REDEFINIR LA Sécurité des Mots de Passe

Par Julia O' Toole
Fondatrice et PDG de MyCena Limited

À mesure que le monde se digitalise, notre dépendance aux mots de passe s'accroît. Il n'y a pas si longtemps, nous pouvions compter sur quatre ou cinq mots de passe. Aujourd'hui, la plupart des internautes en ont plus d'une centaine.

Un monde de plus en plus digitalisé signifie que le nombre de mots de passe utilisés dépassera les 300 milliards d'ici 2020.[1]

A mesure que le monde se digitalise, notre dépendance aux mots de passe s'accroit. Il n'y a pas si longtemps, nous pouvions compter sur quatre ou cinq mots de passe. Aujourd'hui, la plupart des internautes en ont plus d'une centaine. Et le problème ne fait que s'aggraver. Un rapport récent indique que l'utilisation des mots de passe augmente rapidement et devrait dépasser les 300 milliards d'ici 2020[1].

Ce livre blanc couvre le paysage actuel de la sécurité des mots de passe, de l'usage le plus répandu des mots de passe à la présentation d'une nouvelle façon de protéger vos mots de passe, sécurisée et décentralisée.

1. Cybersecurity Ventures The World Will Need to Protect 300 Billion Passwords by 2020 https://www.inc.com/joseph-steinberg/300-billion-thats-how-many-passwords-may-be-in-use-by-2020.html

Pourquoi les mots de passe existent

Les mots de passe sont les clés qui ouvrent les portes de notre monde numérique. Tout comme nos clés ouvrent les portes de notre espace physique, les mots de passe ouvrent les portes de notre espace numérique. Ils ont été conçus pour offrir un moyen simple de prouver notre identité lors de l'utilisation de sites web, messagerie et applications. Ils sont notre première ligne de défense contre les intrus.

Les mots de passe sont les clés qui ouvrent les portes de notre monde numérique

Pourquoi les mots de passe ne protègent plus nos portes

Mais les mots de passe ne font plus leur travail. En fait, un rapport d'investigation des brèches de données de Verizon montre que 81% des atteintes à la protection des données sont le résultat de mots de passe faibles, réutilisés ou volés[1].

Pourquoi nous utilisons toujours des mots de passe à haut risque

Notre dépendance accrue aux applications mobiles et web a entraîné une augmentation du nombre de nos mots de passe, qu'il s'agisse de simples comptes de messagerie ou de services bancaires en ligne.

Même si nous savons qu'il faut utiliser des mots de passe forts, nous ne pouvons tout simplement pas nous rappeler de centaines de combinaisons telles que 45@fag54hF8sD pour déverrouiller chacune de nos portes. Par conséquent, nous avons tendance à recourir à des combinaisons simples comme Nom1234 ou à réutiliser un seul mot de passe avec des variantes.

10% des gens ont utilisé au moins l'un des 25 pires mots de passe

Les dix pires mots de passe de 2018

La liste annuelle des pires mots de passe de l'année[2] de SplashData révèle que les internautes utilisent toujours les mêmes mots de passe prévisibles et facilement devinables, malgré le risque important d'être piraté et de voir leur identité volée. Près de 10% des gens ont utilisé au moins l'un des 25 pires mots de passe de la liste de cette année, et près de 3% ont utilisé le pire mot de passe, 123456.

1. 123456
2. password
3. 123456789
4. 12345678
5. 12345
6. 111111
7. 1234567
8. Sunshine
9. Qwerty
10. iloveyou

En outre, la majorité d'entre nous utilise des méthodes dangereuses pour stocker nos mots de passe[3]:

- 53% Mémoire humaine
- 32% Enregistrer dans le navigateur
- 26% Fichier électronique
- 26% Écrit sur papier
- 1% Autre


