Pourquoi votre système de sécurité n'est pas infaillible ? Les risques décryptés et les solutions pratiques !

Juin 2021

Alors que le **télétravail** est de plus en plus présent et le nombre de **cyberattaques** en forte hausse, sécuriser l'identité des employés n'est plus une priorité mais une urgence absolue. Et pour cause, selon le *Rapport d'enquête 2020 sur les compromissions de données* de Verizon, 80 % des **fuites de données** liées à du **piratage** impliquent encore des identifiants faibles et compromis.

Pour une adoption et une **protection optimales,** les entreprises doivent opter pour un outil facile à utiliser pour l'ensemble des collaborateurs et à gérer pour les **équipes IT**, pertinent pour tous les profils, aussi bien nomades, qu'en télétravail ou en présentiel, et qui offre un retour sur investissement avéré. En effet, si les campagnes malveillantes gagnent en sophistication, la défense en face doit s'armer en conséquence.

Quels sont les enjeux de la **sécurité informatique** pour les entreprises en 2021 ? Quels sont les risques liés aux mots de passe, et surtout, comment les surmonter ?

Réponses dans ce livre blanc.

Sommaire

État des lieux de la sécurité des données en entreprise 1

- Les risques du phishing
- Le travail à distance, canaliseur de risques numériques
- La prise de conscience nécessaire des entreprises

Les enjeux liés aux mots de passe et leurs risques..... 4

- Multiplication des services en ligne = multiplication des mots de passe ?
- Le coût des mots de passe
- Des mots de passe faibles : la porte vers la violation de données
- Les identifiants volés disponibles à la vente

Les solutions à disposition pour plus de sécurité et leurs avantages 9

- Expérience utilisateur améliorée et sécurité renforcée, c'est possible
- La norme d'authentification FIDO2, l'avenir de la sécurité de vos comptes
- Avant toute chose, établir une stratégie de déploiement claire

Libérez-vous des mots de passe pour plus de sécurité ! Qu'est-ce que le passwordless?..... 18

État des lieux de la sécurité des données en entreprise

Les risques du phishing

Le **phishing** est la principale cause des **brèches de sécurité** et a le meilleur taux de réussite de tous les vecteurs de menaces. **L'identité** est la surface d'attaque privilégiée des cybercriminels, du fait d'une **sécurisation peu optimale**, parfois, dans certaines entreprises.

En 2020, de nombreuses organisations ont été contraintes d'adopter en quelques jours le **télétravail** du fait de la crise sanitaire. Elles ont alors tant bien que mal **fait évoluer leur stratégie de sécurité** pour inclure leurs employés désormais distants. Mais, bien souvent, ces **solutions d'urgence** n'ont pas été modifiées depuis et comportent toujours des **failles**. En parallèle, compte tenu de la **sophistication croissante des cyberattaques**, les solutions traditionnelles d'authentification ne sont plus suffisantes.

Le phishing continue d'être un énorme problème de sécurité au fur et à mesure que les **techniques d'attaques continuent à évoluer**. De **faux messages électroniques** incitant les utilisateurs à saisir à nouveau leurs informations d'identification peuvent être utilisés pour les récolter et les utiliser pour les **piratages de comptes**.

Environ **30 % des e-mails de phishing sont ouverts par leurs destinataires** et plus de 7 % des destinataires d'e-mails ont été persuadés d'ouvrir une pièce jointe ou de cliquer sur un lien, qui est souvent un lien de connexion. (*Source : Rapport d'enquête 2020 sur les compromissions de données de Verizon*)

La plupart des attaques de phishing conduisent ensuite à **l'installation de logiciels malveillants** qui aident à créer une brèche. Même si les utilisateurs définissent des mots de passe complexes, les pirates peuvent y accéder par le biais du phishing et détourner **les comptes des utilisateurs**.

Protection des utilisateurs

57 % des professionnels de l'IT ont déclaré que leur entreprise a subi une **attaque par phishing, 17 %** un vol d'identifiants, et **8 %** une attaque de type MITM (**homme du milieu**).

