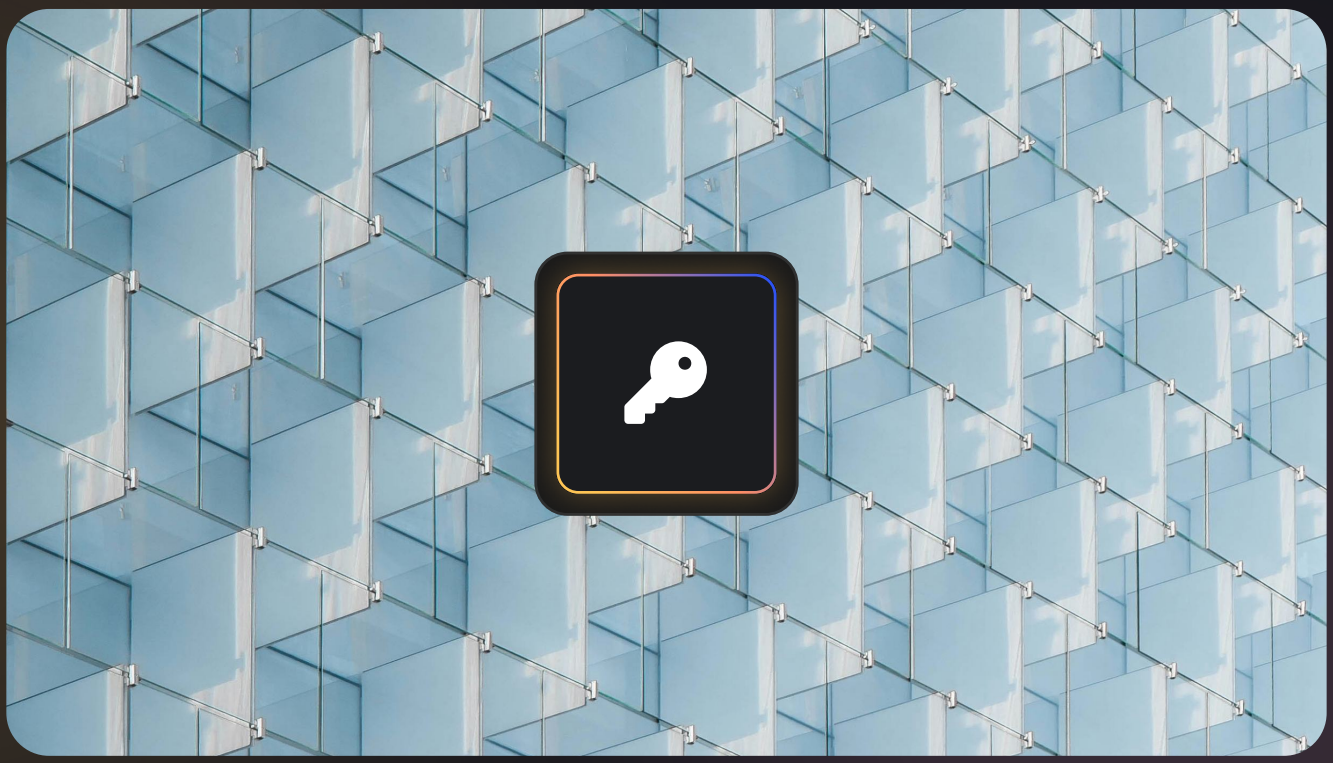
LIVRE BLANC

Sécurité des données et gestion des mots de passe

Les meilleures pratiques pour prévenir les fuites et les attaques



MAILINBLACK

Contexte

PUBLIC SÉNAT

Cyberattaques :
« La recrudescence que nous voyons aujourd'hui n'est que la partie visible de l'iceberg ».

Cette déclaration intervient à la suite des dernières attaques informatiques qui ont touché France Travail, 800 sites administratifs et ministériels et plusieurs mutuelles. Des intrusions malveillantes qui ont donné lieu à des opérations de déstabilisation et à la fuite massive de données sensibles et confidentielles.

Lorsque l'auteur parle de partie visible de l'iceberg c'est qu'en effet, sur les nombreuses attaques informatiques qui ciblent depuis plusieurs décennies tous les secteurs d'activité, beaucoup passent sous les radars ou sont gardées secrètes par les organisations ciblées.

Comme l'indique l'ANSSI, les pirates informatiques améliorent constamment leurs pratiques pour garantir leur anonymat et leur furtivité.

Pour avoir un ordre de grandeur de la cybermenace réelle, notre baromètre CYBER 2024 fait état de **plus de 140 millions de cyberattaques arrêtées** par notre solution de protection de messagerie.

L'intrusion démarre généralement par la **compromission de mots de passe**. Pour obtenir cet accès initial et mener leurs cyberattaques, les hackeurs utilisent différentes méthodes :

- forcebrute
- attaque par dictionnaire

Ils profitent aussi de nombreuses vulnérabilités logicielles ainsi que de la multiplication d'objets périphériques connectés non supervisés. Autre faille du dispositif, l'humain, qui est régulièrement victime de vol d'identifiants et de mots de passe via notamment l'envoi automatisé et en masse d'emails corrompus.

- rançongiciel
- phishing
- spearphishing

Une pratique à l'origine de 90% des cyberattaques. Les hackeurs disposent aussi d'informations d'identification qu'ils peuvent acheter auprès de courtiers d'accès non autorisés (IAB pour Initial Access Broker).

Quelle que soit la méthode utilisée, on constate que les hackeurs ciblent en priorité les mots de passe, qui sont le maillon faible de la sécurité numérique.

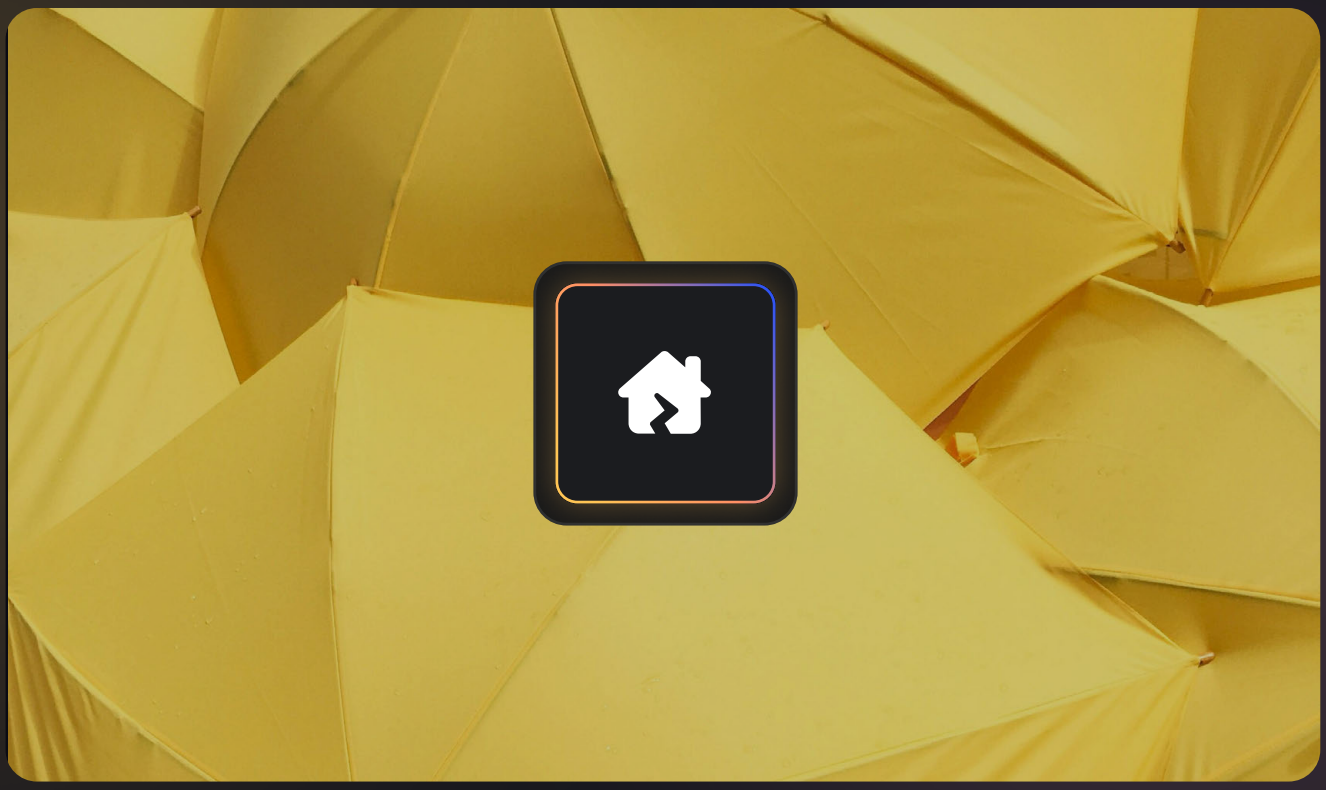
Les capacités des hackeurs boostées par l'IA et les opportunités pour compromettre les systèmes d'information se développent de manière exponentielle. Face à cette cybermenace persistante et agile, la gestion des identifiants de connexion représente un élément crucial de la sécurisation des accès aux données et aux services numériques des entreprises.

