DIGITALISERINGSSTYRELSEN

Notat

06. januar 2023
AMANT/MJN
J.nr. 2021 - 5522

Sikkerhedsrapport: NemID/MitID og NemKonto

Indhold

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 NemID/MitID og NemKonto 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 del af monitoreringen af tre af Digitaliseringsstyrelsens systemer, NemID/MitID og NemKonto, udarbejdes der sikkerhedsrapporter, som har fokus på sikkerheden i systemerne. Den første rapport tilgik Folketinget i marts 2022[1]. Denne rapport udgør den anden afrapportering og dækker perioden fra primo januar 2022 til og med den 30. november 2022.

I rapporten redegøres for igangsatte sikkerhedstiltag i NemID/MitID og NemKonto i den nævnte periode, samt sikkerhedstiltag og erfaringer på bagkant af NemID–nedbruddet i sommeren 2022.

I takt med digitaliseringen af samfundet vil der opstå nye typer 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 NemID/MidID eller NemKonto. Der er sket en stigning i sager, hvor svindleren bruger den såkaldte "social engineering" metode, hvor de kontakter borgeren og snyder denne til at videregive personlige oplysninger eller foretage en handling til skade for sig selv[2]. Fokus er på at imødegå denne type svindel, ligesom der løbende arbejdes med forebyggende indsatser rettet mod at styrke borgernes 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 den første sikkerhedsrapport udgangspunkt i sikkerheden i NemID/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.

---

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

[2] Kilde: https://politi.dk/-/media/mediefiler/landsdaekkende-dokumenter/statistikker/oevrige-udgivelser/ncik-aarsrapport-2021.pdf

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 både NemID og MitID 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/kodeviser/kodeoplæser. Ligesom i den første sikkerhedsrapport fra marts 2022 har Digitaliseringsstyrelsen blandt andet iværksat løbende vurderinger, evaluering og kontrol af it- og informationssikkerhed. Det sker ved egenkontroller, penetrationstest, eksterne audits og eksterne tilsyn ved indhentning af revisionserklæringer hos leverandører. 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 ISO-standarden for informationssikkerhed og reglerne for databeskyttelse. I MitID er der indarbejdet tiltag, der øger sikkerheden og mindsker muligheden for svindel.

De tekniske sikkerhedstiltag kan ikke stå alene. Ud over aktiviteter rettet mod konkrete trusler, så 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 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 NemID/MitID og NemKonto 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 giver borgeren mulighed for at autentificere sig i en række selvbetjeningsløsninger. MitID blev lanceret bredt primo oktober 2021 som en erstatning for den eksisterende NemID-løsning til privat brug. MitID driftes parallelt med NemID frem til medio 2023, hvor NemID bliver nedlukket. Den lange paralleldrift er med til at sikre den bedst mulige overgang for borgerne.

NemID var fra den 22. til den 26. juni påvirket af et nedbrud, der bl.a. skyldtes, at leverandøren, Nets, ikke overholdt sine egne procedurer. Blandt andet er det efterfølgende kommet frem, at Nets ikke siden 2020, havde gennemført en disaster recovery test, hvor evnen til at genoprette systemer efter et nedbrud testes, på den del af løsningen, der var ramt af nedbruddet.

Nets har efter nedbruddet foretaget en række driftsforbedrende tiltag i NemID, og Nets har endvidere præsenteret en plan for implementering af en række yderligere aktiviteter, som skal rette op på de fejl og mangler, som hændelsen har bragt frem i lyset. I arbejdet hermed forholder Nets sig både til MitID og NemLog-in, da Nets er leverandør på disse løsninger. Digitaliseringsstyrelsen har bedt Nets afrapportere på effekten af og fremdriften i disse aktiviteter.