État des lieux de la sécurité des données en entreprise

Le travail à distance, canaliseur de risques numériques

Alors que les entreprises d'aujourd'hui sont en route vers la **transformation numérique,** le **télétravail** augmente. Grâce aux progrès technologiques, les employés peuvent travailler depuis n'importe où, ce qui crée aussi de **nouveaux défis de sécurité pour les services informatiques**.

Les **réseaux WiFi** non sécurisés, les **appareils mobiles personnels** non managés et les arnaques par **hameçonnage** rendent à la fois facile de voler les identifiants/mots de passe des utilisateurs et difficile de gérer en toute sécurité des équipes qui sont géographiquement éparses.

.

Si le concept de télétravail n'est pas nouveau, il est de plus en plus présent dans les entreprises modernes. Les événements internationaux récents n'ont fait qu'accroître ces chiffres, obligeant les organisations à mettre en place **des procédures et des systèmes qui sécurisent les employés** en télétravail sans affecter leur productivité.

On peut déjà constater que des pirates profitent de l'**incertitude** qui entoure les entreprises en lançant des **attaques par hameçonnage ciblées**, ce qui conduit ces dernières à développer des **plans de secours** pour protéger les collaborateurs qui sont en télétravail. Les entreprises doivent se demander : « Les employés peuvent-ils accéder aux systèmes à distance sans créer de nouveaux risques et de nouvelles faiblesses ? »

État des lieux de la sécurité des données en entreprise

La prise de conscience nécessaire des entreprises

La **prise de conscience des cyber-risques** liés à l'identité croît actuellement au sein des organisations, notamment par l'observation des campagnes de cyberattaques visant des concurrents et de leurs impacts, directs, mais aussi indirects,tels que :

- ➔ baisse ou interruption d'activité,
- ➔ réputation ternie,
- ➔ chute du cours de l'action en Bourse, etc.

C'est pourquoi la volonté de **renforcer et moderniser la sécurité** des accès provient désormais régulièrement du comité exécutif. Les **résultats attendus** sont multiples, mais visent tous à faire face aux cybermenaces actuelles :

- ➔ renforcement de la sécurité, et en particulier blocage des impacts du phishing ;
- ➔ déploiement d'une solution unique à toutes les équipes, les couches de sécurité ayant eu tendance à se multiplier et à différer d'un employé à l'autre au fur et à mesure des années ;
- ➔ expérience utilisateur simplifiée, afin de garantir une adoption de tous,
- ➔ rationalisation des budgets en optimisant les coûts d'acquisition, et en réduisants fortement les coûts de support ;
- ➔ et, enfin, une conformité avec les législations en vigueur, dont RGPD.

Il est cependant difficile d'y voir clair pour les entreprises tant la multitude d'outils et de types de couches de sécurité disponibles actuellement sur le marché troublent la vision

Pour cette raison, elles doivent **définir leurs besoins** précisément :

- ➔ le rapport sécurité/risque,
- ➔ l'accompagnement technique dans toutes les régions où les organisations sont présentes,
- ➔ les différents profils d'utilisateurs en fonction du niveau de sécurité attendu et du contexte d'usage.

💡 Les employés peuvent alterner présence physique au bureau, nomadisme et télétravail au cours de leur carrière, et l'outil choisi doit se montrer **compatible avec toutes les situations possibles**.

Les enjeux liés aux mots de passe et leurs risques

Multiplication des services en ligne = multiplication des mots de passe ?

Les entreprises cherchent aujourd'hui des moyens de **tirer parti de la technologie du cloud et du mobile** afin de fournir des produits et services améliorés plus rapidement et plus efficacement. Cependant, celles qui poursuivent des plans ambitieux de rationalisation du parcours des clients et employés se trouvent rapidement confrontées à des **défis de sécurité.**

Les technologies et les **contrôles de sécurité** sont mis en place pour **protéger l'entreprise.** Cependant, ces mêmes contrôles de sécurité peuvent **frustrer les utilisateurs**.

