Retsudvalget 2020-21
REU Alm.del - Bilag 456
Offentligt

Nationalt Efterforskningscenter (NEC)

POLITI

Uretmæssig adgang til NemID

Kortlægning af politianmeldte forsøg på tilegnelse af og uretmæssig anvendelse af andre personers NemID i perioden 2017-2020

Indholdsfortegnelse

Resumé

Antallet af anmeldelser om forsøg på uretmæssig adgang til og/eller anvendelse af andre personers NemID-oplysninger steg i perioden 2017-2020 fra 3012 til 9172. Den største stigning forekom fra 2019 til 2020, hvor antallet af anmeldelser steg fra 3645 til 9172.
Hovedårsagerne til stigningen formodes at være udbredelse af krav om verificering med NemID i forbindelse med betaling på webshops og onlinetjenester samt ændringer i kriminalitetsbilledet under Covid-19pandemien. Begge årsager har ført til, at berigelseskriminelle har øget interesse i at anskaffe og anvende andre personers NemID.
Gerningspersonerne opnår primært uberettiget adgang til NemID ved at franarre forurettede oplysningerne gennem såkaldt social engineering, som eksempelvis phishing mails og fupopkald (vishing).

Baggrund for temarapporten

It-relateret økonomisk kriminalitet er i hastig og konstant udvikling. Dette antages også at gælde uretmæssig anvendelse af NemID. I takt med at flere onlineydelser og tjenester forudsætter verificering med NemID, er gerningspersoner tvunget til at tilegne sig oplysninger fra deres ofre for at kunne gennemføre internet-relateret økonomisk kriminalitet.
I 2019 udarbejdede Nationalt Efterforskningscenter i Rigspolitiet (NEC) en analyse af omfanget af misbrug af identitetsbeviser til it-relateret økonomisk kriminalitet for årene 2013-2018. I analysen indgik også uretmæssig anvendelse af NemID, og det blev konstateret, at antallet af anmeldelser om uretmæssig anvendelse af NemID også i den periode var stigende. Der er fra flere myndigheders side en interesse i at afdække, om dette fortsat er tilfældet. Dette for at have et overblik over erkendte sårbarheder ved NemID og

som risikovurdering til det kommende MitID, der bliver lanceret fra oktober 2021[1].

Denne temarapport er udarbejdet med henblik på at afdække omfanget af anmeldelser, hvor gerningspersoner har forsøgt at få uretmæssig adgang til og/eller har misbrugt andre personers NemID-oplysninger i perioden 2017-2020. Endvidere gennemgås de væsentligste årsager til årlige udsving samt de hyppigste modi operandi brugt ved forsøg på illegal tilegnelse af andres NemID-oplysninger.

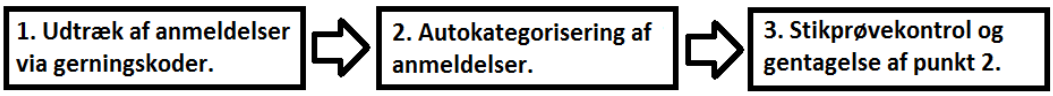
Datagrundlag, metode og dokumentation

De data, der ligger til grund for temarapporten er trukket fra Politiets Sagsstyringssystem (POLSAS) via dataanalysesystemet QlikView.
Det er ikke muligt at identificere NemID-relaterede anmeldelser direkte via QlikView. Det skyldes, at der ikke er en specifik kategori for anmeldelser i politiet, der omhandler NemID.
Dog kan en række *gerningskoder* baseret på straffeloven anvendes til at identificere sagskategorier, der involverer misbrug af NemID[2]. Derfor er der trukket anmeldelser, der ligger inden for disse gerningskoder. Disse gerningskoder indeholder dog også mange anmeldelser, der ikke indebærer misbrug af NemID.

[1]Jævnfør https://digst.dk/it-loesninger/mitid/fra-nemid-til-mitid/.

[2] Disse er identificeret ved hjælp af søgenøgler, som er et andet kategoriseringsværktøj, der anvendes i politiets systemer. Det ligger dog uden for dette notat at beskrive denne proces i detaljer.

