Redegørelse: Dansk Journalistforbund
Udsendelse af password reset emails

18/10-2016 kl. 11.47 blev der fra journalistforbundet.dk udsendt emails med links, der kan bruges til engangslogin for medlemmerne. Dette skyldes, at DJ ønskede at give nem adgang til det nye website for alle deres medlemmer.

Desværre har der været en fejl i koden der genererede disse mails, hvilket har betydet, at mange medlemmer har modtaget et forkert medlemsnummer og forkert engangslogin link, hvilket har givet dem mulighed for at logge ind som en anden bruger.

Selve mailen kan ses herunder:

Fra: **Dansk Journalistforbund** <webmaster@journalistforbundet.dk>
Dato: 18. oktober 2016 kl. 12.13
Emne: Login til Mit DJ
Til: [redacted]

Kære medlem

Du kan nu logge ind på Mit DJ på det nye journalistforbundet.dk.

Du logger på ved at klikke på dette link:
https://journalistforbundet.dk/user/reset/[redacted]

- Bemærk: du skal oprette et kodeord, når du logger på første gang.
- Engangslogind'et kan kun bruges denne ene gang.
- Bemærk: dit brugernavn er dit medlemsnummer: [redacted]

På Mit DJ får du et overblik over dit medlemsskab i DJ. Du kan se, hvilke nyhedsbreve, du er tilmeldt, du kan til-/framelde Journalisten, og du kan opdatere dit telefonnummer, stillingsbeskrivelse mm.

God fornøjelse!

Det er her vigtigt at pointere, at en given brugers oplysninger maksimalt kan have været vist til én anden udestående medlem, idet linket kun fungerer for den første der trykker på det.

I den time der gik, inden vi fik lukket ned for adgangen, nåede 732 personer at logge ind - vi kan ikke se hvor mange der var uretmæssige logins. Det svarer til ca. 4% af de samlet udsendte mails.

Forløbets detaljer, specifikke omfang og konsekvenser er beskrevet herunder.

Forløb

- **11:47**: Proces med udsendelse af engangsloginsmails startes
- **12:30**: DJ kontakter Reload og gør opmærksom på problemet
- **12:52**: Reload sætter sitet offline. Dermed kan sitet ikke tilgås af normale brugere og engangslogins kan ikke anvendes.
  Reload sletter herefter alle engangslogins og alle sessions. Dermed virker engangslogins i allerede udsendte emails ikke længere og brugere, der måtte have brugt engangslogins til at logge ind på sitet, før det blev sat offline, bliver logget ud.
- **13:15**: Reload sætter sitet online igen.
- **14:50**: Reload nulstiller alle passwords som en ekstra sikkerhedsforanstaltning og alle ændringer til profiloplysninger bliver rullet tilbage.
- **16:50**: Reload identificerer root cause, igangsætter udbedring.

Omfang

Problemet har medført at én modtager kan logge ind på journalistforbundet.dk som et andet medlem. Dermed kan modtageren tilgå profilsiden for dette andet medlem samt ændre nogle af medlemmets oplysninger i systemet.

Profilsiden indeholder personfølsomme oplysninger for medlemmet herunder:

- Medlemsnummer
- For- og efternavn
- Adresse
- Emailadresse
- Telefonnummer
- Titel
- Arbejdsgiver
- Gruppe
- Kredsmedlemskab
- Mulighed for til- og framelding af nyhedsbreve

Profilsiden indeholder *ikke* CPR-nummer.

Problemet har ramt ni ud af ti medlemmer. For hvert ti medlemmer er der altså ét medlem, der har modtaget en korrekt email og ni medlemmer, der har modtaget en kopi af denne email.

Ud fra systemet kan det ses at der er blevet anvendt 732 engangslogins i de udsendte emails inden problemet blev adresseret. Hvert link kan kun bruges til at logge ind én gang. Det er ikke

muligt at afgøre, om det er den korrekte modtager eller et andet medlem, der har anvendt engangsloginet.