Ce livre blanc vous fournit une compréhension approfondie des enjeux de la protection des données et des stratégies pour renforcer la sécurité liée à la gestion des mots de passe.

Sommaire

1

Gérer les fuites de données pour la sécurité de votre entreprise



Identification et gestion des risques de fuite de données

Les enjeux liés à la cybersécurité s'amplifient de jour en jour. Il est donc essentiel de redoubler de vigilance pour se prémunir contre les retombées irrémédiables (en particulier juridiques et financières) d'une fuite de vos données personnelles.
Pour endiguer ce phénomène, il faut commencer par le comprendre et connaître les facteurs qui favorisent la menace.

Qu'est-ce qu'une fuite de données ?

Une fuite de données constitue un incident de sécurité lors duquel des acteurs internes malveillants ou des attaquants externes parviennent à accéder de manière non autorisée à des données confidentielles, telles que des :

- dossiers médicaux
- informations financières
- données personnelles

Ces incidents, parmi les plus anciens et les plus coûteux en matière de cybersécurité, touchent des entreprises de toutes tailles et de tous secteurs à travers le monde, et se produisent à une fréquence alarmante.

L'objectif pour les hackeurs ? Se servir de ces datas afin de :

- nuire à la réputation
- vendre les données sur le Dark Web
- exercer un chantage

En effet, certaines informations, telles que les données bancaires, les pièces d'identité ou simplement les identifiants de connexion, sont très prisées sur le marché clandestin.

235 millions

d'utilisateurs de X ont vu leurs adresses électroniques diffusées sur un célèbre forum de hackeurs en janvier 2024

L'une des fuites les plus importantes de l'histoire est celle qu'a connue X (Twitter). Cette fuite a malheureusement entraîné une vague massive de piratage, de phishing ciblé (hameçonnage) et de doxxing (divulgation d'informations personnelles dans le but de nuire à une personne).

C'est pour réduire ce genre de fuite de données que la nouvelle directive NIS2 veut améliorer les mesures de sécurité des organisations afin de lutter contre les nouvelles formes de cyberattaque.

Les causes de la fuite de données en entreprise

- **Les cyberattaques**

Sans étonnement, les cyberattaques demeurent la principale source de fuites de données.

92%

des violations de données découlent de cyberattaques, au cours du premier trimestre de 2022, selon un rapport de Identity Theft Resource Center

Trois principaux procédés se distinguent :

Tentative de phishing

C'est la principale cause de fuite de données. Lors de cette cyberattaque, le hackeur se fait passer pour une personne de confiance afin d'induire la victime en erreur et d'accéder à ses informations.

Attaque par force brute

Cette méthode consiste pour le hackeur à accéder à différents dossiers et applications en testant systématiquement tous les mots de passe possibles.

Utilisation de malwares

Cette technique se caractérise par l'introduction de logiciels malveillants dans les systèmes, permettant le vol de données sans que l'organisation ne s'en rende compte. Cette opération est facilitée par la présence de failles dans ces systèmes.

- **L'exposition sur Internet**

À l'heure de l'hyperconnexion, beaucoup ne comprennent pas l'impact et l'ampleur de l'exposition de nos datas sur Internet, alors même que nous utilisons quotidiennement divers appareils connectés.

Certaines entreprises autorisent par exemple leurs salariés à recourir à leurs smartphones personnels. Pourtant, ces appareils présentent souvent des failles de sécurité, permettant aux hackeurs d'y insérer facilement des malwares pour accéder aux informations de la société.

Un autre comportement à risque consiste à se connecter à un réseau Wi-Fi public dans le cadre du télétravail ou encore d'un déplacement professionnel.

Vous l'aurez compris, la source du problème reste, la plupart du temps, les comportements imprudents dus à un manque de formation à la cybersécurité.

- **La négligence de l'entreprise et des collaborateurs**

Les comportements imprudents se révèlent être une opportunité pour les malfaiteurs, puisque ces derniers exploitent généralement les failles de sécurité d'une entreprise pour commettre leurs actes malveillants.
Ces failles peuvent résulter de problèmes techniques, mais aussi de comportements inappropriés. Il est important de rappeler que les tentatives de phishing demeurent la principale source de fuites de données, soulignant ainsi que trop de personnes tombent encore dans ce piège.
En outre, la négligence peut également englober le vol ou la perte de matériel, comme un ordinateur ou une clé USB. Si ces dispositifs tombent entre des mains malveillantes, la vigilance s'impose.

- **Le vol interne**

Il est important de ne pas négliger une réalité regrettable : les employés peuvent aussi délibérément s'approprier des données confidentielles et sensibles de l'organisation dans le but de lui nuire (par exemple, par vengeance) ou dans le but de réaliser un profit. En effet, les données confidentielles d'une société se revendent à prix d'or au marché noir.

Pourquoi ? Parce que beaucoup de concurrents ou même d'entités étrangères peuvent être intéressés par les informations sensibles d'une entreprise afin d'obtenir un avantage concurrentiel sur le marché.

Stratégies de prévention et de réaction aux fuites de données

Audit de sécurité

Où en est réellement votre organisation en matière de protection de ses informations ? Pour obtenir une vision plus claire, nous vous recommandons de réaliser une Analyse d'Impact relative à la Protection des Données (AIPD).

Habituellement mise en œuvre pour se conformer au RGPD, cette démarche implique de faire un audit des pratiques au sein de votre entreprise afin :

- d'identifier les risques potentiels
- de comprendre les conséquences en cas de faille de sécurité ou de violation de vos informations

Ainsi, vous obtenez un état des lieux précis permettant de mettre en place les mesures appropriées.

Processus de gestion de crise

La mise en place de processus de gestion de crise efficaces permet entre autres :

- **D'identifier les réponses rapides** à apporter en cas de problème, en se basant sur des scénarios préalablement déterminés
- De constamment **développer des moyens techniques** pour prévenir les risques
- De sensibiliser les équipes à la gestion de crise, ainsi qu'aux risques cyber de manière générale
- De réaliser régulièrement des **tests pour détecter les vulnérabilités**, y compris les comportements inappropriés
- D'effectuer des **sauvegardes périodiques**, facilitant une reprise plus efficace en cas d'attaques sans paralyser l'activité
- D'apprendre des erreurs survenues suite à un incident, en remettant en question les pratiques en vigueur

Renforcer sa politique de mots de passe

La corrélation entre les fuites de données et les mots de passe faibles est fréquente.
En effet, la fragilité des identifiants de connexion sert souvent de point d'entrée dans vos systèmes. C'est pourquoi il est crucial de mettre en place une politique de mots de passe robustes afin de prévenir les comportements risqués tels que l'utilisation des mêmes identifiants pour plusieurs comptes.

Parmi les bonnes pratiques à adopter, il est recommandé :

D'utiliser exclusivement des **mots de passe complexes** (au moins 8 caractères, incluant des chiffres, des majuscules et des caractères spéciaux)

De les **renouveler** régulièrement

D'utiliser des **identifiants différents** pour chaque service

De **garantir leur confidentialité**, en évitant notamment de les partager par **email** ou de les noter sur un support physique

De favoriser **l'authentification forte** ou la **double authentification**

D'utiliser un **gestionnaire** de mots de passe

Comment réagir à une fuite de données ?

Si vous avez connaissance d'une éventuelle violation de vos données personnelles, contactez, si nécessaire, le service ou l'organisme concerné pour confirmer l'incident et obtenir des détails sur les informations potentiellement compromises.

1

Changez rapidement votre mot de passe sur les sites ou services touchés par la fuite de données, ainsi que sur tous les autres sites où vous auriez pu utiliser le même mot de passe.

2

En cas d'inclusion de vos coordonnées bancaires dans la fuite de données, **informez immédiatement votre banque** et prenez les mesures nécessaires, y compris l'opposition aux moyens de paiement concernés. Surveillez régulièrement vos comptes pour détecter toute opération inhabituelle.

3

Signalez les pages, comptes ou messages divulguant vos informations personnelles aux plateformes concernées et demandez leur suppression. Pour les principaux réseaux sociaux tels que Facebook, X, LinkedIn, Instagram, Snapchat, YouTube, utilisez les liens de signalement fournis. Contactez directement le service approprié s'il ne figure pas dans cette liste.

4

Demandez la non-indexation de vos données personnelles divulguées par les moteurs de recherche s'il y a lieu. Utilisez les formulaires de demande de suppression pour les principaux moteurs de recherche tels que Bing, Qwant, Google, Yahoo, entre autres. Pour en savoir plus, consultez les informations fournies par la CNIL.

5

Si, un mois après avoir demandé leur suppression, vos données personnelles restent accessibles sur la plateforme concernée, vous avez la possibilité de déposer une réclamation auprès de la CNIL via son téléservice de plainte en ligne.

6

En cas d'utilisation frauduleuse de vos données personnelles divulguées, **conservez toutes les preuves**, par exemple des messages, l'adresse du site web, des captures d'écran, et déposez une plainte auprès du commissariat de police, de la brigade de gendarmerie, ou envoyez une plainte écrite au procureur de la République du tribunal judiciaire compétent.

7

Le cas échéant, **envisagez une action de groupe ou un recours collectif**, permettant aux victimes de demander la cessation de la violation de données personnelles et la réparation du préjudice.

