Groupe de travail sur la coopération internationale en matière d'application de la loi

Lignes directrices sur le bourrage d'identifiants, v. 1, 30 mars 2022

Organismes membres du sous-groupe de travail sur le bourrage d'identifiants :

- Commissariat à la protection de la vie privée du Canada
- Autorité de réglementation de Gibraltar
- Commissariat à l'information de Jersey
- Préposé fédéral Suisse à la protection des données et à la transparence
- Autorité de protection des données de Turquie
- Commissariat à l'information du Royaume-Uni

Table des matières

Sommaire

Le Groupe de travail sur la coopération internationale en matière d'application de la loi est un groupe de travail permanent de l'Assemblée mondiale pour la protection de la vie privée (AMVP), coprésidé par le Commissariat à la protection de la vie privée du Canada; le Commissariat à la protection des données personnelles de Hong Kong, Chine; la Surintendance de l'industrie et du commerce de Colombie et l'Autorité norvégienne de protection des données.

Les travaux du Groupe de travail font partie intégrante de l'Assemblée dans sa mission de promotion du respect de la vie privée à titre de chef de file mondial en la matière et de la coopération mondiale à cet effet à l'ère numérique. En particulier, le Groupe de travail a la responsabilité première de diriger la mise en œuvre des actions relevant du pilier de coopération en matière de réglementation et de mise en application du plan stratégique 2021-2023 de l'AMVP (en anglais seulement).

Le Groupe de travail a établi que la situation entourant le bourrage d'identifiants devenait préoccupante lors d'une séance d'étude à huis clos[1] en mars 2021. En conséquence, il a été déterminé qu'un suivi était nécessaire, et donc un sous-groupe de travail a été formé, celui-ci ayant comme mission de se pencher sur le dossier et de produire des documents visant à aider les autorités à faire face à la menace croissante du bourrage d'identifiants.

Les présentes lignes directrices établissent le danger que représente le bourrage d'identifiants pour les données personnelles et les mesures éprouvées que peuvent utiliser les organisations pour réduire ce danger. Bien qu'elles ne constituent pas des obligations légales pour tous les pays, elles peuvent aider les organisations à se conformer aux lois sur la protection des données et la vie privée, qui exigent généralement d'elles qu'elles protègent adéquatement les renseignements personnels contre les menaces telles que les attaques par bourrage d'identifiants.

[1] Lors de ses séances d'étude à huis clos, le Groupe de travail cerne et examine des enjeux ou des organisations d'importance qui ont des retombées mondiales en matière de protection des données et de droits à la vie privée des personnes. Ces séances constituent des plateformes pour favoriser une coopération concrète en matière d'application de la loi. En général, ces séances commencent par une présentation sur un sujet, suivie d'une discussion ouverte sur les motifs de préoccupation qui y sont associés, les stratégies de réglementation possibles et les options de coopération.

Remerciements

Beaucoup de publications d'une variété d'organisations ont servi à la rédaction des présentes lignes directrices, qui les intègrent lorsqu'il convient de le faire. Nous dressons ci-dessous la liste des documents que nous avons utilisés et auxquels nous faisons référence. Des références sont également incluses dans le document.

Outre les documents mentionnés ci-dessous, les présentes lignes directrices intègrent également le fruit de consultations et de contributions d'experts dans le domaine de la cybersécurité[2], à savoir :

- Membres du groupe de référence de l'Assemblée mondiale pour la protection de la vie privée
    - Bojana Bellamy, Centre for information Policy Leadership (avec la participation de Lisa Sotto, Hunton Andrews Kurth)
    - Clarisse Girot, Asian Business Law Institute (avec la participation de James McLeary, Kroll, et Rajesh Sreenivasan, Rajah & Tann LLP)
- Centre national de cybersécurité du Royaume-Uni
- Open Web Application Security Project – Shuman Ghosemajumder, F5

Agence de l'Union européenne pour la cybersécurité

« Principaux incidents dans l'UE et dans le monde de janvier 2019 à avril 2020 »
https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-main-incidents

Akamai

Akamai, *[State of the Internet]/security credential stuffing: attacks and economies* (vol. 5 | 2019)

Akamai, *[State of the Internet]/security web attacks and gaming abuse* (vol. 5, nº 3 | 2019)

Akamai, *[State of the Internet] phishing for finance* (vol. 7, nº 2 | 2021)

Arkose Labs

« Click Farm: What is it and How to Stop it »
https://www.arkoselabs.com/explained/click-farm/

Autorité norvégienne de sécurité nationale

« Passordanbefalinger fra Nasjonal sikkerhetsmyndighet » [Password Recommendations]
https://nsm.no/aktuelt/passordanbefalinger-fra-nasjonal-sikkerhetsmyndighet

[2] L'approche collaborative adoptée a permis au groupe de travail de bénéficier de l'expérience et du savoir-faire de spécialistes qui ont enrichi les travaux effectués. Les consultations et collaborations externes contribuent également à donner une voix et de l'influence à l'AMPV, conformément à sa priorité stratégique 2.

British Broadcasting Corporation News

« Yahoo 2013 data breach hit 'all three billion accounts' »
https://www.bbc.com/news/business-41493494

Bureau du procureur général de l'État de New York (États-Unis)

The People of the State of New York by Letitia James, Attorney General of the State of New York v Dunkin' Brands, Inc (2019), plainte nº 451787/2019
https://ag.ny.gov/sites/default/files/dunkin_complaint.pdf

The People of the State of New York by Letitia James, Attorney General of the State of New York v Dunkin' Brands, Inc (2020), jugement et ordonnance sur consentement nº 451787/2019
https://ag.ny.gov/sites/default/files/proposed_consent_order_and_judgment.pdf

Bureau of Internet and Technology du bureau du procureur général de l'État de New York (États-Unis)

« Business Guide for Credential Stuffing Attacks »
https://ag.ny.gov/sites/default/files/businessguide-credentialstuffingattacks.pdf

Centre canadien pour la cybersécurité

« Conseils de sécurité sur les gestionnaires de mots de passe »
https://cyber.gc.ca/fr/orientation/conseils-de-securite-sur-les-gestionnaires-de-mots-de-passeitsap30025

« Déclaration au sujet de l'attaque de bourrage de justificatifs touchant le service CléGC »
https://cyber.gc.ca/fr/nouvelles/declaration-au-sujet-de-lattaque-de-bourrage-de-justificatifs-touchant-le-service-clegc

« Repensez vos habitudes en regard de vos mots de passe de manière à protéger vos comptes des pirates informatiques »
https://cyber.gc.ca/fr/orientation/repensez-vos-habitudes-en-regard-de-vos-mots-de-passe-de-maniere-proteger-vos-comptes

Centre national pour la cybersécurité du Royaume-Uni

« Multi-factor authentication for online services »
https://www.ncsc.gov.uk/guidance/multi-factor-authentication-online-services

« NCSC Glossary »
https://www.ncsc.gov.uk/information/ncsc-glossary

« Password administration for system owners »
https://www.ncsc.gov.uk/collection/passwords/updating-your-approach

« Preventing lateral movement »
https://www.ncsc.gov.uk/guidance/preventing-lateral-movement

« Secure system administration: Use privileged access management »
https://www.ncsc.gov.uk/collection/secure-system-administration/use-privileged-access-management

« Three random words or #thinkrandom »
https://www.ncsc.gov.uk/blog-post/three-random-words-or-thinkrandom-0

« Top tips for staying secure online »
https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/activate-two-factor-authentication-on-your-email

« Use of credential stuffing tools »
https://www.ncsc.gov.uk/news/use-credential-stuffing-tools

CloudFlare

« What Is Credential Stuffing? »
https://www.cloudflare.com/learning/bots/what-is-credential-stuffing/

Code de réglementation fédérale de l'électronique (États-Unis)

« Standards for safeguarding customer information »
https://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&sid=1e9a81d52a0904d70a046d0675d613b0&rgn=div5&view=text&node=16%3A1.0.1.3.38&idno=16

Commissariat à l'information du Royaume-Uni

« ICO fines Uber £385,000 over data protection failings »
https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/11/ico-fines-uber-385-000-over-data-protection-failings/

« Passwords in online services »
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/passwords-in-online-services/

Commission fédérale du commerce des États-Unis

« Operator of Online Tax Preparation Service Agrees to Settle FTC Charges That it Violated Financial Privacy and Security Rules »
https://www.ftc.gov/news-events/press-releases/2017/08/operator-online-tax-preparation-service-agrees-settle-ftc-charges

« Stick with Security: Require secure passwords and authentication »
https://www.ftc.gov/news-events/blogs/business-blog/2017/08/stick-security-require-secure-passwords-authentication

« Taxslayer complaint, Docket NO. C-1623063 »,
https://www.ftc.gov/system/files/documents/cases/1623063_taxslayer_complaint.pdf

« Taxslayer Decision and Order, Docket NO. C-1623063 »
https://www.ftc.gov/system/files/documents/cases/1623063_taxslayer_decision_and_order.pdf

Commission irlandaise de protection des données

« Know your obligations – data security »
https://www.dataprotection.ie/en/organisations/know-your-obligations/data-security-guidance

ComputerWeekly.com

« Over 15 billion credentials for sale on dark web »
https://www.computerweekly.com/news/252485713/Over-15-billion-credentials-for-sale-on-dark-web

Digital Shadows Photon Research Team

« From Exposure to Takeover: The 15 billion stolen credentials allowing account takeover »
https://resources.digitalshadows.com/whitepapers-and-reports/from-exposure-to-takeover

F5

« 2021 Credential Stuffing Report »
https://www.f5.com/labs/articles/threat-intelligence/2021-credential-stuffing-report

Federal Bureau of Investigation (FBI) des États-Unis
« Cyber Actors Conduct Credential Stuffing Attacks Against US Financial Sector »
https://www.documentcloud.org/documents/7208239-FBI-PIN-on-credential-stuffing-attacks.html