Les **mots de passe** sont une réalité depuis les années 1960, tant pour les utilisateurs professionnels que pour les consommateurs. Presque toutes les expériences numériques en ont besoin, des **réseaux sociaux** comme Facebook, aux **banques** et **détaillants** comme H&M et Zara, en passant par les applications commerciales comme Salesforce et QuickBooks Online

💡 *Les mots de passe figurent en haut de la liste des contrôles de sécurité pénibles et irritants..*

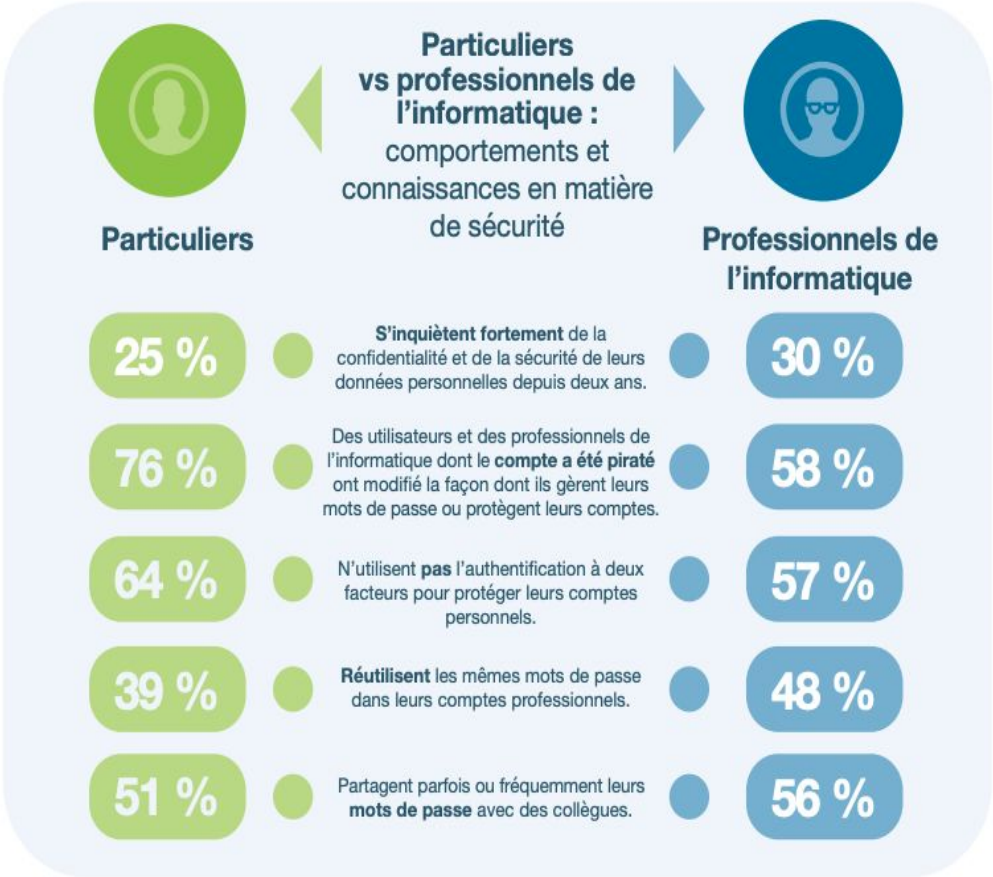
Les enjeux liés aux mots de passe et leurs risques

Multiplication des services en ligne = multiplication des mots de passe ?

👉 **À savoir :**

Le consommateur américain moyen essaie de se rappeler de **plus de 70 mots de passe différents**, qu'il utilise sur tous ses sites Web et services, tandis que les utilisateurs **professionnels** seraient responsables de la mémorisation et de l'utilisation d'un nombre encore plus important de mots de passe, **jusqu'à 191** !

