L'authentification des utilisateurs : un indispensable de votre sécurité informatique

Ordinateurs, smartphones, télétravail, Cloud… Ce sont autant de « portes ouvertes » dans votre réseau informatique qui peuvent être à l'origine d'une fuite de données ou d'une infection par un virus. L'authentification des utilisateurs est indispensable.

Pour accéder à leur messagerie ou à des documents de travail, certains salariés utilisent leur tablette et le Wi-Fi, d'autres téléchargent des dossiers depuis leur ordinateur de bureau et une connexion Ethernet. Quels dossiers ont-ils ouverts ? Ont-ils réellement besoin d'accéder à ces fichiers pour leur travail ? Est-ce que le compte de l'intérimaire qui a fini sa mission est bloqué ?

Toutes ces questions doivent avoir des réponses précises et justifiées. Chaque collaborateur doit être doté d'un identifiant qui lui est propre et doit s'authentifier avant toute utilisation des moyens informatiques.

L'authentification des salariés et le traçage des accès sont indispensables, car :

- ils permettent d'avoir une **vision globale de son réseau** et de ses équipements informatiques ;
- ils renforcent la **sécurité des données** à caractère personnel afin d'être en conformité avec le RGPD ;
- ils constituent des **preuves en cas de fraude interne**.

Authentification des utilisateurs : les principales mesures à prendre

- **Première mesure : répartir les salariés par métier**
  La constitution de groupes de travail par métiers (ou par profils d'habilitation pour télécharger ou modifier des documents par exemple) évite que tous les salariés ouvrent des fichiers sensibles. Un commercial peut utiliser le logiciel permettant de faire des devis, mais il n'a pas besoin de consulter la comptabilité et les données financières de l'entreprise.

- **Seconde mesure : renforcer l'authentification**
  Les salariés doivent avoir un identifiant et un mot de passe différents pour chaque usage (accès à Office 365, aux réseaux sociaux, aux dossiers partagés sur le serveur ou dans le Cloud…). Pour améliorer cette authentification, le responsable informatique doit mettre en place des procédures techniques imposant des mots de passe « forts » avec l'utilisation d'au moins 8 caractères (lettres en majuscule et en minuscule, chiffres et symboles).

- **Troisième mesure : la signature d'un engagement de confidentialité**
  Elle peut être indiquée dans la charte informatique ou dans une clause des contrats de travail. Ces documents doivent aussi rappeler que les salariés ne doivent communiquer leurs mots de passe à quiconque.

- **Quatrième mesure : supprimer les comptes anonymes et génériques (admin, user, contact...)**
  Chaque personne doit être identifiée nommément afin de pouvoir relier une action sur le système informatique à un utilisateur. Cette mesure permet aussi de bloquer les connexions anonymes pouvant être à l'origine d'une tentative d'infiltration.

Ce qu'il ne faut pas faire

- **Multiplier les comptes « administrateur »**
  Seul le responsable informatique doit avoir ce profil afin d'assurer la maintenance (gestion des groupes utilisateurs, installation ou suppression de logiciels…) et la mise à jour (téléchargement des correctifs de sécurité) du parc informatique et du réseau.

- **Laisser visibles tous ses mots de passe**
  Lors des formations de sensibilisation, la Direction de l'entreprise doit rappeler aux collaborateurs qu'ils ne doivent pas conserver leurs mots de passe sur des post-its collés sur l'écran du PC ou une feuille mise dans un tiroir.
- **Ne jamais changer tous ses mots de passe**
  Régulièrement (tous les six mois par exemple), il est recommandé de modifier tous les mots de passe des salariés. Cette opération doit être aussi l'occasion de vérifier si des comptes sont toujours actifs alors qu'une personne a démissionné ou que l'intérimaire a terminé sa mission.
- **Sauvegarder sans chiffrement les identifiants et mots de passe**
  Ces données sont une cible privilégiée par les attaquants désireux d'accéder à votre réseau. Le responsable informatique doit protéger cette base de données par des solutions de chiffrement afin de disposer d'accès aussi « sécurisés » qu'un coffre-fort.

Pour aller plus loin

Si certaines authentifications envisagées ont recours à des **dispositifs biométriques**, il est nécessaire d'effectuer une demande d'autorisation auprès de la CNIL (Commission nationale de l'informatique et des libertés).

Concernant **des dispositifs basés sur l'empreinte digitale**, il convient de se référer au Guide de la CNIL.

L'ANSSI (Agence nationale de la sécurité des systèmes d'information) publie une **liste de logiciels certifiés** et permettant de renforcer l'authentification des utilisateurs.

Generali vous propose une offre alliant prévention, protection et accompagnement contre les cyber risques. Découvrez l'offre Generali Protection Numérique !

LEXIQUE

Lexique : Les authentifications biométriques

Il s'agit de technologies permettant d'identifier de manière unique une personne grâce à une ou plusieurs caractéristiques biologiques, telles que l'empreinte digitale, le visage, la morphologie de la main, la voix…

La biométrie remplit deux fonctions distinctes :
• l'identification répond à la question **« Qui êtes-vous ? »**. Dans ce cas, la personne est identifiée parmi d'autres (vérification) ;
• l'authentification répond à la question : **« Êtes-vous bien celui que vous prétendez être ? »**. Dans ce cas, elle certifie l'identité d'une personne en comparant les données qu'elle va présenter avec celles préenregistrées de la personne qu'elle prétend être.

Generali IARD, Société anonyme au capital de 94 630 300 euros. Entreprise régie par le Code des assurances - 552 062 663 RCS Paris. N° d'identifiant unique ADEME FR232327_01NBYI.
Siège social : 89 rue Taitbout - 75009 Paris.
Société appartenant au Groupe Generali immatriculé sur le registre italien des groupes d'assurances sous le numéro 026.

SG2685MARK-25 - Décembre 2025 - Studio graphique