personoplysningerne tilgås af uvedkommende, og der vil derfor være tale om et brud på persondatasikkerheden.

Tiltag der kan overvejes

- Sørg for at kryptere enhederne. Kryptering er normalt en let tilgængelig teknisk understøttelse, idet alle gængse styresystemer kan sættes op til at kryptere harddiske og lagringsmedier.
- Indfør procedurer som sikrer, at alle organisationens enheder administreres ens og dermed f.eks. altid krypteres og beskyttes af adgangskoder. Dette kan I supplere med en jævnlig manuel eller automatiseret kontrol af, at beskyttelsen stadig er aktiv.



- Sørg for at beskytte de kryptografiske nøgler, I anvender. Kryptografiske nøgler er ikke det samme som adgangskoder. Kryptografiske nøglers funktion er at kryptere og dekryptere data, mens adgangskoder typisk skal indtastes for at kunne "åbne for" anvendelsen af kryptografiske nøgler.
- Uden tilstrækkelig beskyttelse af de kryptografiske nøgler, har de ingen værdi. Hvis nøglerne kan tilgås af uvedkommende, vil krypteringen nemlig ikke længere i sig selv være en beskyttelse imod, at uvedkommende kan læse de krypterede data
- Etablér et teknisk set-up, hvor medarbejdere som udgangspunkt ikke kan lagre dokumenter, filer mv. med personoplysninger lokalt på bærbare computere, mobiltelefoner eller tablets. Dette kan være et alternativ til kryptering. Vær dog opmærksom på, at hvis der ikke kan sikres fuldstændigt imod lokal lagring af personoplysninger, så er krypteringen det bedste udgangspunkt – især fordi kryptering ofte er nemt at anvende.
- At forhindre brugeren i at lagre dokumenter lokalt kan således være et supplement til kryptering. Det indebærer den ekstra fordel, at det kan tvinge brugerne til at lagre dokumenter et sted, hvor der bliver taget backup af dem.
- Hvis I anvender medier, der ikke kan krypteres, f.eks. hukommelseskort i et kamera, skal I sikre, at mediet beskyttes fysisk – dvs. opbevares sikkert.

Fysisk sikring kan f.eks. bestå af sikringsskabe, dørlåse, nøgleadministrering, alarmer og tv-overvågning. I skal desuden lave en procedure, som sikrer, at data fra hukommelseskortet hurtigt overføres til et internt it-system, hvorefter kortet formateres eller om muligt slettes/overskrives.

Praksis

12-05-2022: Politianmeldelse: Civilstyrelsen indstilles til bøde

29-09-2022: Politianmeldelse: Hørsholm Kommune idømt bøde på 50.000 kr.

16-09-2021: Politianmeldelse: Favrskov Kommune indstilles til bøde

10-03-2020: Politianmeldelse: To kommuner indstillet til bøde

Se også

- Center for cybersikkerhed: Sikkerhed på mobile enheder.
- Center for cybersikkerhed: Cybersikkerhed på rejsen.
- Krav til kryptering af harddiske i de 20 tekniske minimumskrav til sikkerheden i it-løsninger (sikkerdigital.dk).
- NIST 800-111 om best practice inden for informationssikkerhed (National Institute of Standards and Technology (.gov)).
- Kommunernes Landsforenings anbefalinger om tekniske minimumsstandarder i kommuner (kl.dk).

7. For bred adgang til data på netværksdrev mv.

Datatilsynet ser løbende eksempler på denne type af brud, og de opstår særligt på følgende måder:

- Oplysninger lagres et forkert sted, hvor der ikke er den nødvendige adgangsbegrænsning.
- En medarbejder opretter en mappe på et netværksdrev uden at have tilstrækkelig forståelse for, hvordan adgangsbegrænsning etableres og administreres korrekt.
- Der ændres i et it-system, uden at den eksisterende adgangsbegrænsning videreføres.
- Adgangsrettigheder opdateres ikke, hvorved medarbejdere, der ikke længere har behov for adgang, ikke får frataget deres adgang.

Tiltag der kan overvejes

- Lav retningslinjer om og styring af adgangsrettigheder for at sikre, at medarbejdere udelukkende har adgang til personoplysninger, som de har et arbejdsbetinget behov for at have adgang til.
- Anvend værktøjer til løbende at screene netværksdrev, SharePoint, OneDrive og lignende for bestemte datatyper med henblik på at opdage fejlagtig lagring af oplysninger på steder uden tilstrækkelig adgangsbegrænsning.
- Læs om 'Centraliseret rettighedsstyring' i Datatilsynets foranstaltningskatalog.

Se også

- Datatilsynets vejledning 'Styr på rettighedsstyring'.
- Datatilsynets foranstaltningskatalog.

8. Uautoriseret adgang til data grundet dårligt design, kodefejl og utilstrækkelige tests

Fejl i forbindelse med udvikling eller opdatering af software og manglende efterfølgende test kan føre til brud på persondatasikkerheden i form af uautoriseret adgang til personoplysninger. Det kan f.eks. ske ved, at rettighedsstyringen bliver ødelagt eller helt forsvinder i forbindelse med ændring af et it-system. Hvis man tester med fokus på sikkerhed, kan man opdage fejl, som er opstået i forbindelse med ændring af it-systemet.