Med henblik på at frasortere de irrelevante anmeldelser, er der benyttet *autokategorisering*. Autokategorisering består i, at en række søgeord anvendes til at fremfinde relevante anmeldelser[3]. Det gøres ved at holde søgeordene op mod *sagens resumé*, som er et tekstfelt tilknyttet samtlige anmeldelser i politiets systemer, der kort angiver, hvad anmeldelsen omhandler.
I figuren nedenfor ses proceduren for udtræk af data.



Figur 1: Procedure for udtræk af data og identificering af anmeldelser relateret til misbrug af NemID.

Autokategoriseringen gør det muligt at identificere relevante anmeldelser, men der tages forbehold for falsk positive og falsk negative tilfælde. I nogle tilfælde vil de anvendte søgeord resultere i, at irrelevante anmeldelser udpeges som relevante (falsk positive). Dette sker, fordi sagens resumé indeholder søgeordene, til trods for at anmeldelsen ikke beror på forsøg på tilegnelse eller uretmæssig anvendelse af NemID. I andre tilfælde, hvor sagens resumé ikke er udfyldt med et anvendt søgeord, vil en ellers relevant anmeldelse blive udeladt (falsk negativ).

Ideelt ville det være muligt at gennemgå alle de udtrukne anmeldelser manuelt i stedet for at anvende autokategorisering. Som det fremgår af nedenstående tabel, der viser antallet af anmeldelser, som er udtrukket via gerningskoder samt anmeldelser, der er udpeget som værende NemID-relaterede, er dette ikke muligt, da det ville kræve et betydeligt tidsforbrug. I tabellen ses det, at 18.624 ud af 269.066 udtrukne anmeldelser på baggrund af autokategorisering antages at involvere misbrug af NemID.

[3] Eksempelvis forskellige måder, hvorpå 'NemID' kan skrives. Dertil kommer forskellige kriterier for, hvornår sager skal udelades. Dette eftersom ordet "NemID" i nogle sager optræder, uden at sagen vedrører misbrug af NemID. Dette er der så vidt muligt taget højde for ved brug af ekskluderingskriterier i autokategoriseringen.

	Antal anmeldelser
Ikke NemID-relaterede anmeldelser	250.442
NemID-relaterede anmeldelser	18.624
I alt	269.066

Tabel 2: NemID og ikke NemID-relaterede anmeldelser.

Som det fremgår af trin 3 i figur 1 ovenfor, er der lavet stikprøvekontrol på de 18.624 autokategoriserede anmeldelser for at sikre, at mængden af falsk positive anmeldelser ikke er uhensigtsmæssigt stor. Der er udpeget i alt 300 tilfældigt udvalgte autokategoriserede anmeldelser, som er gennemgået manuelt[4]. Disse fremgår af tabel 3. Ud af de 300 manuelt gennemgående anmeldelser er 23, svarende til 7 procent, falsk positive, mens 5, svarende til 2 procent, ikke kan bedømmes ud fra manglende beskrivelse i sagens resumé.

	Procent	Antal
Falsk positiv	7	23
Kan ikke bedømmes	2	5
Rigtigt kategoriseret	91	272
I alt	100	300

Tabel 3: Stikprøvebaseret hitrate på autokategoriserede NemID-relaterede anmeldelser.

