Fatigue MFA et contournement de l'authentification multi-facteurs

L'authentification multifacteur (MFA) consiste à exiger plusieurs preuves d'identité pour se connecter). Cette précaution renforce nettement la sécurité, cependant, la fatigue MFA ou MFA bombing/push bombing est une nouvelle ruse d'attaquants qui vise ce second facteur. L'assaillant récupère d'abord un identifiant compromis (généralement par phishing), puis tente de se connecter en enchaînant des demandes d'authentification sur le téléphone de la victime. L'idée est d'user l'utilisateur : submergé par le flot de notifications, il finit par approuver par lassitude ou automatisme. Par exemple, dans le piratage d'Uber en 2022, le groupe Lapsus$ a multiplié les tentatives de connexion sur un compte de prestataire pour inonder sa cible de requêtes MFA. L'attaquant a ensuite fait passer un message par WhatsApp pour inciter la victime à cliquer afin de « faire cesser les invites », ce qui lui a donné accès au compte. Ce mécanisme agit sur un réflexe humain : l'utilisateur veut stopper le harcèlement d'alertes et peut valider sans réfléchir une demande d'authentification, croyant à tort exécuter une action légitime.

Pour se prémunir de ces attaques, les entreprises doivent combiner mesures techniques et politiques de sécurité. D'un côté, on privilégiera des facteurs MFA résistants au phishing (clés FIDO2, biométrie, applications robustes, etc.) plutôt que des codes SMS ou simples notifications, et on activera des mécanismes avancés comme le number matching (l'utilisateur doit saisir sur son appli le code affiché sur l'écran de connexion). On peut également limiter par configuration le nombre de requêtes MFA par unité de temps et mettre en place des alertes en cas de rafales suspectes. De l'autre, la formation des utilisateurs est cruciale : ils doivent être entraînés à rejeter toute demande MFA inattendue et à considérer toute avalanche de notifications comme anormale. Un message d'alerte ou un bouton « Signaler une activité suspecte » peuvent inciter à prévenir l'équipe sécurité plutôt qu'à valider machinalement.

Ces attaques gagnent en ampleur. En 2024, une alerte conjointe CISA/FBI note que des groupes d'État (notamment iraniens) ont visé des infrastructures critiques (santé, énergie, administration, IT…) en utilisant le « push bombing » MFA. Les attaques de type fatigue MFA apparaissent régulièrement dans les campagnes d'APT aux côtés du phishing ou de la compromission de tierces parties. En réaction, les éditeurs durcissent leurs solutions : Okta promeut le passwordless et l'authentification adaptative pour éviter les piles de notifications, et Microsoft a déployé dans son appli Authenticator le système de numéro à saisir pour lutter contre l'approbation accidentelle. En somme, la MFA reste essentielle, mais il faut la mettre en œuvre pour éviter que le « renfort » de sécurité ne devienne un harcèlement inversé que l'utilisateur accepte par inadvertance.

Sources : LeMagIT – The Hacker News – CISA (advisory AA24-290A) – Okta blog – Office 365 IT Pros trustbuilder.com - lemagit.fr - office365itpros.com - thehackernews.com - sbscyber.com