

LES 10 PRINCIPALES
ERREURS DE
SÉCURITÉ COMMISES
PAR LES ENTREPRISES

Table des matières

PRÉFACE

La cybersécurité, un enjeu majeur à ne pas négliger.....3

ERREUR N° 1

Omettre d'appliquer une politique de mots de passe forts.....4

ERREUR N° 2

Utiliser des logiciels obsolètes et non corrigés.....6

ERREUR N° 3

Utiliser des périphériques vulnérables.....7

ERREUR N° 4

Négliger la surveillance et la protection adéquate des services de messagerie.....8

ERREUR N° 5

Avoir une mauvaise visibilité du réseau.....10

ERREUR N° 6

Mal gérer les appareils mobiles.....11

ERREUR N° 7

Négliger l'application des politiques de privilèges d'accès.....12

ERREUR N° 8

Mal gérer les répertoires.....13

ERREUR N° 9

Mal protéger les services infonuagiques.....14

ERREUR N° 10

Utiliser de mauvaises pratiques de destruction des données.....15

La sécurité du bon sens.....16

PRÉFACE


La cybersécurité, un enjeu majeur à ne pas négliger

La cybersécurité est souvent considérée comme un enjeu technologique qui nécessite des réponses technologiques. Des milliers de fournisseurs vendent des outils pour détecter, prévenir et se relever des cyberattaques. Les dépenses mondiales en cybersécurité devraient dépasser [150 milliards de dollars](#) cette année, indiquant que des sommes considérables sont investies dans la recherche de solutions.

Mais en réalité, la grande majorité des problèmes de sécurité résultent d'erreurs humaines, du manque de connaissance et de mauvaises politiques. Plutôt que d'acquérir de nouvelles technologies, les entreprises doivent utiliser plus efficacement les outils dont elles disposent.

Gardien Virtuel, une filiale à part entière d'ESI Technologies, fournit des produits et services de cybersécurité aux entreprises nord-américaines afin de s'assurer que leurs actifs numériques et leurs technologies sont protégés contre les menaces internes et externes. Gardien Virtuel est un partenaire de choix pour aider à protéger les entreprises et les PME canadiennes contre les vecteurs de menaces modernes grâce à une gamme complète de services de sécurité informatique, allant des projets de consultation ponctuels à la surveillance de la sécurité en continu.

ESI a mis à profit les nombreuses années d'expérience de son équipe de sécurité pour développer cette liste des 10 failles de cybersécurité rencontrées le plus souvent par ses experts. Si les technologies font évidemment partie des solutions pour contrer les menaces, la plupart de ces lacunes peuvent être comblées en élaborant des politiques robustes, en formant les utilisateurs et en suivant les meilleures pratiques, sans négliger la surveillance et la détection des activités de votre organisation sur les sites malveillants connus du Dark Web.



Avec le nombre croissant de violations de données, prendre soin de ses mots de passe est plus essentiel que jamais. L'un des éléments clés d'un mot de passe fort est son caractère unique.

[Cybernews](#)

ERREUR N° 1

Omettre d'appliquer une politique de mots de passe forts

C'est l'erreur de cybersécurité numéro 1 et la plus facile à corriger. Malgré des années de mises en garde sur l'importance de choisir des mots de passe composés de chaînes de caractères aléatoires, plusieurs personnes persistent à utiliser les noms des membres de leur famille, des dates de naissance, des chaînes de numéros séquentiels ou d'autres codes faciles à deviner.

Pendant ce temps, les logiciels utilisés par les criminels pour déchiffrer les mots de passe ne cessent de s'améliorer. Même les algorithmes de force brute, qui consistent à simplement combiner des caractères aléatoires jusqu'à ce qu'une correspondance soit trouvée, peuvent traiter jusqu'à 350 milliards de suppositions par seconde.

Les statistiques sur les défaillances de mot de passe sont alarmantes. Selon le rapport 2020 de [Verizon Data Breach Investigations](#), 81% du nombre total de violations ont été causés par des mots de passe volés ou faibles.

Une analyse de [Cybernews](#) portant sur plus de 15 milliards de mots de passe révèle que près de 30% de tous les mots de passe sont composés de huit caractères, tandis que les mots de passe à six caractères arrivent en deuxième position et représentent un peu moins de 20% du total.

Une pratique tout aussi dangereuse consiste à utiliser le même mot de passe sur plusieurs comptes. Des milliards de mots de passe ont été volés dans des violations au cours des dernières années. Un attaquant pouvant compromettre un compte avec un mot de passe volé peut souvent accéder à de nombreux autres comptes détenus par le même utilisateur.