« Private Industry Notification 20200910-001 »
https://www.ic3.gov/media/news/2020/200929-1.pdf

« Scams and safety: Business email compromise »
https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/business-email-compromise

Google

« Online Security Survey »
https://services.google.com/fh/files/blogs/google_security_infographic.pdf

Institut national des normes et des technologies des États-Unis

« Digital Identity Guidelines »
https://pages.nist.gov/800-63-3/sp800-63b.html#throttle

Microsoft

« Your Pa$$word doesn't matter »
https://techcommunity.microsoft.com/t5/azure-active-directory-identity/your-pa-word-doesn-t-matter/ba-p/731984

US Securities and Exchange Commission, Office of Compliance Inspections and Examinations Officers (OIEC)
« Cybersecurity: Safeguarding Client Accounts against Credential Compromise »
https://www.sec.gov/files/Risk%20Alert%20-%20Credential%20Compromise.pdf

US Securities and Exchange Commission v Altaba Inc., f/d/b/a Yahoo! (2018)
https://www.sec.gov/litigation/admin/2018/33-10485.pdf

Open Web Security Project Foundation

« Credential stuffing »
https://owasp.org/www-community/attacks/Credential_stuffing

« Credential Stuffing Prevention Cheat Sheet »
https://cheatsheetseries.owasp.org/cheatsheets/Credential_Stuffing_Prevention_Cheat_Sheet.html

« Cross-Site Request Forgery Prevention Cheat Sheet »
https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html

Shape Security

Shape Security, *The 2018 credential spill report* (2018)

Shape Security, *Attacker economics* (2020)

Verizon

« 2019 data breach investigations report »
https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf

1. Introduction

Une attaque par bourrage d'identifiants est une méthode de cyberattaque qui exploite la tendance d'une personne à utiliser les mêmes justificatifs d'identité (une même combinaison de nom d'utilisateur ou courriel et de mot de passe, par exemple) sur de multiples plateformes en ligne. Les attaques sont automatisées et souvent à grande échelle et font appel à des justificatifs volés (à la suite de fuites et de ventes sur le Web clandestin) pour accéder illégalement aux comptes des utilisateurs sur d'autres sites Web.

Les attaques par bourrage d'identifiants réussis peuvent ouvrir la voie à la fraude ou d'autres types de pertes financières, car les pirates peuvent, par exemple, effectuer des achats en utilisant le compte compromis ou transférer des fonds à leur propre compte. Après avoir réussi à établir un point d'entrée dans les affaires d'une victime, le pirate peut tenter d'accéder à d'autres données et systèmes en récoltant d'autres justificatifs d'identité visibles ou accessibles. Les attaques peuvent également servir à causer des dégâts immatériels, notamment l'atteinte à la réputation par la diffusion de fausses informations ou de fausses déclarations sur une personne à partir du compte compromis.

Les secteurs public et privé ont tous les deux signalé que le bourrage d'identifiants gagnait du terrain et devenait un risque important pour les données personnelles à l'échelle mondiale. Notre dépendance envers les services numériques ne montre aucun signe de ralentissement, pas plus que les méthodes d'exploitation et les moyens utilisés par les cybercriminels pour mener des attaques sur ces services, semble-t-il.

Par les présentes lignes directrices, le Groupe de travail reconnait l'importance la menace que représente le bourrage d'identifiants pour les données personnelles. Ces lignes directrices devraient aider les organisations à protéger les données contre les attaques par bourrage d'identifiants. L'utilisation qu'en feront les autorités dépendra d'un cas à l'autre. Par exemple, les lignes directrices peuvent servir de référence pour les autorités dans une optique de diffusion des connaissances; aider les autorités à publier des lignes directrices, des avertissements ou des avis sur le bourrage d'identifiants et contribuer à établir un ensemble de mesures éprouvées contre les dangers du bourrage d'identifiants, que les autorités peuvent utiliser dans leur évaluation des mesures de sécurité.

2. Comment fonctionne le bourrage d'identifiants?

Bien que les attaques par bourrage d'identifiants soient parfois intégrées dans la catégorie des attaques par force brute, il est important de différencier ces deux types d'attaques :

(a) Une **attaque par force brute** est une tentative d'accès non autorisé à des comptes ou services en ligne au moyen d'un logiciel qui génère et saisit automatiquement un grand nombre de combinaisons de valeurs possibles sur les pages d'ouverture de session de sites Web, jusqu'à ce que le bon mot de passe soit trouvé et que l'accès soit accordé[3].

(b) En revanche, une **attaque par bourrage d'identifiants** consiste à obtenir frauduleusement des justificatifs d'identité valides (combinaisons de nom d'utilisateur ou courriel et mot de passe, par exemple) à partir de justificatifs de comptes compromis, qui sont saisis automatiquement en masse dans les pages d'ouverture de session de sites jusqu'à ce qu'une correspondance soit trouvée.

Les attaques par bourrage d'identifiants sont largement reconnues comme une cybermenace pour la sécurité des données par les principales organisations de cybersécurité[4]. Elles sont relativement simples à réaliser, et il existe beaucoup de logiciels automatisés facilement accessibles à cet effet[5]. À cet égard, on utilise notamment des botnets (c'est-à-dire des collections de robots Internet ou d'appareils connectés à Internet) et des applications de vérification de comptes pour insérer automatiquement les justificatifs d'identité dans les bons champs dans un grand nombre de sites[6]. Parmi les outils utilisés, notons par exemple Sentry MBA, Account Hitman, Vertex et Apex[7].

Les attaques peuvent être réalisées assez facilement en se procurant l'un des outils susmentionnés ainsi qu'un fichier de configuration du site, accompagné d'une liste de justificatifs d'identité valides[8]. Une fois l'attaque lancée, les tentatives d'ouverture de session sont généralement menées par des serveurs mandataires afin de cacher la source de l'attaque et d'éviter la détection[9]. Afin de contourner les mesures de sécurité de plus en plus strictes, les pirates peuvent également « sous-traiter » leurs activités frauduleuses à des travailleurs non qualifiés et mal payés dans des usines à clics ou à fraudes[10]. Ces travailleurs gagnent généralement un petit

---

[3] Le Centre national de cybersécurité du Royaume-Uni a un glossaire qui contient la définition à https://www.ncsc.gov.uk/information/ncsc-glossary (consulté le 25 mai 2021).

[4] Par exemple le Centre national de cybersécurité du Royaume-Uni (https://www.ncsc.gov.uk/news/use-credential-stuffing-tools, consulté le 25 mai 2021), le Centre canadien pour la cybersécurité (https://cyber.gc.ca/fr/orientation/repensez-vos-habitudes-en-regard-de-vos-mots-de-passe-de-maniere-proteger-vos-comptes, consulté le 25 mai 2021) et l'Open Web Security Project Foundation (https://owasp.org/www-community/attacks/Credential_stuffing, consulté le 25 mai 2021).

[5] Centre national de cybersécurité du Royaume-Uni, « Use of credential stuffing tools », https://www.ncsc.gov.uk/news/use-credential-stuffing-tools, consulté le 25 mai 2021.

[6] Centre canadien pour la cybersécurité, « Repensez vos habitudes en regard de vos mots de passe de manière à protéger vos comptes des pirates informatiques », https://cyber.gc.ca/en/guidance/rethink-your-password-habits-protect-your-accounts-hackers-itsap30036, consulté le 25 mai 2021.

[7] Centre national de cybersécurité du Royaume-Uni, « Use of credential stuffing tools », https://www.ncsc.gov.uk/news/use-credential-stuffing-tools, consulté le 25 mai 2021.

[8] *Ibid.*

[9] *Ibid.*

[10] Arkose Labs, « Click Farm: What is it and How to Stop it », https://www.arkoselabs.com/explained/click-farm/, consulté le 18 mars 2022.

salaire fixe pour remplir les CAPTCHA ou les autres modes d'authentification que les robots ne peuvent pas remplir eux-mêmes pour mener à bien une attaque[11].

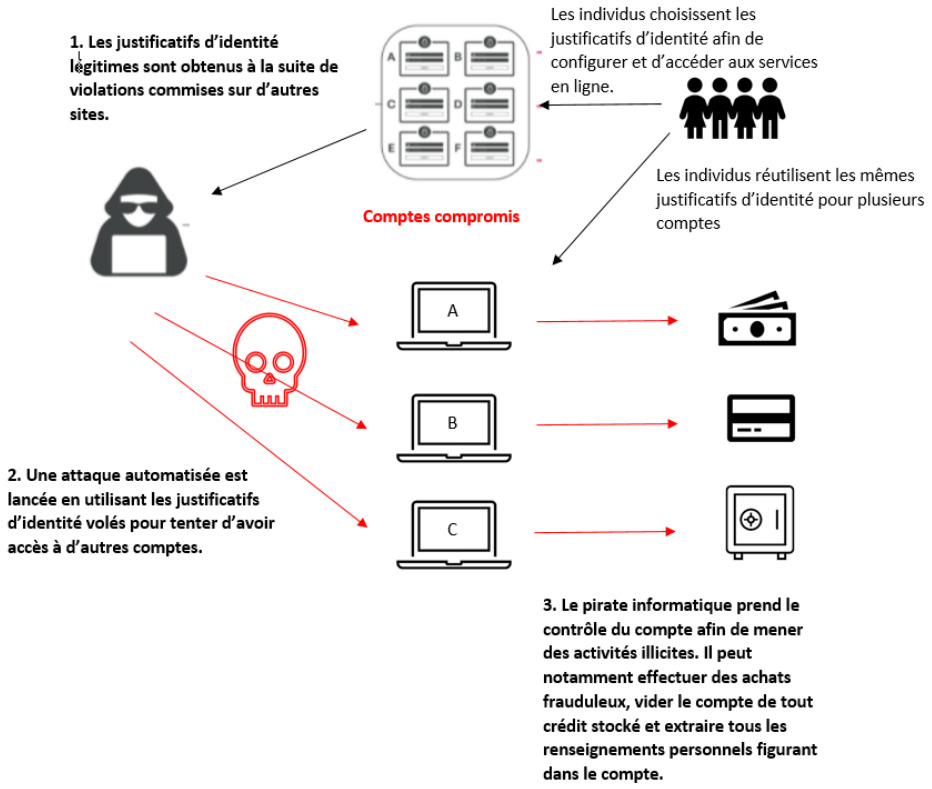
Voici les étapes typiques d'une attaque par bourrage d'identifiants, illustrée à la figure 1.

