Authentification multifactorielle conçue par CSL

Définition de l'authentification multifactorielle (MFA)

Processus d'authentification reposant sur deux méthodes de vérification de l'identité de l'utilisateur considéré, la MFA renforce la sécurité d'accès à tout système.

Cette forme d'authentification protège tout système contre le hameçonnage, l'ingénierie sociale et les attaques brutales sur les mots de passe. En outre, ce processus est à même de sécuriser les identifiants en les mettant à l'abri d'assaillants susceptibles d'exploiter des données d'accès faibles ou volées.

Importance de l'authentification MFA

La MFA est une composante vitale d'un modèle de sécurité à vérification systématique. Afin de protéger les données sensibles, les utilisateurs qui souhaitent accéder à ces données doivent confirmer leur identité. La MFA assure une protection satisfaisant contre de nombreuses menaces informatiques prenant pour cible les comptes et mots de passe d'utilisateurs, à l'instar de celles mentionnées ci-avant.

Si un assaillant distant avait accès à un ordinateur par le biais de la connexion Internet d'un utilisateur, cet assaillant pourrait accéder au mot de passe de ce dernier ainsi qu'à une seconde forme d'authentification, dans l'éventualité où ces deux identifiants lui seraient livrés par le même canal.

Toute tentative de d'usurpation d'identité d'un utilisateur par un assaillant distant (pour accéder frauduleusement à des informations enregistrées dans diverses applications) est vouée à l'échec si ce dernier ne dispose pas du périphérique physique appartenant à cet utilisateur.

L'intégration de la MFA empêche tout assaillant éventuel d'accéder à des comptes privés sans disposer du périphérique privé d'un utilisateur indispensable à la deuxième forme d'authentification.

Nature de la MFZ employée par CSL

CSL a recours à une authentification temporelle, que l'on qualifie parfois de Time-Based One Time Password (TOTP) [mot de passe à usage unique fondé sur le temps]. La méthode TOTP MFA génère un code à intervalles temporels définis que l'utilisateur doit entrer pour accéder au système. Le code de déverrouillage généré par les authentificateurs (ou par SMS/courriel) expire au bout d'un certain laps de temps. Un nouveau code sera généré la prochaine fois qu'un utilisateur tentera d'accéder à son compte. Le TOTP est l'un des éléments clés de l'architecture

CSL DualCom Ltd
Building 4, Croxley Park
Hatters Lane, Watford
WD18 8YF, United Kingdom

T +44 (0) 1895 474 474
E sales@csl-group.com
W www.csl-group.com
@CSLGroupLtd

Registered in England No. 03155883
CSL2137V1 06082021

CSL s'est livré à l'implémentation d'une authentification temporelle par mot de passe à usage unique, courriel et SMS. Voici une liste des authentifiants couramment utilisés et approuvés par CSL :

- Free OTP
- Google Authenticator
- Microsoft Authenticator
- LastPass Authenticator
- 2FA Authenticator (2FAS)
- Aegis Authenticator
- Authy
- Due Mobile
- IBM Security Verify

Procédure

1. Entrez, comme à l'accoutumée, votre nom d'utilisateur et votre mot de passe sur CSL Live
2. Recevez un code transmis par courriel, par SMS, par un programme ou par votre appli d'authentification
3. Entrez ce code sur CSL Live
4. À présent vous êtes connecté en toute sécurité.

Secteurs d'activité ayant recours à la MFA

La sécurité des terminaux est rapidement en passe de devenir une préoccupation majeure dans de nombreux secteurs d'activité. Quelles que soient les applications auxquelles accèdent les utilisateurs, la protection des identifiants revêt une importance primordiale pour garantir la sécurité des entreprises au sens large.