Les gens font ces erreurs pour de bonnes raisons. Mémoriser ou noter des mots de passe différents pour chaque compte est un exercice laborieux et une source d'erreurs. La conservation dans un fichier électronique consolidé n'offre qu'une protection minimale, à moins que le document ne soit chiffré.

Une meilleure option consiste à utiliser l'un des nombreux gestionnaires de mots de passe numériques en vente à un coût faible ou nul. Ces produits stockent des mots de passe dans des coffres chiffrés, remplissent automatiquement des formulaires et peuvent même conserver des informations de cartes de crédit et autres données personnelles critiques. Ils peuvent également suggérer des mots de passe qui sont presque impossibles à déchiffrer. Les utilisateurs doivent se souvenir d'un seul mot de passe pour accéder à l'ensemble de leur coffre.

Les bonnes pratiques à mettre en œuvre en entreprise

Les organisations peuvent aider à renforcer la sécurité des mots de passe avec quelques procédures de base.



1

Forcer la modification immédiate des mots de passe par défaut chaque fois que de nouveaux périphériques sont installés. Le fait de laisser les valeurs par défaut sur un routeur, par exemple, peut permettre à un attaquant d'accéder facilement à l'ensemble du réseau d'une entreprise.



2

Définir les règles que les utilisateurs doivent respecter, comme la modification des mots de passe des applications stratégiques à chaque trimestre, à l'aide d'un gestionnaire de mots de passe pour permettre aux administrateurs d'imposer des modifications de mots de passe selon un calendrier prédéfini.



3

Fournir aux employés des conseils sur la sélection de bons mots de passe. Les logiciels de piratage de mots de passe sont devenus tellement sophistiqués que les experts affirment désormais qu'une longueur minimum de 13 caractères est nécessaire. Une pratique de plus en plus répandue consiste à adopter de très longs mots de passe, tels que des citations mémorables ou des passages de livres.



4

Encourager les employés à utiliser une authentification à deux facteurs (2FA) chaque fois que c'est possible. Cette technique, qui complète le mot de passe avec une seconde forme de vérification, telle qu'un message texte au téléphone portable de l'utilisateur, est de plus en plus répandue. Selon un [rapport de 2019 de Microsoft](#), l'utilisation de l'authentification multifactorielle bloque 99,9% des piratages de comptes.



Même avec ces protections en place, l'immunité n'est pas garantie. Par exemple, les exploits « zero-day » sont un type d'attaque qui frappe en même temps que de nouvelles vulnérabilités sont découvertes.

ERREUR N° 2

Utiliser des logiciels obsolètes et non corrigés

Se tenir au courant des mises à jour et des correctifs logiciels constitue un défi de taille pour les entreprises informatiques les plus riches en ressources. Pour les petites entreprises disposant d'un budget limité, la tâche est presque impossible. Une vérification du [National Vulnerability Database](#) du NIST illustre l'ampleur du problème. Des centaines de correctifs (qui ne sont pas tous critiques) sont publiés chaque mois et par conséquent impossibles à maintenir à jour. Ceux qui doivent être appliqués doivent souvent être téléchargés, testés et déployés rigoureusement afin d'éviter de causer d'autres problèmes.

Le réputé [Ponemon Institute](#) a estimé que 60% des organisations victimes d'une violation de données sur une période de deux ans ont été victimes d'un exploit d'une vulnérabilité connue, mais non corrigée.

La prévalence d'anciens ordinateurs et systèmes d'exploitation est un problème important. En date d'avril 2021, une [étude menée par Kaspersky](#) a révélé que pas moins de 22% des utilisateurs d'ordinateurs personnels utilisent encore Windows 7, dont la prise en charge par Microsoft a pris fin en janvier 2020.

L'enjeu des appareils mobiles

Une complication additionnelle est le nombre croissant d'appareils mobiles que les entreprises doivent prendre en charge. Les ordinateurs

portables, les téléphones intelligents et les tablettes sont difficiles à rassembler et les utilisateurs en déplacement sont plus susceptibles aux virus introduits par le biais de canaux tels que les réseaux sans fil ouverts et les clés USB.

Poursuivre le déluge de correctifs, il faut automatiser et définir des priorités. Les administrateurs de serveurs doivent souscrire à toutes les alertes pertinentes de leurs fournisseurs de logiciels stratégiques et accorder la priorité aux correctifs jugés les plus critiques. Une bonne stratégie de test consiste à utiliser un deuxième serveur dans une partition virtuelle qui reflète l'environnement de production.

La protection des terminaux client

La sécurité des terminaux est un problème plus difficile. L'organisation doit auditer tous les points d'entrée potentiels du réseau sur une base régulière, idéalement une fois par trimestre. Cela inclut les ordinateurs de bureau, les ordinateurs portables et les équipements réseau connectés à Internet. Tous les systèmes exécutant des systèmes d'exploitation non pris en charge tels que Windows XP ou Windows 98 doivent être immédiatement supprimés et remplacés. Les ordinateurs fonctionnant sous Windows 7 doivent être mis à jour vers Windows 10 avec les correctifs automatiques activés.

