DIGITALISERINGSSTYRELSEN

Notat

10. marts 2022
.

Halvårlig sikkerhedsrapport: NemKonto, NemID og MitID

Indhold

0. Resumé ... 2
1. Baggrund ... 2
2. Håndtering af sikkerhed ... 3
2.1. Teknisk sikkerhed ... 3
2.2. Sikker brugeradfærd og mitigerende handlinger ... 3
3. NemID og MitID ... 4
3.1. Øget sikkerhed i MitID i forhold til NemID ... 4
3.2. Sikkerhedstiltag i perioden ... 5
4. NemKonto ... 6
4.1. Sikkerhedstiltag i perioden ... 6
5. Lovforslag om kompensationsordning ... 6
6. Etablering af hotline ... 7

0. Resumé

De offentlige digitale løsninger spiller en stor og vigtig rolle i Danmark. Svindel med løsningerne stiller ofrene i en ulykkelig situation, og borgerne skal trygt kunne bruge dem. Både NemKonto, NemID og MitID er generelt præget af meget høj sikkerhed, og Digitaliseringsstyrelsen arbejder løbende med forskellige aktiviteter, som er med til at sikre en fortsat høj sikkerhed.

Som opfølgning på Digitaliseringsstyrelsens redegørelse om håndtering af henvendelser vedrørende sikkerheden i NemID og NemKonto[1], som senest tilgik Folketinget i august 2021, rapporteres der halvårligt på sikkerheden i løsningerne. Denne rapport udgør den første afrapportering og dækker perioden fra primo marts 2021 til og med 31. december 2021. Rapporten vil fremadrettet blive oversendt til Folketinget halvårligt.

I rapporten redegøres for igangsatte sikkerhedstiltag i NemKonto, NemID og MitID i den nævnte periode. Derudover beskrives den øgede sikkerhed i regi af overgangen fra NemID til MitID.

Digitaliseringsstyrelsen tager svindel med de digitale løsninger meget alvorligt. I takt med digitaliseringen af samfundet, vil der opstå nye typer og muligheder for kriminalitet. Det er dog 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 virksomme i forbindelse hermed. Der ses en stigning i svindel, hvor svindleren kontakter borgeren og snyder denne til at videregive personlige oplysninger eller foretage en handling til skade for sig selv. Der er fokus på at imødegå sådanne risici, ligesom der løbende arbejdes med forebyggende indsatser rettet mod at styrke borgernes bevidsthed om sikker adfærd. Denne form for svindel udnytter ikke tekniske mangler ved de digitale løsninger, men drager i stedet fordel af ofres uopmærksomhed og manglende viden.

1. Baggrund

Rapporten tager udgangspunkt i sikkerheden i NemID og NemKonto, som var genstandsfelt for omtalte redegørelse. Rapporten vil have fokus på at beskrive igangsatte sikkerhedstiltag i den nævnte periode. Da MitID, der blev lanceret bredt i oktober 2021, på sigt skal erstatte NemID, er løsningen medtaget i denne rapport og vil også indgå i de fremtidige rapporter.

Rapporten vil ikke behandle oplysninger om omfanget af svindel med NemID og NemKonto, da Digitaliseringsstyrelsen i løbet af rapporteringsperioden har igang-

[1] https://www.ft.dk/samling/20201/almdel/BOU/bilag/163/index.htm

sat et arbejde, som har til formål at skabe et bedre og bredere overblik over omfanget af digitalt identitetstyveri af NemID og NemKonto i samarbejde med relevante parter. Resultaterne af dette arbejde forelægges i en særskilt rapport.

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 NemID sikret med to-faktor autentifikation, hvor brugerne skal identificere sig med to uafhængige redskaber i form af, på den ene side et brugernavn og adgangskode og på den anden side fx et nøglekort eller nøgleapp. 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 såkaldte "social engineering"-angreb, hvor svindlere eksempelvis ringer op til borgeren og snyder borgeren til at videregive personlige oplysninger eller foretage en handling til ugunst for sig selv, ved at give sig ud for at være fx fra banken, politiet eller en offentlig myndighed.

Digitaliseringsstyrelsen har som en del af den daglige forvaltning af de digitale løsninger etableret og tilpasset organisering og processer, som sikrer, at der løbende kan håndteres ændringer i trusselsbilledet og eventuelle konkrete sikkerhedshændelser i løsningerne.

2.1. Teknisk sikkerhed

Den tekniske sikkerhed i løsningerne bliver udviklet med udgangspunkt i det reelle trusselsbillede. Høj teknisk sikkerhed i de digitale løsninger er et kontinuerligt fokus i forvaltningen.

For at understøtte den løbende vurdering, evaluering og kontrol af it- og informationssikkerheden i de store it-løsninger i Digitaliseringsstyrelsen, som fx NemID og NemKonto, er det blandt andet implementeret løbende egenkontroller, penetrationstests, eksterne audits og eksterne tilsyn ved indhentning af revisionserklæringer hos leverandøren. Ydermere udarbejdes der ved hvert årsskifte et årshjul med konkrete opfølgningsindsatser med udgangspunkt i ISO-standarden for informationssikkerhed og reglerne for databeskyttelse. Aktiviteterne er målrettet de større it-systemer som fx NemKonto, NemID og MitID.