Avoir un mot de passe faible, c'est comme n'avoir aucun mot de passe du tout

1. Verizon Data Breach Investigations Report https://www.verizondigitalmedia.com/blog/2017/07/2017-verizon-data-breach-investigations-report/
2. SplashData's Top 100 Worst Passwords of 2018 https://www.teamsid.com/splashdatas-top-100-worst-passwords-of-2018/
3. Cyber Security Breaches Survey 2018 from the Department for Digital, Culture, Media and Sport https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/702074/Cyber_Security_Breaches_Survey_2018_-_Main_Report.pdf

Pourquoi les mots de passe représentent une énorme menace pour les entreprises

Comment opèrent les pirates

Vous devez savoir comment les pirates opèrent pour éviter d'être piraté

Pour comprendre pourquoi les mots de passe sont une telle menace pour la sécurité, il est important de comprendre comment les pirates fonctionnent.

- Hameçonnage ('phishing') - Les pirates peuvent se faire passer pour de véritables contacts, par exemple des banques, pour convaincre les utilisateurs de mettre leurs informations d'identification.
- Ingénierie sociale ('social engineering') - les pirates extraient des informations de votre profil et activités en ligne pour voler votre identité.
- Bourrage d'identifications ('credential stuffing') - les pirates utilisent généralement les noms d'utilisateur et mots de passe volés lors de brèches de données passées pour essayer d'ouvrir d'autres comptes à l'aide d'outils d'automatisation Web.
- Force brute - les pirates exécutent des scripts pour tester des combinaisons d'informations d'identification pour « deviner » votre mot de passe.

Une alternative appelée spidering consiste à étudier une entreprise pour en connaitre le langage. Généralement destinée aux grandes entreprises qui donnent beaucoup d'informations sur elles-mêmes en ligne, cette méthode est souvent utilisée pour accéder aux mots de passe Wi-Fi, de nombreux routeurs de bureau étant protégés par un mot de passe qui se rapporte à l'entreprise, tel que 'société1234'.

Plus de 90% des attaques sont gérées par des bots qui vont «bourrer» ou «saupoudrer» de nouvelles combinaisons, souvent à partir d'identifications précédemment divulguées et d'informations trouvées sur les médias sociaux. La plupart des mots de passe peuvent être trouvés dans les 24 heures à l'aide d'un outil de force brute qui peut être téléchargé gratuitement.

Les collections #2-5 représentent 845 gigaoctet ou 2,2 milliards d'identifications volées, comprenant noms d'utilisateur et mots de passe.

Pourquoi la transformation numérique augmente les vulnérabilités

Alors que plus de 60% des entreprises du Fortune 500 ont entrepris leur transformation numérique, leur permettant ainsi une meilleure collaboration, leurs réseaux connectés sont également devenus un rêve pour les hackers. La surface d'attaque des hackers est maintenant l'ensemble des employés et personnes connectées à l'entreprise. Qu'il s'agit de dirigeants ou d'employés juniors, toute personne connectée au système est vulnérable aux cyberattaques et présente un risque potentiel.

Dans le même temps, le besoin croissant de nouveaux comptes signifie que les gens sont plus susceptibles de réutiliser les mots de passe ou des variantes sur plusieurs comptes, augmentant ainsi leur risque d'être piraté. Certaines entreprises utilisant la commodité de l'authentification unique (Single Sign On ou SSO) sont encore plus vulnérables, les pirates pouvant infiltrer leurs réseaux d'informations et leurs bases de données à partir d'un seul point d'accès.

Il n'est donc pas surprenant que les vols d'identifications soient à la hausse. 2018 a été la pire année pour les atteintes à la cybersécurité. Elle a été suivie de deux des plus importantes fuites de noms d'utilisateur et de mots de passe de l'histoire, nommées Collection 1[1] et Collections #2-5[2] en janvier 2019. Il y a actuellement plus de 3 milliards d'identifiants et mots de passe en vente en ligne et ce chiffre ne cesse d'augmenter chaque jour.