Avec la génération du millénaire qui compose une part croissante de la population active, les résultats d'une étude IBM montrent qu'ils font preuve de **moins de patience avec la mémorisation** de tous ces secrets. Ils sont plus susceptibles de réutiliser les mots de passe, n'en mémorisant pas plus de huit, compromettant la sécurité au nom de la commodité. *(Source : article Millennial Habits May Bring an End to the Password Era, de Limor Kessem, dans SC Magazine)*



Source : Étude Ponemon 2020 sur les comportements liés à la sécurité des mots de passe et à l'authentification

Les enjeux liés aux mots de passe et leurs risques

Le coût des mots de passe

Lorsque les utilisateurs **oublient leurs mots de passe,** ils finissent souvent par appeler les services ou les centres d'assistance, ce qui leur fait **perdre un temps précieux.**

Les demandes de réinitialisation de mot de passe représentent jusqu'à 6 % des activités des centres d'appels, ce qui coûte aux grandes entreprises entre 5 et 20 millions de dollars par an ! *(Selon la même étude d'IBM parue dans SC Magazine)*

Les identifiants et mots de passe sont lourds à gérer et font augmenter les coûts. En effet, Forrester estime que chaque appel au service d'assistance pour réinitialiser un mot de passe coûte environ 35 dollars à une entreprise.

👉 Ce calcul a été fait sur une année de travail de 2 088 heures, un salaire annuel de 85 000 dollars pour un employé du service d'assistance, et 12 minutes passées par appel à résoudre le cas.*

** Oct 7 2019 Forrester Report: Making the business case for identity and access management*

👉 **Exemple :**

Pour économiser du temps et de l'argent, l'équipe informatique de Microsoft est passée à **l'authentification sans mot de passe**.

Conséquences :

- ➔ aujourd'hui, 90 % des employés de Microsoft se connectent sans entrer de mot de passe ;
- ➔ les **coûts** matériels et immatériels liés à la prise en charge des mots de passe ont **diminué de 87 %**.

À mesure que les entreprises continuent d'ajouter de nouvelles applications commerciales à leur portefeuille, le coût des mots de passe ne fait qu'augmenter.

💡 *En fait, les entreprises consacrent 30 à 60 % de leurs appels au service d'assistance à la réinitialisation des mots de passe. Et ce n'est pas là la seule limite des mots de passe.*

Les enjeux liés aux mots de passe et leurs risques

Des mots de passe faibles : la porte vers la violation de données

C'est un fait : les utilisateurs sont fatigués de créer de nouveaux mots de passe pour différents services et de devoir changer de mot de passe tous les quelques mois en fonction des exigences des politiques de sécurité.

👉 Pour réduire la mémorisation, de nombreux utilisateurs finissent par se fier à des **mots de passe simplistes** qui sont malheureusement **faciles à craquer** ou par les **réutiliser sur plusieurs sites**, où la violation d'un service peut ouvrir la porte à plusieurs autres.

Selon le rapport d'enquête sur les atteintes à la protection des données de Verizon (DBIR) de 2019, **80 % des piratages sont encore liés à des identifiants compromis et faibles**. Il est incroyable de constater qu'après des années de piratage de données très médiatisés, la plupart impliquent un **mot de passe faible**.

👉 **À savoir** :

L'analyse des failles de sécurité de la NCSC 2019 UK Cyber Survey a révélé que 23,2 millions de comptes de victimes dans le monde entier utilisaient **123456** comme mot de passe.

Les enjeux liés aux mots de passe et leurs risques

Les identifiants volés disponibles à la vente

Lorsque des pirates informatiques sont parvenus à s'introduire dans une organisation et à **voler des identifiants**, ils accèdent non seulement aux comptes de cette organisation, mais aussi aux **comptes d'autres organisations** où les consommateurs ont utilisé la même paire nom d'utilisateur-mot de passe.

👉 Par exemple, lorsque les pirates ont volé **1 milliard d'identifiants de connexion de Yahoo**! en 2016, ils ont obtenu **l'accès à tous les autres comptes accessibles** avec les mêmes paires adresse e-mail + mot de passe. Des milliards d'identifiants volés sont disponibles à la vente sur le Dark Web et les cybercriminels lancent maintenant des **tentatives de connexion automatisées** avec ce trésor de mots de passe volés.