Utiliser des périphériques vulnérables

De nombreuses organisations offrent un service sans fil gratuit à leurs visiteurs et clients, mais le fait de ne pas respecter quelques protections de base peut transformer cette gracieuseté en un cauchemar de sécurité.

Les risques des services sans fil

Les points d'accès sans fil publics ne doivent jamais être connectés au réseau de l'entreprise. Les organisations peuvent négliger ce blocage de base et ce suivi pour des raisons de coût ou de commodité, mais elles le font à leurs risques et périls. Ajouter la sécurité par mot de passe aux points d'accès publics est une protection faible pour toutes les raisons mentionnées au point 1. La meilleure approche consiste à faire appel à un fournisseur de services Internet commercial dont le réseau est indépendant du vôtre.

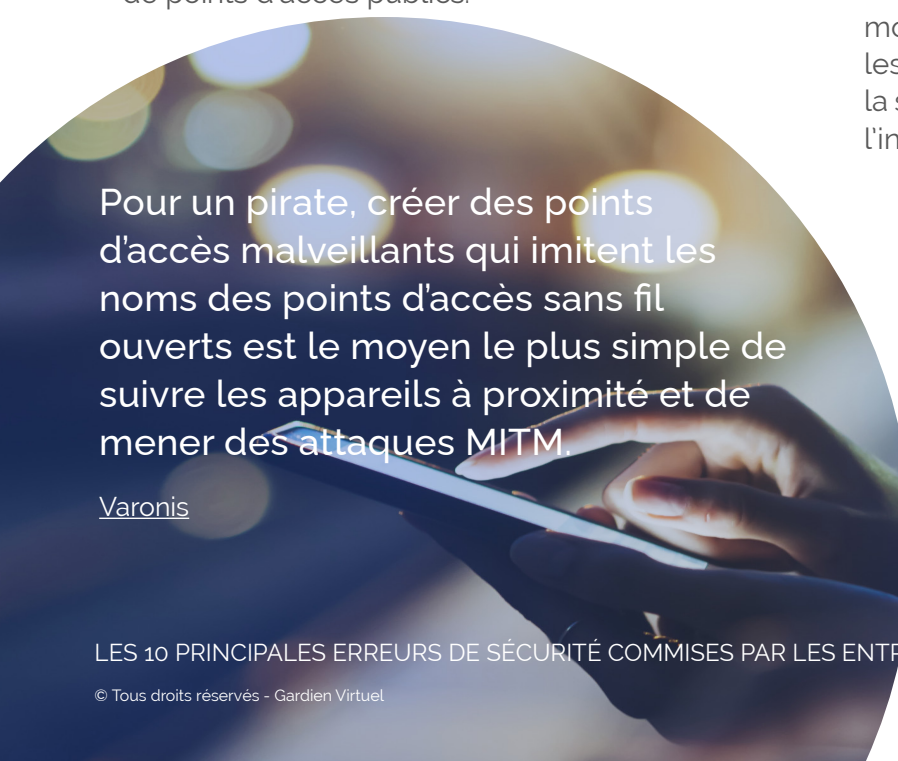
La plupart des points d'accès sans fil publics ne sont pas chiffrés, ce qui signifie que les données qui y sont transmises restent au format texte. Les cybercriminels peuvent facilement « renifler » ce trafic pour capturer tous les paquets traversant le réseau. Pour cette raison, les employés, les sous-traitants et même les clients doivent être mis en garde contre l'utilisation à des fins professionnelles de points d'accès publics.

Face à leur prolifération, les entreprises ont du mal à dénombrer tous leurs points d'accès potentiellement vulnérables.

Un facteur qui contribue à cette ignorance est la facilité avec laquelle des périphériques individuels peuvent désormais créer des vulnérabilités à l'insu du service informatique. Par exemple, de nombreux ordinateurs et téléphones intelligents sont livrés avec une option par défaut pour les configurer en tant que point d'accès sans fil ouverts. Les employés peuvent utiliser cette fonctionnalité pratique pour configurer des groupes de travail au besoin ou économiser sur les coûts de données sans fil, mais oublient ensuite de la désactiver. Lorsqu'ils se connectent à leur réseau professionnel, ils créent essentiellement une rampe d'accès ouverte au réseau de l'entreprise.