Dermed er der op til 732 medlemmer, der har fået eksponeret ovenstående oplysninger.
En liste over de berørte medlemmer er sendt til DJ, således de kan informeres direkte.

Problem

Problemet skyldes en lille men fatal kodefejl i den del af systemet, der har til formål at udsende information om brugerlogin til journalistforbundet.dk.

Koden benytter en emailskabelon med markører til at indsætte medlemsnummer og et personligt engangsloginlink. Emails bliver udsendt til ti medlemmer ad gangen, men kodefejlen medførte at skabelonen ikke blev nulstillet korrekt mellem hver udsendelse. Dermed fungerede skabelonen efter hensigten til det første medlem i hver gruppe. For de efterfølgende ni medlemmer indeholdt skabelonen derimod den tekst, der var blevet sendt til det første medlem - uden markører.

For at løse fejlen har vi en rettelse klar, der nulstiller skabelonen for hver mail. Derved vil hvert medlem få tilsendt de korrekte oplysninger.

Håndtering

For at håndtere situation og afledte konsekvenser har vi gjort følgende:

- Vi har afskåret brugernes adgang til sitet og herefter nulstillet engangslogins. Dermed har problemet været afgrænset til tidsperioden 11:47 til 12:52.
- Vi har nulstillet alle passwords til sitet. Hvis et medlem har brugt et engangslogin til et andet medlem og herefter angivet et kodeord, virker dette kodeord ikke længere.
- Vi har rullet alle ændringer til medlemsprofiler lavet vha. journalistforbundet.dk tilbage. Hvis et medlem har lavet ændringer til andet medlems email, telefonnummer, titel, ansættelse etc. har det altså ingen effekt.

Årsag

Den primære årsag til at fejlen kunne opstå er en menneskelig fejl.

Udvikleren, der har været ansvarlig for denne del af systemet, har ikke fået gennemtestet funktionaliteten tilstrækkeligt med et forløb, der involverede udsendelse til mere end én bruger.

Fejlen er desværre heller ikke blevet fundet af den efterfølgende test hos DJ. Dette på trods af at et forløb med flere modtagere er beskrevet som en del af testscenariet.

Håndtering af personfølsomme data på journalistforbundet.dk

journalistforbundet.dk er et website for en fagforening, hvor en vigtig del af funktionaliteten er at give medlemmerne mulighed for selvbetjening - blandt andet i forhold til håndtering af profiloplysninger. For at gøre dette muligt er det nødvendigt at websitet har adgang til oplysninger for hvert medlem fra Dansk Journalistforbunds medlemssystem, Modulus, og integrerer disse på bedst mulig vis. Websitet har ikke adgang til CPR-numre for medlemmerne og data mellem de to systemer overføres over en krypteret forbindelse for at undgå at det kan opsnappes af tredjepart.

Websitet er konfigureret til, at det kun er det enkelte medlem samt medarbejdere hos Dansk Journalistforbund, der har adgang til medlemmets personfølsomme oplysninger. Derudover anvender websitet best practices inden for adgangsstyring: Login foregår over en krypteret forbindelse, brugerens password gemmes ikke i systemet og kan derfor heller ikke udleveres i emails, links til nulstilling af passwords kan kun bruges én gang.

Vi mener derfor at sitet er forsvarlig sikkert.

Den fejl, der ligger til grund for ovenstående problem, skyldes ikke en fejlkonfiguration af adgangsstyringen eller et sikkerhedshul, men en funktionalitet specialudviklet til journalistforbundet.dk, som havde en kodefejl.

På vegne af Reload og hele vores DJ udviklingsteam beklager jeg dybt fejlen og de gener det har måttet give. Vi tager dette meget alvorligt og vil gøre vores ypperste for det ikke sker igen.

Rasmus Luckow-Nielsen
Adm. direktør