Aujourd'hui, neuf tentatives de connexion sur dix sur des sites populaires de vente au détail et de banque sont en fait des **attaques de robots.** Tant que l'informatique de l'entreprise doit s'appuyer sur des mots de passe pour l'authentification, des besoins d'assistance coûteux, une sécurité faible et des expériences clients frustrantes sont inévitables.

💡 *Les mots de passe oubliés et volés dégradent l'expérience des clients, réduisent la fidélité à la marque et contribuent à la perte de revenus.*

Les solutions à disposition pour plus de sécurité et leurs avantages

Expérience utilisateur améliorée et sécurité renforcée, c'est possible

Les solutions à disposition pour plus de sécurité : avantages et inconvénients

Finalement, sur le sujet de **l'authentification**, peu de solutions sont apparues depuis la naissance du login mot de passe, datant des années 1960.

Dans les années 80 apparaît la **solution carte à puce** (Smart Card), avec comme avantage un très bon niveau de sécurité, mais comme contrainte une complexité de déploiement et des coûts importants associés. Cette solution ne s'est finalement assez peu démocratisée, si ce n'est pour certains grands comptes, qui aujourd'hui se tournent vers d'autres solutions.

En effet, la carte à puce n'est **pas adaptée aux nouveaux usages**, tels que la mobilité, l'accès aux données de l'entreprise sur des smartphones ou le télétravail.

Enfin, de moins en moins de postes de travail embarquent nativement ces lecteurs de carte à puce, ce qui oblige ces organisations à revoir totalement leur stratégie pour adapter l'authentification aux postes de travail et aux enjeux actuels.

Depuis les années 90, apparaît la possibilité de **s'authentifier avec son smartphone**, à travers un **One Time Password (OTP)**, ou code à usage unique, l'intérêt étant que tout salarié équipé d'un smartphone d'entreprise puisse l'utiliser. Cependant, la contrainte réside dans le manque de sécurité, et l'obligation de fournir des mobiles à tous les salariés, si l'organisation veut déployer cette méthode de MFA massivement.

Les solutions à disposition pour plus de sécurité et leurs avantages

Expérience utilisateur améliorée et sécurité renforcée, c'est possible

Pour combler le manque de sécurité, les éditeurs ont apporté une évolution à cette authentification, à travers le **push d'application**. Toutefois, cette méthode est aujourd'hui interceptable, notamment à travers le sim swapping et des outils comme Evilginx.

De manière plus générale, toutes les solutions d'authentification basées sur des protocoles fonctionnant avec des secrets partagés (OTP mais également Push Notification) restent **interceptables par un attaquant**. Il est préférable d'opter pour des outils dotés de **standards modernes ouverts, tels que WebAuthn et FIDO2**. Ces normes font appel au chiffrement et ont fait leurs preuves dans l'élimination de contrôle de comptes.

🕰️ **20 ans plus tard :**

L'évolution des usages, des compétences des hackers, les contraintes de certaines solutions historiques, ou leurs failles de sécurité, ont conduit le marché, paradoxalement, à revenir vers des solutions matérielles, comme les clés de sécurité physiques.

Les solutions à disposition pour plus de sécurité et leurs avantages

Expérience utilisateur améliorée et sécurité renforcée, c'est possible

Ne pas oublier l'expérience utilisateur

Il est possible aujourd'hui avec les **clés de sécurité** de trouver un **compromis alliant le maximum de sécurité, tout en simplifiant l'expérience utilisateur**, ce qui est primordial pour obtenir l'adhésion des utilisateurs.

Facilitant l'adoption au sein des organisations, elles deviennent progressivement l'outil le plus adapté pour répondre à l'évolution des risques de cybersécurité et des usages.