Importance de la sensibilisation et de la formation continue en matière de sécurité des données

Pour une sécurisation optimale de vos données, optez pour la formation à la cybersécurité ainsi que la sensibilisation au phishing. En effet, grâce à ces outils, vos collaborateurs monteront en compétence et connaîtront toutes les bonnes pratiques cyber.

Pour en savoir plus sur ces différents outils, découvrez nos **solutions de cybersécurité** !

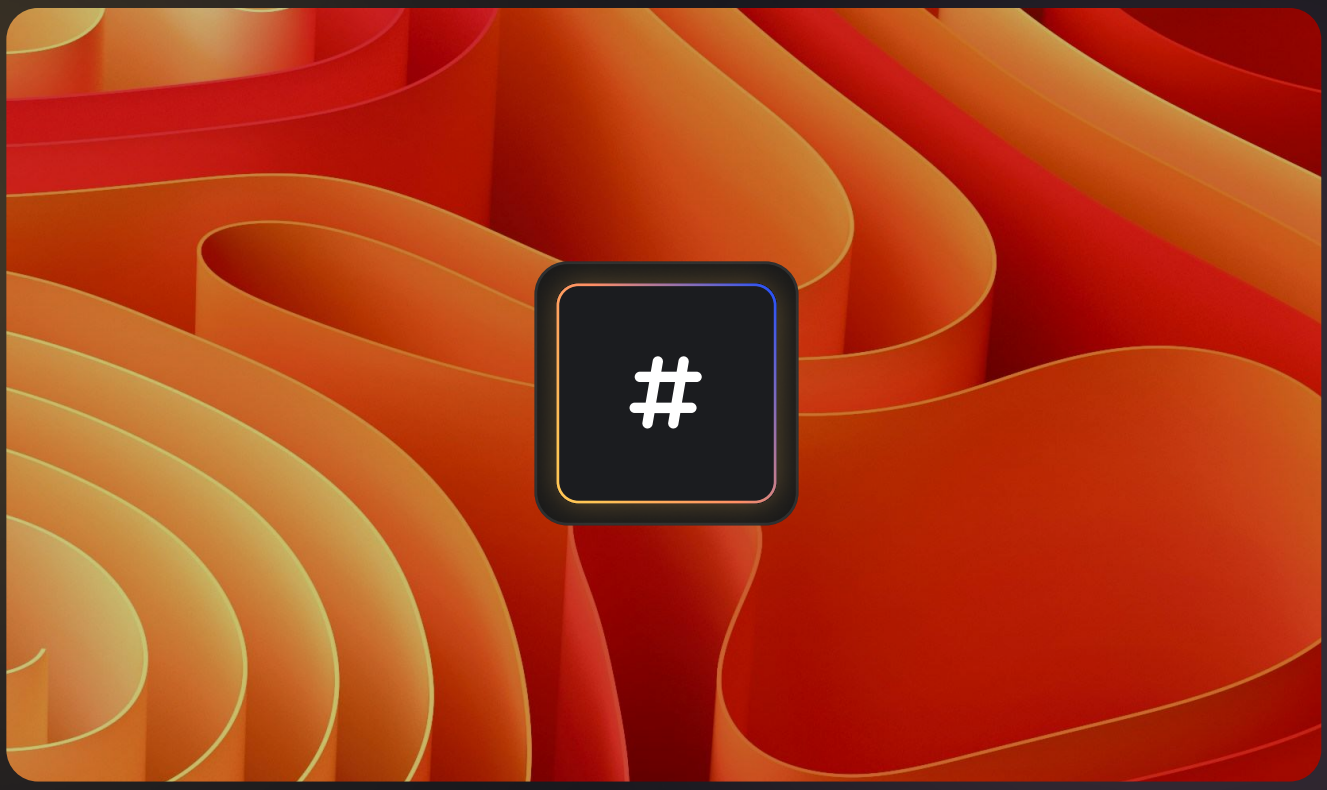
DÉCOUVRIR

Pour compléter les outils de formation et de sensibilisation à la cybersécurité, il est indispensable de protéger vos accès par des mots de passe solides. Pour vous aider dans cette démarche, le gestionnaire de mots de passe peut faire figure de solution idéale.

La mise en œuvre d'une stratégie proactive et efficiente pour lutter efficacement contre les cybermenaces repose sur plusieurs composantes, dont des solutions logicielles de cryptographie pour sécuriser de bout en bout vos transactions sur Internet.

2

Le hachage : une méthode de sécurité infaillible



Importance et principes de base du hachage des mots de passe

Les fonctions de hachage jouent un rôle essentiel en cryptographie et sont d'une importance fondamentale pour la technologie de la blockchain.

Dans le domaine de la sécurité, ces fonctions sont particulièrement bénéfiques car elles contribuent à :

- réduire la quantité d'informations à chiffrer
- authentifier les communications
- assurer le contrôle de l'intégrité des messages

Le hachage désigne une fonction ou un algorithme mathématique générant un résultat unique, appelé empreinte ou signature (hash). Il est apparu en informatique au cours des années 1950/1960 avec l'objectif de réduire la taille des fichiers, et est désormais fortement utilisé dans la blockchain.

Ces fonctions de hachage ont pour but principal de sécuriser le transfert de données ou d'informations entre deux systèmes qui, a priori, ne disposent d'aucun moyen intrinsèque pour assurer la sécurité de l'échange. Il existe de nombreuses fonctions de hachage, parmi lesquelles la fonction SHA-256, qui est particulièrement célèbre puisque utilisée par le Bitcoin pour assurer une sécurité complète des échanges.

Rôle du hachage dans la prévention des fuites de données

Le hachage, son rôle et ses fonctions dans la blockchain

Le hachage joue un rôle crucial dans la technologie blockchain en assurant l'intégrité et la sécurité des données.

Voici les principales fonctions du hachage dans le contexte de la blockchain :

Intégrité des données

Le hachage garantit l'intégrité des données en créant une empreinte numérique unique pour chaque bloc de données. Chaque bloc de la blockchain contient le hachage du bloc précédent, formant ainsi une chaîne. Si une seule modification est apportée à n'importe quel bloc, le hachage de ce bloc et de tous les blocs suivants est modifié, alertant ainsi les participants du réseau de la survenance d'une altération.

Sécurité

Les fonctions de hachage utilisées dans la blockchain sont conçues pour être unidirectionnelles et difficilement inversibles. Cela signifie que même une petite modification des données d'entrée va entraîner une modification significative du hachage, ce qui rend difficile pour un attaquant de prédire ou de reproduire le hachage sans connaître les données d'origine.

Preuve de travail (proof of work)

Dans certaines blockchains, comme celle du Bitcoin, le hachage est utilisé dans le processus de preuve de travail. Les mineurs doivent résoudre des problèmes mathématiques complexes qui nécessitent une puissance de calcul significative. Le hachage est au cœur de ce processus, et le mineur qui trouve la solution en premier est récompensé.

Adressage

Les adresses des participants et les identifiants de transaction dans la blockchain sont souvent dérivés à partir du hachage des clés publiques et des données de transaction. Cela permet de sécuriser l'identité des participants et de garantir que les données sont authentiques.

Accélération de la recherche

L'utilisation de hachages permet de faciliter et d'accélérer la recherche d'informations dans la blockchain. Plutôt que de comparer des blocs de données entiers, les participants peuvent comparer rapidement les hachages pour vérifier l'intégrité et la validité des données.

Quelles sont les différentes applications du hachage ?

Le hachage est une technique largement utilisée en informatique et trouve des applications dans divers domaines en raison de ses propriétés uniques. Voici quelques-unes des principales applications du hachage :

Sécurité des mots de passe

Les fonctions de hachage sont couramment utilisées pour stocker les mots de passe de manière sécurisée dans un logiciel tel qu'un gestionnaire de mots de passe. Au lieu de conserver les mots de passe en texte brut, les systèmes stockent généralement les hachages des mots de passe. Cela rend plus difficile pour les attaquants d'obtenir les mots de passe réels à partir des bases de données, car ils doivent casser le hachage, ce qui est une tâche complexe.

Cryptographie

Le hachage est une composante essentielle des algorithmes cryptographiques, notamment dans la création de signatures numériques, la génération de clés, et la vérification d'intégrité des messages.

Blockchain

Comme mentionné précédemment, le hachage est utilisé pour assurer l'intégrité et la sécurité des données dans la blockchain. Chaque bloc contient le hachage du bloc précédent, créant une chaîne sécurisée et immuable.

Stockage de données

Les systèmes de gestion de bases de données utilisent souvent des hachages pour accélérer la recherche et l'accès aux données. Les index basés sur les hachages permettent des recherches rapides dans de grandes bases de données.

Techniques et meilleures pratiques pour un hachage efficace

Comment protéger vos transactions avec le hachage ?

Protéger les transactions avec le hachage implique principalement l'utilisation de fonctions de hachage cryptographiques.
Tout d'abord, choisissez des algorithmes de hachage robustes et cryptographiquement sécurisés tels que SHA-256 (Secure Hash Algorithm 256 bits) ou SHA-3.

