

Identificatie op afstand met zo min mogelijk rompslomp

REMOTE VETTING IS UITDAGENDE OPLOSSING VOOR 2FA

IDENTIFICATIE VAN DE GEBRUIKER IS EEN BELANGRIJKE VOORWAARDE VOOR BETROUWBARE TWEEFACTORAUTHENTICATIE. ZO MIN MOGELIJK ROMPSLOMP VAN FYSIEKE IDENTIFICATIE IS HIERBIJ DE UITDAGING, VOLGENS PETER CLIJSTERS EN PIETER VAN DER MEULEN. DAAR ZIJN VERSCHILLENDE METHODEN VOOR, DIE ELK HUN VOOR- EN NADELEN HEBBEN. SURF EXPERIMENTEERT NU MET NIEUWE METHODEN VOOR IDENTIFICATIE OP AFSTAND.

door Peter Clijsters en Pieter van der Meulen beeld Shutterstock

DE RECENTE PROBLEMEN BIJ CITRIX EN DE RISICO'S VAN RANSOMWARE HEBBEN DE URGENTIE VAN EEN GOEDE TOEGANGSBEVEILIGING WEER EENS ONDERSTREEPT. Ook de onderwijs- en onderzoekssector loopt risico's op dit gebied, zoals te zien was bij de gijzeling van de Universiteit Maastricht eind vorig jaar. Toegangsbeveiliging is dan ook een belangrijk thema voor SURF, de ICT-samenwerkingsorganisatie die er samen met de onderwijs- en onderzoeksinstituten voor zorgt dat ze kunnen beschikken over veilige en innovatieve ICT-voorzieningen.

De klanten van SURF werken met waardevolle gegevens. Denk aan studentinformatiesystemen, applicaties met onderzoeksdata of privacygevoelige patiëntinformatie. Voor deze gegevens en systemen zijn sterkere vormen van beveiliging nodig om de risico's af te dekken. TwEEfactorauthenticatie is dan een noodzakelijk middel: SURF biedt hiervoor een gedegen proces aan met SURFsecureID (zie kader). Daarbij logt de gebruiker in met een gebruikersnaam, wachtwoord én met een tweede factor: een sms, USB-sleutel of app.

PRAKTISCHE PROBLEMEN

Het proces is weliswaar gedegen, maar ook omslachtig: het grote nadeel is dat elke gebruiker fysiek bij de ICT-service-desk moet langskomen om zich te identificeren. Daar moeten de gebruiker, het

bestaande account en de tweede factor met voldoende zekerheid aan elkaar worden verbonden. Bij de ontwikkeling van SURFsecureID is gekozen voor maximaal betrouwbare identiteiten, waarbij wordt geverifieerd dat de tweede factor ook echt in het bezit is van de gebruiker. Een organisatie wil zeker weten dat degene aan wie ze een tweede factor hebben gegeven, ook degene is die in de gebruikersadministratie staat. Daarin verschilt het product met veel andere producten in de markt. Alleen: de hoge betrouwbaarheid gaat wel ten koste van de gebruikersvriendelijkheid. De problemen zijn nog te overzien als het gaat om medewerkers van de instellingen. De procedure is vooral lastig voor gebruikers van andere organisaties, die samenwerken met universiteiten en hogescholen, en voor gebruikers in het

'BIJ EEN EN/OF-REKENING ZOU DE ACHTERNAAM VAN DE PARTNER DOORGEGEVEN KUNNEN WORDEN'



buitenland. Soms worden daar ad-hoc-oplossingen voor bedacht. Denk aan het opzetten van een (remote) videoverbinding met een gebruiker in het buitenland. Omdat een identiteitsbewijs dan moeilijk te verifiëren is, wordt bijvoorbeeld de manager van de medewerker gevraagd om de identiteit van de medewerker te bevestigen. Dat is een maatregel tegen misbruik, maar ideaal is het niet.

IDENTIFICATIE OP AFSTAND

Om dat proces eenvoudiger te maken en toch de betrouwbaarheid te waarborgen, is gekozen voor identificatie op afstand, ook wel 'remote vetting' genoemd. Dat proces moet gemakkelijker, goedkoper en schaalbaarder worden gemaakt. Daarvoor is het nodig om zo praktisch mogelijk te werk te gaan, met een goede balans tussen kosten, gebruikersvriendelijkheid en betrouwbaarheid. De oplossing moet passen bij de vragen van klanten. Het doel is om een voor de gebruiker volledig selfserviceproces te ontwikkelen, met behoud van betrouw-

baarheid. Inmiddels zijn er al verschillende methoden in omloop die gebruikt kunnen worden voor betrouwbare identificatie. Een bekend voorbeeld is DigiD, maar het gebruik daarvan is grotendeels beperkt tot de overheid. Een van de dingen waar ontwikkelaars in Nederland tegenaan lopen, is de strenge privacywetgeving; om die reden kan geen enkele partij buiten de overheid

SURFSECUREID

SURFsecureID is een dienst van SURF voor het onderwijs (mbo, hbo en wo) en onderzoek in Nederland om as-a-service een tweede authenticatiefactor (sms, USB-sleutel of app) toe te voegen aan de bestaande accounts van gebruikers bij instellingen. Hiermee kan worden ingelogd bij diensten binnen

en buiten de instelling. SURFsecureID maakt gebruik van de door SURF ontwikkelde opensourcesoftware OpenConext Stepup.