(a) **Obtenir des justificatifs d'identité valides :** Le pirate obtient une grande quantité de noms d'utilisateur, de courriels et de mots de passe qui ont fuité. Bien qu'il arrive qu'un pirate paye pour obtenir des justificatifs d'identité, une étude récente révèle que plus de 15 milliards de justificatifs circulent librement en ligne à la suite de plus de 100 000 cas de fuites[12].

(b) **Lancer l'attaque :** Le pirate acquiert un outil de vérification de comptes, qui lance ensuite des bots automatisés pour cibler des sites à partir desquels il tentera d'accéder à des comptes. C'est en raison de la nature automatisée des attaques que le pirate peut tenter d'accéder à beaucoup de comptes à grande vitesse. Certains outils permettent aux bots de contourner la sécurité d'un site, et certains sont même capables de remplir des CAPTCHA[13].

(c) **Prendre le contrôle :** L'outil de vérification de comptes testera tous les justificatifs d'identité disponibles et informera le pirate des correspondances trouvées. Le pirate pourra alors prendre contrôle du compte.

Figure 1 :



[11] *Ibid.*

[12] Digital Shadows Photon Research Team, « From Exposure to Takeover: The 15 billion stolen credentials allowing account takeover », https://resources.digitalshadows.com/whitepapers-and-reports/from-exposure-to-takeover, consulté le 27 janvier 2022.

[13] CAPTCHA signifie *Completely Automated Public Turing test to tell Computers and Humans Apart* (test public de Turing complètement automatique ayant pour but de différencier les humains des ordinateurs).

Comme le montre la figure 1 ci-dessus, les comptes d'utilisateurs de tout site Web nécessitant une ouverture de session sont potentiellement exposés à des attaques par bourrage d'identifiants, et les attaques qui ne sont pas détectées peuvent exposer les utilisateurs et les organisations à d'autres attaques sur d'autres comptes utilisant les mêmes justificatifs compromis. On ouvre ainsi potentiellement la porte à un effet domino.

3. Pourquoi fait-on des attaques par bourrage d'identifiants?

La motivation première de ce type de cyberattaque est le gain financier. En particulier, et comme il est mentionné plus haut, l'auteur est potentiellement en mesure d'effectuer des achats frauduleux depuis le compte compromis, de transférer des fonds vers son propre compte, de vider le compte de tout crédit stocké, de copier des informations relatives au compte bancaire ainsi que de vendre toutes les données personnelles dans le compte compromis pour toucher un profit supplémentaireavec les justificatifs utilisés. L'acquisition d'informations financières, telles que les données relatives aux cartes de crédit, peut également entraîner une usurpation d'identité, un autre motif pour la réalisation de ces attaques[14].

Si les attaques par bourrage d'identifiants sont principalement motivées par des raisons financières, les pirates peuvent aussi chercher à causer des dégâts moins tangibles au titulaire du compte. Par exemple, les pirates peuvent divulguer publiquement des informations personnelles sensibles afin de porter atteinte à la réputation d'organisations ou de personnalités publiques. Après avoir obtenu l'accès à un compte d'entreprise, un pirate peut tenter d'utiliser les privilèges d'utilisateur pour s'infiltrer dans le réseau interne d'une organisation et mener des cyberattaques plus importantes[15]. En outre, un pirate peut également utiliser un compte compromis pour se faire passer pour une source connue et envoyer des demandes qui ont l'air tout à fait légitimes à des membres du personnel ou à des fournisseurs et partenaires externes peu méfiants. C'est ce qu'on appelle l'escroquerie au faux ordre de virement[16].

Des rapports en ligne indiquent qu'un nombre croissant de listes de justificatifs d'identité valides sont vendues en ligne[17]. En outre, des tutoriels (comme des vidéos sur YouTube) expliquent étape par étape comment mener des attaques efficaces par bourrage d'identifiants, en particulier dans les secteurs des médias, des jeux en ligne et des divertissements[18].

Voici certains des facteurs qui peuvent expliquer l'augmentation des attaques par bourrage d'identifiants :

(a) Les combinaisons de nom d'utilisateur et de mot de passe sont un moyen simple et universel pour créer et accéder à des comptes en ligne

Presque tous les sites Web qui demandent à un utilisateur de créer un compte exigent que celui-ci crée un nom d'utilisateur, qui est souvent un courriel, ainsi qu'un mot de passe. Sans l'utilisation de l'authentification multifactorielle, les comptes demeurent la cible à ces types d'attaques.

(b) La tendance à réutiliser le même mot de passe pour plusieurs comptes

---

[14] Centre national de cybersécurité du Royaume-Uni, « Use of credential stuffing tools », https://www.ncsc.gov.uk/news/use-credential-stuffing-tools, consulté le 25 mai 2021.

[15] Centre national de cybersécurité du Royaume-Uni, « Preventing lateral movement », https://www.ncsc.gov.uk/guidance/preventing-lateral-movement, consulté le 23 novembre 2021.

[16] Federal Bureau of Investigation (FBI), « Scams and safety: Business email compromise », https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/business-email-compromise, consulté le 8 février 2022.

[17] Cloudflare, « What Is Credential Stuffing? », https://www.cloudflare.com/learning/bots/what-is-credential-stuffing/, consulté le 25 mai 2021; ComputerWeekly.com, « Over 15 billion credentials for sale on dark web », https://www.computerweekly.com/news/252485713/Over-15-billion-credentials-for-sale-on-dark-web, consulté le 25 mai 2021.

[18] Akamai, *[State of the Internet]/security credential stuffing: attacks and economies* (vol. 5 | 2019) | p. 5-6.

Compte tenu de l'obligation omniprésente de créer un mot de passe pour chaque service en ligne, il devient plus difficile pour tous de trouver des mots de passe et de se souvenir de chacun d'eux. Pour cette raison, le même mot de passe est souvent réutilisé dans plusieurs applications et comptes. Dans une enquête sur la sécurité en ligne réalisée par Google en 2019[19], 52 % des personnes ont admis réutiliser le même mot de passe pour plusieurs comptes et 13 % des personnes ont confirmé qu'elles utilisaient le même mot de passe pour **tous** leurs comptes.

(c) L'arrivée des mégafuites

Au cours des dernières années, un certain nombre de mégafuites se sont produites exposant ainsi des milliards de justificatifs d'identité. L'une des attaques les plus connues s'est produite en août 2013[20]. Yahoo a été victime d'une attaque par bourrage d'identifiants et a annoncé qu'au moins un milliard de comptes avaient été compromis, ce qui a entraîné des vols, des accès non autorisés et l'acquisition de centaines de millions de données de ses utilisateurs, notamment des noms d'utilisateur, des dates de naissance et des numéros de téléphone[21]. En 2017, il a été confirmé que cette attaque avait probablement touché les trois milliards d'utilisateurs de Yahoo[22].

(d) Le ratio coût/efficacité d'une attaque

Selon certains rapports, les attaques par bourrage d'identifiants ont généralement un taux de réussite de 0,2 à 2 %[23]. Bien que le chiffre puisse sembler bas, la menace est élevée étant donné l'ampleur des attaques par bourrage d'identifiants. Par exemple, une recherche du secteur privé a mis au jour 55 milliards d'attaques par bourrage d'identifiants dans l'industrie du jeu en ligne de novembre 2017 à mars 2019[24], ce qui équivaut à plus de 3 000 millions d'attaques par mois et plus de 107 millions d'attaques par jour. D'autres recherches ont révélé 193 milliards d'attaques par bourrage d'identifiants dans le monde en 2020[25], ce qui équivaut à plus de 16 milliards d'attaques par mois et à plus de 500 millions d'attaques par jour.

Si un pirate obtient des justificatifs d'identité à très faible coût, il peut être en mesure d'accéder à un nombre important de comptes, qu'il peut exploiter à fond pour lui-même, et il peut après coup profiter de la vente des justificatifs usagés.

(e) Les pirates disposent d'un temps considérable pour mener à bien leurs attaques

Les pirates disposent d'un temps considérable pour mener leurs attaques, car le délai entre un incident et sa détection est très long. En 2018, on a constaté qu'il fallait environ 15 mois à une organisation pour découvrir une atteinte à la sécurité découlant d'un bourrage d'identifiants et en informer ses utilisateurs[26]. Bien que la

---

[19] Google, « Online Security Survey », https://services.google.com/fh/files/blogs/google_security_infographic.pdf, consulté le 25 mai 2021.

[20] Bien que l'attaque ait eu lieu en 2013, elle n'a été signalée par Yahoo qu'en 2016.

[21] *US Securities and Exchange Commission v Altaba Inc., f/d/b/a Yahoo!* (2018), https://www.sec.gov/litigation/admin/2018/33-10485.pdf, consulté le 8 février 2022.

[22] BBC News, « Yahoo 2013 data breach hit 'all three billion accounts' », https://www.bbc.com/news/business-41493494, consulté le 23 novembre 2021.

[23] Shape Security, *Attacker Economics* (2020).

[24] Akamai, *[State of the Internet]/security web attacks and gaming abuse*, (vol. 5, nº 3 | 2019).

[25] Akamai, *[State of the Internet] phishing for finance* (vol. 7, nº 2 | 2021).

