Authentification biométrie en entreprise

Bloc 3 – Cybersécurité des services informatiques

Sommaire

1. Introduction

À l'ère numérique actuelle, la gestion des mots de passe est devenue une préoccupation majeure. La compromission d'un seul mot de passe peut ouvrir la porte à des attaques malveillantes, mettant en péril la sécurité des données et des services en ligne.

Face à ces défis, l'authentification biométrique émerge comme une solution prometteuse, offrant une alternative sécurisée et pratique aux méthodes traditionnelles.

Dans ce document, nous explorerons les enjeux de la gestion des mots de passe, les risques associés, et les avantages de l'authentification biométrique, tout en fournissant des recommandations pour une adoption efficace de ces technologies.

2. Définition de la biométrie

La biométrie comprend tout un ensemble de technologies et procédés de reconnaissance, d'authentification et d'identification des personnes à partir de certaines de leurs caractéristiques physiques ou comportementales.

Elles ont, pour la plupart, la particularité d'être uniques et permanentes (ADN, empreintes digitales, etc.).

Certains dispositifs comme l'utilisation du contour de la main, pour assurer le contrôle d'accès et la gestion des horaires et de la restauration sur les lieux de travail, sont soumis à une simple déclaration de conformité.
Tous les dispositifs de reconnaissance biométrique sont soumis à l'autorisation de la CNIL.

Source : https://www.editions-tissot.fr/

3. Les différentes technologies biométriques

Il existe plusieurs technologies biométriques, ça je ne vous apprends rien mais les plus couramment utilisés au cours de ces dernières années sont :

a) La reconnaissance par les empreintes digitales

La biométrie repose sur le principe selon lequel chaque empreinte digitale contient environ une centaine de points distincts, appelés minuties. En général, seulement une douzaine de ces minuties correspondantes sont nécessaires pour confirmer l'identité de deux empreintes digitales et ainsi identifier une personne avec certitude.

b) La reconnaissance faciale

Cette méthode transforme une image en un modèle 3D, où les différents éléments, comme la distance entre les yeux, sont comparés à une base de données biométriques, qu'elle soit locale ou distante. Son efficacité est influencée par la qualité de l'image, la taille de la base de données et la performance des algorithmes utilisés pour comparer ces caractéristiques.

c) La reconnaissance de l'iris

Fondé sur le fait que les iris d'une personne sont aussi différents les uns des autres que de ceux d'une autre personne, y compris entre des jumeaux homozygotes*. Ils varient peu au cours de la vie d'une personne et peuvent être identifiés même si elle porte des lunettes ou des lentilles de contact.

** : Se dit d'une cellule ou d'un individu qui possède deux gènes identiques sur chaque chromosome de la même paire.*

Source : https://www.idemia.com/fr/biometrie

4. Les différents usages

Il y a seulement quelques années, cette technologie était encore inconnue du public, on était plus proche d'un film de SF (Science Fiction) que de la vraie vie, mais maintenant la biométrie prend une place important voir même obligatoire pour des questions de sécurités. Certains domaine l'utilise au quotidien et nous allons voir lesquels.

a) Dans l'administration

Un système biométrique permet aux autorités de délivrer des documents d'identité sécurisés tels que des passeports et des permis de conduire, et de s'assurer que les personnes reçoivent les prestations auxquelles elles ont droit, en toute simplicité.

Que ça soit au niveau régional, local ou à échelle nationale.

b) Dans les contrôles

Dans les contrôles, je parlais bien évidemment de contrôle aux frontières, pour une meilleure expérience pour les voyageurs. Les portiques automatisés de vérification des identités dotés des technologies biométriques accélèrent et optimisent les contrôles, tout en améliorant l'expérience des voyageurs.

Il y a aussi que la biométrie permet des contrôles d'accès efficaces, les technologies biométriques peuvent fluidifier et sécuriser l'accès soit à des zones réservées, telles que des installations industrielles, soit à des services confidentiels, tels que des dossiers médicaux ou des systèmes financiers.

c) Dans les enquêtes criminelles

Oui, elle est aussi dans les enquêtes criminelles, permet aux forces de l'ordre d'accélérer les enquêtes, Des contrôles d'identité de routine aux analyses des scènes de crime et des dossiers, les systèmes biométriques contribuent à l'efficacité des enquêtes et à la sécurité publique.

d) Dans les transactions

L'utilisation des cartes de paiement biométriques, ainsi que l'autorisation de paiements ou la signature de contrats au moyen de la reconnaissance faciale ou d'empreintes digitales depuis un smartphone font partie des cas où la biométrie est utilisée pour sécuriser des transactions.