Les dangers de l'Internet des objets

Malheureusement, l'IoT ne fera qu'aggraver la situation. Les entreprises installent de plus en plus de dispositifs, tels que des thermostats programmables, des caméras et des systèmes d'éclairage intelligents, et les connectent à leur réseau. Ces dispositifs peuvent être peu ou pas sécurisés, ce qui en fait des proies faciles pour les criminels. En tant que protection de base, modifiez les mots de passe par défaut sur tous les périphériques ajoutés à votre réseau et utilisez la segmentation du réseau pour limiter l'accès à l'infrastructure et aux informations critiques.



Pour un pirate, créer des points d'accès malveillants qui imitent les noms des points d'accès sans fil ouverts est le moyen le plus simple de suivre les appareils à proximité et de mener des attaques MITM.

[Varonis](#)



Les attaques par hameçonnage
représentent plus de 80% des
incidents de sécurité signalés.

CSO Online

ERREUR N° 4

Négliger la surveillance et la protection adéquate des services de messagerie

Malgré les efforts des administrateurs de la sécurité pour appliquer les bonnes pratiques en matière de mots de passe et pour colmater les failles des réseaux, ils ne peuvent rien faire pour protéger les utilisateurs contre leurs propres erreurs. La boîte de réception reste une menace persistante pour la sécurité.

Les statistiques parlent d'elles-mêmes. Selon [CSO Online](#), 94% des logiciels malveillants sont diffusés par courrier électronique. Le [rapport d'enquête de Verizon](#) sur les violations de données 2020 indique que 30% des violations de données impliquent des acteurs internes.

Des attaques de plus en plus raffinées

Les attaques par courrier électronique ont évolué au cours des dernières années, car les criminels ont affiné leur capacité à cibler les messages. Les filtres anti-pourriel sont maintenant tellement efficaces que peu d'utilisateurs voient même les pourriels, mais grâce à la technique de l'hameçonnage, les criminels peuvent contourner même les meilleurs contrôles.

L'origine du problème est la confiance. Le courrier électronique est un outil tellement essentiel pour les professionnels qu'il est facile pour les gens de tomber dans le piège consistant à croire que chaque message est authentique.

Le harponnage profite de cette complaisance. Les criminels extraient des informations personnelles

issues de profils de réseaux sociaux et les font correspondre à des adresses électroniques. Ils peuvent également analyser l'activité récente d'une personne pour rechercher des éléments qui établissent une relation de confiance, tels que l'appartenance à une organisation ou des achats récents. Et ils consultent les réseaux d'amis pour trouver le nom des personnes que leurs cibles connaissent déjà. Munis de ces informations, les attaquants peuvent facilement usurper l'identité d'un expéditeur d'un message électronique pour qu'il semble provenir d'un ami. Le fait d'inclure une information personnelle glanée sur un réseau social rassure le destinataire. Le message inclut un lien vers un site Web malveillant qui installe un logiciel ou demande des informations de connexion. Les habitués de l'hameçonnage sont si compétents aujourd'hui que même les professionnels de la cybersécurité ont avoué en être la proie.

Les attaques par courrier électronique sont extrêmement difficiles à défendre, car elles sont spécifiques à chaque utilisateur du réseau. Un simple clic sur une pièce jointe ou un lien malveillant peut déclencher une multitude de maliciels qui se propagent rapidement dans toute l'organisation.

Le rançongiciel est un facteur particulièrement nocif. Il chiffre instantanément le disque dur de l'utilisateur et exige une rançon en cryptomonnaie en échange de la clé de déchiffrement. Certaines de ses formes se copient sur les périphériques du réseau et les chiffrent également.

Les moyens d'améliorer la protection

La mise en place d'un programme de sensibilisation et de formation des employés est indispensable. Adoptez un programme basé sur des exercices de simulation d'événements de cybersécurité pour accroître la vigilance des employés et mieux prévenir les attaques.

Heureusement, la défense contre les attaques par courrier électronique est assez simple. Elle consiste à éduquer les gens sur quelques pratiques de base :



Ne cliquez jamais sur des liens ou des pièces jointes dans les messages, sauf si vous êtes absolument certain de l'identité de l'expéditeur. Cette information peut être facilement vérifiée en consultant l'en-tête du message, qui est différent du champ « de ».




N'envoyez jamais d'informations personnelles telles que des numéros de compte bancaire ou des mots de passe par courrier électronique. Aucune organisation réputée ne vous demandera jamais de le faire.



Si vous êtes dirigé vers une page de connexion à partir d'un courrier électronique, vérifiez que l'adresse Web correspond à celle attendue. Les pirates peuvent créer de fausses pages Web très semblables aux sites légaux des banques, commerces en ligne et réseaux sociaux.



Choisissez judicieusement les informations que vous partagez publiquement sur les réseaux sociaux.