[26] Shape Security, *The 2018 credential spill report* (2018) | p. 6-7 et 14.

recherche laisse entendre qu'il y a eu des améliorations au cours des trois dernières années, le délai demeure bien présent[27]. Par conséquent, les pirates ont beaucoup de temps pour exploiter les justificatifs d'identité volés.

[27] F5, « 2021 Credential Stuffing Report », https://www.f5.com/labs/articles/threat-intelligence/2021-credential-stuffing-report, consulté le 8 février 2022.

4. Une situation de plus en plus inquiétante dans le monde

La section qui suit recense les rapports des secteurs public et privé et donne des exemples de cas qui illustrent les préoccupations grandissantes des acteurs mondiaux concernant cette méthode de cyberattaque.

(a) Rapports d'organismes publics :

(i) L'**Agence de l'Union européenne pour la cybersécurité** (**ENISA**) a publié un rapport sur les principaux incidents dans l'Union européenne et dans le monde de janvier 2019 à avril 2020[28], dont on retiendra ce qui suit :

- *« […] [L]a quantité d'informations financières et d'identifiants d'utilisateur volés augmente. »*
- *« En 2019, les techniques les plus fréquemment utilisées pour lancer une cyberattaque ont été la force brute avec vol d'identifiants, l'ingénierie sociale, les erreurs de configuration et l'exploitation d'applications web. »*
- *« Chaque mois, les entreprises subissent en moyenne 12 attaques par bourrage d'identifiants (credential stuffing), au cours desquelles l'attaquant parvient à trouver des identifiants valides. »*

(ii) Le **Federal Bureau of Investigations (FBI)** des États-Unis a émis une alerte en septembre 2020[29] mettant en garde le secteur des services financiers contre les cyberrisques liés aux menaces de bourrage d'identifiants. On peut lire dans l'alerte :

- Depuis 2017, la technique avait conduit à près de 50 000 compromissions de comptes dans le secteur, ce qui a entraîné des coûts financiers pour les particuliers et les entreprises.
- Le bourrage d'identifiants a représenté le plus grand nombre d'atteintes à la sécurité contre le secteur financier, soit 41 % du total des incidents.

(iii) Le 15 septembre 2020, la **Securities and Exchange Commission's Office of Compliance Inspectors and Examinations (OIEC)** a publié une alerte au risque[30] sur le bourrage d'identifiants mettant en garde contre une augmentation de ces attaques.

(iv) Le **Centre national de cybersécurité du Royaume-Uni** a publié en novembre 2018 un avis d'alerte concernant le bourrage d'identifiants[31].

---

[28] Agence de l'Union européenne pour la cybersécurité, « Principaux incidents dans l'UE et dans le monde de janvier 2019 à avril 2020 », https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-main-incidents, consulté le 25 mai 2021.

[29] Federal Bureau of Investigation, « Private Industry Notification 20200910-001 », https://www.ic3.gov/media/news/2020/200929-1.pdf, consulté le 25 mai 2021.

[30] Office of Compliance Inspections and Examinations Officers, « Cybersecurity: Safeguarding Client Accounts against Credential Compromise », https://www.sec.gov/files/Risk%20Alert%20-%20Credential%20Compromise.pdf, consulté le 25 mai 2021.

[31] Centre national de cybersécurité du Royaume-Uni, « Use of credential stuffing tools », https://www.ncsc.gov.uk/news/use-credential-stuffing-tools, consulté le 25 mai 2021.

(b) Rapports du secteur privé :

(i) En 2019, un **rapport de Verizon sur les violations de données** a révélé que 29 % des violations impliquent l'utilisation de justificatifs d'identité volés, avec un volume élevé d'attaques par bourrage d'identifiants[32].

(ii) Selon un rapport de **Shape Security** en 2017, 2,3 milliards de justificatifs d'identité auraient été compromis. Shape Security estime les pertes financières annuelles à 300 millions de dollars, 400 millions de dollars, 1,7 milliard de dollars et 6 milliards de dollars pour les secteurs de l'aviation, de l'hôtellerie, des services bancaires aux consommateurs et de la vente au détail, respectivement[33].

(iii) La société de cybersécurité **Akamai** a dénombré 193 milliards d'attaques par bourrage d'identifiants dans le monde en 2020[34].

[32] Verizon, « 2019 Data Breach Investigations Report », https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf, consulté le 25 mai 2021.

[33] Shape Security, *The 2018 credential spill report* (2018) | p. 25.

[34] Akamai, *[State of the Internet] phishing for finance* (vol. 7, nº 2 | 2021).

5. Exemples de cas de bourrage d'identifiants

TaxSlayer

En 2017, la Commission fédérale du commerce des États-Unis (FTC) a pris des mesures contre TaxSlayer pour avoir violé les exigences relatives à la sécurité des données, ce qui a permis à des pirates d'obtenir un accès complet à près de 9 000 de ses comptes entre octobre et décembre 2015 et ainsi d'obtenir des remboursements d'impôts en remplissant des déclarations fiscales frauduleuses[35].

La FTC a constaté que TaxSlayer n'avait pas mis en œuvre des mesures d'authentification adéquates en fonction des risques, mesures qui auraient permis de réduire les risques d'attaques de pirates informatiques utilisant des justificatifs d'identité volés pour accéder aux comptes des clients de TaxSlayer, selon la plainte. À cet égard, la FTC a accusé TaxSlayer d'avoir violé la Safeguards Rule de la loi Gramm-Leach-Bliley, qui exige des institutions financières qu'elles mettent en œuvre des mesures de protection pour assurer la sécurité, la confidentialité et l'intégrité des renseignements des clients, et la Privacy Rule, qui exige des institutions financières qu'elles fournissent des avis de confidentialité aux clients[36].

Dunkin' Brands, Inc.

En 2019, le bureau du procureur général de New York a déposé une plainte[37] contre Dunkin' Brands, Inc. pour avoir omis de réagir à des cyberattaques (y compris des attaques par bourrage d'identifiants).

En 2015, une série d'attaques par bourrage d'identifiants a permis de compromettre les comptes de dizaines de milliers de clients[38]. De nombreux comptes contenaient des cartes Dunkin' sur lesquelles avaient été déposés des montants; après la compromission, ces cartes ont été revendues en ligne ou utilisées par le pirate pour effectuer des achats frauduleux. En conséquence, des dizaines de milliers de dollars ont été volés sur les cartes Dunkin'. L'enquête a révélé que Dunkin' a été mise au courant des attaques par un développeur d'applications tiers, qui a même fourni à Dunkin' une liste de près de 20 000 comptes clients qui avaient été compromis par des pirates sur une période de cinq jours. Cependant, Dunkin' n'a rien fait[39].

Les attaques se sont poursuivies au cours de l'année 2018, lorsqu'un fournisseur a informé Dunkin' qu'on avait eu accès à 300 000 comptes clients[40]. Bien que Dunkin' ait joint les clients concernés dans ce cas, elle a omis

---

[35] Commission fédérale du commerce des États-Unis (FTC), « Operator of online tax preparation service agrees to settle FTC charges that it violated financial privacy and security rules », https://www.ftc.gov/news-events/press-releases/2017/08/operator-online-tax-preparation-service-agrees-settle-ftc-charges, consulté le 25 mai 2021; FTC, Taxslayer Complaint, dossier nº C-1623063, https://www.ftc.gov/system/files/documents/cases/1623063_taxslayer_complaint.pdf, consulté le 25 mai 2021; FTC, Taxslayer Decision and Order, dossier nº C-1623063, https://www.ftc.gov/system/files/documents/cases/1623063_taxslayer_decision_and_order.pdf, consulté le 25 mai 2021.

[36] *Ibid.*

[37] *The People of the State of New York by Letitia James, Attorney General of the State of New York v Dunkin' Brands, Inc* (2019), nº de dossier de plainte 451787/2019, https://ag.ny.gov/sites/default/files/dunkin_complaint.pdf, consulté le 8 février 2022.

[38] *Ibid.*, paragr. 4.

[39] *Ibid.*, paragr. 7.

[40] *Ibid.*, paragr. 64.

de les informer que l'accès sans autorisation avait bien eu lieu et a plutôt déclaré qu'un tiers avait « tenté » sans succès[41] d'accéder à leur compte.

En 2020, Dunkin' a réglé la poursuite. Le règlement exige que Dunkin' informe les clients touchés par les attaques, réinitialise les mots de passe de ces clients et effectue des remboursements pour l'utilisation non autorisée des cartes sur lesquelles des montants avaient été versés. Dunkin' a également dû mettre en œuvre des mesures pour se protéger contre de futures attaques, respecter les procédures d'intervention en cas d'attaque et payer 650 000 $ d'amende et de frais à l'État de New York[42].

Uber

En 2018, Uber a été condamnée à une amende de 385 000 livres sterling par le Commissariat à l'information du Royaume-Uni (ICO) pour ne pas avoir protégé les informations personnelles de ses clients contre une attaque par bourrage d'identifiants en octobre et novembre 2016[43]. L'ICO a confirmé qu'un certain nombre de failles évitables dans la sécurité des données avaient permis aux pirates d'exposer les données personnelles de 2,7 millions de clients britanniques, y compris les noms complets, courriels et numéros de téléphone, ainsi que les dossiers d'environ 82 000 coursiers britanniques, y compris les détails des paiements et des itinéraires[44]. Au cours de l'enquête de l'ICO, il a été établi qu'Uber n'avait pas informé ses clients pendant plus d'un an, car elle avait payé les pirates 100 000 $ pour détruire les données qu'ils avaient obtenues[45].

[41] *Ibid.*, paragr. 68.

[42] *The People of the State of New York by Letitia James, Attorney General of the State of New York v Dunkin' Brands, Inc* (2020), jugement et ordonnance sur consentement nº 451787/2019, paragr. 4 à 19, https://ag.ny.gov/sites/default/files/proposed_consent_order_and_judgment.pdf, consulté le 8 février 2022.