Vos mots de passe sont vulnérables au bourrage d'identifications, au phishing, à l'ingénierie sociale

1. Forbes https://www.forbes.com/sites/kateoflahertyuk/2019/01/17/collection-1-breach-how-to-find-out-if-your-password-has-been-stolen/#3c2d829a2a2e
2. Wired https://www.wired.com/story/collection-leak-usernames-passwords-billions/

Pourquoi les nouvelles lois sur la protection des données affectent toutes les entreprises

Qu'il s'agisse de petites ou grandes entreprises, les entreprises dans toutes les industries ont besoin de mots de passe forts pour protéger leurs données et celles de leurs clients.

Avec l'entrée en vigueur de lois sur la confidentialité et la protection des données comme le RGPD dans le monde entier, les conséquences financières du non-respect de la protection des données des clients peuvent être dévastatrices, les entreprises étant désormais passibles d'amendes allant jusqu'à €20.000.000, ou 4% de leur chiffre d'affaires mondial total.

Les attaques de spidering consistent à étudier une entreprise et à récupérer leur 'langage'

Le risque d' être un "gros poisson"

L'industrie du piratage est composée d'un large éventail d'acteurs, des petits criminels aux États-nations. Alors que certains pirates brassent large, d'autres se concentrent sur des cibles plus stratégiques.

Des attaques visant les secteurs de la défense, de la police, du gouvernement, de l'énergie, de l'eau, des services publics, des infrastructures, de la technologie, des télécommunications, des universités, des banques, des services financiers, de la santé, des produits pharmaceutiques, des transports, de la logistique, du commerce de détail ou de la loi peuvent avoir des effets sans précédent sur toute la société.

En mai 2017, l'attaque ransomware WannaCry a entraîné l'annulation de 19 000 opérations médicales et rendez-vous au Royaume-Uni, coûtant 92 millions d'euros au National Health Service (NHS) en perturbations et remédiation[1]. Et en septembre 2019, la quasi-totalité de la population équatorienne a vu ses données personnelles divulguées[2].

La société Nortel, aujourd' hui défunte, a fait l' objet d' une attaque de plusieurs années qui est remontée à des pirates informatiques parrainés par l' État chinois.

Lorsqu'un « gros poisson » est touché, cela affecte aussi leurs fournisseurs, partenaires et clients. En mars 2019, une brèche de données chez Citrix a pu affecter les accès et identifications aux réseaux privés virtuels de 400.000 entreprises dans le monde, y compris 98% des organisations du Fortune 500[3].

À l'ère de la cyberguerre, il y a aussi des preuves accablantes que certaines attaques sont parrainées par des États. Des pays comme la Corée du Nord, l'Iran et la Chine sont connus pour mener des cyberattaques et des vols de propriété intellectuelle. Par exemple, l'entreprise de télécommunications canadienne Nortel, aujourd'hui défunte, a fait l'objet d'une attaque qui a duré des années, au cours de laquelle des pirates informatiques avaient volé des mots de passe de cadres supérieurs pour accéder à des courriels, recherches, business plans et secrets commerciaux. Les attaques ont ensuite été attribuées à des pirates informatiques directement parrainés par l'État chinois[4].

Les entreprises ne réalisent pas toujours qu'il y a eu violation

De nombreuses entreprises ne reconnaissent pas une faille de sécurité lorsqu'elle se produit, 93% des atteintes à la protection des données n'ayant pas été découvertes durant des semaines[5] .

Les brèches de sécurité peuvent passer inaperçues pendant des semaines

Pendant ce temps, une énorme quantité de dégâts peut être faite. Par exemple les pirates peuvent installer des logiciels malveillants sur l'ordinateur d'un employé et extraire des informations sensibles du réseau de l'entreprise avant même que l'entreprise réalise que sa sécurité a été violée.

1. Department of Health and Social Care https://www.hsj.co.uk/technology-and-innovation/cyber-attack-cost-nhs-92m-dhsc/7023560.article
2. The New York Times https://www.nytimes.com/2019/09/17/world/americas/ecuador-data-leak.html
3. Forbes https://www.forbes.com/sites/kateoflahertyuk/2019/03/10/citrix-data-breach-heres-what-to-do-next/#47a1e6b11476
4. The Register https://www.theregister.co.uk/2012/02/15/nortel_breach/
5. Verdict https://www.verdict.co.uk/password-security-surveillance-fears/

Votre entreprise prend-elle la cybersécurité au sérieux?

