La double authentification par SMS bientôt abandonnée

Excepté le paragraphe introductif, les notes et les intertitres, c'est quasiment le seul élément en gras dans la dernière révision des recommandations du NIST (National Institute of Standards and Technology) : le SMS est considéré comme obsolète pour l'authentification forte.

L'agence rattachée au département du Commerce des États-Unis recommande de se tourner vers des mécanismes dits « plus sécurisés », notamment les applications mobiles et la biométrie*.

Si ces consignes ont une valeur générale, elles ne s'imposent, dans la pratique, qu'aux organes gouvernementaux qui implémentent des dispositifs d'authentification électronique dans leurs systèmes d'information. Leur dernière rédaction – datée du 26 juillet 2016 – n'est, par ailleurs, encore qu'à l'état d'ébauche.

Pour autant, le ton est donné. En premier lieu au point 4, qui concerne les garanties minimales correspondant à chaque niveau d'authentification. Y est inséré un renvoi vers la section 5.1.3 pour obtenir plus de détails sur la « révision partielle » du statut de l'authentification de type « Out of Band », c'est-à-dire via un appareil physique disposant d'un identifiant propre et capable de recevoir, via un canal de communication séparé, un élément à usage unique.

Au point 5.1.3.1, le NIST détaille les caractéristiques que doit présenter ce dispositif physique. Par « identifiant propre », l'agence entend notamment une clé de sécurité ou une carte SIM.

SMS obsolète, le code PIN survit

C'est au point 5.1.3.2 qu'il est fait mention du SMS. Si l'authentification se fait par ce moyen sur un réseau de téléphonie mobile à l'usage du public, le fournisseur du service d'authentification « devrait » s'assurer que le numéro de téléphone est bien associé à un forfait et non à un service logiciel de type VoIP.

Le problème avec ces services qui envoient des messages texte ou passent des appels téléphoniques pour communiquer un code de sécurité ? Ils peuvent, selon le NIST, être détournés par un tiers qui n'est pas en possession du « dispositif physique » sus-évoqué. Même constat pour les e-mails et les SMS, qui « n'attestent généralement pas de la possession d'un appareil spécifique ».

L'ensemble de ces recommandations devraient, en respect des considérations d'obsolescence prononcées à l'égard du SMS, disparaître dans une prochaine version du document, souligne ITespresso.

Les conseils concernant les mots de passe et les codes PIN devraient quant à eux perdurer : au moins 8 caractères en cas de définition par l'utilisateur, possibilité d'exploiter exclusivement des caractères numériques si défini de manière automatique par le fournisseur du service, mise en place d'un liste de termes interdits, etc.

* Par exemple, le protocole UAF (Universal Authentication Factor), spécifié dans la norme FIDO (Fast IDentity Online) chapeautée par l'alliance du même nom, et qui permet l'identification biométrique à travers des dispositifs comme le lecteur d'empreintes digitales, la reconnaissance faciale et l'analyse rétinienne.

A lire aussi :

Double authentification et numéros premium, attention au hold-up !

La double authentification affaiblie par la synchronisation

crédit photo © LDprod – shutterstock