Source : https://www.idemia.com/fr/biometrie

5. Avantages

L'utilisation de la biométrie présente de nombreux avantages dont le premier, l**e niveau de sécurité et de précision qu'elle garantit**. Contrairement aux mots de passe, aux badges, aux documents, les données biométriques ne peuvent pas être oubliées, échangées, volées, et demeurent infalsifiables.

Identification et authentification : vitesse et précision. la technologie de sécurité biométrique désigne les mots de passe biologiques qui ne peuvent être falsifiés. La reconnaissance d'iris ou faciale est de plus en plus souvent intégrée aux processus de sécurité, du fait de la rapidité et de la simplicité de la détection.

Efficacité maximale : Ce système est même pratique pour les employés qui n'ont plus besoin d'avoir leur badge ou carte d'accès sur eux en permanence. Les systèmes de contrôle biométrique renforcent non seulement la sécurité, mais ils facilitent et améliorent également l'efficacité de la gestion de fonctions

Mot d'ordre : l'aspect pratique, comme dit précédemment avec l'utilisation de moins en moins récurrente des cartes d'accès ou des badges, une fois le test biométrique activé, la reconnaissance des empreintes digitales, de l'iris et du visage peut s'effectuer et les employés peuvent ensuite vaquer à leurs occupations. Ce n'est pas comme des mots de passe ou certaines entreprises demande à leurs employés de changer de les changer, là les empreintes n'ont pas besoin d'être réinitialisées.

Utilisation simple et ergonomique : La gestion, l'ajustement, et même l'analyse des contrôles biométriques se distinguent par leur ergonomie, une fois le tableau des entrées et des sorties créé, l'analyse et la gestion des données deviennent un jeu d'enfant.

6. Risques et limites

6bis Les Risques

a) Atteintes à la vie privée

La collecte et le traitement de données biométriques peuvent compromettre la vie privée des individus, car ces informations sont très sensibles et peuvent être utilisées à des fins de surveillance ou de profilage sans leur consentement.

b) Discrimination et biais

Les algorithmes utilisés dans les systèmes biométriques peuvent être sujets à des biais, ce qui peut entraîner des discriminations à l'encontre de certaines populations, notamment sur la base de l'origine, du sexe, du genre, de l'apparence, etc.

c) Erreur et fausse identification

Malgré leur sophistication, les systèmes biométriques ne sont pas infaillibles et peuvent produire des erreurs, ce qui peut conduire à l'identification erronée ou à la fausse accusation de personnes innocentes.

d) Surveillance de masse

La généralisation de l'utilisation des technologies biométriques, notamment dans les espaces publics, peut conduire à une surveillance de masse, ce qui soulève des préoccupations en matière de liberté d'expression, de mouvement et d'association.

e) Effet dissuasif sur les droits fondamentaux

L'utilisation omniprésente de la biométrie peut avoir un effet dissuasif sur l'exercice des droits fondamentaux, car les individus peuvent craindre d'être surveillés et ainsi modifier leur comportement par peur de représailles ou de discrimination.

6ter Les Limites

a) Le coût

Comme première limite nous avons le coût, une technologie aussi poussée demande un coût élevé, comme toutes les technologies de pointe, ces systèmes représentent un investissement conséquent pour les entreprises. Investissement qu'elles ne sont pas toutes prêtes à faire comme l'a montré le rapport de la CDSE*.

** : Club des directeurs de sécurité des entreprises*

b) Faux positifs et faux négatifs

Aucun système biométrique n'est parfait et peut générer des erreurs. Les faux positifs se produisent lorsque le système identifie incorrectement une personne comme étant une autre, tandis que les faux négatifs se produisent lorsque le système ne parvient pas à reconnaître correctement une personne autorisée

c) Acceptation sociale

Certaines personnes peuvent être réticentes à l'idée de partager leurs données biométriques en raison de préoccupations liées à la vie privée et à la sécurité.