Secteur de la distribution

Difficiles à prévenir, les attaques à distance prédominent dans ce secteur devenu premier employeur du pays. En outre, les solutions de sécurité ne cessent de gagner en importance dans le secteur de la distribution à l'heure où les technologies de l'information sont en train de s'adapter à un environnement sans périmètre. La MFA procure aux entreprises du secteur de la distribution une certaine sérénité en leur permettant d'authentifier les identités des utilisateurs qui accèdent à leurs réseaux par le biais d'ordinateurs distants ou d'appareils mobiles personnels.

Secteur bancaire

Les banques ont recours à la MFA pour se protéger contre les nombreuses tentatives de piratage dont sont victimes leurs systèmes internes et ceux de leurs clients. La MFA a aidé de nombreuses banques d'envergure à améliorer leur résilience face à de tels assauts.

Il est devenu primordial pour les banques d'être à même d'identifier à tout moment les utilisateurs et périphériques qui accèdent à leurs systèmes. La MFA permet au secteur bancaire de sécuriser les périphériques distants et d'authentifier toute tentative d'entrée en session.

Réseaux sociau

Nombre d'agences et de plates-formes de réseaux sociaux se servent de la MFA pour protéger les données personnelles de plusieurs milliards d'utilisateurs disséminés dans le monde entier. Des entreprises telles que Facebook ont recours à une méthode d'authentification pour mettre leurs développeurs à l'abri de toute tentative de piratage lorsqu'ils travaillent sur les réseaux internes de l'entreprise.

La MFA facilite également la sécurisation des entreprises gestionnaires de réseaux sociaux en simplifiant les procédures d'accès conçues pour les développeurs. Une solution MFA basée sur l'infonuagique protège les développeurs et partant les utilisateurs en les dispensant d'installer quelque matériel et/ou logiciel que ce soit.

Pouvoirs publics

L'évolution actuelle des technologies de l'information met les pouvoirs publics au défi de modifier rapidement leur infrastructure dans leur effort d'adaptation à la transition vers le Cloud et la mobilité.

La technologie MFA aide les pouvoirs publics à mettre en oeuvre des systèmes à vérification systématique s'adressant aux millions d'utilisateurs qui ont besoin d'y accéder.

Foire aux questions

Que faire en cas de perte ou de remplacement d'un appareil mobile par un utilisateur ?

La MFA repose sur la détention par les utilisateurs d'un appareil mobile leur permettant de s'identifier. En cas de perte, de vol ou de remplacement de leur smartphone ou de leur ordinateur portable, les utilisateurs peuvent enregistrer un nouvel appareil en réinitialisant leur mot de passe via CSL Live. Cette fonction s'utilise aussi en cas d'acquisition d'un nouveau téléphone ou d'un nouveau portable pour enregistrer la MFA sur cet appareil. Quelles que soient la position géographique d'un utilisateur et la technologie utilisée par ce dernier, ses données personnelles seront sécurisées.

Puis-je installer la MFA sur de multiples appareils?

Oui, vous pouvez installer la MFA sur de multiples appareils. La MFA permet d'associer de multiples appareils à votre compte.

L'authentifiant de mon choix ne figure pas dans la liste ; puis-je l'utiliser?

CSL a testé et approuvé les authentifiants répertoriés dans ce document. Nous vous recommandons d'utiliser ces authentifiants pour garantir la fiabilité et l'accessibilité de votre compte CSL Live.

Je ne parviens à utiliser aucune appli d'authentification; quelles sont les autres options dont je dispose?

Dans l'éventualité où, pour quelque raison que ce soit, vous ne parviendriez à utiliser aucune appli d'authentification, nous avons développé plusieurs options de sauvegarde des SMS et courriels. Il vous suffit de sélectionner l'option SMS ou courriel lorsque le système vous invite à introduire un code à usage unique. Le délai d'expiration de tous les SMS/courriels s'élève à 60 secondes.

Comment en apprendre davantage?

Pour plus d'informations concernant les pratiques et directives standard MFA, veuillez cliquer sur les liens ci-après.

National Cyber Security Centre
National Institute of Standards and Technology