

Afvisning af påstande om sikkerhedsbrist i NemIDs Java applet

11. august 2010

Børsen bragte den 10. august 2010 en artikel med overskriften "Sikkerhedsbrist truer den nye digitale signatur", hvori der fremsættes en række påstande omkring en sikkerhedsbrist i den Java applet, som NemID anvender.

IT- og Telestyrelsen og DanID kan hermed dementere, at der er en sikkerhedsbrist i NemID eller den Java applet, som NemID gør brug af.

DanID, som varetager udvikling og drift af NemID, har talt med den ene af de to citerede eksperter, Mikael Hertig. Han har erkendt, at der er tale om en misforståelse, og han har efterfølgende udtalt følgende: "Mikael Hertig udtaler til Nensome Note, at han med større vægt burde have pointeret overfor Børsen, at han ikke selv er i stand til at vurdere, om der er noget hul i NemID eller ikke." Udtalelsen kan læses i sin helhed her:

<http://www.nensome.dk/default.asp?Dok=239&Emne=0>.

DanID har forgæves forsøgt at komme i kontakt med den anden citerede ekspert, Niels Elgaard Larsen, men IT-politisk Forening, som Niels Elgaard Larsen repræsenterer, har gennem bestyrelsesmedlem Jørgen Elgaard Larsen i en kommentar på Computerworld udtalt, at "Kommunikationschefen har uden tvivl ret i at deres konkrete, nuværende applet ikke i sig selv giver adgang til brugerens computer, og det har IT-pol da heller aldrig sagt.". Hele kommentaren kan findes her: <http://www.computerworld.dk/art/100522/quot-nemid-aabner-ikke-for-personlige-oplysninger-quot?threadid=20880#postauthor62673>.

Professor i IT-sikkerhed afviser påstandene

Professor i it-sikkerhed ved Aarhus universitet, Ivan Bjerre Damgård, bekræfter over for Computerworld, at NemIDs Java applet ikke lider af de påståede sikkerhedsbrister. "Det, IT-Politisk Forening siger, er, at en vilkårlig applet kan give adgang til personlige oplysninger, hvilket er korrekt, men i forbindelse med NemID er der ikke tale om en vilkårlig applet," siger han. Artiklen kan læses i sin helhed her: http://www.computerworld.dk/art/100522/quot-nemid-aabner-ikke-for-personlige-oplysninger-quot?a=fp_1&i=0.

IT- og Telestyrelsen

Holsteinsgade 63
2100 København Ø
Telefon 3545 0000
Telefax 3545 0010
E-post itst@itst.dk
Netsted www.itst.dk
CVR-nr. 26769388

Sagsbehandler

Stine Kern Licht
Telefon 3545 0388
Telefax 3545 0010
E-post skli@itst.dk

Sagsnr. 10-091414
Dok nr. 1478480
Side 1/1

Afvisning af de enkelte påstande

Af Børsens artikel fremgår følgende påstande:

1. Det er muligt for en myndighed at snage i den enkelte NemID-brugers personlige forhold.
2. Tjenesteudbydere, der er koblet på systemet, kan gå baglæns i transmissionen og aflure brugeren.
3. Når brugeren besøger en tjenesteudbyder, har ikke alene denne tjenesteudbyder, men alle tjenesteudbydere, der er tilsluttet NemID, fuld adgang til brugerens computer.
4. Appletten bliver automatisk installeret på brugerens computer.
5. En tjenesteudbyder har adgang til oplysninger, som brugeren har liggende hos andre tjenesteudbydere.
6. En kvik Java ekspert vil kunne lave en applet, der kan sættes i gang uden brug af engangskoder.

IT- og Telestyrelsen

Nedenfor gennemgås og tilbagevises de enkelte påstande fra Børsens artikel.

