SMS als tweede factor?

In juli 2016 kondigde NIST (National Institute of Standards and Technology in de V.S.) aan dat het alle vormen van authenticatie die gebruik maken van het telefoonnetwerk, zoals SMS-authenticatie, niet meer toe wil staan in toekomstige versies van haar veelgebruikte standaard voor sterke authenticatie. De achterliggende reden is het risico dat berichten die via het telefoonnetwerk verzonden worden door derden kunnen worden afgeluisterd of omgeleid [1].

De aankondiging staat in de draft van de nieuwe versie van de NIST standaard voor sterke authenticatie SP800-63-3:

> "5.1.3.2. Out-of-Band Verifiers
>
> Due to the risk that SMS messages or voice calls may be intercepted or redirected, implementers of new systems SHOULD carefully consider alternative authenticators. If the out-of-band verification is to be made using the public switched telephone network (PSTN), the verifier SHALL verify that the pre-registered telephone number being used is not associated with a VoIP (or other software-based) service. It then sends the SMS or voice message to the pre-registered telephone number. Changing the pre-registered telephone number SHALL NOT be possible without two-factor authentication at the time of the change.
>
> Note: Out-of-band authentication using the PSTN (SMS or voice) is deprecated, and is being considered for removal in future editions of this guideline."

NIST is het instituut dat standaarden en beleid voor de Amerikaanse overheid ontwikkelt en hun standaarden worden vaak als *best practices* beschouwd. We volgen deze ontwikkeling en de doorontwikkeling van de standaarden voor sterke authenticatie op de voet.

Het gebruik van SMS voor twee-factor authenticatie is altijd nog beter dan geen tweede factor, maar we realiseren ons dat er andere, modernere en veiligere twee-factor authenticatiemiddelen op de markt zijn. We laten het initieel over aan de keuzevrijheid van de instelling of zij SMS wel /niet willen gebruiken als twee-factor authenticatiemiddel en merken al dat een aantal instellingen overwegen om SMS als 2^{e} factor niet meer toe te staan.

Ook de instelling heeft een rol bij het veilig gebruiken van SMS. Het veiligheidsrisico bij het gebruik van SMS bestaat uit de mogelijkheid het SMS bericht te kunnen onderscheppen. Dit risico ligt deels in het netwerk van de telecomaanbieder en daarmee buiten de directe invloedssfeer van de instelling, maar voor een belangrijk gedeelte ligt dit risico daar waar de instelling en/of de gebruiker er wel invloed op hebben namelijk: het automatisch doorsturen van SMS berichten via VOIP, email of andere *messaging* technologieën. Dit doorsturen leidt tot extra risico omdat deze protocollen vaak niet versleuteld zijn of toegankelijk zijn met de eerste factor (gebruikersnaam/wachtwoord) van de gebruiker.

Mede naar aanleiding van dit advies van NIST zullen wij in overleg met de instellingen op zoek gaan naar alternatieve authenticatiemiddelen waarin we aspecten als beveiliging, gebruiksvriendelijkheid en toepasbaarheid (denk aan: kosten, browserondersteuning, apparaat-onafhankelijkheid) zorgvuldig moeten afwegen. We bieden als alternatief voor SMS natuurlijk al de tiqr-app (voor iOS en Android gebruikers) en hebben bijvoorbeeld ook al geëxperimenteerd met U2F, maar gezien de beperkte browser-ondersteuning is dat voorlopig geen volwaardig alternatief voor SMS. Tenslotte komt binnenkort de mogelijkheid beschikbaar voor een instelling om op de registratie-portal van Sterke Authenticatie bepaalde *tokens* (zoals SMS) niet te tonen, zodat gebruikers deze *tokens* niet kunnen kiezen als tweede factor.

Wordt vervolgd...

---

[1] Hier een aantal verhalen die illustratief zijn voor het omleiden van SMS verkeer:
https://medium.com/coinmonks/the-most-expensive-lesson-of-my-life-details-of-sim-port-hack-35de11517124
https://www.forbes.com/sites/laurashin/2016/12/20/hackers-have-stolen-millions-of-dollars-in-bitcoin-using-only-phone-numbers/