Test kan f.eks. være sårbarhedstest med henblik på at finde sårbarheder, som kan udnyttes af personer med onde hensigter, men det kan også være test for fejl, som giver almindelige brugere (uden onde hensigter) uautoriseret adgang til personoplysninger. Det kan endvidere være en test af, om systemet i det hele taget stadig fungerer som forventet, herunder at rettighedsstyringen stadig fungerer som forventet. Der kan være særlig grund til at være opmærksom ved nyanskaffelser, væsentlige systemændringer eller hvis risikobilledet ændrer sig væsentligt.

Tiltag der kan overvejes

- Hav fokus på om alle risici ved ændringer i dit it-miljø er afdækket. Læs mere om 'ændringsstyring' i Datatilsynets foranstaltningskatalog.
- Opstil krav om tilstrækkelige kompetencer hos udviklerne. Kravene kan eventuelt sikres opnået via en databehandleraftale eller en it-kontrakt, hvis udviklingen foregår hos en anden part/softwareleverandør.
- Opstil krav om, at der er indbygget sikkerhed i it-systemet. Se vejledningsmateriale om databeskyttelse gennem design og standardindstillinger her.
- Opstil krav om et kodereview, hvor programkode gennemgås af anden end programmøren med henblik på at finde fejl. Det kan I evt. sikre via en databehandler-aftale eller en it-kontrakt.
- Opstil krav til test af sandsynlige fejlscenarier og sårbarheder, evt. via en databehandleraftale eller it-kontrakt. Eksempler på relevante tests:
    - Sårbarhedstest (en test, der identificerer eksisterende sårbarheder).
    - Penetreringstest (en test, der forsøger at udnytte sårbarheder i et it-system).
    - Test af omgåelse af login (f.eks. problemstillinger som ’brute for-ce’-angreb).
    - Test af om adgangsrettigheder er begrænset som forventet.
    - Test af om der logges som forventet.
    - Andre tests med fokus på funktionalitet, som ikke har været tiltænkt, og som kan misbruges.

Praksis

08-11-2021: Region Nordjylland får kritik for manglende sikkerhed omkring selvbetjeningsløsning (journalnummer: 2021-442-12924)

23-02-2022: Datatilsynet udtaler alvorlig kritik af KOMBITs behandling af personoplysninger som databehandler for en række kommuner (journalnummer: 2020-442-6168)

12-05-2022: Alvorlig kritik af Syddansk Universitets utilstrækkelige testning af softwareopdatering (journalnummer: 2021-442-13989)

04-07-2022: Alvorlig kritik af Sports Connection for manglende behandlingssikkerhed (journalnummer: 2021-441-10210)

17-07-2020: Brud på persondatasikkerheden hos Region Syddanmark (journalnummer: 2018-442-0026)

27-06-2022: Alvorlig Kritik: Manglende overholdelse af princippet om databeskyttelse gennem design hos LB Forsikring A/S (journalnummer: 2021-441-10244)

9. Videregivelse af data gemt i skabelon- og blanketløsninger

En skabelon, blanket eller lignende (f.eks. en Word-fil) kan være designet sådan, at en bruger kan indtaste personoplysninger i skabelonen, hvorefter den næste bruger, der åbner skabelonen, kan se disse oplysninger. Idet den næste bruger (som er en uvedkommende) får adgang til personoplysningerne, vil der være tale om et brud på persondatasikkerheden.

Tiltag der kan overvejes

- Begræns rettighederne til det sted, hvor skabelonen ligger gemt. Hvis det alene er få medarbejdere, som har redigeringsrettigheder til dokumenterne i mappen, reduceres sandsynligheden for, at personoplysninger ved en fejl bliver gemt i skabelonen. Dermed vil oplysningerne ikke fremgå, når den næste bruger åbner skabelonen.
- Sørg for at selve filen, som udgør skabelonen, er skrivebeskyttet. På den måde kan ændringerne kun gemmes ved at omdøbe dokumentet eller ved at gemme det et nyt sted. Dette kan fungere som en ekstra foranstaltning, der giver brugeren anledning til at tænke sig om en ekstra gang.
- Håndter sikkerhed i design og tests, hvis der er tale om skabelon i form en af en online formular. Se tiltag, der kan overvejes i forbindelse med design og test under brud nr. 7: For bred adgang til data på netværksdrev mv.

10. Ondsindet software (ransomware) medfører tab og misbrug af data

I de seneste år er flere danske virksomheder og myndigheder 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' til at opnå adgang til data på it-systemerne, hvorefter de krypterer data og forlanger løsepenge for at dekryptere dem. Ofte sker det først efter at data er trukket ud af it-systemerne, og hvis løsesummen ikke betales, kan hackerne i stedet afpresse ved at true med at offentliggøre data.

Der ses også 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 stjålet, selv bliver udsat for afpresning.

Tiltag der kan overvejes

- Basale sikkerhedsforanstaltninger som backup, flerfaktorautentifikation, firewall, antivirus, opdatering af software, segmentering af netværk, mv. er tekniske foranstaltninger, der beskytter imod mange trusler, herunder ransomware.
- Awareness: Medarbejderne er ofte det første "lag" i sikkerheden, som hackerne går igennem. Derfor er medarbejdernes evne til at opdage begyndelsen til et ondsindet angreb en vigtig foranstaltning.
- Læs mere om 'backup og flerfaktorautentifikation (MFA) i Datatilsynets foranstaltningskatalog.

Se også

- Datatilsynets vejledning om rettighedsstyring.
- Center for Cybersikkerheds vejledninger:
  - Reducerer risikoen for ransomware
  - Cyberforsvar der virker
  - Passwordsikkerhed
  - DMARC - Reducer risikoen for falske mails

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