Ces algorithmes sont conçus pour être résistants aux attaques, même avec l'utilisation de puissantes capacités de calcul. Ensuite, pour garantir leur intégrité et pour éviter l'**usurpation d'identité**, assurez-vous de hacher l'ensemble des données de la transaction, y compris les champs critiques tels que :

- le montant
- l'emetteur
- le destinataire
- les horodatages

Cela crée une empreinte unique qui représente l'état de la transaction.
Enfin, si le hachage est utilisé pour stocker des mots de passe dans un système, ajoutez une valeur aléatoire appelée « salt » avant le hachage. Le **salage** rend plus difficile l'utilisation de tables arc-en-ciel (rainbow tables) et d'autres attaques par force brute.

Comment protéger vos mots de passe avec le hachage ?

La mise en œuvre du hachage de mot de passe est une mesure de sécurité fondamentale

En l'absence de cette pratique, chaque mot de passe enregistré est susceptible d'être compromis en cas d'intrusion dans le support de stockage, généralement

une base de données. Un tel accès non autorisé permettrait d'entrer frauduleusement non seulement dans cette application, mais également dans d'autres applications si l'utilisateur utilise le même mot de passe ailleurs.

En appliquant un hachage au mot de passe avant de le stocker, vous compliquez considérablement la tâche d'un attaquant pour découvrir le mot de passe d'origine. De plus, vous conservez la possibilité de comparer le mot de passe haché avec une chaîne reçue pour des vérifications ultérieures.
Pour vous aider, il existe des outils tels que le **générateur de mots de passe** ainsi que des guides qui vous donneront des **exemples de mots de passe**.

Savoir résoudre le hash

Résoudre un hachage, dans le contexte de la cryptographie et de la sécurité informatique, ne signifie pas trouver une solution unique au hachage, car les fonctions de hachage sont conçues pour être résistantes à l'inversion. En d'autres termes, elles sont conçues pour être difficiles à inverser, ce qui signifie qu'il est compliqué de partir d'un hachage pour retrouver les données d'origine.

Cependant, dans le contexte du minage de cryptomonnaie (comme le Bitcoin), on parle de « résoudre un hachage » en référence au processus de preuve de travail. Voici comment cela fonctionne :

1

Sélection du nonce

Un nonce (nombre utilisé une seule fois) est choisi de manière aléatoire.

2

Hachage des données

Les données du bloc, y compris le nonce, sont hachées à l'aide d'une fonction de hachage cryptographique.

3

Vérification de la difficulté

Le hachage résultant est vérifié pour voir s'il commence par un certain nombre de zéros, conformément à la difficulté définie par le réseau. La difficulté est ajustée régulièrement pour maintenir un taux constant de production de blocs.

4

Répétition

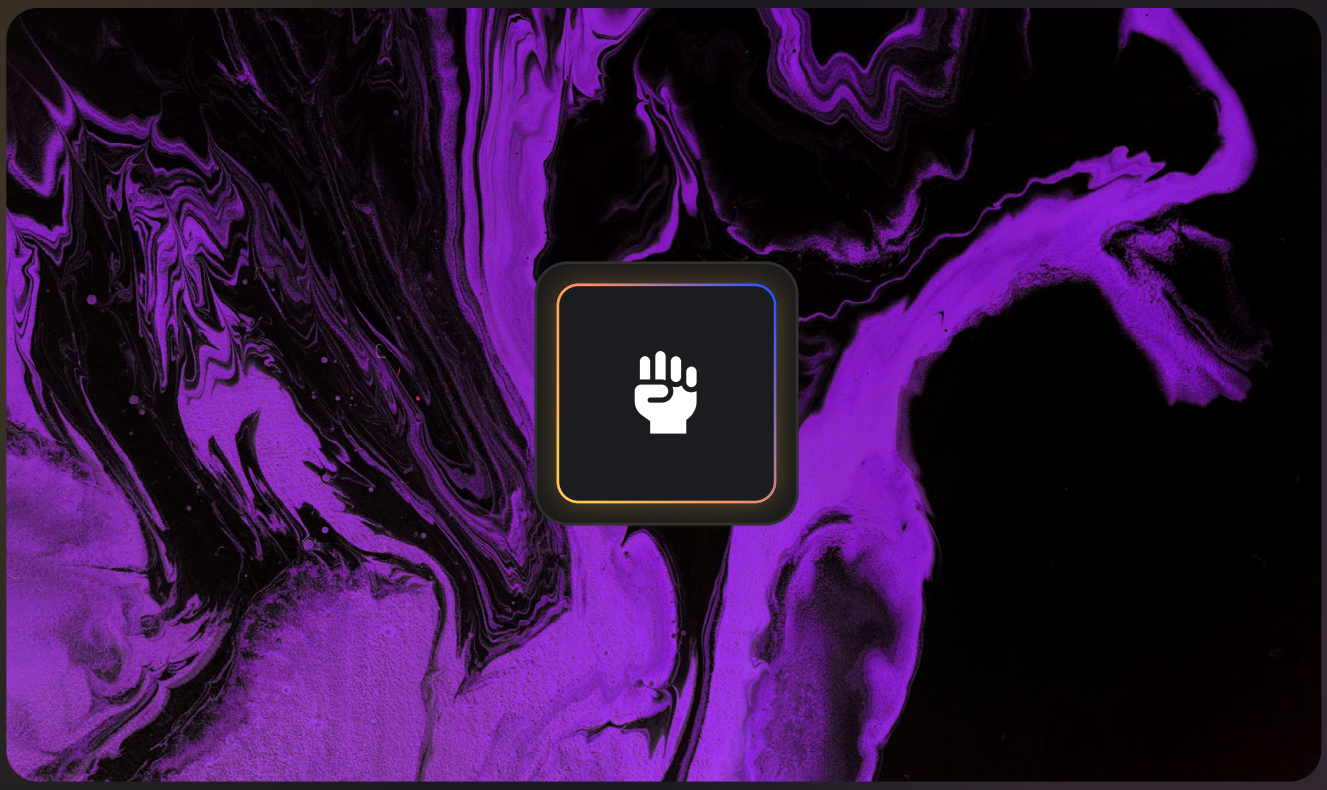
Si le hachage ne satisfait pas la difficulté, un autre nonce est choisi et le processus est répété. Cela continue jusqu'à ce qu'un mineur trouve un hachage qui répond aux critères de difficulté.

En dehors du contexte du minage de cryptomonnaie, résoudre un hachage peut également faire référence à des attaques telles que la recherche de collisions (deux ensembles de données différents produisant le même hachage), mais cela nécessite des méthodes et des ressources spécifiques. Dans le cadre de l'utilisation normale des fonctions de hachage en cryptographie, l'objectif est généralement de garantir l'intégrité des données et de rendre difficile toute tentative de manipulation.

Les fonctions de hachage permettent d'assurer un niveau de sécurité élevé pour garantir l'intégrité des données qui transitent sur la Toile. C'est un dispositif logiciel essentiel pour lutter contre les stratégies malveillantes comme les attaques bruteforce que les cyber-hackeurs utilisent pour récupérer les identifiants de connexion et les mots de passe.

3

Attaque bruteforce : comprendre et contrer la menace



Comprendre les attaques bruteforce et leur fonctionnement

L'attaque bruteforce est indubitablement l'une des méthodes d'attaque les plus simples. La raison principale est que le maillon faible de la chaîne de cybersécurité demeure le facteur humain. Il n'est pas nécessaire de mettre en œuvre des tactiques d'ingénierie sociale complexes ou des attaques d'injection SQL sophistiquées pour dérober des identifiants, car les habitudes persistent: les mots de passe des utilisateurs restent souvent faibles et donc facilement devinables. Grâce à des outils appropriés, même les hackeurs les moins expérimentés parviennent à compromettre les données et à paralyser les systèmes de grandes entreprises.

Qu'est-ce qu'une attaque bruteforce ?

Une attaque par force brute, également connue sous le terme de bruteforce, est une méthode utilisée par les cybercriminels pour compromettre les informations d'identification des comptes et principalement les mots de passe.

Lors d'une attaque par bruteforce, le hackeur dispose généralement d'un dictionnaire contenant des termes et des mots de passe couramment utilisés, dont il se sert pour « deviner » le mot de passe d'un utilisateur. Après avoir épuisé les termes du dictionnaire, l'attaquant explore des combinaisons de caractères jusqu'à ce qu'une correspondance soit trouvée.
Il peut être nécessaire d'effectuer des milliers de tentatives avant de réussir à cracker un mot de passe. Cela explique pourquoi les attaquants recourent à des outils d'automatisation pour réaliser rapidement un grand nombre de tentatives.

Comment les attaques bruteforce fonctionnent-elles ?

Les attaques par force brute sont fréquemment orchestrées par des scripts ou des robots ciblant la page de connexion d'un site ou d'une application. Ils examinent des clés, des mots de passe connus et des chaînes de caractères potentiels. Les applications les plus

répandues doivent se protéger contre ce type d'attaque en mettant en place des mesures telles que :

- le chiffrement
- l'utilisation de clés API
- le suivi du protocole SSH

Cracker un mot de passe n'est qu'une étape dans la chaîne de destruction d'un hackeur. En effet, cela peut servir à accéder à des :

- profils utilisateur
- boîtes de messagerie électronique
- comptes bancaires

ou à compromettre des API et d'autres services nécessitant une connexion et des informations d'identification.

Quelles sont les différentes attaques bruteforce ?