2.2. Sikker brugeradfærd og mitigerende handlinger

Det er ikke muligt at sikre sig fuldstændigt mod svindel, og it-kriminelle kan ikke stoppes fuldstændigt. It-kriminelle vil fortsat forsøge at kompromittere borgeres NemID-loginoplysninger med intention om at misbruge den pågældendes identitet, ofte med økonomisk gevinst for øje. Digitaliseringsstyrelsen arbejder løbende på at imødegå denne risiko, ligesom der løbende arbejdes med forebyggende ind-

satser rettet mod at styrke borgernes bevidsthed om sikker adfærd. Ud over aktiviteter rettet mod konkrete trusler som fx nedtagning af falske hjemmesider, har styrelsen stort fokus på at holde borgerne løbende orienteret om sikker digital adfærd og give konkrete råd til, hvordan de kan sikre sig imod identitetssvindel fx i form af informationskampagner. Digitaliseringsstyrelsen gennemfører fx 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, vil der opstå nye typer og muligheder for kriminalitet. Der foretages derfor løbende ændringer i de digitale løsninger som NemKonto, NemID og MitID for blandt andet at imødegå udviklingen i de it-kriminelles metoder. Dette uddybes for de enkelte løsninger nedenfor.

3. NemID og MitID

NemID/MitID-løsningen er en digital infrastruktur, der giver borgeren mulighed for at autentificere sig i en række selvbetjeningsløsninger. MitID blev lanceret bredt i primo oktober 2021 og skal i løbet af 2022 erstatte NemID løsningen til privat brug.

3.1. Øget sikkerhed i MitID i forhold til NemID

Med MitID-løsningen er der indarbejdet en række tiltag, der øger sikkerheden og mindsker muligheden for svindel. I MitID stilles der derfor højere krav til sikringen af brugernes identiteter.

- Med MitID introduceres en række nye identifikationsmidler, som er afgørende for løsningens generelle sikkerhed. Dette kan eksemplificeres ved, at nøglekortet udgår i MitID, og i stedet introduceres MitID app, som i store træk minder om NemID nøgleappen. Derudover introduceres nye fysiske identifikationsmidler til borgere, der ikke har lyst til eller mulighed for at bruge MitID appen.
- Der indføres med MitID sikkerhedstiltag, som gør det lettere for borgere at verificere, at deres MitID-oplysninger indtastes på en pålidelig hjemmeside, da mit.dk-domænet altid vil blive vist som sidste led i browserens adresselinje.
- Derudover benyttes notifikationer til at sikre, at borgerne altid bliver orienteret om kritiske hændelser i MitID – fx, hvis der logges ind på en ny enhed. Derudover kan borgere vælge at få besked, hver gang deres personlige MitID bliver anvendt.
- Til forskel fra NemID får man ikke en notifikation, når der er noget man skal godkende. I stedet skal man selv finde appen frem og åbne den. Tiltaget skærper opmærksomheden omkring anvendelsen af MitID-appen – og dermed brugernes opmærksomhed på ikke at godkende anmodninger, som de ikke selv har startet. En anmodning har en levetid på fem minutter, hvorefter den ikke længere kan anvendes til godkendelse.

