Communiqués de presse

Enquête IBM : La dépendance numérique générée par la pandémie crée des effets secondaires à long terme en matière de sécurité

• Les gens ont créé en moyenne 15 nouveaux comptes pendant la pandémie selon l'enquête, 82 % d'entre eux réutilisant les mêmes mots de passe d'un compte à l'autre

• Plus de la moitié des millennials interrogés préfèrent passer une commande en utilisant une application ou un site web potentiellement non sécurisé plutôt que d'appeler ou de se rendre en personne dans un lieu physique

Cambridge, MA, le 15 juin 2021 : IBM Security a annoncé aujourd'hui les résultats d'une enquête mondiale examinant les comportements numériques des consommateurs pendant la pandémie, ainsi que leur potentiel impact à long terme sur la cybersécurité. Alors que la société s'habitue de plus en plus aux interactions numériques, l'étude a révélé que les préférences pour la facilité d'utilisation l'emportaient souvent sur les préoccupations de sécurité et de confidentialité chez les personnes interrogées - ce qui a conduit à de mauvais choix en matière de mots de passe et d'autres comportements de cybersécurité.

L'approche laxiste des consommateurs en matière de sécurité, combinée à la transformation numérique rapide des entreprises pendant la pandémie, pourrait fournir aux attaquants des munitions supplémentaires pour propager les cyberattaques dans tous les secteurs d'activité - du ransomware au vol de données. Selon l'IBM Security X-Force, les mauvaises habitudes personnelles en matière de sécurité pourraient se répercuter également sur le lieu de travail et peuvent entraîner des incidents de sécurité coûteux pour les entreprises, les informations d'identification compromises des utilisateurs représentant l'une des principales sources des cyberattaques signalées en 2020.[1]

L'enquête mondiale[2], menée par Morning Consult pour le compte d'IBM Security auprès de 22000 personnes sur 22 marchés, a identifié les effets suivants de la pandémie sur les comportements des consommateurs en matière de sécurité :

- **Le boom numérique survivra aux protocoles de pandémie** : Les personnes interrogées ont créé en moyenne 15 nouveaux comptes en ligne pendant la pandémie, ce qui équivaut à des milliards de nouveaux comptes créés dans le monde. Comme 44 % d'entre eux déclarent qu'ils ne prévoient pas de supprimer ou de désactiver ces nouveaux comptes, ces consommateurs auront une empreinte numérique accrue pour les années à venir, ce qui élargira considérablement la surface d'attaque des cybercriminels.

- **La surabondance de comptes a entraîné l'épuisement des mots de passe** : La multiplication des comptes numériques a entraîné un relâchement des comportements en matière de mots de passe parmi les personnes interrogées, 82 % d'entre elles admettant réutiliser les informations d'identification au moins de temps en temps. Cela signifie que beaucoup des nouveaux comptes créés pendant la pandémie reposaient probablement sur des combinaisons d'adresses électroniques et de mots de passe réutilisés, qui ont peut-être été déjà exposées via des violations de données au cours de la dernière décennie.

- **La facilité d'utilisation l'a souvent emporté sur la sécurité et la confidentialité** : Plus de la moitié (51 %) des millennials interrogés préfèrent passer une commande en utilisant une application ou un site web potentiellement non sécurisé plutôt que d'appeler ou de se rendre en personne dans un lieu physique.

Ces utilisateurs étant plus enclins à négliger les problèmes de sécurité au profit de la facilité de la commande numérique, le fardeau de la sécurité pèsera probablement davantage sur les entreprises fournissant ces services pour éviter les fraudes.

Les consommateurs se tournant de plus en plus vers les interactions numériques, ces comportements ont également le potentiel de stimuler l'adoption de technologies émergentes dans une variété de contextes - de la télésanté à l'identité numérique[3].

« La pandémie a entraîné une augmentation du nombre de nouveaux comptes en ligne, mais la préférence croissante de la société pour la commodité numérique peut avoir un coût pour la sécurité et la confidentialité des données », a déclaré **Charles Henderson, Global Managing Partner et Head of IBM Security X-Force***. « Les organisations doivent désormais prendre en compte les effets de cette dépendance numérique sur leur profil de risque en matière de sécurité. Les mots de passe devenant de moins en moins fiables, l'une des façons dont les organisations peuvent s'adapter, au-delà de l'authentification multifacteur, est de passer à une approche « zero trust » - en appliquant une IA et des analyses avancées tout au long du processus pour détecter les menaces potentielles, plutôt que de supposer qu'un utilisateur est de confiance après l'authentification. »*

Les consommateurs ont des attentes élevées en matière de facilité d'accès

L'enquête a mis en lumière une variété de comportements des consommateurs qui ont un impact sur le paysage de la cybersécurité aujourd'hui et dans le futur. Alors que les individus tirent de plus en plus parti des interactions numériques dans un plus grand nombre de domaines de leur vie, l'enquête a révélé que nombre d'entre eux ont également des attentes élevées en matière de facilité d'accès et d'utilisation.