La définition globale des attaques par bruteforce implique de tenter de « deviner » les informations d'identification des utilisateurs en explorant toutes les combinaisons de caractères jusqu'à obtenir une correspondance.

Cependant, les attaquants emploient différentes stratégies de force brute pour maximiser leurs chances de succès. Il est crucial pour les entreprises de comprendre tous les types d'attaques par force brute afin de développer des stratégies de protection efficaces.

Les catégories d'attaques par force brute comprennent :

Attaques par dictionnaire

De nombreuses attaques par force brute font usage d'une liste de dictionnaires comprenant des mots, des phrases et des mots de passe couramment utilisés, téléchargés depuis Internet.

Password spraying

Ici, l'attaquant tente d'accéder à plusieurs comptes sur un même domaine en utilisant des mots de passe courants. En exploitant une liste de mots de passe faibles et répandus, tels que 123456 ou password1, un pirate peut potentiellement compromettre des centaines de comptes en une seule attaque.

Credential stuffing

Il est fréquent que les utilisateurs adoptent les mêmes mots de passe pour plusieurs sites. Un attaquant qui réussit à obtenir l'accès aux mots de passe des utilisateurs sur un site tentera ces mêmes mots de passe sur d'autres sites, un phénomène connu sous le nom de « credential stuffing ».

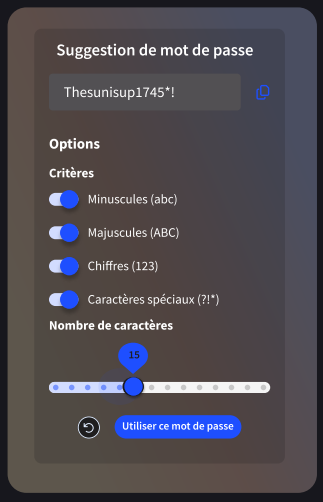
Stratégies de prévention et de protection contre les attaques bruteforce

Amélioration de votre politique de mots de passe

Contrer une attaque par force brute requiert inévitablement la mise en place d'une politique de mots de passe efficace. Dans cette optique, le seul critère véritablement essentiel est sa taille, car plus un mot de passe est long, plus il devient difficile à deviner lors d'une attaque par bruteforce.

Malheureusement, ce critère de longueur est souvent négligé par les entreprises lorsqu'elles définissent ces politiques de mots de passe, et les utilisateurs se retrouvent souvent soumis à des consignes contreproductives, voire dangereuses en termes de sécurité. Les directives stipulant au moins 8 caractères pour un mot de passe, incluant au moins une majuscule, un chiffre et un caractère spécial, sont obsolètes et peuvent être trompeuses.

Prenons **l'exemple du mot de passe** suivant : « Password2! ». En suivant les directives mentionnées, ce mot de passe est considéré comme sécurisé, bien qu'il soit en réalité plus facile à deviner lors d'une attaque par force brute que le mot de passe suivant : « ceciestmonmotdepasseettuneleconnaispas » qui ne contient ni chiffre, ni majuscule, ni caractère spécial. Ainsi, la longueur est l'élément clé pour définir un mot de passe sécurisé (15 à 20 caractères, quelle que soit leur nature), car cela réduit considérablement les chances qu'on le devine. Mais il est évident qu'il convient d'éviter les suites de caractères (comme « 12345678910111213 »). Pour vous aider à générer un mot de passe robuste et sécurisé, vous pouvez utiliser notre générateur de mots de passe.



Il est également essentiel de partir du principe qu'un attaquant n'utilise généralement pas cette technique, en saisissant manuellement des mots de passe un par un, bien que cela puisse se produire pour des mots de passe par défaut.

En effet, de nombreuses applications web et frameworks créent des utilisateurs par défaut lors de l'installation (par exemple, ID : admin/mot de passe : admin). Si ces comptes utilisateur ne sont pas supprimés ou modifiés, ils représentent des cibles faciles pour une attaque par force brute qui repose généralement sur un outil automatisé effectuant des milliers de requêtes par minute avec des informations d'identification générées à partir d'une longue liste de valeurs possibles (attaques par dictionnaire).

De plus, diverses solutions existent pour **former à la cybersécurité** vos collaborateurs. L'une d'entre elles consiste à les responsabiliser en les incitant à vérifier régulièrement si leurs mots de passe, identifiants ou numéros de téléphone n'ont pas été compromis et divulgués lors d'une fuite de données.

Implémentation d'une authentification multifacteur

L'introduction d'un facteur d'authentification supplémentaire complique également la tâche d'un attaquant tentant de compromettre un compte par le biais d'une attaque par bruteforce. En effet, avec la mise en place d'une authentification à deux facteurs (2FA), l'attaquant se heurtera à une nouvelle barrière, souvent extrêmement difficile voire impossible à contourner, notamment s'il est confronté à un code généré aléatoirement avec une durée limitée. Par conséquent, même en ayant accès au bon identifiant et au bon mot de passe, l'attaquant ne pourra pas accéder au compte de l'utilisateur.

Création d'un algorithme plus sécurisé pour le stockage des mots de passe

Il est impératif de sécuriser le stockage des mots de passe des utilisateurs dans la base de données. En cas de compromission de cette dernière, tous les mots de passe deviennent accessibles s'ils sont stockés en clair. Il est formellement déconseillé de stocker les mots de passe de manière non cryptée. Ainsi, il est crucial d'opter pour l'utilisation d'un **gestionnaire de mots de passe** robuste.

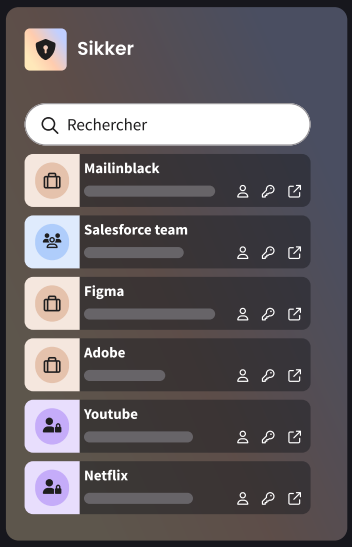
Gestion de crise et réaction en cas d'attaque réussie

Comme l'indique l'ANSSI : "La gestion d'une crise cyber ne s'improvise pas : il est nécessaire de se préparer, s'outiller, s'entraîner et de connaître les bonnes pratiques de gestion de crise."

L'utilisation du mot de passe demeure le moyen d'accès le plus répandu. Cependant, bien que peu sophistiquées, les attaques par force brute se révèlent extrêmement efficaces pour compromettre des données personnelles. Il est donc impératif de mettre en place des mécanismes de sécurité appropriés.

La première et principale stratégie pour vous prémunir contre une attaque par force brute consiste à imposer à tous vos collaborateurs de choisir des mots de passe robustes. Ainsi, les directives traditionnelles, comme celles exigeant une longueur minimale de 8 caractères avec une combinaison de lettres majuscules et de minuscules, de chiffres et de signes de ponctuation, sont dépassées. Pour une protection optimale, le coffre-fort numérique s'avère être l'outil parfait pour vous permettre de mettre en œuvre et de renforcer votre politique de mots de passe.

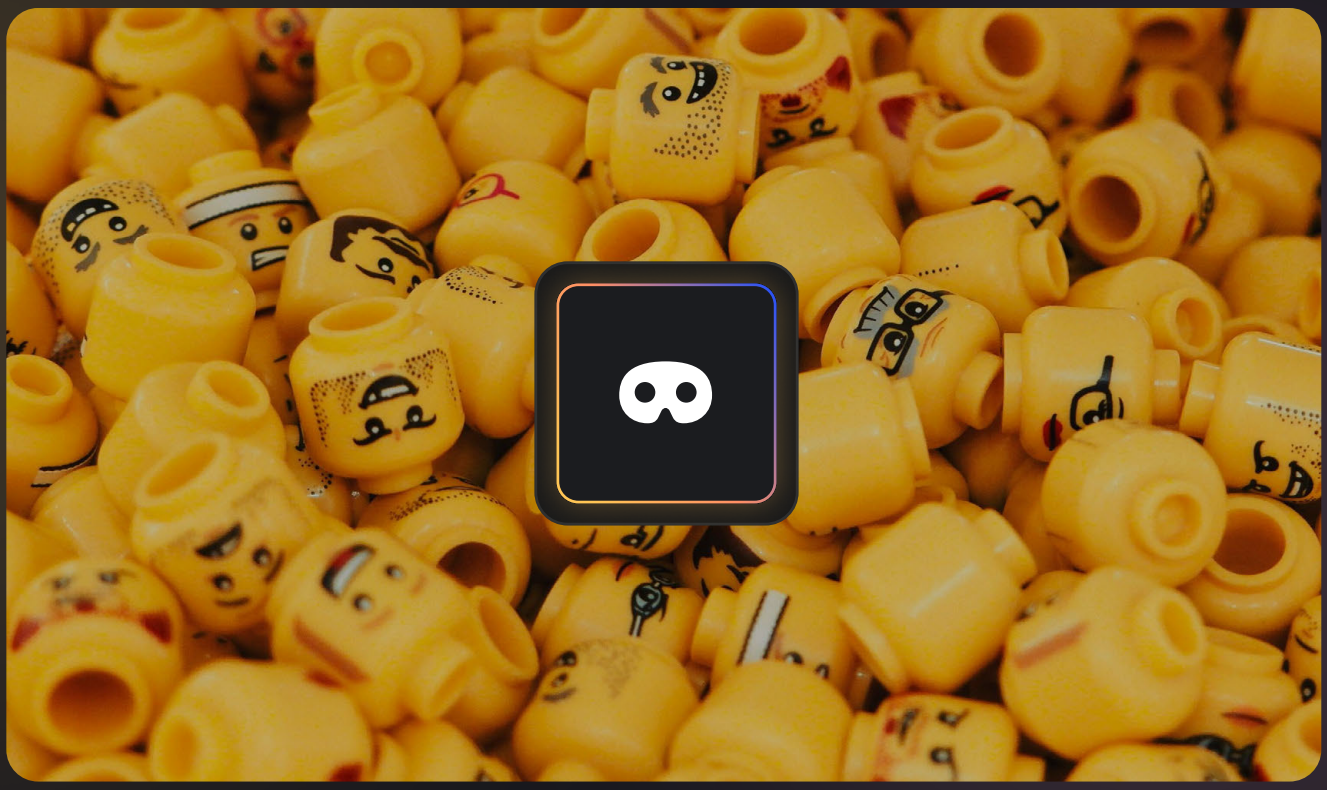
Enfin, il peut être intéressant de sensibiliser régulièrement vos collaborateurs aux attaques comme les bruteforce. Le meilleur exercice reste la simulation de cyberattaques pour préparer vos salariés à faire face à ce genre de menace.