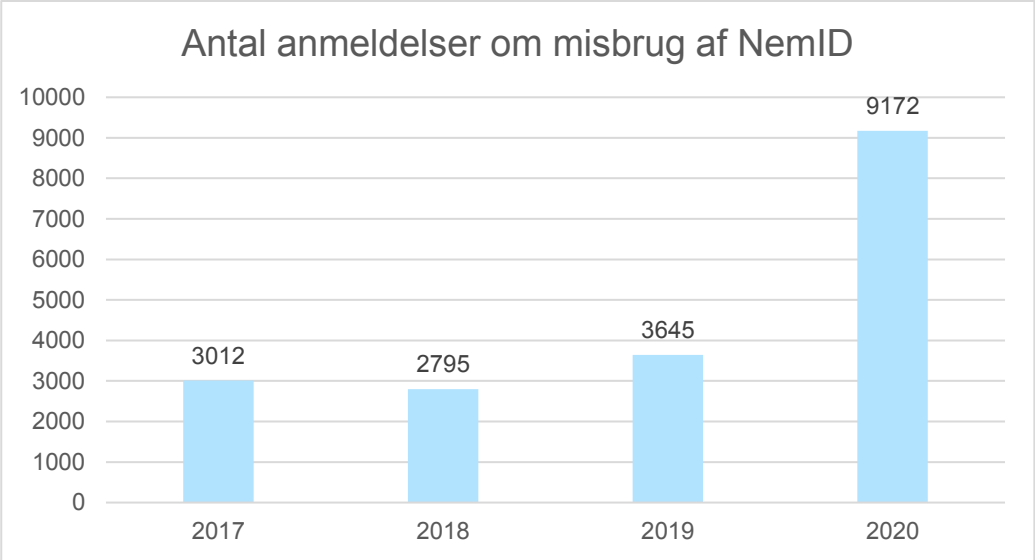
Således er 272, dvs. 91 procent, rigtigt kategoriseret. Dette vurderes at være en acceptabel hitrate, om end stadig behæftet med en vis fejlmargin. Dog vil mængden af falsk *negative* tilfælde med overvejende sandsynlighed

[4] Der er desuden lavet flere andre stikprøvekontroller i autokategoriseringsprocessen for at finde de mest rammende søgeord. Dette belyses dog ikke nærmere her.

opveje resultatet[5]. Derfor vurderes det ikke relevant at nedjustere antallet af anmeldelser.

Anmeldelser om forsøg på uberettiget tilegnelse eller anvendelse af NemID

Som det fremgår af nedenstående tabel, er der et fald i antallet af anmeldelser fra 3012 til 2795 i perioden 2017 til 2018. Fra 2018 til 2019 er antallet steget til 3645, hvorefter en yderligere stigning ses fra år 2019 til 2020, hvor anmeldelsestallet er 9172. Den største stigning ses fra 2019 til 2020, hvor antallet af anmeldelser er mere end fordoblet.



Tabel 1: Antal anmeldelser om misbrug af NemID i perioden 2017-2020.

De to væsentligste årsager til den markante stigning fra 2019 til 2020 formodes at bestå i indførelsen af EU's Payment Service Directive 2 (PSD2),

[5]Det vurderes for tidskrævende at lave en repræsentativ manuel gennemgang af de ikke NemID-relaterede anmeldelser med henblik på at identificere falsk negative tilfælde. Dette fordi antallet af ikke NemID-relaterede anmeldelser er mere end 25 gange større end antallet af NemID-relaterede anmeldelser. Derved har de falsk negative tilfælde en markant større pulje at "gemme sig" i.

og det deraf følgende krav om Strong Customer Authentication (SCA) samt Covid-19pandemien.

PSD2 omhandler skærpede sikkerhedsmæssige krav til elektroniske betalinger og trådte i kraft 14. september 2019. Et af kravene, der følger af PSD2, er SCA, der. indebærer, at betalinger på internettet skal verificeres af kunden[6]. Konkret betyder dette, at tofaktorgodkendelse, i form af eksempelvis NemID[7], er påkrævet for at kunne gennemføre elektroniske betalinger i Danmark eller i andre EU-lande. Dermed er det ikke længere tilstrækkeligt for kriminelle at opsnappe et betalingskort fra en forurettet og anvende kortnummeret til at gennemføre økonomisk kriminalitet. Da implementeringen af kravet om SCA var varslet til september 2019, er det vores vurdering, at den kriminelle efterspørgsel efter NemID fra dette tidspunkt var stigende, hvilket delvist kan forklare den markante stigning i antallet af anmeldelser fra 2019 til 2020[8].

Covid-19 har ændret forholdene for kriminelle aktører, ikke mindst på berigelsesområdet. I den forbindelse formodes f.eks. borgernes øgede tidsforbrug i eget hjem at have forskubbet fysisk berigelseskriminalitet og svindel til internettet. Dette ændrede adfærdsmønster i befolkningen vurderes at være den væsentligste årsag til stigningen i anmeldte sager om forsøgt tilegnelse eller uberettiget anvendelse af NemID tilhørende andre personer.