7. Fiabilité et failles

a) La fiabilité

Étant donné qu'un système biométrique dépend d'algorithmes statistiques, les faux rejets et les fausses acceptations sont inévitables. Utilisée seule, aucune forme de biométrie ne peut être infaillible à 100 %. Cela dit, les solutions biométriques les plus performantes visent le juste équilibre entre faux rejets et fausses acceptations, elles s'appuient sur la biométrie multimodale et elles sont capables d'assurer une vérification fiable dans des situations difficiles.

Les systèmes biométriques les plus puissants peuvent surmonter un certain nombre de situations difficiles. Les lecteurs d'empreintes haut de gamme peuvent ainsi a**uthentifier des empreintes digitales humides, sèches ou endommagées.** Quant aux meilleurs appareils de reconnaissance faciale, ils fonctionnent quels que soient les changements d'éclairage, l'angle du visage ou les changements de celui-ci (casque de moto, casque audio, coupe de cheveux, lunettes, etc.) et ne demandent quasiment pas à l'utilisateur de s'arrêter.

b) Les failles

Contrefaçon et falsification : Les caractéristiques biométriques peuvent être contrefaites ou falsifiées, compromettant ainsi l'authentification. Par exemple, des empreintes digitales peuvent être dupliquées à partir de moules en silicone ou de résidus laissés sur des surfaces. Les visages peuvent être contournés à l'aide de photos ou de masques spécialement conçus.

Attaques par imitation : Des techniques telles que la création de prothèses d'iris ou d'empreintes digitales peuvent être utilisées pour tromper les systèmes biométriques. Ces attaques d'imitation peuvent contourner les mesures de sécurité basées sur la reconnaissance d'empreintes digitales ou d'iris.

Rétention et stockage des données : La collecte et le stockage de données biométriques soulèvent des préoccupations en matière de protection de la vie privée. Les bases de données biométriques peuvent être ciblées par des cyberattaques, entraînant le vol ou la compromission des informations personnelles sensibles.

8. Cadre légal et réglementaire

a) Cadre légal

L'article 9 du RGPD interdit formellement le traitement des données biométriques dans le but d'identifier de manière unique les individus, classant ainsi ces données parmi les catégories spéciales de données sensibles.

Néanmoins, cette interdiction n'est pas absolue. Des exceptions spécifiques, énumérées dans le même article, peuvent être appliquées dans des situations définies exhaustivement :

- Obtention explicite du consentement de la personne concernée

- Informations biométriques nécessaires pour l'exécution des obligations du responsable du traitement ou de la personne concernée dans les domaines de l'emploi, de la sécurité sociale et du droit de la protection sociale

- Impératif de protection des intérêts vitaux de la personne, en cas d'incapacité physique ou juridique de donner son consentement

- Traitement nécessaire pour contester, exercer ou défendre un droit en justice

- Obligation de traitement pour des motifs d'intérêt public, notamment dans le domaine de la santé publique.

b)Réglementaire

Par ailleurs, la nature même des données biométriques a évolué : désormais qualifiées de « données sensibles » par le RGPD, leur traitement devient en principe interdit sauf à s'inscrire dans l'une des exceptions limitativement prévues par le texte.

Sensible à ces évolutions, le législateur français a confié à la Commission une mission nouvelle, qui est celle de concevoir et de publier en concertation avec des organismes représentatifs des acteurs concernés, des règlements type en matière notamment de traitement des données biométriques.

Source

https://www.editions-tissot.fr/

https://www.idemia.com/fr/biometrie

https://www.globalsign.com/fr/blog/7-avantages-de-la-biometrie-pour-la-securite

https://mesinfos.fr/ile-de-france/identification-biometrique-etat-des-lieux-et-limites-du-cadre-legal-190505.html#:~:text=L'article%209%20du%20RGPD,cat%C3%A9gories%20sp%C3%A9ciales%20de%20donn%C3%A9es%20sensibles.

https://www.cnil.fr/fr/le-controle-dacces-biometrique-sur-les-lieux-de-travail