Si la méthode de bruteforce est ancienne, les pirates informatiques exploitent aussi des méthodes plus actuelles comme l'ingénierie sociale, une technique de manipulation utilisée pour extorquer les mots de passe à leurs victimes.

4

Comprendre le catfishing et ses risques



Définition et implications du catfishing pour les entreprises

Le catfishing (pêche au poisson-chat ou cyberimposture) est un phénomène récent en matière de cybersécurité, puisqu'il a émergé comme une préoccupation sérieuse seulement au début des années 2010. Le terme a ensuite été popularisé par le documentaire « Catfish » et la série télévisée du même nom, diffusée sur MTV en 2012.

Qu'est-ce que le catfishing ?

En cybersécurité, le catfishing se réfère à la création par un cybercriminel d'une fausse identité en ligne dans le but de :

- tromper
- frauder
- exploiter

Cette attaque est principalement associée à des escroqueries à la romance sur les :

- applications de rencontres
- sites web
- réseaux sociaux

Les hackeurs qui pratiquent cette tromperie séduisent leurs victimes sur la durée. Ils utilisent des tactiques d'ingénierie sociale afin d'établir une relation de confiance visant à diminuer la vigilance de leurs cibles.

Les signes révélateurs du catfishing

Il faut garder en tête que certains vrais profils peuvent correspondre à quelques-uns des points énumérés ci-dessous. :

Un profil avec très peu de photos peut susciter des interrogations. Il peut s'agir d'une personne extrêmement mystérieuse, mais cela est souvent révélateur d'un catfisher dont l'apparence ne correspond pas à celle figurant sur les photos.

A contrario, un profil avec des photos un peu trop « parfaites » peut également être suspect. Alors que la plupart des utilisateurs utilisent simplement l'appareil photo de leur téléphone, la personne avec qui vous discutez préfère, elle, recourir à des professionnels pour se faire photographier. Si vous avez un doute, n'hésitez pas à aller sur Google pour voir si les photos de ce profil ne proviennent pas du réseau social d'un mannequin ou d'une personnalité publique.

Le manque de liens vers d'autres comptes ou réseaux sociaux peut également être suspect. La plupart des utilisateurs aiment partager leur compte Spotify ou Instagram. Cela leur permet de faire connaître leurs goûts musicaux ou leurs activités sociales.

Si un profil coche plusieurs de ces points, ou même tous, il est préférable de passer votre chemin pour éviter tout risque !

Les différents dangers et effets du catfishing

Le phénomène du catfishing peut avoir des conséquences dévastatrices pour les victimes et toucher également leur famille et leur cercle proche. Voici quelques-uns des risques et des impacts les plus fréquemment observés liés au catfishing :

Perte financière

Les individus pratiquant le catfishing cherchent généralement à duper leurs victimes en simulant une situation de détresse et en exploitant leur compassion pour obtenir de l'argent.

+24 000

personnes aux États-Unis ont perdu environ 1 milliard de dollars cumulés en 2021, à cause de ces arnaques sentimentales, d'après le « Internet Crime Complaint Center » du FBI

Atteinte à la réputation

En menaçant de divulguer des informations privées ou compromettantes pour la victime, entraînant ainsi des dommages considérables à sa réputation, le catfishing peut être un puissant moyen de chantage. Les personnalités publiques comme les célébrités, les athlètes et d'autres individus très exposés médiatiquement peuvent voir leur image fortement altérée en raison de situations de catfishing.

Usurpation d'identité

Le catfishing peut également entraîner l'usurpation d'identité sous différentes formes. En effet, les informations personnelles de la victime peuvent être exploitées pour créer une nouvelle identité ou commettre des actes frauduleux. De plus, les pseudonymes créés par les catfishers peuvent compromettre la véritable identité d'une personne.

Détresse émotionnelle

Le catfishing peut toucher toutes les générations, mais les principales victimes sont généralement les individus plus âgés et vulnérables. Les conséquences émotionnelles chez les personnes dupées peuvent être sévères, induisant fréquemment des sentiments de trahison, de douleur, d'humiliation, voire d'anxiété et de dépression.

Hack de vos profils sociaux

Pour éviter que les hackeurs aient accès à tous vos profils sociaux suite à l'obtention de vos mots de passe, nous vous conseillons d'opter pour des mots de passe forts et uniques pour chacun de vos comptes. Cela permettra de maintenir votre sécurité malgré la compromission de l'un de vos mots de passe. Pour vous aider à en créer des robustes, il y a le générateur de mots de passe. Mais mieux encore, il est recommandé d'utiliser un gestionnaire de mots de passe. Cet outil permet une sécurité optimale.

Stratégies pour identifier et éviter les pièges du catfishing

Avant de vous expliquer comment détecter du catfishing, il est essentiel de rappeler la complexité de cette tâche dans le cadre d'une rencontre. Lorsqu'on fait connaissance, il est tout à fait naturel d'échanger certaines informations personnelles. Cependant, si vous observez plusieurs des signes énumérés ci-dessous au cours de votre conversation, il est probable que vous soyez en présence d'un escroc. Soyez attentif !

Demande d'informations personnelles

Lors d'une conversation sur une application de rencontre, il est normal de chercher à en savoir davantage sur son interlocuteur. Cependant, un escroc aura tendance à solliciter des informations personnelles plus rapidement que lors d'une conversation habituelle. Des questions inhabituelles devraient susciter votre méfiance, concernant :

- votre salaire
- votre adresse
- votre adresse e-mail
- vos identifiants de connexion

Les informations récoltées par les hackeurs peuvent ensuite alimenter leurs attaques de spearphishing.

Pas de contact en personne/en vidéo

Une personne malintentionnée cherchera systématiquement à éviter les rencontres physiques ou les contacts vidéo, car cela augmente les risques de se faire démasquer. Ainsi, elle annulera fréquemment les rendez-vous au dernier moment. Bien sûr, une personne dénuée d'intentions malveillantes peut avoir des imprévus l'empêchant de vous rejoindre, mais des annulations à répétition peuvent être un indicateur de catfishing.

Manque de cohérence dans certains propos

Selon le niveau de préparation de l'attaquant, sa fausse identité et ses justifications peuvent présenter des incohérences. Soyez attentif aux détails et n'hésitez pas à confronter votre interlocuteur à ses contradictions.

Demande d'aide financière

La sollicitation d'une assistance financière est l'objectif principal de la plupart des attaques de catfishing visant les individus. Il est évident que dans ce contexte l'envoi d'argent à une personne est une erreur et un signal d'alarme important.

Identité numérique incomplète

Fréquemment, les profils créés à des fins de catfishing sont superficiels, limités à la plateforme utilisée pour l'attaque. Pour déceler une possible tromperie, effectuez des recherches sur l'individu sur d'autres réseaux sociaux. Si vous ne trouvez aucun résultat et qu'aucun compte supplémentaire, comme LinkedIn, n'est associé au profil, il est possible que vous soyez confronté à une situation de catfishing.
Par ailleurs, ces profils, en tant qu'éléments de l'identité numérique, doivent fournir du contexte et faciliter la vérification de la cohérence des informations échangées au cours des conversations.

Comment vous protéger du catfishing ?

Nous avons exploré les divers signes permettant de détecter un cas de catfishing. À présent, nous allons examiner les mesures à prendre pour vous prémunir contre de telles attaques.

L'intuition

En cas d'incertitude quant à l'identité de votre interlocuteur, fiez-vous à votre intuition. Un sentiment de malaise n'est jamais infondé et peut vous épargner une situation dangereuse et inconfortable.

Recherche d'image inversée

Capturez l'image de profil de votre interlocuteur, ensuite effectuez une recherche d'image inversée sur des plateformes telles que Google, TinEye ou PimEyes pour trouver d'autres sources de cette image. En général, les photos de profil utilisées dans des cas de catfishing sont souvent associées à des profils existants.