Les organisations ont mis en moyenne 280 jours pour découvrir une brèche en 2020. L'économie moyenne réalisée en contenant une brèche en moins de 200 jours par rapport à plus de 200 jours est de 1.12 million de dollars.

[2020 Cost of Data Breach Security](#)
[Ponemon Research](#)

ERREUR N° 5

Avoir une mauvaise visibilité du réseau

Vous ne pouvez pas empêcher les attaques d'appareils que vous ne voyez pas. Malheureusement, plusieurs organisations n'ont pas une visibilité complète de leurs réseaux. Elles voient peut-être les adresses IP, mais elles ont peu d'informations sur ce que sont ces périphériques.

Une mauvaise visibilité augmente le risque que les attaquants pénètrent dans un réseau et restent inconnus pendant des semaines ou des mois, ce qu'on appelle un « temps d'arrêt ». Pendant cette période, les intrus peuvent siphonner de grandes quantités d'informations graduellement afin d'échapper à la détection.

Partage d'informations

Le problème est aggravé par la nature ouverte des réseaux IP. Le protocole Internet a été conçu pour que les informations puissent être découvertes librement, ce qui signifie que les périphériques partagent volontiers des informations sur les autres périphériques du même sous-réseau, notamment les versions du système d'exploitation et les applications en cours d'exécution. Un pirate peut exploiter ces informations pour trouver un logiciel vulnérable qui pourrait être exploité pour prendre le contrôle d'autres machines.

Défaillances de segmentation réseau

Les mauvaises pratiques de segmentation du réseau amplifient le problème. La segmentation est un moyen utile pour les administrateurs de limiter l'accès à certains types d'informations en regroupant des périphériques dans des sous-réseaux dotés de niveaux d'autorisation différents.

Cependant, de nombreuses entreprises ne prennent pas la peine de créer des sous-réseaux, exposant ainsi l'ensemble de leur réseau à toute personne pouvant franchir un pare-feu. À l'inverse, la sursegmentation crée une complexité qui peut également révéler des vulnérabilités. Par exemple, 30 sous-réseaux avec 25 stratégies de permission créent chacun 750 règles à administrer. Les erreurs et les oublis sont facilement omis dans un environnement aussi complexe.

Mal gérer les appareils mobiles

Presque tout le monde possède désormais un téléphone intelligent mais plusieurs entreprises ont du mal à les traiter comme faisant partie de leur infrastructure informatique. Les règles de type BYOD qui ont dominé les premières années de la révolution du téléphone intelligent, sont dangereusement inadéquates pour régir l'utilisation des puissants appareils actuels.

Que les utilisateurs se servent de leurs propres téléphones ou que l'entreprise les leur fournisse, les appareils mobiles exigent les mêmes considérations de sécurité que les ordinateurs de bureau et portables. En fait, ils exigent une attention supplémentaire en raison de la facilité avec laquelle ils sont perdus ou volés, à raison de quelque [70 millions](#) chaque année.

Les appareils mobiles présentent de nouvelles menaces uniques pour la sécurité. En raison de leurs caméras et de leurs enregistreurs audio intégrés, les téléphones compromis peuvent devenir des dispositifs d'écoute et d'enregistrement vidéo à l'insu de l'utilisateur. Leur GPS intégré les rend également vulnérables à la localisation, une fonctionnalité particulièrement utile aux criminels se livrant à l'espionnage d'entreprise.

La sécurité des téléphones mobiles s'améliore,

mais les organisations informatiques ne doivent pas compter uniquement sur les fonctionnalités intégrées pour la protection. Des chercheurs ont montré que les codes NIP et les motifs de balayage peuvent être détectés à une distance maximale de 4,5 mètres et qu'aucune protection biométrique n'est à toute épreuve. Une meilleure pratique consiste à utiliser deux formes d'authentification.

Tandis que certains de ces programmes malveillants se frayent un chemin vers des magasins légitimes d'applications, beaucoup se propagent par le biais de programmes d'hameçonnage qui envoient des messages texte à des utilisateurs involontaires, les dirigeant vers des sites Web qui installent des programmes malveillants sur leurs appareils.

Une sécurité mobile efficace commence par des règles bien définies et bien communiquées. Les étapes de base incluent la mise à jour des périphériques avec les dernières versions du système d'exploitation et des correctifs de sécurité, la sauvegarde régulière des données et l'utilisation du chiffrement pour les données à la fois sur le périphérique et en transit. Les utilisateurs doivent éviter les points d'accès sans fil publics et ne jamais cliquer sur des liens inconnus dans les messages texte ou le courrier électronique.