Les entreprises ont peut-être de bonnes intentions, mais cela ne se reflète pas toujours dans leurs pratiques. 74% des entreprises et 53% des charités affirment que la cybersécurité est une priorité pour leur direction. Malgré cela, nous voyons encore que:

- Seulement 27% des entreprises et 21% des charités ont une politique en matière de cybersécurité[1].
- Seulement 9% des entreprises et 4% des charités ont une police d'assurance cybersécurité en place.

Arbitrer entre prévention, surveillance et remédiation

Avec de plus en plus d'attaques qui ont lieu chaque jour, il ne s'agit plus de savoir si, mais quand votre entreprise sera ciblée. Il y a une pression croissante sur les DSSI de couvrir de plus en plus de risques avec des ressources limitées. Environ 99% des dépenses en cybersécurité des entreprises sont actuellement consacrées à la surveillance et à la remédiation. Cependant, même les meilleurs systèmes de surveillance ne protègent pas votre entreprise contre un vol de mot de passe.

Alors que 81% des risques de brèches sont liés aux mots de passe, la sécurité des mots de passe ne représentait en 2017 que 0,53% des dépenses totales en cybersécurité, un chiffre qui devrait augmenter à seulement 0,58% d'ici 2023[2]. Pour protéger leur personnel, leurs clients et des communautés entières contre les menaces à la sécurité, les entreprises doivent donner la priorité à la prévention et mieux organiser leur première ligne de défense.

Comment empêcher une violation de données par mots de passe

Une première étape consiste à mettre en place un système de gestion des identités et des accès (Identity and Access Management IAM) qui permet aux gestionnaires d'attribuer différents niveaux d'accès à différents utilisateurs au sein d'une organisation. Mais ce n'est souvent pas la première considération des petites et moyennes entreprises, en particulier si elles n'ont pas de DSSI.

Une deuxième étape consiste à mettre en place un système de gestion de mots de passe à la fois pratique et sécurisé, et cela pour empêcher les gens d'utiliser des mots de passe faibles ou de les réutiliser. Beaucoup d'entreprises échouent dans ce domaine parce qu'elles n'ont pas réussi à implémenter un système de gestion de mot de passe effectif, augmentant de par ce fait les risque de brèches.

Dans son rapport, SplashData offre aux entreprises les conseils suivants pour se protéger contre les pirates en ligne:

- Utilisez des phrases de douze caractères ou plus avec des types de caractères mixtes.
- Utilisez un mot de passe différent pour chacun de vos identifiants, donc si un pirate accède à l'un de vos mots de passe, il ne pourra pas l'utiliser pour accéder à d'autres sites.
- Protégez vos informations et votre identité personnelle en utilisant un gestionnaire de mots de passe cloud pour organiser vos mots de passe, générer des mots de passe aléatoires sécurisés et vous connecter automatiquement à différents sites et applications.

1. Cyber Security Breaches Survey 2018 from the Department for Digital, Culture, Media and Sport https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/702074/Cyber_Security_Breaches_Survey_2018_-_Main_Report.pdf
2. Stratistics MRC https://www.strategymrc.com/report/password-management-market-2017 https://www.strategymrc.com/report/cyber-security-market https://www.strategymrc.com/report/cyber-security-market-2016; MyCena estimates

Comprendre les risques associés aux gestionnaires de mots de passe cloud

Offrant une méthode centralisée de stockage des mots de passe, les gestionnaires de mots de passe cloud sont devenus de plus en plus populaires ces dernières années. Cela s'explique en grande partie par le fait que:

- Ils vous aident à générer des mots de passe forts - vous n'avez qu'à vous souvenir d'un seul mot de passe principal. Vous tapez votre mot de passe principal et accédez à tous vos autres mots de passe stockés dans le cloud.
- Ils offrent une alternative beaucoup plus sûre à l'utilisation de post-its ou de mots de passe faibles tels que '123456'.