[43] Commissariat à l'information du Royaume-Uni, « ICO fines Uber £385,000 over data protection failings », https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/11/ico-fines-uber-385-000-over-data-protection-failings/, consulté le 25 mai 2021.

[44] *Ibid.*

[45] *Ibid.*

6. La sécurité des données dans la législation sur la protection des données et de la vie privée

Les exigences en matière de sécurité des données prévues par la législation sur la protection des données et de la vie privée sont souvent génériques et ne comprennent pas d'exigences spécifiques pour la protection des données contre le bourrage d'identifiants. Par exemple, le règlement général de l'Union européenne sur la protection des données 2016/679 précise que les organisations doivent traiter les données « *de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle […]* »[46]. La Safeguards Rule aux États-Unis fait référence à la mise en œuvre de mesures de protection administratives, techniques et physiques adaptées à la taille, à la complexité, à la nature et à la portée des activités ainsi qu'au caractère sensible des renseignements des clients en cause et visant à protéger contre tout accès non autorisé[47].

Les deux exemples font référence à la mise en œuvre d'une sécurité appropriée et à la protection contre les traitements/accès non autorisés. Compte tenu de la menace évidente que les attaques par bourrage d'identifiants font peser sur les données à caractère personnel (en particulier pour les organisations dont les comptes d'utilisateurs sont accessibles en ligne) et du traitement/de l'accès non autorisé qui pourrait en résulter, la mise en œuvre de mesures visant à protéger les données à caractère personnel contre les attaques par bourrage d'identifiants sera généralement requise, au moins implicitement, aux termes des lois sur la protection des données et de la vie privée. Les mesures indiquées dans les présentes lignes directrices ne constituent pas des exigences légales, mais peuvent aider les organisations à respecter leurs obligations légales où qu'elles soient.

Nonobstant les exigences génériques susmentionnées, des réglementations plus spécifiques sont possibles pour répondre à des problèmes de sécurité particuliers. Par exemple, la Commission fédérale du commerce a mis à jour la Safeguards Rule en 2021 qui, entre autres modifications, contient maintenant des exigences plus détaillées sur les mesures de protection qui doivent être mises en œuvre par les institutions financières pour protéger les données personnelles contre les cyberattaques. Il s'agit notamment de l'adoption d'une authentification multifactorielle, de contrôles d'accès, du chiffrage et de la désignation d'une personne qualifiée chargée de superviser, de mettre en œuvre et de renforcer le programme de sécurité informatique d'une organisation[48].

[46] Article 5(1)f) du règlement général sur la protection des données (https://eur-lex.europa.eu/eli/reg/2016/679/oj, consulté le 25 mai 2021).

[47] Electronic Code of Federal Regulations, Safeguards Rule (article 314), Standards for safeguarding customer information (https://www.ecfr.gov/current/title-16/part-314, consulté le 22 novembre 2021).

[48] *Ibid.*

7. Mesures de détection, de prévention et d'atténuation du risque de bourrage d'identifiants

Après avoir reconnu et établi la menace que représentent les attaques par bourrage d'identifiants pour les données personnelles, une menace devenue réalité inévitable pour de nombreuses organisations, les organisations doivent mettre en œuvre des mesures pour atténuer les risques de ces attaques et ceux qui en découlent.

La nature d'une attaque par bourrage d'identifiants (c'est-à-dire qu'un acteur malveillant utilise des justificatifs d'identité valides) peut rendre difficile pour les organisations de défendre efficacement leurs clients contre de telles attaques. Toutefois, plusieurs mesures peuvent être mises en œuvre pour tenter de détecter, de prévenir et d'atténuer le risque d'attaques par bourrage d'identifiants. La présente section comprend une liste de mesures reconnues comme utiles et recommandées pour atténuer les risques liés au bourrage d'identifiants.

Cette liste peut servir de guide aux organisations quant aux mesures qu'elles devraient envisager pour se protéger contre le bourrage d'identifiants. De même, la liste peut également servir de point de référence utile aux autorités pour évaluer les mesures prises par une organisation pour se protéger contre le bourrage d'identifiants. Toutefois, la législation relative à la protection des données et de la vie privée est généralement souple dans la mesure où elle adopte souvent une approche fondée sur le risque[49] en matière de sécurité. On n'attend donc pas nécessairement d'une organisation qu'elle mette en œuvre toutes les mesures expliquées plus en détail ci-dessous, car chaque activité est différente et nécessitera des approches ou des niveaux de sécurité différents. Il est important qu'une organisation soit en mesure de démontrer qu'elle dispose de mesures appropriées et efficaces et qu'elle puisse justifier les décisions de ne pas mettre en œuvre des mesures reconnues pour se protéger contre le bourrage d'identifiants.

(a) Achats à titre d'invité

Le site Web d'une organisation pourrait permettre de faire des achats à titre d'invité. Ainsi, les personnes pourraient utiliser le service sans avoir à créer un compte, ce qui réduirait le risque de réutilisation de justificatifs d'identité et de cyberattaques par bourrage d'identifiants.

(b) Mots de passe

Dans un contexte de croissance continue des services en ligne qui exigent de créer des comptes en ligne, les gens ont tendance à réutiliser les mêmes combinaisons de nom d'utilisateur et de mot de passe sur plusieurs comptes. C'est de cette habitude que profitent les cybercriminels pour mener à bien des attaques par bourrage d'identifiants. Lorsqu'elles envisagent l'application d'un système de mots de passe, les organisations doivent tenir compte de diverses considérations, notamment :

(i) Protection par mot de passe[50]

[49] Par exemple, l'article 32 du règlement général sur la protection des données et le considérant 76 sur l'évaluation des risques (https://eur-lex.europa.eu/eli/reg/2016/679/oj, consulté le 25 mai 2021).

[50] Office of Compliance Inspections and Examinations Officers, « Cybersecurity: safeguarding client accounts against credential compromise », https://www.sec.gov/files/Risk%20Alert%20-%20Credential%20Compromise.pdf, consulté le 25 mai 2021.

Les mots de passe ne doivent jamais être stockés en clair, et il convient plutôt de mettre en œuvre un algorithme de hachage de mot de passe spécialement conçu pour stocker les mots de passe en toute sécurité[51]. Il est important de noter que les mots de passe doivent être hachés plutôt que chiffrés, car il est extrêmement difficile (voire impossible) d'inverser un hachage et de révéler le texte original, alors que le chiffrage est une fonction bidirectionnelle qui devient futile si la clé de déchiffrage n'est pas sécurisée.

Bien qu'un hachage soit généralement irréversible, il est possible, dans certaines circonstances, de pirater[52] un hachage et d'exposer le mot de passe. Par conséquent, les applications doivent effectuer le salage[53] d'un mot de passe avant de le hacher. Il devient alors plus difficile pour un pirate d'accéder aux justificatifs d'identité d'un utilisateur, car le salage est unique pour chaque utilisateur, ce qui oblige le pirate à craquer un hachage à la fois et augmente considérablement le temps et les efforts nécessaires.

Il est important que les organisations revoient régulièrement l'algorithme de hachage qu'elles décident d'utiliser, car ces techniques peuvent rapidement devenir obsolètes, et donc moins sûres, compte tenu des progrès rapides de la technologie. Les organisations doivent remplacer tous les algorithmes de hachage qui deviennent obsolètes afin d'empêcher l'exploitation de toute faille de sécurité.

(ii) Application de politiques de mots de passe robustes[54]

Lors de la mise en place d'un système de mots de passe, il faut tenir compte de trois exigences :

(1) Longueur du mot de passe – Pour éviter les mots de passe trop courts et faibles, il est bon d'exiger une longueur minimum. Le nombre de caractères maximal, qui n'est pas obligatoire d'ailleurs, ne doit pas être trop bas, afin que les utilisateurs créent des mots de passe ou des phrases de passe plus longs.

(2) Caractères spéciaux – Les utilisateurs doivent être autorisés à inclure des caractères spéciaux. Toutefois, les utilisateurs ne devraient pas être **obligés** de le faire, car les mots de passe deviennent ainsi difficiles à mémoriser, ce qui peut encourager la réutilisation des mêmes mots de passe[55].

[51] Commissariat à l'information du Royaume-Uni, « Passwords in online services », https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/passwords-in-online-services/, consulté le 25 mai 2021.

[52] Un hachage est piraté lorsqu'on devine ce que pourrait être le mot de passe, puis on compare le hachage du mot deviné avec le hachage réel. S'ils correspondent, on considère que le hachage a été piraté.

[53] Le salage est une séquence de caractères unique, générée de manière aléatoire, qui est ajoutée à chaque mot de passe dans le cadre du processus de hachage.

[54] Office of Compliance Inspections and Examinations Officers, « Cybersecurity: safeguarding client accounts against credential compromise », https://www.sec.gov/files/Risk%20Alert%20-%20Credential%20Compromise.pdf, consulté le 25 mai 2021); Autorité norvégienne de sécurité nationale, « Passordanbefalinger fra Nasjonal sikkerhetsmyndighet », https://nsm.no/aktuelt/passordanbefalinger-fra-nasjonal-sikkerhetsmyndighet, consulté le 27 avril 2022.

[55] Centre national de cybersécurité du Royaume-Uni, « Password administration for system owners », https://www.ncsc.gov.uk/collection/passwords/updating-your-approach, consulté le 25 mai 2021.

(3) Listes de refus de mots de passe – Une liste de refus empêche les utilisateurs de créer un mot de passe communément utilisé, et donc facile à deviner ou faible, par exemple :

- les mots de passe révélés par des violations antérieures (voir la section sur la divulgation de mots de passe piratés);
- des caractères répétitifs ou séquentiels (comme 12345);
- des mots ou des expressions qui se rapportent au service (comme « paie » comme mot de passe pour ouvrir une session dans une application de paie du personnel).