Cependant, soyez vigilant car il devient de plus en plus facile de créer des photos de profil à l'aide de générateurs basés sur l'intelligence artificielle.

Demander des photos et vidéos dans différents contextes

Malgré l'existence de technologies telles que les deepfakes, demander des photos dans différents contextes rend plus coûteux pour l'attaquant le maintien de la cohérence. Demandez des vidéos de votre interlocuteur ou des photos de groupe, car ces éléments sont plus complexes à produire que de simples photos de profil.

Éviter de transférer de l'argent à un inconnu

Il va de soi que vous ne devez jamais transférer d'argent à quelqu'un que vous n'avez pas rencontré en personne. Évitez également de partager trop d'informations personnelles lors de vos conversations avec des inconnus. Cela diminuera considérablement les risques d'escroquerie.

Cloisonnement

Une règle fondamentale en matière de cybersécurité pour éviter la fuite des données est de maintenir la séparation des usages. Cela implique que le matériel (ordinateur, téléphone) ainsi que les sites web et adresses email utilisés pour vos activités et conversations personnelles soient distincts de ceux utilisés à des fins professionnelles.
De cette manière, une éventuelle infection d'un ordinateur personnel par un logiciel malveillant provenant d'une opération de catfishing ne pourra pas se propager sur le réseau de l'entreprise.

Protections logicielles

La première précaution pour prévenir toute infection consiste à être très prudent lors de l'échange de fichiers sur les plateformes.
En cas de transmission de malwares, la présence d'un antivirus à jour et d'un pare-feu peut potentiellement atténuer l'impact de l'attaque en détectant le malware ou toute activité réseau suspecte associée.

Signaler

Comme c'est le cas pour la plupart des cyberattaques, le signalement des arnaques contribue à permettre aux autorités de localiser les hackeurs.
Vous avez également la possibilité de signaler l'attaque sur signal-spam.fr, une plateforme en ligne où la CNIL (Commission nationale de l'informatique et des libertés) prend en charge votre signalement.

Sensibilisation et formation des employés aux risques du catfishing

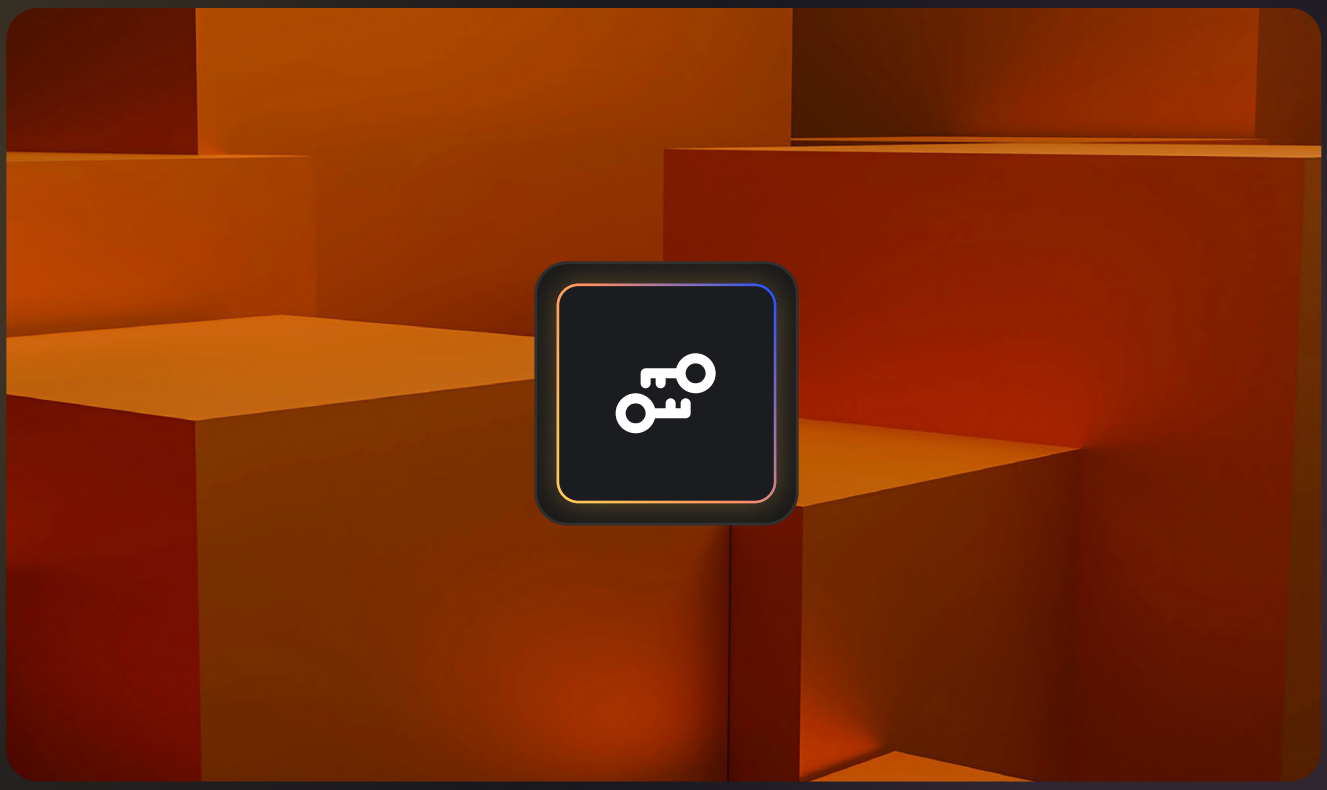
Première étape de votre stratégie de cybersécurité, la sensibilisation vise à donner des clés de compréhension à vos collaborateurs. Le meilleur moyen ? Les mettre en situation en simulant des cyberattaques, analyser leur comportement et les former avec des modules simples, courts et ludiques. Le tout de manière 100 % automatisée !

Le rêve de tout cyberattaquant ? Des collaborateurs non sensibilisés, mal informés et isolés. Transformez votre équipe en cauchemar des hackeurs en la formant de manière interactive et engageante grâce à notre solution **Cyber Academy**.

Pour parfaire votre dispositif logiciel de cybersécurité face à des techniques de piratage toujours plus sophistiquées et renforcer la robustesse de vos identifiants de connexion, utilisez la technique du salage de mots de passe en complément du hachage.

5

Le salage de mots de passe : une couche de sécurité indispensable



Explication du salage des mots de passe et de son importance

L'élaboration de mots de passe robustes est essentielle pour préserver vos informations en cas de compromission de données. Cependant, même avec un mot de passe aléatoire de plus de 12 caractères comprenant des symboles et des chiffres : la sécurité de vos identifiants dépend largement de la façon dont les divers services stockent ces mots de passe.

Qu'est-ce que le salage de mots de passe ?

En général, vos mots de passe ne sont pas stockés en texte clair. Lorsque vous vous connectez à un compte, le mot de passe transite par un algorithme de hachage unidirectionnel. Il est ainsi transformé en une chaîne de caractères indéchiffrable et totalement distincte. Cette séquence est ensuite comparée aux autres hachages dans la base de données, et si elle correspond, l'accès au compte est autorisé.

Bien que cette méthode semble sécurisée pour le stockage des mots de passe, elle présente un problème. En effet, si deux mots de passe sont identiques, leur hachage sera également identique, facilitant ainsi le déchiffrage par les hackeurs. C'est ici que le salage intervient.

Le salage des mots de passe, appelé « password salt » en anglais, consiste à ajouter une portion de données aléatoires au mot de passe avant de le soumettre à l'algorithme de hachage de façon sécurisée.
Prenons l'exemple du mot de passe « maison ». Si un autre utilisateur utilise le même mot de passe, les hachages correspondants seront identiques. Toutefois, en ajoutant quelques caractères aléatoires aux deux mots de passe, tels que « maison+7Ko# » et « maison8p?M », on obtient des hachages complètement différents.

Comment fonctionne le salage de mots de passe ?

Le salage des mots de passe est donc un système de cryptage qui consiste à ajouter un élément aléatoire au mot de passe associé à un nom d'utilisateur avant de hacher la nouvelle chaîne de caractères. Cela se fait généralement à l'aide d'un algorithme de

hachage MD5. Le salage des mots de passe est fréquemment utilisé dans les systèmes d'exploitation Linux, considéré généralement comme un modèle de cryptage de mot de passe plus sécurisé que ceux employés dans diverses distributions Microsoft.

Quelle est la différence entre hachage et salage ?

Le hachage des mots de passe est une pratique serveur utile lorsque les opérateurs du serveur n'ont pas besoin de connaître le texte en clair, mais seulement de savoir que l'utilisateur le connaît. Ce processus unidirectionnel convertit un mot de passe en texte chiffré à l'aide d'algorithmes de hachage. Un mot de passe haché ne peut pas être déchiffré, mais les hackeurs peuvent tenter de la rétro-ingénierie.

Le salage des mots de passe ajoute quant à lui des caractères aléatoires avant ou après le mot de passe, avant son hachage, pour dissimuler le mot de passe réel. Comme le salage est aléatoire, il devient extrêmement difficile pour les hackeurs de déterminer les vrais mots de passe à partir des mots de passe salés et hachés. En raison de cette variabilité, leurs tentatives d'utilisation de tableaux de mots de passe précalculés sont inefficaces.