[6] Der findes en række undtagelser. Eksempelvis er køb for mindre beløb, dvs. 30 euro eller mindre, undtaget. Reference: https://info.nets.dk/blog/sca-og-psd2-s%C3%A5dan-fungerer-de-nye-eu-krav-til-online-kortbetalinger

[7] Et andet eksempel er, at den betalende part modtager en sms med et kodeord, som derefter skal bruges til at verificere transaktionen. Reference: https://euipo.europa.eu/ohimportal/da/news/-/action/view/8410243

[8] Det skal anføres, at kravet om SCA blev udskudt til først at træde i kraft januar 2021. Dog formodes den først varslede dato om SCA-kravet, 14. september 2019, at være anledning til erhvervelse af tofaktorgodkendelse for mange webshops og lignende. SCA antages derfor alligevel at have influeret omfanget af NemID-svindel i ultimo 2019 og hele 2020.

Øget digitalisering i samfundet samt oprettelse af politiets Landsdækkende Center for It-relateret økonomisk Kriminalitet (LCIK) og deraf en mere detaljeret registreringspraksis af anmeldelser vurderes også at være blandt årsagerne til stigningen i hele perioden fra 2017 – 2020.

Typer anmeldelser

De identificerede anmeldelser dækker over uberettiget adgang til NemID på to forskellige stadier:

1) Anmelderen opdager, at nogen forsøger at få adgang til vedkommendes NemID-oplysninger. Dette kan eksempelvis være en borger, der bliver ringet op af en påstået myndighedsperson, som forsøger at franarre anmelderen NemID-oplysninger. Undervejs bliver anmelderen skeptisk, afbryder samtalen og anmelder svindelforsøget til politiet.
2) Anmelderen opdager, at vedkommendes NemID er misbrugt. Dette eksempelvis ved, at der er forsvundet store pengesummer fra vedkommendes bankkonto, hvorefter forholdet anmeldes.

Ved anmeldelser på første stadie har anmelderen ikke lidt et økonomisk tab. Det er derimod ofte tilfældet på andet stadie. En andel af anmeldelserne i tabel 1 omfatter således ikke uberettiget anvendelse af NemID, men blot forsøg på at få adgang til NemID-oplysninger. Der formodes desuden at være væsentlige mørketal vedrørende tilfælde på første såvel som andet stadie. For tilfælde på første stadie vurderes eksempelvis kun en begrænset andel af det totale antal forsøg på phishing at blive anmeldt til politiet, da fraværet af økonomisk tab mindsker incitamentet til anmeldelse. For tilfælde på andet stadie, hvor ofre har lidt økonomisk tab, kan ofrene føle skam over at være blevet snydt eller mangle kendskab til, at eller hvordan de har mistet penge, hvilket kan medføre, at forseelsen ikke anmeldes.

Typiske modi operandi

I det følgende gennemgås de hyppigst observerede måder, hvorpå gerningspersoner tilegner sig ofres adgangsoplysninger om NemID. De nævnte eksempler skal ses som oplagte modi operandi i perioden 2017-2020. Sikkerhedsbrister ved NemID er løbende identificeret og elimineret af såvel myndigheder som digitale udbydere. Således kan sårbarheder, der tidligere har muliggjort de enkelte modi operandi, være helt eller delvist elimineret i dag.

Phishing

Phishing består i, at gerningspersonen kontakter forurettede via eksempelvis e-mail eller sms (sidstnævnte såkaldt ”smishing”). Henvendelsen kan ligne en myndighedsmeddelelse om, at pågældende myndighed skal bruge vedkommendes NemID-oplysninger. I e-mails er der ofte indsat et link til en falsk hjemmeside i henvendelserne, hvor forurettede anmodes om at indtaste NemID-oplysningerne. Hjemmesiden er udarbejdet af gerningspersonen og ligner en reel myndighedshjemmeside. Når forurettede indtaster sine NemID-oplysninger, gemmes de af gerningspersonen, så denne kun mangler oplysninger om forurettedes nøglekort, hvilket kan omgås ved enten at anvende forurettedes indtastede nøgleoplysning til at bestille nyt nøglekort eller ved at anmode forurettede om at sende et billede af sit nøglekort, f.eks. under påskud af, at der er sket en fejl ved indtastningen.