Les organisations peuvent intégrer une liste de refus de mots de passe dans leur logiciel ou créer la leur en se procurant des listes publiées de mots de passe courants sur des sites Web accessibles au public[56].

(iii) Informer et aider les utilisateurs[57]

Les utilisateurs trouvent souvent qu'il est difficile de créer et de mémoriser des mots de passe. Les organisations doivent aider leurs utilisateurs et leur fournir des conseils à cet effet.

Lors de la création de tout nouveau compte nécessitant un mot de passe, les utilisateurs doivent être informés des risques liés à l'utilisation d'un même mot de passe sur plusieurs sites, et notamment de l'importance d'éviter d'utiliser des mots de passe faciles à deviner, comme des noms, des animaux domestiques ou des équipes sportives.

Les organisations peuvent également recommander la technique du NCSC consistant à utiliser trois mots aléatoires, qui est considérée comme un compromis entre la sécurité et la convivialité, car elle consiste à choisir trois mots aléatoires mémorisables pour un utilisateur, mais difficiles à deviner pour un pirate[58]. Il est important que ces mots soient complètement aléatoires, comme « thémaisonpoisson », et non des expressions courantes, des citations célèbres, des paroles de chansons ou des suites prévisibles comme « undeuxtrois »[59].

Les organisations peuvent également recommander l'utilisation d'un gestionnaire de mots de passe[60] qui non seulement crée des mots de passe forts et uniques, mais fait également office de coffre-fort pour les mots de passe en stockant les justificatifs d'identité pour plusieurs sites Web, applications et services[61]. En particulier, lorsque des justificatifs d'identification à privilèges élevés sont utilisés, il convient d'utiliser un coffre-fort de mots de passe robuste,

---

[56] Par exemple www.haveibeenpwned.com, consulté le 25 mai 2021.

[57] Centre national de cybersécurité du Royaume-Uni, « Password administration for system owners », https://www.ncsc.gov.uk/collection/passwords/updating-your-approach, consulté le 25 mai 2021; Office of Compliance Inspections and Examinations Officers, « Cybersecurity: safeguarding client accounts against credential compromise », https://www.sec.gov/files/Risk%20Alert%20-%20Credential%20Compromise.pdf, consulté le 25 mai 2021.

[58] Centre national de cybersécurité du Royaume-Uni, « Three random words or #thinkrandom », https://www.ncsc.gov.uk/blog-post/three-random-words-or-thinkrandom-0, consulté le 27 mai 2021.

[59] *Ibid.*

[60] Centre canadien pour la cybersécurité, « Conseils de sécurité sur les gestionnaires de mots de passe », https://cyber.gc.ca/fr/orientation/conseils-de-securite-sur-les-gestionnaires-de-mots-de-passeitsap30025, consulté le 27 mai 2021.

[61] Bien que les gestionnaires de mots de passe soient utiles pour composer avec l'excès de mots de passe, ils comportent également des risques. En effet, si un pirate parvient à accéder au gestionnaire de mots de passe, tous les mots de passe qui y sont stockés seront compromis.

soit une solution de gestion des accès avec privilège. La solution de gestion des accès avec privilège exige une authentification supplémentaire et permet de mieux contrôler l'accès et les autorisations pour les comptes, les processus et les systèmes, ce qui peut atténuer le risque d'attaques externes et de méfaits internes[62].

Les organisations qui autorisent l'utilisation de gestionnaires de mots de passe doivent s'assurer que leur utilisation est prise en charge sur toutes les plateformes actuelles et prévues et qu'elle est compatible avec tous les navigateurs actuels et prévus. Les gestionnaires de mots de passe qui ne sont pas compatibles avec certains appareils peuvent obliger les utilisateurs à recourir à une autre méthode de gestion des mots de passe moins sûre.

(iv) Autres considérations

En dehors de ce qui précède, les utilisateurs ne devraient pas être davantage limités lors de la création d'un mot de passe, car les effets pourraient être négatifs[63]. Par exemple, le fait d'imposer des changements réguliers de mot de passe peut entraîner des changements prévisibles, comme l'augmentation séquentielle d'un nombre, par exemple de *MathieuDubois1* à *MathieuDubois2.* Un utilisateur pourrait aussi remplacer son mot de passe initial fort par une série de mots de passe plus faibles. À cet égard, il est recommandé de n'exiger la réinitialisation du mot de passe qu'en cas de violation de données ayant pu compromettre un compte, ou à la réception d'autres informations laissant entendre une violation[64].

En remplacement du changement régulier de mots de passe, on pourrait « verrouiller » automatiquement les comptes inactifs pendant une période donnée et encourager les utilisateurs à joindre directement l'organisation s'ils ont remarqué une activité suspecte sur leur compte.

(c) Solutions de rechange aux mots de passe[65]

Avant de mettre en place un système basé sur des mots de passe, il est important de voir si un tel système est approprié ou s'il existe d'autres solutions. L'une de ces autres solutions serait un système d'authentification unique, qui est souvent un portail Web permettant aux utilisateurs de saisir des justificatifs d'identité pour accéder à plusieurs applications et services.

Un système d'authentification unique peut être utile pour réduire le nombre de mots de passe qu'un utilisateur doit créer et retenir. Toutefois, si le système est compromis, le pirate aurait accès à **tous** les systèmes et services et pourrait être en mesure d'exploiter beaucoup plus de renseignements. À cet égard, si une organisation décide de mettre en œuvre un tel système, une authentification multifactorielle devrait être une exigence pour tous les comptes d'utilisateurs.

---

[62] Centre national de cybersécurité du Royaume-Uni, « Secure system administration: Use privileged access management », https://www.ncsc.gov.uk/collection/secure-system-administration/use-privileged-access-management, consulté le 8 février 2022.

[63] Commissariat à l'information du Royaume-Uni, « Passwords in online services », https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/passwords-in-online-services/, consulté le 25 mai 2021.

[64] *Ibid.*

[65] *Ibid.*

Une autre solution consiste à mettre en œuvre des fonctions telles que le masquage du courriel. L'utilisateur peut ainsi créer des comptes sur une application ou un site Web en utilisant des courriels uniques et aléatoires qui transfèrent automatiquement tous les messages reçus vers la boîte de réception personnelle de l'utilisateur. L'utilisateur peut lire ces messages et y répondre directement tout en masquant son courriel personnel.

(d) Authentification multifactorielle

L'authentification multifactorielle est le fait d'exiger plus d'un facteur d'identification pour qu'une personne puisse accéder à son compte. Elle est considérée comme la mesure la plus efficace pour protéger les comptes en ligne contre le bourrage d'identifiants, car le pirate doit entrer d'autres facteurs même s'il a le mot de passe entre les mains[66]. Selon une analyse de Microsoft, l'authentification multifactorielle mettrait fin à la quasi-totalité des compromissions de comptes liées à des attaques par bourrage d'identifiants[67].

En plus d'empêcher l'accès initial, l'authentification multifactorielle peut empêcher un pirate de creuser **plus loin**, s'il infiltre un réseau interne. C'est ce qu'on appelle le « mouvement latéral »[68] : il s'agit des techniques déployées par un pirate pour naviguer dans un réseau ou obtenir un accès privilégié en se faisant passer pour un utilisateur légitime. Une fois à l'intérieur d'un réseau compromis, le pirate peut vouloir s'approprier un contrôleur de domaine, saboter un système essentiel ou exfiltrer des données personnelles sensibles ou importantes. Même si une telle activité peut être difficile à détecter, car elle semble normale, la mise en place d'une authentification multifactorielle pour l'accès aux systèmes, applications et données internes peut limiter, voire empêcher, les mouvements latéraux[69].

En général, les facteurs supplémentaires représenteront quelque chose que l'utilisateur a en sa *possession* et peuvent nécessiter une empreinte biométrique (comme une empreinte digitale) ou la saisie d'un code de passe qui a été envoyé à une autre voie de communication (courriel, numéro de téléphone ou appareil secondaire)[70]. En outre, il existe d'autres dispositifs tels que les cartes à puce ou les jetons qui authentifient un utilisateur en générant un NIP à usage unique à saisir ou qui contiennent une puce authentifiée par le système[71].

Compte tenu de la menace que représentent les attaques par bourrage d'identifiants pour les données personnelles, de son perfectionnement et du coût relativement faible de sa mise en œuvre, l'authentification multifactorielle devrait être considérée comme une mesure de sécurité essentielle. Bien que l'authentification multifactorielle ne soit pas pratique dans toutes les situations, elle doit être mise en œuvre chaque fois que possible. Dans certains cas, l'authentification multifactorielle peut

---

[66] Centre national de cybersécurité du Royaume-Uni, « Top tips for staying secure online », https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/activate-two-factor-authentication-on-your-email, consulté le 25 mai 2021.

[67] Microsoft, « Your Pa$$word doesn't matter », https://techcommunity.microsoft.com/t5/azure-active-directory-identity/your-pa-word-doesn-t-matter/ba-p/731984, consulté le 25 mai 2021.

[68] Centre national de cybersécurité du Royaume-Uni, « Preventing lateral movement », https://www.ncsc.gov.uk/guidance/preventing-lateral-movement, consulté le 15 octobre 2021.

[69] *Ibid.*

[70] Commission irlandaise de protection des données, « Know your obligations - data security », https://www.dataprotection.ie/en/organisations/know-your-obligations/data-security-guidance, consulté le 25 mai 2021.

[71] *Ibid.*

être facultative, mais pour tous les comptes qui contiennent des informations sensibles, ou les comptes externes sur le nuage, elle devrait être obligatoire[72].