3.2. Sikkerhedstiltag i perioden

- I august blev en ny funktionalitet til identitetssikring i NemID nøgleappen lanceret, der gør det muligt for borgere at opdatere deres id-oplysninger selvbetjent og digitalt via en identitetssikringsproces. Identitetssikringsprocessen er lanceret, fordi der i MitID er større krav til identitetssikring af borgere, end der har været gældende i NemID.
- Der opleves en stigning i phishing-angreb. Phishing-angrebene består i overvejende grad af, at kriminelle udgiver sig for at være Digitaliseringsstyrelsen med det formål at franarre uopmærksomme borgere deres NemID-oplysninger. Alene i tredje og fjerde kvartal i 2021 har Digitaliseringsstyrelsen anmodet om at få lukket 31 phishing-sider, som styrelsen er blevet gjort opmærksom på. Digitaliseringsstyrelsen har optimeret sine processer, når oplysninger om phishing-angreb modtages fra supporten, borgerhenvendelser eller lignende kanaler. Det betyder, at siderne kan tages hurtigere ned end hidtil. Dertil er det i kommunikation omkring de nye løsninger søgt at tydeliggøre, at offentlige myndigheder, herunder Digitaliseringsstyrelsen, kun sender breve til borgere via deres digitale postkasse, og at e-mails modtaget på private mail-domæner derfor aldrig vil være afsendt af Digitaliseringsstyrelsen.
- I oktober 2021 gennemførtes en opdatering af MitID-systemet. Opdateringen skulle sikre, at borgere, i alle situationer og uden mulighed for at fravælge det, modtager en øjeblikkelig advarsel, hver gang der foretages ændringer i borgerens personlige oplysninger på MitID.dk, således at borgeren kan spærre deres MitID, såfremt handlingen ikke er udført af borgeren selv. Opdateringen blev gennemført på baggrund af en artikel fra DR med kritik fra en række eksperter. Kritikken gik blandt andet på, at det ved et social engineering angreb, hvor det er lykkedes en kriminel at lokke en borger til at udlevere sit brugernavn og godkende anmodningen om log-in på MitID selvbetjening, er muligt at begå identitetstyveri via MitIDs selvbetjening, uden at borgeren får notifikationer om, at der er blevet ændret i borgerens personlige oplysninger. Denne mulighed blev fjernet med opdateringen.
- Dertil blev der i december 2021 indført endnu en ændring af MitID systemet, der højner sikkerheden i selvbetjeningsuniverset. Ændringen indfører en karensperiode for sikkerhedsmæssige kritiske indstillinger i selvbetjeningsuniverset, der betyder, at indstillingerne først kan udføres efter en karensperiode. Det betyder, at kritiske indstillinger kræver to autentifikationer, med en times mellemrum, og der sendes samtidig to notifikationer til borgeren om, hvad der sker. Dette tiltag beskytter derfor borgeren bedre mod social engineering-angreb. Digitaliseringsstyrelsen overvåger løbende udviklingen og vurderer løbende nye trusler.
- MitID's infrastruktur er, til forskel fra NemID, modulært og fleksibelt opbygget, og dermed har Digitaliseringsstyrelsen bedre mulighed for hurtigt at reagere det til enhver tid værende trusselsbillede.

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.

4.1. Sikkerhedstiltag i perioden

- Den 19. april 2021 blev der implementeret aktiveringsbrev i NemKontos selvbetjening. Det betyder, at borgere nu skal godkende og aktivere ændringer i deres NemKonto foretaget via selvbetjeningsløsningen på www.nemkonto.dk via en kode i et fysisk aktiveringsbrev, som borgeren får tilsendt til deres postadresse. Digitaliseringsstyrelsen har fra Finans Danmark i oktober 2021 modtaget tilkendegivelse på, at aktiveringsbrevet efter deres vurdering har medført en reduktion svindel med NemKonto.
- I juni 2021 har et eksternt sikkerhedsfirma foretaget en penetrationstest, en såkaldt "hacker-test" af NemKonto-systemet. Ved penetrationstesten er der ikke identificeret sårbarheder, der kan misbruges til at påvirke integriteten eller fortroligheden i systemet. Penetrationstesten medførte en række tekniske anbefalinger af mindre kritisk karakter. Anbefalingerne havde fokus på både at højne sikkerheden i webapplikationerne og sænke risikoniveauet yderligere. På baggrund af disse anbefalinger blev der sat en række udbedringer i værk, samt udarbejdet en plan for implementering af de resterende anbefalinger. De resterende anbefalinger forventes at være fuldt implementeret af leverandøren i 1. kvartal 2022.
- Der blev i august 2021 igangsat en auditundersøgelse i form af en analyse af, om der er sikkerhedsmæssige udfordringer forbundet med, at en borgers NemKonto kan tilknytte en 3. mands bankkonto. Undersøgelsen udføres af eksternt konsulentfirma og forventes færdig i næste afrapporteringsperiode.

5. Lovforslag om kompensationsordning

Finansministeren nedsatte i maj 2021 en arbejdsgruppe bestående af Justitsministeriet, Erhvervsministeriet og Digitaliseringsstyrelsen (på vegne af Finansministeriet), der har haft til formål at analysere problemstillinger i de nuværende gældende regler, som regulerer spørgsmål om hæftelse, erstatning og kompensation i forbindelse med misbrug af NemID/MitID i forhold til et eventuelt økonomisk tab. Arbejdet har vist, at der kan være situationer ved udbetalinger via NemKonto, hvor en borger lider et økonomisk tab ved svindel, også selvom borgeren ikke har handlet uagtsomt. Regeringen har udarbejdet et lovforslag, der er sendt i høring og forventes fremsat i foråret 2022. Med lovforslaget etableres en kompensationsordning, der skal sikre, at borgere kan få genudbetalt svindlede NemKonto-udbetalinger. Kompensationsordningen vil være gældende med ti års tilbagevirkende kraft, såfremt eventuelle krav bliver fremsat senest et halvt år efter lovens ikrafttrædelse.

6. Etablering af hotline

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. Hotlinen har åbent døgnet rundt 365 dage om året. Hotlinen har i perioden fra lanceringen til 2. januar 2022 modtaget ca. 3.500 opkald. Henvendelserne har fortrinsvist drejet sig om identitetstyveri blandt andet vedrørende NemID, MitID, NemKonto og CPR. En stor del af disse omhandler forebyggende rådgivning og formodninger om forsøg på identitetstyveri, eksempelvis gennem phishing-mails.