Quels sont les avantages du salage de mots de passe ?

Le salage de mots de passe offre plusieurs avantages en matière de sécurité des données :

1

La résistance aux attaques par dictionnaire

En ajoutant une valeur aléatoire (le sel) à chaque mot de passe, même des mots de passe couramment utilisés deviennent uniques, rendant inefficaces les attaques par dictionnaire qui tentent de deviner les mots de passe en utilisant des listes prédéfinies.

2

La prévention des attaques par rainbow tables

Les tables arc-en-ciel sont des bases de données précalculées contenant des hachages de mots de passe courants. Le salage rend ces tables moins utiles, car chaque hachage est unique, même pour des mots de passe identiques.

3

Le renforcement de la confidentialité

Le sel, qui est habituellement stocké de manière sécurisée sur le serveur, rend difficile pour les attaquants de prévoir ou de reproduire les mêmes conditions d'entrée pour un hachage donné.

4

La protection contre les attaques par force brute

Les attaques par force brute impliquent de tester de nombreuses combinaisons de mots de passe. Le salage augmente le nombre possible de combinaisons, rendant ces attaques beaucoup plus difficiles et coûteuses en temps.

5

Une sécurité en cas de fuites de bases de données

En cas de fuite de la base de données, les mots de passe demeurent difficiles à récupérer en raison de la présence du sel, ce qui réduit le risque d'utilisation malveillante des informations volées et d'usurpation d'identité.

6

Vérification de la difficulté

Le salage contribue à maintenir la sécurité même face aux progrès de la puissance de calcul, des algorithmes de hachage et des techniques d'attaque, en introduisant une couche de complexité supplémentaire.

Le salage des mots de passe est une cryptographie efficace pour renforcer la sécurité des identifiants en rendant les attaques plus difficiles à exécuter avec succès.

Intégration du salage dans les pratiques de sécurité des mots de passe

Implanter une stratégie de salage de mots de passe dans votre entreprise

Implémenter une stratégie de salage de mots de passe au sein de votre entreprise est une étape cruciale pour renforcer la sécurité des données des utilisateurs.

Voici une liste de bonnes pratiques pour mettre en œuvre cette stratégie :

Évaluer ses besoins de sécurité

Évaluez les besoins spécifiques de sécurité de votre entreprise. Considérez le type de données stockées, leur niveau de sensibilité et les réglementations en vigueur.

Mettre à niveau ses anciens mots de passe

Si possible, encouragez vos collaborateurs à mettre à jour leurs anciens mots de passe pour qu'ils bénéficient du nouveau processus de salage.

Utiliser un générateur de mots de passe

Le générateur de mots de passe est un outil grâce auquel l'utilisateur peut générer des mots de passe aléatoires, robustes et uniques pour chacun de ses comptes à partir d'exigences définies préalablement.

Opter pour un gestionnaire de mots de passe

Le gestionnaire de mots de passe est une bonne pratique de sécurité grâce à laquelle l'utilisateur peut gérer ses mots de passe de manière centralisée en les stockant dans une base de données appelée portefeuille.

Effectuer des tests de sécurité

Effectuez des tests de sécurité réguliers pour identifier et corriger les vulnérabilités potentielles dans le système.

Former ses utilisateurs

Proposez une formation à la cybersécurité à vos collaborateurs pour les sensibiliser à l'importance de maintenir des mots de passe forts et sécurisés.

Vérifier la conformité aux réglementations

Assurez-vous que la stratégie de salage est en conformité avec les réglementations en matière de protection des données, telles que le RGPD.

Implémenter une stratégie de salage de mots de passe demande une planification méticuleuse et une communication claire avec les utilisateurs. Cela contribue grandement à renforcer la sécurité des identifiants au sein de votre entreprise.

Le mot de la fin

La protection de vos données et de vos systèmes d'information passe par une gestion opérationnelle de vos mots de passe combinant :

La mise en œuvre de solutions logicielles de cryptographie spécialisées dans la sécurisation des transactions sur Internet (fonction de hachage, salage des mots de passe).

La sensibilisation de vos collaborateurs aux risques cyber, aux enjeux de la cybersécurité et à l'importance de mots de passe forts pour protéger l'accès aux données et services de l'entreprise.

La formation aux bonnes pratiques liées à la cybersécurité. Avec la sensibilisation, c'est le seul moyen de responsabiliser vos collaborateurs et de les mobiliser sur des enjeux communs. Cette formation est essentielle pour savoir comment gérer les fuites de données et acquérir les bons réflexes en matière de gestion des mots de passe de connexion.

Pour être réellement efficace, une stratégie de cybersécurité doit être exhaustive. En plus de la gestion des mots de passe sécurisés, elle doit intégrer :

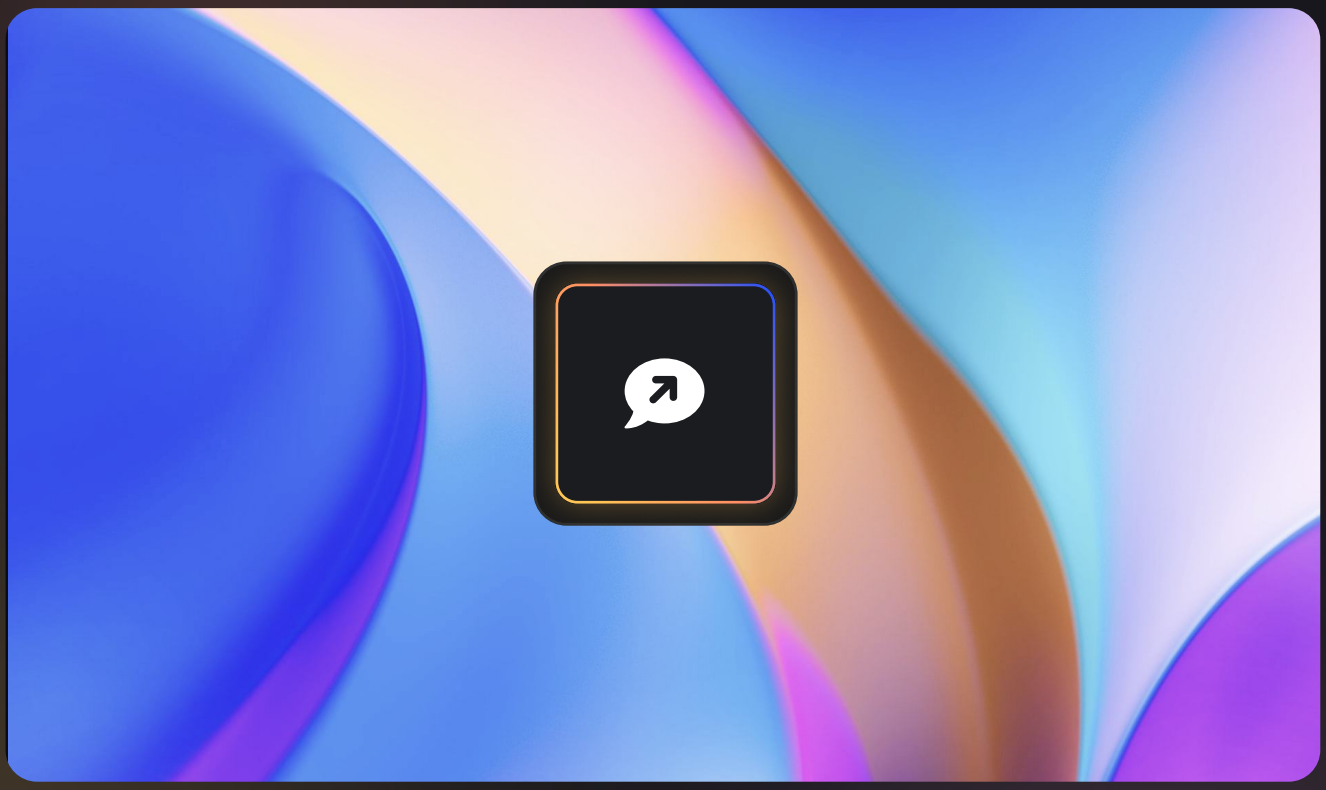
- la protection et le stockage de vos données
- la sécurisation de vos navigations web
- la récupération des données perdues
- la protection de la messagerie

L'impact d'une cyberattaque sur l'entreprise est considérable. Elle engendre des coûts financiers importants avec les pertes liées à l'attaque elle-même, les frais de réparation et de protection, et pénalise les capacités opérationnelles de l'entreprise. Il faut également tenir compte des impacts non quantifiables comme la dégradation de l'image de l'entreprise, l'augmentation du stress des collaborateurs… Selon son ampleur, une cyberattaque peut remettre en cause la compétitivité de l'entreprise et sa pérennité !

Pour anticiper cette cybermenace et contrer les multiples tentatives d'intrusion, mettez en place une gestion proactive de vos mots de passe et la sécurisation de votre système d'information avec l'offre Mailinblack de cybersécurité la plus complète, fiable et innovante du marché.

Protection de vos données et gestion de vos mots de passe avec une solution sur mesure et 100 % made in France. Contactez-nous !

Contactez-nous



contact@mailinblack.com
+33 (0)4 88 60 07 80
www.mailinblack.com
4 place Sadi Carnot, 13002 Marseille

MAILINBLACK