- **La règle des 5 minutes** : Selon l'enquête, la plupart des adultes (59 %) s'attendent à passer moins de 5 minutes à créer un nouveau compte numérique.
- **Après 3 tentatives, c'est fini** : Dans l'ensemble, les personnes interrogées tentent de se connecter trois ou quatre fois avant de réinitialiser leur mot de passe. Ces réinitialisations ne coûtent pas seulement de l'argent aux entreprises, elles peuvent également constituer une menace pour la sécurité si elles sont utilisées en combinaison avec un compte de messagerie déjà compromis.
- **Stockées dans la mémoire** : 44% des personnes interrogées stockent les informations relatives aux comptes en ligne dans leur mémoire (méthode la plus courante), tandis que 32% écrivent ces informations sur papier.
- **Authentification multifacteur** : Alors que la réutilisation des mots de passe est un problème croissant, l'ajout d'un facteur de vérification supplémentaire pour les transactions à haut risque peut contribuer à réduire le risque de compromission des comptes. L'enquête a révélé qu'environ deux tiers des personnes interrogées dans le monde avaient utilisé l'authentification multifacteur au cours des dernières semaines précédent l'enquête.

Plonger plus profondément dans la santé numérique

Pendant la pandémie, les canaux numériques sont devenus un élément crucial pour répondre aux demandes massives de vaccins, de tests et de traitements liés à la COVID-19. L'adoption par les consommateurs d'une grande variété de canaux numériques pour les services liés à la COVID-19 pourrait encourager un plus grand engagement numérique avec les prestataires de soins de santé à l'avenir, en réduisant la barrière à l'entrée pour les nouveaux utilisateurs, selon l'analyse d'IBM Security[4]. Selon l'enquête :

- 63 % des personnes interrogées ont utilisé des services liés à la pandémie[5] par le biais d'un canal numérique (web, application mobile, e-mail et SMS).
- Alors que les sites Web et les applications Web étaient la méthode d'engagement numérique la plus courante, les applications mobiles et les SMS ont également été largement utilisés - avec respectivement 39 % et 20 % d'engagement via ces canaux.

Alors que les prestataires de soins de santé se lancent dans la télémédecine, il sera de plus en plus important que leurs protocoles de sécurité soient conçus pour faire face à cette évolution, qu'il s'agisse de maintenir les systèmes informatiques critiques connectés, de protéger les données sensibles des patients ou de maintenir la conformité à la loi HIPAA. Cela inclut la segmentation des données et la mise en place de contrôles stricts afin que les utilisateurs ne puissent accéder qu'à des systèmes et des données spécifiques, limitant ainsi l'impact d'un compte ou d'un appareil compromis. Pour se préparer à l'éventualité d'attaques par ransomware et extorsion, les données des patients doivent être chiffrées, de préférence à tout moment, et des sauvegardes fiables doivent être mises en place afin que les systèmes et les données puissent être rapidement restaurés avec un minimum d'interruption.

Ouvrir la voie aux identifiants numériques

Le concept de pass sanitaire numérique, ou passeports vaccinaux, a permis aux consommateurs de découvrir un cas d'utilisation réel des justificatifs numériques, qui offrent une approche technologique pour vérifier des aspects spécifiques de notre identité. Selon l'enquête, 65 % des adultes dans le monde disent connaître le concept de justificatif numérique, et 76 % seraient susceptibles de l'adopter s'il devenait communément accepté.

Cette exposition à l’idée d’une preuve d'identité numérisée pendant la pandémie peut aider à favoriser une adoption plus large des systèmes modernisés d'identité numérique, qui pourraient potentiellement remplacer le besoin de formes traditionnelles d'identité comme les passeports et les permis de conduire, offrant un moyen pour les consommateurs de fournir les strictes informations requises pour une transaction spécifique. Si l'utilisation d'une forme numérique d'identité a le potentiel de créer un modèle durable pour l'avenir, des mesures de sécurité et de protection de la vie privée doivent être mises en place pour contribuer à la protection contre la contrefaçon - faisant appel aux capacités des solutions blockchain pour vérifier ces informations d'identification et fournir la possibilité de les mettre à jour dans le cas où elles seraient compromises.

Comment les organisations peuvent-elles s'adapter à l'évolution du paysage de la sécurité des consommateurs ?

