DIGITALISERINGSSTYRELSEN

Notat

3. januar 2024
CHRHOU
J.nr. 2023 - 10660

Sikkerhedsrapport 2023: MitID/MitID Erhverv og NemKonto

Indhold

0. Resumé

De offentlige digitale løsninger spiller en stor og vigtig rolle i Danmark, og borgerne skal derfor trygt kunne bruge dem. Både MitID og MitID Erhverv samt NemKonto har generelt et meget højt niveau af sikkerhed, og Digitaliseringsstyrelsen arbejder løbende med forskellige aktiviteter, som er med til at sikre et fortsat højt niveau i lyset af, at svindlerne hele tiden udvikler nye metoder.

Som del af monitoreringen af Digitaliseringsstyrelsens systemer, MitID og MitID Erhverv samt NemKonto, udarbejdes rapporter med fokus på sikkerheden i systemerne. Denne rapport dækker perioden fra den 1. december 2022 til og med den 30. november 2023. I rapporten redegøres for igangsatte sikkerhedstiltag i MitID og MitID Erhverv samt NemKonto i den nævnte periode.

I takt med digitaliseringen af samfundet opstår nye typer af og muligheder for kriminalitet. Digitaliseringsstyrelsen tager svindel med de digitale løsninger meget alvorligt og arbejder løbende på at forbedre sikkerheden. Det er dog desværre ikke muligt at sikre sig fuldstændigt mod svindel – hverken i den fysiske eller digitale verden.

Digitaliseringsstyrelsen orienterer sig løbende i de it-kriminelles metoder, og implementerer tiltag, der vurderes at gøre det vanskeligere for de it-kriminelle at foretage svindel med MitID og MitID Erhverv eller NemKonto. Der ses forsat en væsentlig udbredelse af den såkaldte "social engineering"-metode, hvor svindlere kontakter borgeren og snyder vedkommende til at videregive personlige oplysninger eller foretage en handling til skade for sig selv. Fokus er derfor stadig på at imødegå denne type svindel, ligesom der løbende gennemføres forebyggende indsatser med det formål at styrke borgernes og medarbejdernes bevidsthed om sikker adfærd. Det skal bemærkes, at "social engineering" ikke udnytter tekniske mangler ved de digitale løsninger, men i stedet udnytter borgeres uopmærksomhed og manglende viden.

1. Baggrund

Rapporten tager i lighed med tidligere sikkerhedsrapporter udgangspunkt i sikkerheden i MitID og NemKonto og vil have fokus på at beskrive igangsatte sikkerhedstiltag i den nævnte periode.

Den første sikkerhedsrapport blev oversendt til Folketingets Indenrigs- og Boligudvalg i marts 2022. Den anden og seneste sikkerhedsrapport tilgik Udvalget for Digitalisering og It i januar 2023.

2. Håndtering af sikkerhed

Digitaliseringsstyrelsen arbejder til stadighed med at højne sikkerheden i de digitale løsninger, og de digitale løsninger bliver designet med henblik på at styrke sikkerheden. Eksempelvis er MitID sikret med to-faktor autentifikation, hvor brugerne skal identificere sig med to uafhængige redskaber i form af på den ene side et bru-

gernavn og adgangskode og på den anden side fx nøgleapp/kodeviser/kodeoplæser. Derudover har Digitaliseringsstyrelsen blandt andet iværksat løbende vurderinger, evaluering og kontrol af it- og informationssikkerhed. Det sker eksempelvis ved egenkontroller eller penetrationstest (sikkerhedstest). Dette grundlæggende sikkerhedsdesign bliver løbende vedligeholdt og justeret med henblik på at opretholde sikkerheden.

Det er dog afgørende, at brugerne anvender de digitale løsninger på måder, der ikke udfordrer sikkerheden. Brugerne bør således være opmærksomme på risikoen for misbrug, hvor brugerne selv bliver snydt til at foretage handlinger, der er til ugunst for dem selv.

2.1. Teknisk sikkerhed og sikker adfærd

Der er fortsat fokus på tekniske tiltag, samt på sikker brugeradfærd. Der arbejdes eksempelvis med konkrete opfølgningsindsatser med udgangspunkt i standarden for styring af informationssikkerhed (ISO 27001) og reglerne for databeskyttelse. I MitID indarbejdes der løbende tiltag, som skal øge sikkerheden og mindske muligheden for svindel.