Bien que les gestionnaires de mots de passe cloud puissent être pratiques, ils présentent trois risques majeurs, émanant de leur architecture:

- Tout d'abord, par construction, tous vos mots de passe sont centralisés et accessibles à partir d'un mot de passe maître, qui devient ainsi un point unique de vulnérabilité. Imaginez si ce mot de passe principal est compromis d'une manière ou d'une autre, vous exposez tous vos mots de passe à la fois. Vous pouvez penser à votre mot de passe maître comme à la clé d'un directeur d'hôtel. Un pirate n'a besoin que de cette clé pour accéder à toutes les chambres. Pour de nombreuses entreprises, c'est un risque trop gros à prendre.
- Deuxièmement, tous vos mots de passe sont sur le cloud, centralisés, dans le même panier de mots de passe que des millions d'autres utilisateurs. Ce serveur devient un gigantesque aimant pour les pirates, qui attirés par cette 'mine d'or', entreprendront d'entrer par effraction.
- Troisièmement, les serveurs sont fréquemment victimes de brèches de sécurité, que ce soit par le biais de mots de passe ou d'autres biais. Et vous n'avez aucun visibilité sur ces serveurs. Laisseriez-vous les clés de votre maison à quelqu'un que vous ne connaissez pas? Sans doute que non. Et pourtant laisser vos mots de passe dans le cloud revient exactement au même.

Un gestionnaire de mot de passe basé sur le cloud est pratique mais risqué

Votre mot de passe maître est la clé du royaume

Redéfinir les règles de sécurité des mots de passe

Si un problème bien posé est à moitié résolu[1], il nous faut pour trouver une solution, décomposer le problème du début et redéfinir les règles qui permettent aux mots de passe de remplir leur mission de sécurité. Nous avons pour cela trouvé trois règles-clés :

- Les mots de passe sont comme vos clés. Si comme vous n'avez pas besoin de vous rappeler comment couper vos clés chaque fois que vous voulez ouvrir une porte, vous ne devriez pas non plus avoir besoin de vous rappeler vos mots de passe pour ouvrir vos portes numériques.
- Les mots de passe doivent être privés par nature et seulement accessibles par leur propriétaire et personne d'autre.
- Les mots de passe ne doivent pas être vulnérables à un seul point d'accès.

Redéfinir les règles de sécurité des mots de passe

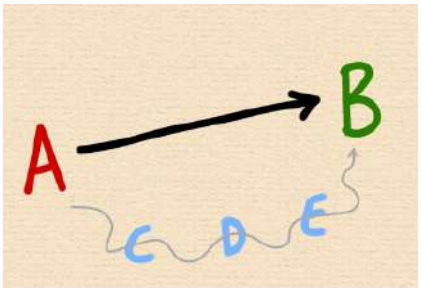
1. Charles F. Kettering, inventeur américain

Leçons de neuroscience : comprendre la commodité

Pour parvenir à faire adopter une nouvelle technologie, il est essentiel qu'elle soit pratique. Cette règle s'applique d'autant plus à la sécurité. S'ils mettent trop de temps à ouvrir une porte plusieurs fois par jour, la plupart des gens cesseront de verrouiller la porte correctement. Par conséquent, la sécurité ne peut être garantie que si les systèmes et les procédures qui la gouvernent restent simples, pratiques et rapides.

Au cours des vingt dernières années, la neuroscience nous a beaucoup appris sur le fonctionnement de notre cerveau. Une conclusion-clé est que notre cerveau a tendance à revenir à la voie la plus facile pour aller de A à B. Voici quelques exemples:

- Quand il s'agit de trouver un objet, il est beaucoup plus facile pour le cerveau de se rappeler un endroit typique où vous mettez habituellement cet objet plutôt que de se rappeler précisément où l'objet est.
- Il est plus facile pour le cerveau de suivre des schémas connus ou reconnaissables que d'en créer de nouveaux. Cela explique pourquoi le cerveau n'est pas bon pour créer de nouveaux mots de passe aléatoires.
- Notre cerveau est visuel et a tendance à faire correspondre ce qu'il recherche avec des objets et des modèles déjà vus.



