23.02.2022

Des criminels en veulent à votre carte SIM puis à votre compte bancaire

Des hackers volent ou copient des cartes SIM pour accéder aux applis et aux données bancaires. L'attaque commence la plupart du temps par un message de phishing.

Des cybercriminels ont escroqué 68 millions de dollars aux États-Unis grâce à la technique du SIM Swapping, c'est-à-dire en détournant ou en copiant la carte SIM de leurs victimes pour arriver aux applications et aux données bancaires (Source : Heise Security, 20 Minuten).

On enregistre des cas de SIM Swapping en Suisse aussi, quoiqu'en nombre relativement plus limité. La plupart du temps, l'attaque intervient initialement via des messages de phishing (https://www.ebas.ch/phishing) (courriels, textos ou messagerie instantanée) contenant un lien vers un site piraté exploité par l'attaquant. Une fois qu'il a atterri sur le site, l'utilisateur ignare est invité à communiquer ses données de téléphonie mobile et/ou ses identifiants d'accès à un service en ligne ou d'e-banking. Il arrive aussi que ces données soient achetées en ligne suite à des fuites de données à grande échelle (p. ex. sur le Darknet).

Dans la mesure où les portails d'e-banking et autres services en ligne utilisent de plus en plus souvent la procédure d'authentification à deux ou plusieurs facteurs, un attaquant doit être en possession non seulement d'un nom d'utilisateur ou numéro de contrat, et d'un mot de passe, mais aussi d'une carte SIM volée ou commandée ultérieurement auprès de l'opérateur de téléphonie mobile pour pouvoir intercepter et utiliser le deuxième facteur de sécurité. Les données et cartes SIM volées ou procurées de tout autre manière que ce soit sont ensuite utilisées par les criminels pour accéder illégalement au portail d'e-banking ou au service en ligne visé.

Pour vous protéger,

- ne cliquez jamais sur un lien reçu par email, SMS ou Messenger, ou que vous auriez obtenu après avoir scanné un code QR, pour vous connecter sur le site d'un institut bancaire ou plus généralement à un service en ligne.
- ne remplissez jamais de formulaires envoyés par courriel et dans lesquels on vous demande d'indiquer vos identifiants de connexion.
- soyez méfiant à l'égard des pièces jointes de vos courriels et SMS.
- ne révélez aucune information confidentielle au téléphone (p. ex. vos mots de passe).
- tapez toujours manuellement l'adresse de la page d'accueil du site du fournisseur de services ou de la banque dans la barre d'adresse de votre navigateur.
- lorsque la page d'accueil s'affiche, vérifiez la connexion SSL (https:// et symbole du cadenas) et contrôlez l'adresse Internet dans la barre d'adresse du navigateur pour vous assurer que vous êtes bien sur le bon site.
- ne perdez pas de vue votre appareil mobile et faites bloquer immédiatement le téléphone et la carte SIM en cas de perte ou de vol.
- en cas de doute, contactez toujours directement votre institut financier.