Meer informatie:

- www.surf.nl/surfsecureid
- <https://openconext.org/stepup>

AUTEUR



PETER CLIJSTERS
is productmanager
SURFsecureID bij SURF.



PIETER VAN DER MEULEN
is technisch productmanager SURFsecureID bij SURF.

‘Bij de NFC-optie wordt een klein filmpje gemaakt om vast te stellen of het gaat om een persoon’

gebruikmaken van het burgerservicenummer (BSN). Een andere methode die voor identificatie gebruikt kan worden, zijn de tokens van de verschillende banken. Omdat de gebruiker van deze tokens zich ooit bij de bank heeft geïdentificeerd, is de betrouwbaarheid ervan redelijk groot.

VOOR- EN NADELEN

Elk van deze methoden heeft zijn voor- en nadelen. Bij de NFC-optie is dat vooral een kwestie van techniek: het

werkt alleen met recente identiteitsbewijzen en smartphones. Zo is de benodigde functionaliteit bij Apple pas sinds de tweede helft van oktober 2019 beschikbaar. Maar de procedure is ook bewerkelijk, omdat de identiteit van de gebruiker moet worden gecontroleerd: is degene wel de eigenaar van het paspoort of rijbewijs? Bij de NFC-optie wordt daarom een klein filmpje gemaakt om vast te stellen of het gaat om een persoon en niet om een foto; ook wel een ‘liveness check’ genoemd.

Het voordeel van de NFC-optie is dat zij ook werkt voor mensen die geen Nederlands identiteitsbewijs hebben, als het identiteitsbewijs maar beschikt over een NFC-chip. Dat geldt weer niet voor de iDIN: dat werkt alleen bij gebruikers die een Nederlandse bankrekening hebben. Een ander mogelijk bezwaar bij iDIN is de gebruikerservaring: mensen zijn bang dat iemand bij hun bankrekening kan. Andere problemen kunnen een en/of-rekening zijn, waarbij de achternaam van de partner doorgegeven zou kunnen worden. Wat bij alle genoemde identificatiemethodes een probleem is, is de betrouwbaarheid waarmee de identiteits-

gegevens gerelateerd kunnen worden aan die van het bestaande instellingsaccount van de gebruiker. Hoe weet je dat een ‘Jan de Boer’ die zich via iDIN heeft geauthentiseerd, een specifieke ‘Jan de Boer’ is bij een instelling? Er is geen gedeelde unieke identifier. De enige methode is daarom om persoonsgegevens als naam en geboortedatum met elkaar te vergelijken: de matching. Om deze matching goed te kunnen doen, moeten de naamgegevens aan beide kanten goed zijn vastgelegd. Zijn de voorletters en de voornaam op dezelfde manier vastgelegd? Is degene getrouwd geweest? SURF wil nagaan hoe goed dat in de praktijk werkt voor de verschillende methoden en de verschillende gebruikersgroepen.

PROOF OF CONCEPT

In de eerste helft van 2020 organiseert SURF een proof of concept (PoC) om deze selfservicemanier van identificatie samen met gebruikers en instellingen te testen. SURF wil daarmee leren wat de kwaliteit, het formaat en de variatie in de identiteitsgegevens is die ze van de instellingen en de identificatiemethoden krijgt. Op die manier is het mogelijk de algoritmes voor matching te optimaliseren. Daarnaast wil SURF leren wat gebruikers van deze manier van werken vinden. Vertrouwen ze het? Is het voldoende laagdrempelig? De verwachting is dat een combinatie van methoden de uitkomst zal zijn. We verwachten dat een methode als iDIN goed werkt voor gebruikers die in Nederland wonen, terwijl voor gebruikers uit andere landen de NFC-optie waarschijnlijk beter werkt. Het veld is sterk in beweging, dus er kunnen ook nog nieuwe middelen bijkomen. Ook wordt gekeken naar de ontwikkelingen in andere landen. Daar zijn dit soort ontwikkelingen ook gaande en kunnen we van elkaar leren. Ook kunnen we elkaar helpen door elkaars gebruikers te authenticeren. 

Meer informatie:
www.surf.nl/remotvetting

DRIE METHODEN VOOR IDENTIFICATIE OP AFSTAND

SURF heeft drie kansrijke methoden geselecteerd:

1. NFC-chip en NFC-reader. Recente paspoorten en rijbewijzen bevatten een NFC-chip, die kan worden uitgelezen met een NFC-reader in een (recente) smartphone. Daarmee leest de NFC-reader een aantal gegevens uit, zoals de naam van de houder en diens pasfoto.
2. Authenticeren met iDIN, via de bank. iDIN is een Nederlands online-identificatiemiddel. ID staat voor ‘identificeren’ en IN voor ‘inlog-

gen’. Voor gebruikers lijkt iDIN erg op een iDEAL-betaling, maar de andere partij ontvangt uiteraard geen financiële gegevens of bankrekeningnummer.

3. Authenticeren met IRMA. IRMA is een app die is ontwikkeld met privacy in het achterhoofd. De afkorting staat voor ‘I reveal my attributes’: de gebruiker bepaalt zelf welke gegevens hij deelt. Daarbij maakt de IRMA-app gebruik van attributen of gegevens die door een andere partij gevalideerd zijn, zoals de Nederlandse overheid.