Vishing

Vishing består i, at gerningspersonen kontakter forurettede telefonisk og ad denne vej forsøger at franarre forurettede NemID-oplysninger. Dette kan foregå på mange forskellige måder. Eksempelvis kan gerningspersonen ringe til forurettede og udgive sig for at være bankansat. Den ”bankansatte”

fortæller forurettede, at der har været indbrud i ofrets netbank, og at forurettede bør oplyse sine NemID-oplysninger for at forhindre gerningspersonen i at tømme forurettedes konti.
I andre tilfælde ringer gerningspersonen til forurettede og udgiver sig for at være ansat i Microsoft, hvorefter gerningspersonen fortæller, at forurettedes computer er blevet hacket. Forurettede oplyses om, at problemet kan løses, såfremt vedkommende oplyser sine NemID-oplysninger.

Gerningspersonen kan også ringe under dække af at være fra offentlige myndigheder eksempelvis politiet. ”Politibetjenten” fortæller forurettede, at vedkommende er offer for en forbrydelse, f.eks. identitetsmisbrug, og at dette kan forhindres, såfremt ofret videregiver NemID-oplysninger.

Dating scam

Dating scam (også kaldet ”romance scam”) består i, at gerningspersonen opnår kontakt til forurettede gennem en datinghjemmeside, dating app, sociale medier eller lignende, under påskud af, at der er tale om en romantisk online-relation. Gerningspersonen misbruger derefter foruretteres tro på relationen til at lokke oplysninger ud af forurettede, herunder NemID.
Dating scam optræder også i samspil med vishing. Eksempelvis er der tilfælde, hvor svindlere gennem datingsites har opnået kontakt til forurettede, der tror, at en romantisk relation er hensigten. Efterfølgende har personerne udvekslet telefonnumre via datingsiden og har skrevet sammen via sms. Svindleren har derefter sendt en sms-besked til forurettede om, at telefonen er blevet hacket og videre ringet til forurettede under påskud af at være en politibetjent, der ønsker at finde svindleren. For at kunne hjælpe forurettede har ”politibetjenten” dog brug for forurettedes NemID-oplysninger, hvilket forurettede derfor oplyser.

Keylogging

Keylogging er software og hardware, der gør det muligt at lagre tastetryk, der bliver foretaget på en computer. Derved kan gerningspersonen opnå kendskab til adgangsoplysninger om NemID. Keylogging er primært set i tilfælde, hvor gerningspersonen installerer en keylogger på en offentlig computer, f.eks. på et bibliotek eller i et jobcenter, der anvendes af mange andre personer til f.eks. at tilgå e-Boks og borger.dk. Herefter har svindleren indblik i koderne til personernes NemID. Nu kan gerningspersonen enten forsøge at stjæle personernes nøglekort eller via sin adgang til den offentlige computer følge med i antallet af tilbageværende nøgler på forurettedes nøglekort. Såfremt et nyt nøglekort sendes til forurettede, vil gerningspersonen kunne stjæle det fra forurettedes postkasse og således have adgang til både koder og nøgler.

Bekendte/familie til forurettede

I visse tilfælde benyttes forurettedes NemID uretmæssigt af personer, som forurettede kender. Det kan være personer, der er ansat til at hjælpe forurettede i hverdagen, f.eks. hjemmehjælpere eller socialpædagoger, der i deres job har fået adgang til forurettedes NemID og misbrugt denne viden. Det kan også være personer med personlige relationer til forurettede, såsom kærester eller anden familie, der har fået NemID-oplysninger udleveret af forurettede selv og derefter misbrugt det til uretmæssig økonomisk vinding.

Konklusion

Antallet af anmeldelser om forsøg på uretmæssig adgang til og/eller anvendelse af andre personers NemID-oplysninger er i perioden 2017-2020 steget fra 3.012 til 9.172 anmeldelser. Gerningspersonerne anvender primært metoder som phising-mails og fupopkald til at franarre NemID-oplysninger. Ingen af disse svindelmetoder involverer tekniske mangler ved NemID-systemet, men udnytter i stedet ofres uopmærksomhed og manglende viden. Fremadrettet forebyggende arbejde på området bør derfor baseres på indsatser, der mindsker risikoen for, at svindlere kan narre brugere af NemID til at udlevere deres oplysninger.