De tekniske sikkerhedstiltag kan imidlertid ikke stå alene. Ud over aktiviteter rettet mod konkrete trusler, har styrelsen stort fokus på at holde borgerne løbende orienteret om sikker digital adfærd og formidle konkrete råd til, hvordan de kan sikre sig imod identitetssvindel eksempelvis i form af informationskampagner. Eksempelvis gennemfører Digitaliseringsstyrelsen sammen med bl.a. politiet, Forbrugerrådet Tænk og kommunerne, løbende en række kampagne- og oplysningsaktiviteter, som skal hjælpe borgerne med at beskytte deres koder og ikke afgive personlige oplysninger til kriminelle.

I takt med, at digitaliseringen af samfundet stiger, er der behov for, at der løbende foretages ændringer i de digitale løsninger som MitID og NemKonto for blandt andet at imødegå udviklingen i de it-kriminelles metoder. Dette uddybes for de enkelte løsninger nedenfor.

3. MitID og MitID Erhverv

MitID-løsningen giver borgeren mulighed for at autentificere sig i en række selvbetjeningsløsninger. MitID blev lanceret bredt primo oktober 2021 som en erstatning for den daværende NemID-løsning til privat brug. MitID blev drevet parallelt med NemID, der fra slutningen af juni gradvist blev afviklet frem til 31. oktober 2023. Hensigten med den lange paralleldrift har været at sikre den bedst mulige overgang for borgere og virksomheder.

Sideløbende med NemID-lukningen er MitID Erhverv blevet indfaset som erstatning for NemID medarbejdersignatur. Dette er en løsning til virksomheder, foreninger og myndigheder, som har medarbejdere eller brugere, der skal logge ind på offentlige selvbetjeningsløsninger og underskrive digitalt med MitID. Da en person

som udgangspunkt skal identitetssikres i MitID Erhverv ved brug af sit private MitID, beror sikkerheden i MitID Erhverv i overvejende grad på sikkerheden i det private MitID.

3.1. Sikkerhedstiltag i perioden

Den 6. juni blev MitID-appen opdateret med såkaldt *kanalsammenbinding*. Kanalsammenbindingen startes, når der anmodes om login med MitID fra en enhed, hvor MitID-appen ikke er installeret, og foregår mellem trinnet hvor brugeren indtaster bruger-ID, og udfører swipe-funktionen. Kanalsammenbinding kan foregå på to måder: 1) Brugeren scanner en QR-kode med sin MitID-app på enheden, hvorfra anmodningen er sendt, hvorefter brugeren swiper og logges ind. 2) Alternativt vises en engangskode (OTP) på enheden, hvorfra anmodningen er sendt, som brugeren indtaster i sin MitID app.

Kanalsammenbinding afbøder den uhensigtsmæssighed, at brugere kan godkende anmodninger i appen, som de ikke selv har igangsat. En senere opdatering har efterfølgende yderligere styrket sikkerheden ved, at QR-koden ændres hvert 15. sekund, så det bliver sværere for svindlere at nå at optage koden og sende den til brugeren.

Den 11. oktober blev der introduceret en række væsentlige slutbrugerrettede ændringer, herunder:

- Mulighed for at brugeren selv midlertidigt kan spærre sit MitID gennem selvbetjeningen på MitID.dk. Hidtil var dette kun muligt ved at ringe til MitID supporten eller møde fysisk op på borgerservice. Den nye funktionalitet skal særligt gøre det lettere for brugere, som har oplevet svindel eller forsøg herpå, at spærre deres MitID midlertidigt og derved sikre sig mod misbrug. Det er endnu for tidligt at konkludere, om det vil påvirke antallet af misbrugsforsøg og dertil opkald til MitID supporten vedrørende spærring. For nuværende er antallet af spærringer via MitID supporten uændret.
- Links i notifikationer fra MitID-appen er blevet fjernet. For brugervenlighedens skyld har visse notifikationer tidligere indeholdt links til MitID.dk eller telefonnummer til MitID supporten. De generelle it-sikkerhedsmæssige anbefalinger foreskriver dog, at links i blandt andet e-mails og sms'er skal undgås, da de kan misbruges til phishing-svindel. Derfor er alle links fjernet og erstattet med en alternativ tekst samt instruks om, hvor brugeren kan finde yderligere information.
- I selvbetjeningen på MitID.dk sløres brugerens telefonnummer og e-mailadresse. Tidligere gjaldt sløringen kun brugerens CPR-nummer. Sløringen er indført for at værne om brugerens personlige oplysninger, og potentielt beskytte brugeren mod identitetstyveri, hvis svindlerne har fået adgang til vedkommendes MitID-selvbetjening.