Le cerveau a tendance à revenir à la voie la plus facile

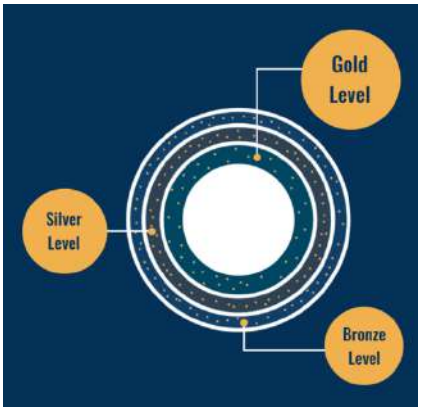
Restaurer la fonction des mots de passe

Après avoir défini le problème, encore faut-il le résoudre.

Méthode d'Accès aux Données Structurées Stockées (MASS Data) - en instance de brevet international

MASS data est une solution révolutionnaire qui permet de délocaliser et décentraliser les mots de passe, distribuant et réduisant le risque de tous les perdre à la fois. Il permet la création de plusieurs niveaux de sécurité pour stocker les mots de passe en fonction de leur sensibilité, avec une authentification locale à plusieurs niveaux, et un contrôle complet des mots de passe et des paramètres de sécurité par l'utilisateur.

- Pas de stockage dans le cloud.
- Pas de mot de passe maître.
- Pas de point de vulnérabilité unique.



MASS Data: clé de voûte de l'architecture multi-couches qui protège vos mots de passe à l'intérieur de votre appareil

La facilité d'usage comme prérequis à la sécurité

Dans un monde connecté, la cybersécurité est une responsabilité partagée. Pour être largement adoptée, la solution doit être rapide, pratique et facile à utiliser.

- Permettre au propriétaire des mots de passe de prouver leur identité facilement et en toute sécurité afin d'accéder à chaque niveau de mots de passe à tout moment avec une combinaison d'empreinte digitale, de reconnaissance faciale, de PIN, de chemin de verrouillage et de phrase secrète vocale.
- Générer des mots de passe forts par défaut.
- Autoriser la recherche, le copier/coller des mots de passe sans avoir à taper ou voir un mot de passe donné.

Créez, enregistrez, recherchez, trouvez, copiez et collez des mots de passe en quelques secondes

Construire une solution de grade entreprise

Pour s'adapter aux besoins des entreprises, la solution doit être facilement déployée et utilisée. Elle se décompose en deux parties:

- Une console à travers laquelle un gestionnaire peut rapidement enrôler tous les employés, renforcer et surveiller les stratégies de mot de passe telles que la configuration de la longueur du mot de passe, la fréquence de changements de mot de passe et les alertes de mot de passe faibles.
- Une application mobile que les employés utilisent pour accéder à leurs mots de passe rapidement et en toute sécurité, qui comprend de riches fonctionnalités : multi-appareils, multi-plateformes, intégration au bureau, mode voyage, synchronisation, migration, rappels automatisés de sauvegarde et partage sécurisé de mots de passe.

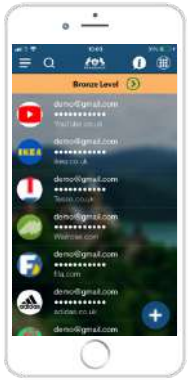
La console permet au manager de renforcer les politiques de mot de passe et d'en surveiller le respect

Respecter la confidentialité par défaut

Après de nombreuses années d'érosion de la vie privée, les législateurs ont commencé à renforcer les lois sur la protection des données et la confidentialité afin de protéger la société et les libertés individuelles. Nous soutenons pleinement ces avancées. De fait notre solution respecte la protection des données et la confidentialité par défaut.