La YubiKey par exemple se distingue, pour plusieurs raisons :

- ➔ Elle embarque le meilleur de la sécurité, avec un élément sécurisé certifié EAL6+, Critères Communs, permettant le meilleur niveau de sécurité par rapport aux risques du phishing *(Google report: Security Keys: Practical Cryptographic Second Factors for the Modern Web)*
- ➔ La clé embarque nativement la plupart des protocoles standards du marché (carte à puce, FIDO2, FIDO U2F, OTP, TOTP, PGP) permettant la compatibilité avec tous les OS, périphériques, et la plupart des applications du marché
- ➔ La clé permet une expérience utilisateur simplifiée, jusqu'au passwordless. L'ajout d'un facteur physique permet de ne plus avoir à changer le secret régulièrement (code pin, mot de passe), et l'authentification est beaucoup plus rapide qu'avec un téléphone mobile (source)

Les solutions à disposition pour plus de sécurité et leurs avantages

Expérience utilisateur améliorée et sécurité renforcée, c'est possible

Ne pas oublier l'expérience utilisateur

La YubiKey permet de répondre, avec un **fort niveau de sécurité**, à l'hétérogénéité des périphériques, fixes ou mobiles, et des cas d'usages, comme par exemple :

- ➔ Renforcer la sécurité sur des solutions d'accès privilégiés, en général pour les administrateurs IT
- ➔ Sécuriser les solutions d'accès distants, pour tous les employés accédant au système d'information depuis l'extérieur
- ➔ Sécuriser l'accès à la plupart des solutions cloud, pour protéger l'accès à la donnée de l'entreprise, externalisée dans des clouds privés ou publics,
- ➔ Sécuriser l'ouverture de sessions pour tous les OS, pour protéger la donnée contenue dans les postes de travail
- ➔ Répondre aux enjeux des postes partagés, en simplifiant la tâche pour l'IT, et en évitant l'utilisation d'un mot de passe commun pour plusieurs utilisateurs, ou le fameux post it collé sur le poste de travail
- ➔ Permettre de renforcer la sécurité pour les utilisateurs BYOD, dépourvus de mobiles
- ➔ Servir de solution de backup en cas d'oubli ou de perte du mobile, lorsqu'il n'y a pas de réseau ou plus de batteries, pour ceux qui s'authentifient avec un mobile, et apporter plus de stabilité

Les solutions à disposition pour plus de sécurité et leurs avantages

La norme d'authentification FIDO2, l'avenir de la sécurité de vos comptes

La **norme d'authentification FIDO2** co-écrite par Microsoft et Yubico en 2018, et ratifiée en mars 2019 par le, World Wide Web Consortium (W3C), répond à **de multiples scénarios et expériences d'utilisation**

FIDO2 comprend deux composants standardisés :

- ➔ une API Web (WebAuthn),
- ➔ et un protocole CTAP (Client to Authenticator Protocol, Protocole client à authentificateur). .

Les deux travaillent ensemble et sont nécessaires pour obtenir une **expérience de connexion sans mot de passe**.

- ➔ **WebAuthn** définit une API Web standard qui peut être intégrée dans les navigateurs et l'infrastructure de la plateforme Web pour donner aux utilisateurs de nouvelles méthodes d'authentification sécurisée sur le Web.
- ➔ **CTAP** permet à un authentificateur externe, comme une clé de sécurité, de communiquer localement des informations d'authentification fortes par USB, NFC ou Bluetooth au PC ou au téléphone portable de l'utilisateur.

Les solutions à disposition pour plus de sécurité et leurs avantages

La norme d'authentification FIDO2, l'avenir de la sécurité de vos comptes

FIDO2 s'appuie sur une paire asymétrique (public/privé) de clés cryptographiques pour authentifier les utilisateurs. La clé publique est stockée sur tout service ou périphérique informatique prenant en charge l'authentification FIDO2, tandis que la clé privée est conservée par l'utilisateur et est protégée par une clé de sécurité physique, telle que la série de clés YubiKey 5 et la Security Key par Yubico.

💡 ***L'authentification est rapide et facile*** : *il suffit d'insérer ou de toucher la clé de sécurité pour que le défi d'authentification soit terminé, et la* ***connexion est immédiate***.