Les entreprises qui sont devenues de plus en plus dépendantes de l'engagement numérique avec les consommateurs en raison de la pandémie devraient considérer l'impact que cela a sur leurs profils de risque de cybersécurité. À la lumière de l'évolution des comportements et des préférences des consommateurs en matière de commodité numérique, IBM Security suggère aux organisations de prendre en compte les recommandations de sécurité suivantes :

- **Approche « zero trust »** : Compte tenu de l'augmentation des risques, les entreprises devraient envisager d'évoluer vers une approche de sécurité « zero trust », qui part du principe qu'une identité authentifiée ou que le réseau lui-même peuvent déjà être compromis, et valide donc en permanence les conditions de connexion entre les utilisateurs, les données et les ressources pour déterminer l'autorisation et le besoin. Cette approche exige des entreprises qu'elles unifient leurs données et leur approche de sécurité, dans le but d'analyser le contexte de sécurité autour de chaque utilisateur, de chaque appareil et de chaque interaction.

- **Modernisation de la gestion des identités et des accès des consommateurs** : Pour les entreprises qui souhaitent continuer à exploiter les canaux numériques pour engager les consommateurs, il est important de fournir un processus d'authentification transparent. Investir dans une stratégie modernisée de gestion des identités et des accès des consommateurs (CIAM) peut aider les entreprises à accroître l'engagement numérique - en offrant une expérience utilisateur fluide sur les plateformes numériques et en utilisant l'analyse comportementale pour aider à réduire le risque d'utilisation frauduleuse des comptes.

- **Protection des données et confidentialité** : L'augmentation du nombre d'utilisateurs numériques signifie que les entreprises auront également davantage de données sensibles à protéger. Les violations de données coûtant en moyenne 3,86 millions de dollars aux entreprises parmi celles interrogées[6], celles-ci doivent mettre en place des contrôles de sécurité des données stricts pour se protéger contre tout accès non autorisé - de la surveillance des données pour détecter toute activité suspecte au chiffrement des données sensibles, où qu'elles se trouvent. Les entreprises doivent également mettre en œuvre les bonnes politiques de confidentialité en local et dans le Cloud afin d'aider à conserver la confiance des consommateurs.

- **Mettre la sécurité à l'épreuve** : L'utilisation des plateformes numériques et la dépendance à ces plateformes évoluant rapidement, les entreprises doivent envisager des tests spécifiques pour vérifier que les stratégies et technologies de sécurité sur lesquelles elles s'appuyaient auparavant tiennent toujours dans ce nouveau paysage. Ré-évaluer l'efficacité des plans de réponse aux incidents et tester les vulnérabilités de sécurité des applications sont deux éléments importants de ce processus.

Pour consulter le rapport complet et les ressources multimédias : http://ibm.biz/IBMSecurity_ConsumerSurvey

À propos d'IBM Security

IBM Security offre aux entreprises l'une des gammes de produits et services de sécurité les plus performantes

et intégrées du marché. Ce portefeuille, qui repose sur les recherches du mondialement célèbre IBM X-Force®, permet aux organisations de gérer efficacement les risques et de se défendre face aux menaces émergentes. IBM compte parmi les plus grandes organisations mondiales dédiées à la recherche, au développement et à la conception de solutions de sécurité, gère plus de 150 milliards d'évènements de sécurité par jour dans plus de 130 pays, et possède plus de 10 000 brevets dans le domaine de la sécurité. Pour de plus amples informations, rendez-vous sur https://www-03.ibm.com/security/fr-fr/, suivez IBMSecurity sur Twitter ou consultez le blog IBM Security Intelligence.

***Méthodologie du rapport** : Une enquête mondiale a été menée par Morning Consult pour le compte d'IBM en mars 2021. L'étude a été menée auprès de 22 000 adultes dans 22 marchés (1 000 personnes interrogées par marché) dont **la France**, l'Argentine, l'Australie, le Brésil, le Canada, le Chili, la Colombie, l'Allemagne, l'Inde, l'Italie, le Japon, le Mexique, le Pérou, Singapour, la Corée du Sud, l'Espagne, le Royaume-Uni, les États-Unis, le Moyen-Orient, l'Europe centrale et orientale, les pays nordiques et le Bénélux (Belgique, Pays-Bas et Luxembourg).*

Contacts presse :

IBM
Gaëlle Dussutour
Tél. : + 33 (0) 6 74 98 26 92
dusga@fr.ibm.com

Weber Shandwick pour IBM

Robin Legros / David Boutet

Tél. : + 33 (0)6 68 04 57 83 / +33 (0)6 6 63 45 03 79

ibmfrance@webershandwick.com

---

[1] IBM X-Force Threat Index 2021: Compromised user credentials were #3 initial attack vector for cyberattacks in 2020, representing 18% of incidents reported.

[2] Global survey was conducted by Morning Consult on behalf of IBM in March 2021. The study was conducted among 22,000 adults in 22 markets.

[3] Prediction based on IBM Security insights

[4] Prediction based on IBM Security analysis

[5] Includes COVID-19 financial relief, testing, treatment and vaccinations

[6] 2020 Cost of a Data Breach Report, benchmark study conducted by Ponemon Institute, analyzed and sponsored by IBM Security