Dans leurs campagnes d'infection des appareils mobiles, les cybercriminels ont toujours recours à des outils d'ingénierie sociale, le plus courant étant de faire passer une application malveillante pour une autre, populaire et désirable. Tout ce qu'ils doivent faire, c'est identifier correctement l'application, ou du moins le type d'applications, qui est actuellement en demande. Par conséquent, les attaquants surveillent constamment la situation dans le monde, recueillant les sujets les plus intéressants pour les victimes potentielles, puis les utilisent pour infecter ou escroquer les utilisateurs de leur argent.

[Mobile Malware Evolution 2020 - Securelist Kaspersky](#)

Négliger l'application de politiques de privilèges d'accès

Au milieu de la pression des affaires quotidiennes, les détails sont facilement oubliés, ou laissés sans solution. Lorsque ces détails concernent les privilèges d'accès, c'est un problème.

De nombreux utilisateurs finaux ne comprennent pas le fonctionnement des privilèges d'accès ou ne prêtent pas attention aux conseils fournis par les services TI. Résultat : des informations confidentielles peuvent facilement être laissées à la vue de tous.

Le [Data Risk Report de 2021](#) pour les services financiers de Varonis a compilé les données de 4 milliards de fichiers dans 56 organisations de services financiers. Parmi ses conclusions :

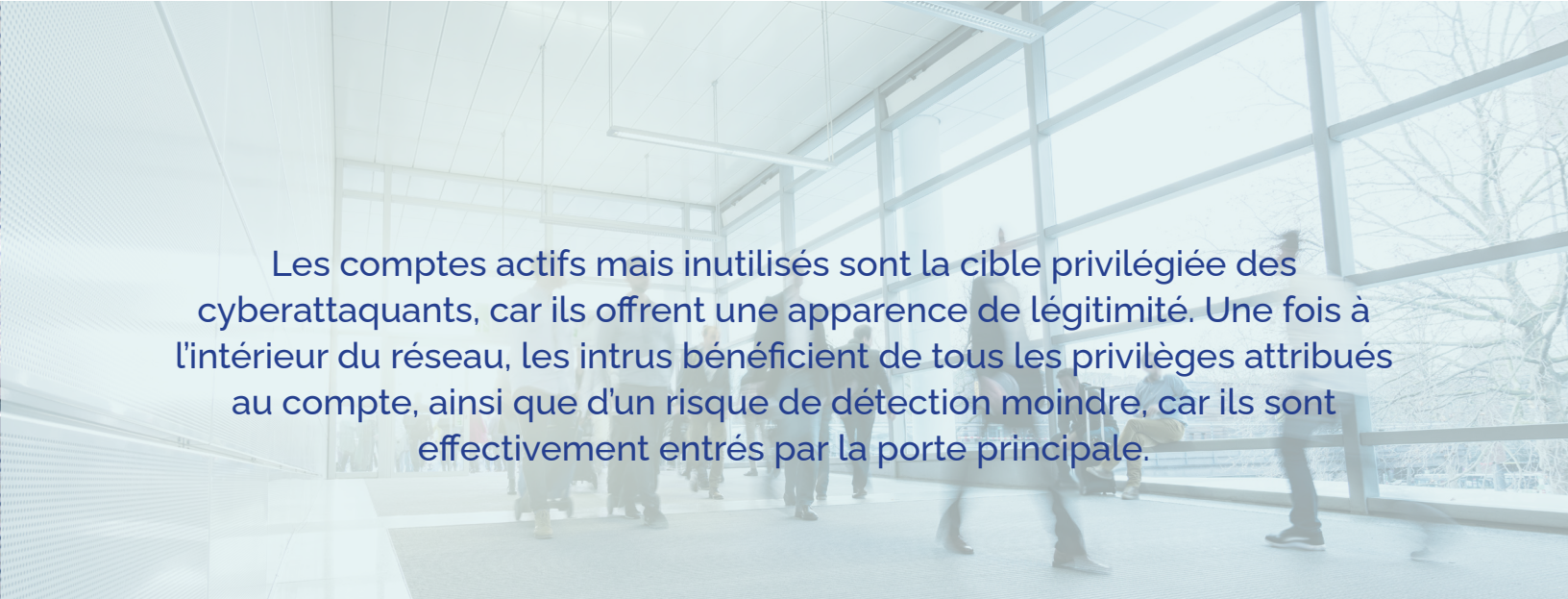
- Chaque employé a accès à près de 11 millions de fichiers;
- Près des deux tiers des entreprises ont plus de 1 000 fichiers critiques accessibles à chaque employé; et
- Environ 60 % des entreprises ont plus de 500 mots de passe qui n'expirent jamais.

Ces oublis sont importants si l'on considère que [CyberAngel](#) a constaté qu'environ 90% des violations de données sont dues à la négligence d'un employé ou d'un tiers, 10% seulement des fuites étant le fait d'acteurs malveillants.