3.1. Sikkerhedstiltag i perioden

- Transaktionsteksten ved login i selvbetjeningen på mitid.dk er forbedret, da brugere havde svært ved at skelne mellem at logge ind med MitID generelt, og decideret at logge ind i selvbetjeningen. Dette er gjort mere klart således, at der nu står, at der logges på hos mitid.dk for at se eller ændre i brugerens MitID-oplysninger.
- Den digitale migreringsproces fra NemID til MitID, som kunne initieres af borgere enten via netbank eller via MitID.dk, er blevet justeret for at imødegå en type af svindel. Svindelscenariet gik ud på, at borgere, som allerede havde migreret til MitID, blev franarret deres NemID, der efterfølgende blev anvendt til at overtage den forurettedes MitID via en funktion i migreringsprocessen. Sikkerhedstiltaget fjernede denne mulighed.

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

- Siden sidste status er der blevet fulgt op på en række tekniske anbefalinger af mindre kritisk karakter, som udsprang af en penetrationstest, der blev udført i 2021. En penetrationstest er en såkaldt hacker-test af NemKonto-systemet. For løbende at teste systemet og for at sikre at fund fra seneste test er udbedret i tilstrækkelig grad, er der i medio december 2022 foretaget endnu en penetrationstest af NemKonto-systemet. Testen er udført af et eksternt sikkerhedsfirma og afrapporteringen forventes i januar 2023. Et eksempel på anbefalinger fra sidste års penetrationstest er implementering af månedlige sårbarhedsscanninger, hvor systemer og netværk automatisk scannes for eventuelle sårbarheder. Resultaterne af disse sårbarhedsscanninger er løbende blevet håndteret, og forekomsten af sårbarheder har været aftagende gennem året.
- I foråret 2022 blev en auditundersøgelse af NemKonto afsluttet af et eksternt konsulentfirma. Auditundersøgelsen fandt, at man med fordel kunne arbejde

for bedre rammer for datadeling og samarbejde med eksterne parter. Endvidere påpegede audit nogle muligheder for ændret funktionalitet i håndteringen af anvisningen af 3. mands konti. Digitaliseringsstyrelsen har forholdt sig til undersøgelsens resultater.

- Der er i 2022 nedsat en samarbejdsgruppe om identitetstyveri af MitID og svindel med NemKonto mellem Digitaliseringsstyrelsen, Finans Danmark, Finans & Leasing og National Enhed for Særlig Kriminalitet. Gruppen videndeler og følger løbende udvikling og tendenser på området.
- Der er i 2022 arbejdet på at klargøre udbuddet af et nyt NemKonto-system. I den forbindelse er der blandt andet afholdt flere workshops med en række parter – herunder finans- og lånesektoren. I denne forbindelse har der især været fokus på mulighederne for i højere grad at udveksle data med henblik på at bekæmpe svindel, og det undersøges, om man i det nye NemKonto kan bidrage til at forebygge og opdage forsøg på svindel gennem udstilling af risikodata. Risikodata kan eksempelvis benyttes til at varsle om usædvanlig aktivitet, der kan indikere svindel, hvilket giver bedre muligheder for at udføre ekstra kontroller.
- 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. Derudover undersøger en tværministeriel arbejdsgruppe, om der kan gøres yderligere for at hjælpe borgere, der har været udsat for svindel med NemKonto.

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. Hotlinen har åbent døgnet rundt 365 dage om året. Hotlinen har i perioden fra 1. januar 2022 til og med 13. november 2022[3] besvaret ca. 6.900 opkald.

De ca. 6900 opkald fra den 1 januar til den 13 november 2022 er kategoriseret således (pct.)[4]:

- 17 pct. er relateret til misbrug af borgerens identitet
- 36 pct. er relateret til risiko for identitetstyveri, da borgerens oplysninger har været tilgængelig i forbindelse med svindel
- 6 pct. relaterer sig til forsøg på identitetstyveri, eksempelvis gennem phising, men hvor borgeren undlod at udlevere oplysninger.
- 17 pct. er relateret til efterspørgsel på vejledning for forebyggelse af identitetstyveri

[3] Det har ikke været muligt at få konsolideret tal fra de sidste to uger i november 2022.
[4] Hotlinen verificerer ikke, hvorvidt det er korrekt om en borger eksempelvis har været udsat for svindel. Tallene skal desuden læses med forbehold for, at 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.

- 23 pct. er uden for scope.