En plus de proposer l'option ou d'imposer l'utilisation de l'authentification multifactorielle à la création du compte, les organisations peuvent également activer l'authentification multifactorielle basée sur les risques pour mettre en œuvre une approche d'équilibre entre sécurité et convivialité, l'authentification multifactorielle étant déclenchée en cas de comportement suspect, par exemple une session ouverte depuis[73] :

- un nouveau navigateur, un nouvel appareil ou une nouvelle adresse IP;
- un pays ou un lieu inhabituel;
- un pays considéré comme non digne de confiance;
- une adresse IP qui figure sur les listes de blocage connues;
- une adresse IP avec laquelle des tentatives d'ouverture de session dans plusieurs comptes ont été faites;
- une tentative d'ouverture de session qui semble être programmée plutôt que manuelle.

Il existe de nombreuses formes d'authentifications multifactorielles et il est important de reconnaître les différences entre elles et de bien savoir comment les mettre en œuvre. Des évaluations doivent avoir lieu régulièrement pour s'assurer que les authentifications sont efficaces contre les pirates.

(e) Mots de passe et NIP secondaires[74]

Les utilisateurs peuvent être invités à fournir des informations de sécurité supplémentaires, par exemple un NIP ou des caractères spécifiques d'un mot de passe secondaire. C'est là une couche supplémentaire de protection lorsque l'authentification multifactorielle ne peut être mise en œuvre.

(f) Empreinte digitale d'appareil[75]

Divers attributs visibles à la connexion d'un appareil peuvent être utilisés pour prendre l'empreinte d'un appareil, par exemple le système d'exploitation, le navigateur et la langue (qui peuvent être obtenus à partir des en-têtes HTTP). D'autres caractéristiques telles que la résolution de l'écran, les polices installées et les plugiciels du navigateur peuvent être obtenues à l'aide de JavaScript. L'empreinte digitale d'appareil peut alors servir à signaler une connexion provenant d'un appareil

---

[72] Centre national de cybersécurité du Royaume-Uni, « Multi-factor authentication for online services », https://www.ncsc.gov.uk/guidance/multi-factor-authentication-online-services, consulté le 25 mai 2021.

[73] Open Web Security Project Foundation, « Credential Stuffing Prevention Cheat Sheet », https://cheatsheetseries.owasp.org/cheatsheets/Credential_Stuffing_Prevention_Cheat_Sheet.html, consulté le 25 mai 2021.

[74] *Ibid.*

[75] *Ibid.*; Office of Compliance Inspections and Examinations Officers, « Cybersecurity: safeguarding client accounts against credential compromise », https://www.sec.gov/files/Risk%20Alert%20-%20Credential%20Compromise.pdf, consulté le 25 mai 2021; Centre national de cybersécurité du Royaume-Uni, « Use of credential stuffing tools », https://www.ncsc.gov.uk/news/use-credential-stuffing-tools, consulté le 25 mai 2021.

inconnu ou suspect. Des mesures supplémentaires peuvent alors être prises s'il y a tentative par un pirate.

(g) Noms d'utilisateurs imprévisibles[76]

Les attaques par bourrage d'identifiants utilisent à la fois le mot de passe et le nom d'utilisateur. Les sites Web utilisent généralement le courriel comme nom d'utilisateur et, comme la plupart des utilisateurs ont un seul courriel qu'ils utilisent pour tous leurs comptes, la combinaison courriel et mot de passe rend particulièrement faciles les attaques par bourrage d'identifiants.

En exigeant des utilisateurs qu'ils créent leur propre nom d'utilisateur lorsqu'ils s'inscrivent sur le site Web, il devient plus difficile pour un pirate d'obtenir des paires de noms d'utilisateur et de mots de passe valides pour le bourrage d'identifiants. Le fait de fournir à l'utilisateur un nom d'utilisateur généré automatiquement ou des conseils sur la façon de créer un nom d'utilisateur personnalisé peut offrir un degré de protection accru (car les utilisateurs sont susceptibles de choisir le même nom d'utilisateur sur la plupart des sites Web). Il faut toutefois veiller à ce que le nom d'utilisateur généré ne soit pas prévisible (c'est le cas par exemple s'il est basé sur le nom complet de l'utilisateur ou sur des identifiants numériques séquentiels) et qu'il ne soit pas si complexe que l'utilisateur soit incapable de s'en souvenir, car la chose pourrait causer de la frustration et démotiver l'utilisateur d'utiliser le service.

(h) Identification des mots de passe qui ont fait l'objet d'une fuite[77]

Le mot de passe choisi par un nouvel utilisateur peut non seulement être comparé à une liste de mots de passe faibles connus, mais aussi à des mots de passe qui ont déjà fait l'objet d'une fuite. Pwned Passwords est un bon exemple de service fournissant de telles listes[78].

(i) Limitation du débit[79]

Il s'agit d'une mesure de sécurité conçue pour limiter le nombre et la fréquence des échecs multiples de tentatives de connexion de la manière suivante :

- limitation du nombre de connexions à partir d'une même adresse IP. Si plusieurs connexions sont établies à partir d'une même adresse IP, ce peut être le signe d'une cyberattaque en cours et, par conséquent, limiter ces connexions peut contribuer à bloquer l'attaque;

- limitation du nombre de tentatives de connexion infructueuses au cours d'une période donnée, également appelée *verrouillage de compte*, qui consiste à geler le compte d'un utilisateur pendant une période déterminée ou jusqu'à ce que l'utilisateur légitime communique avec

[76] Open Web Security Project Foundation, « Credential Stuffing Prevention Cheat Sheet », https://cheatsheetseries.owasp.org/cheatsheets/Credential_Stuffing_Prevention_Cheat_Sheet.html, consulté le 25 mai 2021.

[77] *Ibid.*; Centre national de cybersécurité du Royaume-Uni, « Use of credential stuffing tools », https://www.ncsc.gov.uk/news/use-credential-stuffing-tools, consulté le 25 mai 2021; Office of Compliance Inspections and Examinations Officers, « Cybersecurity: safeguarding client accounts against credential compromise », https://www.sec.gov/files/Risk%20Alert%20-%20Credential%20Compromise.pdf, consulté le 25 mai 2021.

[78] « Pwned Passwords », https://haveibeenpwned.com/Passwords, consulté le 25 mai 2021.

[79] Institut national des normes et des technologies des États-Unis, « Digital Identity Guidelines », https://pages.nist.gov/800-63-3/sp800-63b.html#throttle, consulté le 25 mai 2021.

l'organisation pour réinitialiser son compte. Si vous avez recours à cette méthode, il est recommandé de permettre de 5 à 10 tentatives de connexion[80] afin d'éviter qu'un utilisateur légitime ne verrouille accidentellement son compte. Les organisations peuvent envisager des algorithmes de réémission exponentielle pour gérer et limiter les tentatives de connexion et les verrouillages.

(j) Page et processus d'ouverture de session[81]

La plupart des outils offerts sur le marché sont conçus pour un processus d'ouverture de session en une seule étape, où les justificatifs d'identité sont envoyés au serveur et où la réponse indique si la tentative de connexion a réussi ou non. L'ajout d'étapes à ce processus, comme l'obligation de saisir séquentiellement le nom d'utilisateur et le mot de passe, ou l'obligation pour l'utilisateur d'obtenir d'abord un jeton CSRF[82] aléatoire avant de pouvoir ouvrir une session, rend l'attaque légèrement plus difficile à réaliser et double le nombre de requêtes que doit effectuer le pirate.

Étant donné que de nombreux outils de bourrage d'identifiants nécessitent des fichiers de configuration particuliers, il est possible de les neutraliser en apportant de petites modifications aux pages d'ouverture de session une fois qu'elles sont détectées.

(k) Surveillance de compte et détection[83]

La surveillance des comptes est souvent effectuée parallèlement à la limitation du débit ou au verrouillage des comptes afin de détecter tout comportement anormal qui pourrait être le signe d'une attaque. Les organisations doivent établir, maintenir et revoir ce qui constitue des signes d'activité suspecte :

- plusieurs tentatives d'ouverture de session échouées sur plusieurs comptes;
- un volume plus élevé que d'habitude d'adresses IP étrangères;
- des anomalies dans l'activité du navigateur, comme les navigateurs sans interface graphique ou les navigateurs dépourvus de moteurs d'exécution JavaScript[84];

---

[80] Centre national de cybersécurité du Royaume-Uni, « Password administration for system owners », https://www.ncsc.gov.uk/collection/passwords/updating-your-approach, consulté le 25 mai 2021.

[81] Open Web Security Project Foundation, « Credential Stuffing Prevention Cheat Sheet », https://cheatsheetseries.owasp.org/cheatsheets/Credential_Stuffing_Prevention_Cheat_Sheet.html, consulté le 25 mai 2021; Centre national de cybersécurité du Royaume-Uni, « Use of credential stuffing tools », https://www.ncsc.gov.uk/news/use-credential-stuffing-tools, consulté le 25 mai 2021.

[82] Open Web Security Project Foundation, « Cross-Site Request Forgery Prevention Cheat Sheet », https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html, consulté le 25 mai 2021.

[83] *Ibid.*; Office of Compliance Inspections and Examinations Officers, « Cybersecurity: safeguarding client accounts against credential compromise », https://www.sec.gov/files/Risk%20Alert%20-%20Credential%20Compromise.pdf, consulté le 25 mai 2021; Centre national de cybersécurité du Royaume-Uni, « Use of credential stuffing tools », https://www.ncsc.gov.uk/news/use-credential-stuffing-tools, consulté le 25 mai 2021.

[84] Bureau of Internet and Technology du bureau du procureur général de l'État de New York, « Business Guide for Credential Stuffing Attacks », https://ag.ny.gov/sites/default/files/businessguide-credentialstuffingattacks.pdf, consulté le 27 janvier 2022.

- la forme des tentatives d'ouverture de session qui indiquent l'utilisation potentielle de l'automatisation;

- des échecs de tentatives d'ouverture de session à la deuxième étape d'une authentification multifactorielle;

- des tentatives d'ouverture de session à partir d'adresses IP inhabituelles, y compris les tentatives provenant de fournisseurs de serveurs privés virtuels, comme Amazon Web Service ou des centres de données commerciaux[85];

- un nombre inhabituellement élevé de verrouillages de comptes.