Fra den 3. november blev karensperioden for brugerændringer, der foretages via selvbetjeningen, forlænget fra én time til 24 timer. Ventetiden er sat op for at redu-

cere risikoen for svindelformer, hvor svindlere via telefon eller lignende lokker brugere til at godkende et identifikationsmiddel kontrolleret af svindleren eller til at give dem adgang til brugerens selvbetjeningsside. Det skal bemærkes, at karensperioden kun gælder ændringer, som foretages via selvbetjeningen på MitID.dk. Vil brugeren fx aktivere en ny kodeviser via pas- og ansigtsscanning i MitID appen, er der ingen ventetid.

4. NemKonto

NemKonto-løsningen er en digital infrastruktur, der muliggør udbetalinger fra det offentlige og private til borgere, virksomheder og foreninger, idet løsningen rummer oplysninger, der kobler til CPR- og CVR-numre med tilhørende kontonumre på NemKonto hos borgere og virksomheder. NemKonto-systemets formål er, at effektivisere håndtering af bankkontooplysninger og udbetalinger fra offentlige myndigheder samt private udbetalere.

Den 1. august 2022 trådte kompensationsordningen ved svindel med NemKonto i kraft. Siden da har det været muligt at modtage økonomisk kompensation, hvis man har været udsat for svindel med NemKonto. Fra december 2022 til november 2023 har Digitaliseringsstyrelsen modtaget seks sager vedrørende kompensation.

4.1. Sikkerhedstiltag i perioden

Siden sidste rapport er arbejdet med en række sikkerhedstiltag blevet videreført. Eksempelvis foretages der fortsat regelmæssige sårbarhedsscanninger, hvor systemer og netværk automatisk scannes for eventuelle sårbarheder. På baggrund heraf afholdes der løbende møder, hvor resultaterne af sårbarhedsscanninger bliver håndteret. Forekomsten af sårbarheder er således meget lav på nuværende tidspunkt.

I december 2022 blev der foretaget en penetrationstest af NemKontos webapplikationer samt den underliggende infrastruktur ved en ekstern leverandør. En penetrationstest er en såkaldt hacker-test af NemKonto-systemet. For løbende at teste systemet og sikre, at fundne fra den tidligere test er udbedret i tilstrækkelig grad, påtænkes en ny penetrationstest i 2024, når moderniseringen af NemKonto-systemet er gennemført.

5. Status på hotlinen for identitetstyveri

Digitaliseringsstyrelsen etablerede den 1. juni 2021 en hotline til hjælp ved identitetstyveri, som kan vejlede og rådgive borgeren ved mistanke om identitetstyveri, og hjælpe dem med at håndtere problemer herom. Den 11. september 2023 blev hotlinen lagt sammen med den nyetablerede Cyberhotline for digital sikkerhed under navnet Cyberhotline for digital sikkerhed. Hotlinen har fortsat åbent døgnet rundt 365 dage om året.

Hotlinen har i perioden fra 1. december 2022 til og med 5. november 2023[1] modtaget ca. 20.088 henvendelser.

Opkaldene for perioden er kategoriseret[2] således:

- 20 pct. er relateret til misbrug af borgerens identitet.
- 39 pct. er relateret til risiko for identitetstyveri, da borgerens oplysninger har været tilgængelig i forbindelse med svindel
- 11 pct. relaterer sig til forsøg på identitetstyveri, eksempelvis gennem phising, men hvor borgeren undlod at udlevere oplysninger.
- 15 pct. er relateret til efterspørgsel på vejledning for forebyggelse af identitetstyveri
- 15 pct. er fejlopkald eller på anden vis uden for de øvrige kategorier.

[1] Det har ikke været muligt at få konsolideret tal fra de sidste uger i november 2023.
[2] I forbindelse med sammenlægning overtog Den Samlede Support (DSS) Identitetstyveri-hotlinens opkald i dagtimerne. Efter den 11. september 2023 er tallene behæftet med stor usikkerhed, da supporterne har skullet lære de nye kategorier at kende. Der skal derfor tages forbehold for fejlregistreringer. Bemærk desuden, at hotlinen ikke verificerer, hvorvidt det er korrekt om en borger eksempelvis har været udsat for svindel. Formålet med hotlinen er at hjælpe borgerne, hvorfor registreringen ikke foretages med henblik på specifikt at kortlægge omfang, men for kvalitativt at kunne orientere sig i tidligere samtaler ved genkald. Hotlinen har således registreret antal opkald og ikke antal sager eller individer og beskriver alene borgerens oplevelse.