Authentification

Définitions

L'identification est le procédé qui permet de vérifier l'identité d'un utilisateur. L'objectif de cette opération est de différencier les utilisateurs les uns des autres. Pour ce faire, l'utilisateur répond à la question : ***Qui suis-je ?*** en fournissant un identifiant.

L'authentification est le procédé qui permet de vérifier qu'un utilisateur identifié est bien celui qu'il déclare être. Pour le prouver, l'utilisateur répond à la question : ***Que sais-je ?*** en fournissant un mot de passe.

L'authentification à deux facteurs est un procédé qui complète l'authentification afin de vérifier de manière encore plus certaine que l'utilisateur authentifié n'est pas un individu malveillant. Pour le prouver, l'utilisateur répond à la question : ***Que possédè-je ?*** en :

- fournissant un code aléatoire obtenu sur un générateur OTP ;
- fournissant un code reçu par SMS ;
- validant un notification sur une App mobile dédiée.

L'habilitation est le procédé qui, lorsqu'un utilisateur a été authentifié, permet de déterminer quels accès lui seront accordés. L'habilitation consiste à appliquer une politique de droits pré-établie répondant à la question : ***Qu'as-tu le droit de faire … ou pas ?***.

Notes :

- Aujourd'hui, l'authentification à deux facteurs s'appuie largement sur les smartphones (qui concrétisent naturellement “ce que je possède”). Elle est réellement plus exigeante et, pour s'en convaincre, il suffit de faire l'expérience de ne plus avoir accès à son smartphone (perte, oubli, panne, etc.) au moment où le second facteur est nécessaire. La situation peut être chaotique, voire kafkaïenne ;
- Pour une organisation, la multiplication des besoins d'authentification a conduit à fabriquer des guichets centralisés d'authentification, appelés Single Sign-On (SSO).

Les Fonctionnalités à considérer dans une authentification

Gérer les utilisateurs

Pour gérer efficacement l'authentification, il conviendra de disposer d'une liste à jour des utilisateurs autorisés. Pour ce faire, il faudra gérer les utilisateurs au fil de deux besoins essentiels :

- Ajouter de nouveaux utilisateurs ;
- Désactiver des utilisateurs ;

Gérer les droits

Ensuite, il est important de pouvoir appliquer une **politique d'habilitations** par le biais d'une gestion des droits d'accès. Cela implique de pouvoir **attribuer ou retirer des droits** à chacun. Souvent, l'application des droits à des **groupes d'utilisateurs** facilitera le processus.

Principe fondamental de la sécurité : appliquer à chacun tous les droits nécessaires mais seulement eux, jamais plus.

Gérer l'authentification

Offrir une mire d'authentification et le traitement associé.

Gérer le changement de mot de passe

En outre, il est nécessaire de pouvoir gérer le changement de mot de passe des utilisateurs. Cela permet aux utilisateurs de changer leur mot de passe régulièrement pour **maintenir la sécurité du système**.

Gérer la réinitialisation de mot de passe

Une nécessité supplémentaire consiste à proposer un système de réinitialisation de son mot de passe en cas d'oubli, afin que chacun, en toute autonomie, puisse continuer à accéder au système sans interruption.

Gérer la double authentification

Enfin, de sorte à **renforcer la sécurité du système**, proposer une double authentification implique des traitements et un processus spécifiques.

On le mesure ici, développer un système d'authentification complet ne peut pas s'improviser.

RGPD et Authentification

Le Règlement général sur la protection des données (RGPD) ne traite pas spécifiquement de l'authentification, mais il s'y applique systématiquement puisque celle-ci traite des données à caractère personnel.

Par ailleurs, le RGPD stipule que tout service numérique opéré à destinations d'utilisateurs doit mettre en œuvre un procédé complet de **traçabilité**. L'authentification n'échappe pas à ce principe et se doit d'enregistrer toutes les opérations qui lui sont liées (connexions réussies, connexions en échec, déconnexions, changements de mots de passe, etc.). Les traces ainsi enregistrées pourront servir tant dans le cadre d'une requête judiciaire que pour un usage interne dans la gestion quotidienne.