La liste ci-dessus ne doit pas être considérée comme définitive, car, par exemple, une tentative de connexion à partir d'une adresse IP inhabituelle n'est pas toujours le signe d'une attaque et peut simplement indiquer qu'un utilisateur est parti en vacances ou utilise un réseau privé virtuel[86].

Les organisations devraient préférablement avoir recours à des analyses avancées en utilisant notamment l'historique des données de connexion, la localisation et l'empreinte digitale des appareils pour juger de la crédibilité d'une demande d'ouverture de session.

Pour la plupart des organisations, il est recommandé d'automatiser au moins partiellement la surveillance des comptes pour obtenir des données fiables et comparables et assurer une surveillance 24 heures sur 24[87].

(l) Contrôles supplémentaires pour les réseaux d'anonymat[88]

Les réseaux d'anonymat tels que TOR facilitent la communication anonyme en dissimulant l'adresse IP de l'utilisateur par chiffrage et une série de connexions anonymes et privées. Bien que ces réseaux puissent s'utiliser de manière légitime, le trafic peut également être considérablement malveillant[89]. Par conséquent, des contrôles supplémentaires doivent être effectués sur les tentatives d'authentification provenant de ces réseaux[90].

(m) CAPTCHA[91]

---

[85] Bureau of Internet and Technology du bureau du procureur général de l'État de New York, « Business Guide for Credential Stuffing Attacks », https://ag.ny.gov/sites/default/files/businessguide-credentialstuffingattacks.pdf, consulté le 27 janvier 2022.

[86] Un réseau privé virtuel permet aux utilisateurs à distance d'accéder en toute sécurité aux services d'une organisation.

[87] Bureau of Internet and Technology du bureau du procureur général de l'État de New York, « Business Guide for Credential Stuffing Attacks », https://ag.ny.gov/sites/default/files/businessguide-credentialstuffingattacks.pdf, consulté le 27 janvier 2022.

[88] Centre national de cybersécurité du Royaume-Uni, « Use of credential stuffing tools », https://www.ncsc.gov.uk/news/use-credential-stuffing-tools, consulté le 25 mai 2021.

[89] *Ibid.*

[90] *Ibid.*

[91] Open Web Security Project Foundation, « Credential Stuffing Prevention Cheat Sheet », https://cheatsheetseries.owasp.org/cheatsheets/Credential_Stuffing_Prevention_Cheat_Sheet.html, consulté le 25 mai 2021; Office of Compliance Inspections and Examinations Officers, « Cybersecurity: safeguarding client accounts

Les CAPTCHA sont des énigmes ou de petites tâches à effectuer avant d'accéder à un compte. Ils sont souvent utilisés comme mécanisme de défense contre les cyberattaques, car on suppose que seul un humain sera capable de répondre à la question ou d'effectuer la tâche de sélectionner ou de cocher souvent certaines parties d'une grille de grande taille. Malheureusement, les CAPTCHA ne parviennent pas toujours à empêcher une attaque par bourrage d'identifiants en raison de l'utilisation d'usines à CAPTCHA et des progrès des logiciels qui peuvent reconnaître et résoudre les CAPTCHA[92]. À cet égard, l'utilisation de CAPTCHA ne doit être envisagée que comme **une** composante du régime de sécurité d'une organisation.

Pour en accroître l'efficacité, les CAPTCHA peuvent être adoptés de manière à ce qu'ils ne soient requis que lorsque la demande d'ouverture de session est considérée comme suspecte (voir la section sur l'authentification multifactorielle).

(n) Pare-feu d'applications Web[93]

Un pare-feu est essentiel lorsqu'on doit sortir de son réseau pour se brancher à d'autres réseaux et à Internet, par exemple. Un pare-feu d'applications Web correctement configuré peut se révéler essentiel pour bloquer une attaque par bourrage d'identifiants, car il peut détecter et empêcher l'utilisation de programmes automatisés et de bots avancés. Il peut également détecter si des justificatifs d'identité volés sont utilisés lors d'une tentative d'ouverture de session en comparant les noms d'utilisateur et les mots de passe à une liste connue de justificatifs compromis. Les organisations peuvent ainsi se préparer à une éventuelle attaque par bourrage d'identifiants en surveillant les cas où plusieurs tentatives de connexion ont échoué.

En raison de l'augmentation de la dépendance des organisations et des individus à l'égard des connexions Internet permanentes, les pare-feu sont de la plus haute importance compte tenu de l'exposition accrue aux cyberattaques.

(o) Liste de blocage d'adresses IP[94]

Une liste de blocage entraîne le refus d'accès des adresses IP qui y sont indiquées, par exemple des adresses IP liées à une activité en ligne malveillante, comme la participation à un botnet. Cette liste de blocage sera téléchargée dans un pare-feu d'applications Web, et toute tentative d'ouverture de session effectuée à partir d'une adresse IP de la liste sera alors bloquée. Cependant, il est important de noter que la liste de blocage peut parfois être inefficace contre les attaques par bourrage d'identifiants, car les pirates utilisent des botnets pour distribuer le trafic à partir de différentes adresses IP afin d'apparaître comme un utilisateur légitime. À cet égard, même si une adresse IP figure

---

against credential compromise », https://www.sec.gov/files/Risk%20Alert%20-%20Credential%20Compromise.pdf, consulté le 25 mai 2021.

[92] Open Web Security Project Foundation, « Credential Stuffing Prevention Cheat Sheet », https://cheatsheetseries.owasp.org/cheatsheets/Credential_Stuffing_Prevention_Cheat_Sheet.html, consulté le 25 mai 2021.

[93] Office of Compliance Inspections and Examinations Officers, « Cybersecurity: safeguarding client accounts against credential compromise », https://www.sec.gov/files/Risk%20Alert%20-%20Credential%20Compromise.pdf, consulté le 25 mai 2021.

[94] Open Web Security Project Foundation, « Credential Stuffing Prevention Cheat Sheet », https://cheatsheetseries.owasp.org/cheatsheets/Credential_Stuffing_Prevention_Cheat_Sheet.html, consulté le 25 mai 2021.

sur la liste de blocage, si un pirate utilise 100 adresses IP, il lui restera toujours 99 tentatives pour contourner cette mesure.

(p) Liste d'autorisation de bonnes adresses IP

À l'opposé de la liste de blocage, la liste d'autorisation consiste à indiquer les adresses IP de confiance qui seront chargées dans un pare-feu d'applications Web et pour lesquelles un accès sera accordé, tandis que toute adresse IP qui n'a pas été incluse dans la liste se verra refuser l'accès. La liste d'autorisation peut être moins efficace que la liste de blocage pour les comptes d'utilisateurs standards, car la plupart des connexions Internet domestiques utilisent des adresses IP dynamiques, ce qui signifie qu'au fil du temps, les utilisateurs accèdent à leur compte à partir de différentes adresses IP qui, si elles ne figurent pas dans la liste d'autorisation, aboutiraient à un refus d'accès.

(q) Plans de réponse aux incidents et notifications aux utilisateurs[95]

Lorsqu'une activité suspecte est détectée, il peut être utile d'avertir l'utilisateur.

Il faut toutefois veiller à ne pas submerger les utilisateurs de notifications, car ils pourraient commencer à les ignorer ou à les supprimer. À cet égard, il ne serait pas utile d'informer un utilisateur de l'échec d'une seule tentative d'ouverture de session, car il pourrait s'agir simplement d'un utilisateur légitime qui a oublié son mot de passe ou l'a mal orthographié. Toutefois, si une activité inhabituelle a été détectée sur un compte, par exemple si un mot de passe a été correctement saisi alors qu'un autre facteur d'une authentification multifactorielle a échoué, il convient de communiquer avec l'utilisateur dès que possible afin qu'il puisse changer son mot de passe et, surtout, pour lui permettre de changer les mots de passe de tout autre compte sécurisé avec les mêmes justificatifs d'identité afin d'éviter de nouvelles attaques.

Les utilisateurs doivent également recevoir des informations sur les connexions récentes à leurs comptes telles que la date, l'heure et le lieu des tentatives d'ouverture de session précédentes, et, dans la mesure du possible, les utilisateurs doivent pouvoir visualiser toutes les sessions actives et mettre fin à celles qui sont illégitimes[96].

Dans certaines circonstances, la loi existante peut imposer la méthode, le contenu et le moment de la notification, en fonction des conséquences des attaques par bourrage d'identifiants. Le présent guide doit être interprété d'une manière qui soit conforme à ces lois.

Les organisations devraient également envisager de surveiller systématiquement les signalements de fraudes par les utilisateurs et les accès non autorisés aux comptes[97], qui peuvent être signe d'une attaque par bourrage d'identifiants. Par exemple, les organisations doivent procéder à des examens réguliers et périodiques des rapports de fraude afin de détecter les pics ou la distribution des activités. Les organisations doivent également s'assurer que les équipes du service à la clientèle sont formées de manière à pouvoir reconnaître les signes d'attaques par bourrage d'identifiants et sont en mesure

[95] Open Web Security Project Foundation, « Credential Stuffing Prevention Cheat Sheet », https://cheatsheetseries.owasp.org/cheatsheets/Credential_Stuffing_Prevention_Cheat_Sheet.html, consulté le 25 mai 2021.

[96] *Ibid.*

[97] Bureau of Internet and Technology du bureau du procureur général de l'État de New York, « Business Guide for Credential Stuffing Attacks », https://ag.ny.gov/sites/default/files/businessguide-credentialstuffingattacks.pdf, consulté le 27 janvier 2022.

de communiquer efficacement toute activité inhabituelle ou néfaste aux équipes de sécurité de l'information afin de prévenir ou d'atténuer les attaques.