SMS als tweede factor?

Het gebruik van SMS voor twee-factor authenticatie is altijd nog beter dan geen tweede factor, maar er zijn andere, modernere en veiligere twee-factor authenticatiemiddelen beschikbaar voor SURFsecureID, zoals tiqr, Yubikey en binnenkort FIDO2. We laten het nog over aan de keuzevrijheid van de instelling of zij SMS wel/niet willen gebruiken als twee-factor authenticatiemiddel maar we merken wel dat veel instellingen SMS als 2e factor al niet meer toe staan.

SURF ontmoedigt het gebruik van SMS als tweede factor. Hieronder wat uitleg over waarom we dit doen.

Veiligheid

Al lang zijn er zorgen over de veiligheid van SMS bij gebruik voor authenticatie doeleinden. De achterliggende reden is het risico dat berichten die via het telefoonnetwerk verzonden worden door derden kunnen worden afgeluisterd of omgeleid [1].

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 apps geïnstalleerd op de mobiele telefoon zelf. 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. Niet alleen doorsturen vormt een risico, dezelfde apps kunnen de SMS berichten ook lezen, zo de authenticatie codes uitlezen en mogelijk doorsturen naar derden zonder dat de gebruiker dit weet of merkt.

Kosten

Het versturen van SMS-jes is niet gratis en afhankelijk van het gebruik kan dit aardig oplopen. Als een instelling besluit SMS toe te staan binnen SURFsecureID krijgt de instelling 500 SMS-jes per maand gratis. Daarna kosten de SMS-jes € 0,055 per SMS. Voor een overzicht van deze en andere tarieven en voorwaarden van SURFsecureID, zie Voorwaarden en tarieven.

Gebruikersvriendelijkheid

Bij het gebruik van SMS als tweede factor krijgt de eindgebruiker een code opgestuurd naar de mobiele telefoon en moet deze ingevoerd worden op het apparaat waarmee ingelogd wordt (dit kan dezelfde mobiele telefoon zijn, een tablet, laptop of desktop computer). Dit overtypen van de code is omslachtig en foutgevoelig. Bij tiqr als tweede factor is dit bijvoorbeeld niet nodig. Tiqr werkt met push meldingen waardoor er niks meer overgetypt hoeft te worden door de gebruiker.

---

[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/