Le manque de connaissances est le plus grand coupable. Les employés peuvent ignorer les procédures d'attribution de privilèges ou déposer des fichiers dans des dossiers non sécurisés en pensant qu'ils sont protégés. Les dossiers situés au cœur d'un système de fichiers peuvent contenir des autorisations qui ne sont pas visibles au niveau supérieur, ce qui induit les administrateurs en erreur.

La sensibilisation et la formation sont les meilleurs remèdes. L'équipe TI doit expliquer comment attribuer des autorisations de fichiers et de dossiers et transmettre les meilleures pratiques, telles que l'attribution d'accès au niveau du groupe et jamais à des utilisateurs individuels. Une approche encore plus sécurisée consiste à limiter la création de nouveaux dossiers aux administrateurs informatiques, même si cela n'est pas pratique dans tous les cas.

Des solutions techniques sont disponibles sous la forme de systèmes de gestion de contenu d'entreprise, qui régulent l'accès au contenu et sa distribution dans l'ensemble de l'organisation. Ces systèmes incluent souvent également des fonctionnalités sophistiquées de gestion du flux de travail qui peuvent rationaliser les processus et améliorer l'efficacité.



Les comptes actifs mais inutilisés sont la cible privilégiée des cyberattaquants, car ils offrent une apparence de légitimité. Une fois à l'intérieur du réseau, les intrus bénéficient de tous les privilèges attribués au compte, ainsi que d'un risque de détection moindre, car ils sont effectivement entrés par la porte principale.

ERREUR N° 8

Mal gérer les répertoires

Lorsqu'un employé quitte l'entreprise, les gestionnaires sont naturellement plus soucieux du travail à faire et de pourvoir le poste vacant que de désactiver les privilèges d'accès. Malheureusement, avec le temps, cela peut créer une grande brèche dans les défenses de l'organisation.

Les personnes qui affichent aujourd'hui l'ensemble de leurs antécédents professionnels sur des réseaux sociaux comme LinkedIn, permettent aux pirates d'identifier facilement des candidats en recherchant des personnes qui ont récemment changé d'emploi et dont les informations d'identité sont peut-être encore valables. Ils peuvent mettre en corrélation croisée ces informations avec les milliards de noms d'utilisateur et de mots de passe volés accessibles sur le Dark Web afin de réduire leur liste de candidats.

Le taux de roulement n'est pas la seule vulnérabilité. Les comptes sont souvent configurés pour les sous-traitants et les travailleurs temporaires sans accorder une attention particulière aux autorisations d'accès.

Les administrateurs oublient alors de les fermer à la fin d'un contrat, ou les laissent ouverts en cas de retour du travailleur temporaire.

Le rapport Varonis cité précédemment fait référence à ces entrées de répertoire sous le nom de « comptes fantômes ». Son enquête a révélé que le tiers des comptes sont activés mais inutilisés et que 65% des entreprises ont plus de 1 000 comptes fantômes.

Parmi les autres problèmes fréquents liés aux répertoires, citons l'attribution trop généreuse des privilèges et l'affectation de membres à des groupes sans vérification préalable des exigences en matière d'accès.

Pour traiter le problème des comptes fantômes, les entreprises doivent désigner une personne au sein du service des ressources humaines pour veiller à ce que les privilèges d'accès soient révoqués pour les employés qui quittent. C'est aussi une bonne idée de vérifier annuellement la liste des comptes et de supprimer ceux qui sont inutilisés. L'administration des répertoires doit être limitée à quelques personnes formées aux meilleures pratiques pour le service d'annuaire choisi.

Mal protéger les services infonuagiques

Le chiffrement des données

La plupart des fournisseurs infonuagiques de logiciels (SaaS) et d'infrastructures (IaaS) offrent une excellente sécurité, mais cela ne signifie pas que les clients doivent supposer qu'ils n'ont plus à s'en préoccuper.

Par exemple, les fournisseurs IaaS peuvent prendre en charge le chiffrement des données mais laisser la responsabilité et la gestion des clés de déchiffrement entre les mains de leurs clients. Ils peuvent également fournir des contrôles pour empêcher le téléchargement d'informations mais laisser cette option désactivée par défaut. Chaque fournisseur a ses propres politiques et il appartient aux clients de faire leurs devoirs.

La prévention des fuites de données

Les erreurs utilisateurs sont la cause la plus courante des problèmes de sécurité dans le cloud.

Selon une enquête d'[Ermetic](#), près de 80% des entreprises ont subi au moins une violation de données dans le cloud au cours des 18 derniers mois.