Avec FIDO2, la clé de sécurité peut être utilisée **seule ou en conjonction avec un code PIN** ou un geste pour fournir une authentification forte sans mot de passe. En outre, le mode d'authentification à deux facteurs avec un mot de passe continue d' être pris en charge.

Facteur unique (sans mot de passe)
Utilisation de la clé de sécurité en tant que premier facteur d'authentification forte, ne nécessitant que la possession du périphérique et permettant une expérience tap-and-go sans mot de passe

Deux facteurs (Mot de passe + Authentificateur)
Utilisation de la clé de sécurité comme second facteur dans une solution d'authentification à deux facteurs

Authentification multi-facteurs (sans mot de passe + code PIN ou biométrique)
Utilisation de la clé de sécurité pour l'authentification multi-facteurs nécessitant la possession du périphérique ET d'un code PIN ou biométrique, afin de répondre à des exigences élevées en matière de protection

Les solutions à disposition pour plus de sécurité et leurs avantages

Avant toute chose, établir une stratégie de déploiement claire

Pour assurer la **sécurisation optimale de vos données** avec le passwordless, il est indispensable d'établir une stratégie claire et définie.

👉 Une fois la clé de sécurité physique choisie en fonction des besoins, il est temps d'élaborer la **stratégie de déploiement :**

1. En amont de toute action, il est conseillé de faire une communication auprès de tous pour partager les objectifs du projet, ainsi que sa valeur pour l'entreprise, comme pour les utilisateurs.
2. Puis, la phase pilote peut débuter. Son but est de capitaliser sur les retours d'expérience.
3. Par la suite, on entame un déploiement massif souvent plus rapide et réussi sur la base de ces retours d'expérience.

Pour ce faire, deux types d'utilisateurs doivent être visés : des **profils IT** mais aussi des **employés non techniques**. Le premier groupe soutiendra d'autant plus le projet de déploiement s'il est conquis, et le second témoignera à leurs collègues de la simplicité d'utilisation. Sécuriser ces premiers succès garantit un **impact fort sur le reste des équipes**, et favorise par conséquent l'adhésion d'un plus grand nombre ensuite.

La seconde phase consiste ensuite à **élargir le déploiement aux profils les plus exposés**, tels que les services RH ou financier. À l'inverse, si l'adoption de la clé de sécurité fait suite à une cyberattaque, à une mise en conformité urgente, ou s'effectue auprès d'une entreprise aux effectifs limités, il convient alors d'opter pour une **approche big bang**. Cela signifie que le déploiement est simultané pour l'ensemble des utilisateurs.

Les solutions à disposition pour plus de sécurité et leurs avantages

Avant toute chose, établir une stratégie de déploiement claire

💡 Tout au long des différentes phases, les retours d'utilisateurs ainsi que leur expérience sont à analyser.

Les **métriques de déploiement** et le **reporting** associé sont en effet souvent sous-estimés, mais cruciaux pour **assurer la réussite d'un projet**. Ces indicateurs peuvent notamment inclure :

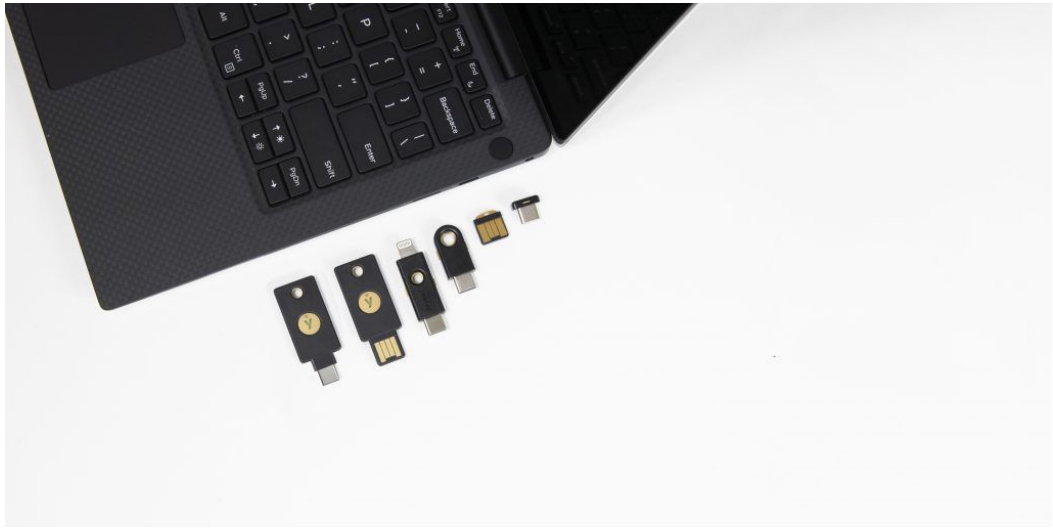
- ➔ le nombre d'applications et d'utilisateurs concernés,
- ➔ le pourcentage d'actifs parmi ces derniers,
- ➔ et la part d'échecs d'authentification avant et après le déploiement.

