Usurpation de sessions : les conseils de l'ANSSI pour s'en protéger

Quelle granularité pour le paramétrage des sessions ? L'ANSSI recommande de tenir compte de cet aspect lorsqu'on choisit des solutions d'authentification. Elle en fait état dans un rapport consacré aux attaques par vol de cookies. En toile de fond, un incident récent qui a impliqué cette technique : la compromission d'Okta. Et, plus globalement, des facteurs favorisant son usage. En l'occurrence, le déploiement du SSO et le recours à des consoles d'administration web.

Ces cookies de session peuvent servir aussi bien de vecteur initial de compromission que de moyen de latéralisation. Ils sont d'autant plus convoités qu'ils permettent de contourner la plupart des solutions MFA.

Face à ce risque, l'ANSSI recommande de limiter la durée de validité des session à « quelques minutes tout au plus ». En particulier si on utilise des sessions sans état (*stateless*, où le cookie ne dépend pas d'une session stockée côté serveur). Avec elles, la révocation dudit cookie peut être complexe.

Autres conseils pour durcir le mécanismes de sessions :

– Exiger une réauthentification pour les opérations sensibles

– Mettre en place des mesures de détection d'usurpation (par exemple, si l'IP et les horaires de connexion sont incohérents)

– Journaliser les actions associées à une session

– Dans le cas d'une authentification mutuelle, vérifier à chaque requête qu'un identifiant de session est toujours associé au même certificat client

Autant d'options qu'on ne peut pas toujours configurer, souligne l'ANSSI. En particulier pour le SaaS. Illustration sur Slack, vraisemblablement utilisé pour usurper l'identité d'un salarié d'Electronic Arts en 2021 (avec, à la clé, entre autres, la fuite de codes sources). Il faut être sur une offre payante pour pouvoir définir un délai d'expiration.

Au possible, on utilisera des postes dédiés à l'administration, sans les exposer aux usages bureautiques, à la navigation web ou à des messageries. De manière générale, plus un système possède de privilèges, plus ses usages doivent être restreints afin d'en limiter la surface d'attaque.

Photo d'illustration © twobee – Fotolia