Les trois principales causes sont :

- Des erreurs de configuration de sécurité (67%)
- Un manque de visibilité adéquate sur les paramètres et les activités d'accès (64%)
- Des erreurs de gestion d'identité et d'accès (IAM) et de permission (61%)

Les entreprises doivent limiter le nombre de fournisseurs de stockage infonuagique qu'elles utilisent et appliquer des contrôles administratifs pour limiter ce que les utilisateurs peuvent partager et télécharger.

La sélection des mots de passe

Une mauvaise sélection de mot de passe peut laisser des applications et des données critiques exposées à tous sur Internet. Le recours à une authentification à deux facteurs peut réduire ce risque. Les utilisateurs doivent également être informés des meilleures pratiques en matière de partage de données infonuagiques. Par exemple, les données sensibles ne doivent être partagées qu'avec des personnes nommées, et non par une URL globale permettant l'accès en édition.

Il est généralement dangereux de supposer, en particulier en ce qui concerne les services infonuagiques. Les employés peuvent se déplacer pour poser des questions relatives à la sécurité à leurs administrateurs TI, mais la plupart de gens ne parlent même jamais aux entreprises qui fournissent des services cloud, ce qui peut conduire à des hypothèses risquées sur qui est responsable de quoi.

Utiliser de mauvaises pratiques de destruction de données

L'équipement qui a atteint la fin de sa vie utile peut constituer un risque important pour la sécurité si des pratiques d'élimination appropriées ne sont pas appliquées. De nombreuses personnes pensent que le simple fait de supprimer toutes les données d'un disque ou de formater le support constitue une protection suffisante, mais aucune de ces mesures ne supprime beaucoup de données.

Au lieu de cela, ils suppriment les pointeurs des répertoires, mais laissent jusqu'à 90% des données intactes et facilement récupérables à l'aide d'un logiciel spécialisé. Même plusieurs séances de formatage peuvent encore laisser des quantités importantes de données en place.

L'élimination des actifs TI (ITAD pour « IT Asset Disposal ») est une discipline spécialisée dans la destruction de données. Les fournisseurs ITAD utilisent des techniques allant de l'effacement avec des aimants puissants à la destruction physique de supports utilisant des machines qui réduisent les disques en poudre.

Les services professionnels fournissent également un certificat de destruction qui répond à la plupart des demandes de renseignements réglementaires.

Certains peuvent également remettre en état des équipements et récupérer une certaine valeur en les vendant sur des marchés secondaires.

Les services ITAD peuvent être coûteux et ne sont pas nécessaires dans tous les cas. Les organisations doivent disposer d'un processus d'évaluation des équipements en fin de vie et d'identification de ceux qui méritent une manutention spécialisée.

Ce processus doit s'appliquer à tout équipement contenant des données, notamment des serveurs, des ordinateurs personnels, des téléphones intelligents et des clés USB.

La sécurité du bon sens

Les propriétaires de petites entreprises peuvent penser être protégés des cyberattaques, car leur taille en fait une cible peu attrayante, mais plus de 55% des attaques par rançongiciels concernent désormais des entreprises de moins de 100 employés.

Les criminels supposent que les petites entreprises ont des ressources limitées et ne disposent pas des technologies sophistiquées de détection et de prévention des grandes entreprises. Si les grandes entreprises sont bien équipées pour résister aux violations de données, même importantes, l'impact peut être dévastateur pour les entreprises dont les marges sont plus faibles. En effet, selon un sondage mené au début de 2021 par la [Fédération canadienne de l'entreprise indépendante](#), les PME sont plus exposées que jamais à la fraude informatique; 25% se disent victimes de tentative de fraude et 56% des entrepreneurs sondés sont plus inquiets pour leur entreprise depuis l'essor du télétravail.

Les cybercriminels veulent avoir un impact sur les opérations quotidiennes d'une organisation. Les responsables informatiques doivent repenser et améliorer la résilience de leur organisation en mettant en oeuvre des plans de reprise et de continuité des activités qui garantiront la poursuite des opérations. C'est l'une des dernières lignes de défense lorsqu'un événement de sécurité se produit.

Plus que jamais, prêter attention aux 10 problèmes énumérés ici peut déjouer la grande majorité des risques et des conséquences dramatiques sur vos activités.

Vous souhaitez obtenir des conseils d'une équipe d'experts en cybersécurité?
Gardien Virtuel vous offre **une heure de consultation gratuite** pour discuter des enjeux de cybersécurité de votre entreprise et évaluer avec vous comment mitiger les risques identifiés dans ce livre.

Contactez-nous pour prendre rendez-vous!

Gardien Virtuel

Centre de service :
1-800-401-TECH (8324)

Parler à un représentant :
514 745-3311

1550 Metcalfe, # 1100, H3A 1X6
Montréal, Québec, Canada

www.gardienvirtuel.com