Une potentielle extension auprès des partenaires est aussi un point positif. En outre, ces chiffres **rassureront le comité exécutif** quant à l'efficacité et aux retours sur investissement de l'outil en place.

Libérez-vous des mots de passe pour plus de sécurité ! Qu'est-ce que le passwordless ?

Permise par l'utilisation des **protocoles d'authentification les plus sécurisés**, Smartcard et FIDO2, basés sur de la cryptographie à clés asymétriques, l'authentification passwordless permet de dispenser l'utilisateur de la saisie de l'identifiant et du mot de passe.

Elle peut être assortie de l'usage d'une **clé de sécurité physique,** pour plus de sécurité et de simplicité d'usage, elle-même protégée un code Pin (secret non partagé) ou de la biométrie (capteur d'empreinte digitale).



💡 D'ici 2022, le Gartner prédit que 60% des grands comptes, et 90% des ETI/PME, vont intégrer du passwordless dans plus de 50% de leurs cas d'usages*
Source: Gartner whitepaper, "IT Leadership Vision for 2021", March 2019

Libérez-vous des mots de passe pour plus de sécurité ! Qu'est-ce que le passwordless ?

Pendant trop longtemps, les mots de passe ont gêné les utilisateurs finaux, les équipes de sécurité et les équipes informatiques. En permettant une **sécurité sans mot de passe**, FIDO2 ouvre une nouvelle ère dans l'informatique d'entreprise, le service client et les interactions personne-machine.

En utilisant la connexion sans mot de passe FIDO2, les entreprises peuvent renforcer la **sécurité** de leur réseau, **réduire leurs dépenses** informatiques et améliorer leur **productivité**

Au cours des deux dernières années, la prise en charge du passwordless avec FIDO2 et WebAuthn est devenue très riche, avec l'adoption de plusieurs services cloud majeurs et de tous les principaux navigateurs et plateformes, mais il est important de comprendre que le passwordless est une transition qui ne se fait pas du jour au lendemain.

C'est pour cette période transitoire que la YubiKey a été conçue - pour pouvoir répondre aux besoins des organisations là où elles se trouvent et évoluer avec leurs exigences de sécurité et l'évolution de leur infrastructure. Les YubiKeys sont conçues pour prendre en charge le plus large éventail de protocoles de sécurité afin de combler le fossé entre l'authentification ancienne et moderne.

appvizer

Appvizer est le premier média en Europe dédié aux logiciels professionnels.

Sa mission est de permettre aux professionnels de trouver facilement les bons logiciels pour être plus compétitifs et travailler plus agréablement au quotidien.

yubico

Yubico a été fondée en Suède en 2007 avec la mission de simplifier l'authentification et de la rendre accessible à tous.

En collaboration avec les principales entreprises du web et des leaders d'opinion, nous avons créé une assistance native pour nos clés de sécurité dans les principaux navigateurs et plateformes en ligne, afin de renforcer la sécurité d'internet pour des milliards de personnes.

© 2021 Appvizer. Tous droits réservés.