Side 2/2

Ad 1 - Det er muligt for en myndighed at snage i den enkelte NemID-brugers personlige forhold

NemID appletten fra DanID anvendes til entydigt at identificere en bruger over for en bestemt tjenesteudbyder, det kan være en bank, en offentlig myndighed eller en privat tjenesteudbyder.

NemID appletten hentes direkte fra DanID ned til brugerens computer uden om tjenesteudbyderen, og når brugeren har identificeret sig selv via NemID appletten, sender den en besked tilbage til tjenesteudbyderen med brugerens identitet. Dialogen mellem NemID appletten på brugerens computer og DanIDs centrale server, der etablerer brugerens identitet, er krypteret og sikret efter de højeste standarder. DanID har fået en lang række af verdens førende sikkerhedseksperter til at teste og reviewe alle dele af systemet.

Tjenesteudbyderen sørger for, at NemID appletten bliver startet hos brugeren, men kommer ikke direkte i kontakt med appletten. Tjenesteudbyderen modtager efterfølgende et simpelt svar fra appletten, der er signeret med brugerens digitale signatur.

Det er derfor på ingen måde muligt for en tjenesteudbyder at anvende NemID appletten til at tilgå personlige data på brugerens computer.

Ad 2 – Tjenesteudbydere, der er koblet på systemet, kan gå baglæns i transmissionen og aflure brugeren

Tjenesteudbyderen modtager kun den signerede log-in besked og har ikke nogen transmission at gå tilbage i.

Ad 3 - Når brugeren besøger en tjenesteudbyder har ikke alene denne tjenesteudbyder, men alle tjenesteudbydere, der er tilsluttet NemID, fuld adgang til brugerens computer

Det, Niels Elgaard Larsen her formentlig henviser til, er det forhold, at NemID appletten kræver læse- og skriveadgang til brugerens harddisk af hensyn til caching. For at et Java program afviklet i en browser kan få sådan en adgang, skal programmet være signeret med en digital signatur, og brugeren skal acceptere, at programmet får denne adgang.

Dette er en helt normalt fremgangsmåde, og det er den samme teknologi, som stort set alle eksisterende netbanksløsninger og den gamle digitale signatur anvender.

Det er kun NemID appletten, der har læse- og skriveadgang, og denne adgang stilles ikke til rådighed for nogen tjenesteudbyder. NemID appletten læser på intet tidspunkt personlige filer fra brugerens computer.

IT- og Telestyrelsen

Side 3/3

Ad 4 - Appletten bliver automatisk installeret på brugerens computer

Der er ikke tale om en installation af et program. På lige fod med andet internetindhold gemmes en lokal kopi på et særligt sted (cache) på brugerens computer. Derved kan appletten startes hurtigere, næste gang brugeren vil logge på med NemID. Brugeren skal aktivt give tilladelse til at køre appletten, før denne afvikles.

Ad 5 - En tjenesteudbyder har adgang til oplysninger, som brugeren har liggende hos andre tjenesteudbydere

En tjenesteudbyder tilsluttet NemID har ingen adgang til de oplysninger, der er registreret hos DanID eller hos andre tjenesteudbydere.

En tjenesteudbyders adgang strækker sig til, at man ved log-in kan sørge for, at NemID appletten bliver startet hos brugeren og efterfølgende få et svar tilbage, der er signeret med brugerens digitale signatur, og som kan anvendes til at etablere brugerens identitet. Efterfølgende laver tjenesteudbyderen et opslag hos DanID, der checker, om brugerens certifikat er gyldigt. Derudover har tjenesteudbyderen ikke andre adgange til oplysninger.

Ad 6 - En kvik Java ekspert vil kunne lave en applet, der kan sættes i gang uden brug af engangskoder

Hvis nogen laver deres egen applet, vil den ikke være signeret af DanID, og den vil ikke kunne komme i kontakt med DanIDs centrale systemer. Det er kun via DanIDs centrale systemer, at brugeren kan generere en gyldig signatur eller signere et dokument.