Les mots de passe sont cryptés à l'intérieur de votre appareil à l'aide du cryptage AES-SHA 256. Cela signifie que même si vous avez perdu votre appareil, un voleur ne serait pas en mesure d'accéder à vos mots de passe. La seule personne qui peut accéder ou télécharger vos mots de passe cryptés est vous.

Vos données biométriques, comme vos empreintes digitales et reconnaissance faciale sont encore plus sensibles. Vous pouvez changer vos mots de passe, mais vous ne pouvez pas changer votre visage ou votre doigt. Toutes vos authentifications personnelles sont donc conservées à l'intérieur de votre appareil. Aucune centrale de données biométriques n'est ainsi créée.



Confidentialité par défaut : Ne plus jamais voir ou taper un mot de passe

Limiter les dommages causés par l' hameçonnage

De surcroit, vous n'avez même plus besoin de connaitre de mots de passe. De leur création à leur utilisation, vous n'avez plus ni à voir ni de taper de mots de passe. Grâce au «copier-coller», plus de faute de frappe ni d'occasion de vous voler vos mots de passe dans votre dos ou derrière votre écran.

Et si un pirate parvient à vous faire entrer un mot de passe sur un faux site, ce mot de passe ne peut pas être réutilisé pour entrer dans vos autres comptes, puisque chacun de vos mots de passe est unique et fort. Un seul acte d'effraction n'exposera donc pas ainsi l'ensemble de votre réseau informatique.

La première ligne de défense de l'entreprise

Une fois la solution déployée au sein de l'organisation, elle devient de facto sa première ligne de défense. Pour entrer dans une application ou un réseau protégé au sein d'une entreprise, vos employés devront d'abord prouver leur identité à leur propre appareil et récupérer leur mot de passe. Ce mot de passe fort et unique prouve que l'employé est le détenteur de la clé unique qui permet d'accéder à cette application ou à ce réseau.

La solution devient la première ligne de défense de l'entreprise

Découvrez les solutions décentralisées de sécurité de mots de passe MyCena

Découvrez MyCena

MyCena Business Fortress est une solution révolutionnaire de sécurité de mot de passe de grade entreprise qui est décentralisée, facile à implémenter, pratique et sécurisée. Découvrez comment installer et configurer MyCena facilement pour votre entreprise.

MyCena Personal Fortress est une solution révolutionnaire de sécurité de mots de passe personnels que les utilisateurs individuels peuvent télécharger sur leur appareil mobile. Découvrez comment protéger vos mots de passe à l'aide de MyCena Personal Fortress.

MyCena as a Service

MyCena as a Service (MaaS) est un ensemble complet de services offrant le meilleur de la solution avec un soutien avancé, réduisant l'effort de mise en œuvre et de gestion de la solution au sein de la société et auprès de ses employés.

Points-clés à retenir

La cybersécurité est la première menace pour les organisations. Le nombre d'atteintes à la sécurité des données augmente de jour en jour, chacune apportant son contingent d'amendes, de procès et de coûts de remédiation, tout en effritant irrémédiablement la réputation des entreprises et la confiance des clients.

Pour protéger leur entreprise, les conseils d'administration et les dirigeants doivent comprendre d'où viennent les menaces et prendre des mesures décisives. Sachant que 81 % des violations de données commencent à partir des mots de passe, la sécurisation des mot de passe est plus seulement une option mais une obligation.

Les DSSI des entreprises peuvent atténuer les risques en aidant leurs employés à utiliser des mots de passe uniques et forts comme première ligne de défense et en décentralisant le stockage des mots de passe avec MyCena Business Fortress. Les DSI peuvent également atténuer les risques d'atteintes aux données en profitant de MyCena en tant que service.

Pour les demandes de renseignements, contactez
support@MyCena.co

Visitez notre site web pour plus d' informations
https://MyCena.co/business
Essai gratuit disponible

Téléchargez les applications à partir de l'App Store ou Google Play.