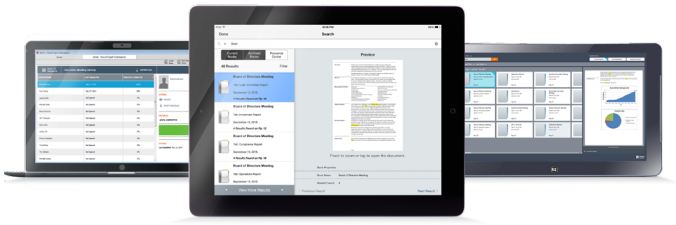
Diligent

Exploiter la puissance de l'information. En toute sécurité.

Pour aider les organisations les plus puissantes du monde à exploiter en toute sécurité la puissance de l'information et de la collaboration, Diligent fournit aux conseils d'administration et équipes de gestion tout pour leur permettre de prendre de meilleures décisions. Plus de 4 000 clients dans plus de 70 pays comptent sur Diligent pour accéder sans délai aux informations les plus urgentes et confidentielles et aux outils pour en discuter, collaborer et les examiner avec les principaux décideurs. Diligent Boards accélère et simplifie la création et la distribution des documents de conseil avec les iPad, les appareils Windows et les navigateurs. Les autres avantages pratiques sont par exemple la réduction des coûts de production, la contribution au développement durable et le gain de temps administratif et informatique.

Rejoignez les plus grands. Choisissez Diligent.



Pour de plus amples informations ou pour recevoir une démo, contactez-nous dès aujourd'hui :

Téléphone : +33 (0)1 56 60 58 58
Courriel : info@diligent.com
Site Web : www.diligent.com

AICPA SOC · ISO 27001 CERTIFIED BY BRIGHTLINE · Télécharger dans l'App Store · Obtenir sur Microsoft

Diligent est une marque de Diligent Corporation, déposée aux États-Unis. Toutes les marques de tiers sont la propriété de leur propriétaire respectif. ©2016 Diligent Corporation. Tous droits réservés.

Cybermenaces et sécurité du conseil d'administration : **Trois idées fausses néfastes à la sécurité de la salle du conseil**

Ben Bourne
Responsable du service à la clientèle, EMEA

Magdalena Borcal
Responsable du service à la clientèle, EMEA

Nathan Birtle
Vice-président des ventes et du développement commercial, EMEA

Le nombre de cyberattaques est en hausse à l'échelle internationale. De plus en plus, les cybercriminels contournent les systèmes de sécurité et les médias du monde entier rapportent régulièrement des atteintes majeures à la sécurité. Malgré cela, bon nombre de conseils d'administration continuent d'ignorer la menace du cybercrime, et parmi ceux qui ont réagi, beaucoup se montrent incapables de prendre les mesures nécessaires à leur sécurité. C'est en réaction à cette situation que nous avons publié cet article : il vise à aider les membres des conseils d'administration et les dirigeants à mieux appréhender le problème du cybercrime et à leur montrer comment réduire les risques de sécurité à dans les conseils.

De nombreux facteurs expliquent la croissance de la cybercriminalité. Le risque de se faire prendre est faible par rapport à d'autres types de crime ; les données peuvent transiter par des milliers d'ordinateurs, de sorte que les attaques sont à la fois anonymes et difficiles à tracer. Les montants que les cybercriminels peuvent espérer sont de l'ordre de plusieurs millions ; la plupart des cyberattaques sont perpétrées par le crime organisé, les analystes estimant que la cybercriminalité coûte à l'économie mondiale 455 milliards de dollars par an.[1]

Une attaque peut causer des dommages considérables à une organisation. Outre les pertes financières, le vol de données et de propriété intellectuelle peut être préjudiciable pour l'entreprise, sa compétitivité, sa capacité d'innovation et sa réputation. Les organisations peuvent se protéger, et en repensant la façon de traiter leurs données et de sécuriser leurs informations, elles peuvent limiter le risque d'attaque.

1 « Net Losses: Estimating the Global Cost of Cybercrime » (Pertes nettes : estimation du coût de la cybercriminalité à l'échelle internationale), McAfee, 2014. http://www.mcafee.com/uk/resources/reports/ rp-economic-impact-cybercrime2-summary.pdf

Diligent

ÉVALUATION DE VOTRE CONSEIL D'ADMINISTRATION

En tant que décideurs, les membres des conseils d'administration doivent comprendre les menaces qui pèsent sur leur organisation, mais la tâche peut s'avérer difficile. Souvent, ils ne voient tout simplement pas à quel point le numérique a envahi le monde des affaires, ils ne comprennent pas que la convergence de l'informatique, des technologies d'exploitation et d'entreprise a donné une forme nouvelle à leur organisation et ouvert de nouveaux moyens d'accès aux cybercriminels.

Il faut également tenir compte des structures hiérarchiques de l'organisation. Comme le conseil d'administration se trouve « au sommet » de la structure, les responsables de la sécurité n'osent parfois pas exprimer leurs doutes sur le système de sécurité de l'entreprise. Des études menées par Deloitte et Systemec indiquent que, dans certaines régions, jusqu'à 70 % des décideurs informatiques ne font pas entièrement confiance aux politiques de sécurité de leur entreprise et elles concluent que plus des deux tiers des organisations sont incapables de se protéger elles-mêmes contre les attaques.[2] De façon similaire, l'équipe responsable de la sécurité n'a pas toujours conscience que la sécurité du conseil est de son ressort, partant du principe qu'elle relève plutôt de la responsabilité du secrétaire général et ne devrait pas être intégrée au système de sécurité de organisation.

« Certains conseils d'administration doivent comprendre les menaces qui pèsent sur leur organisation, mais la tâche peut s'avérer difficile. Souvent, les membres de conseils d'administration ne voient tout simplement pas à quel point le numérique a envahi le monde des affaires. »

Autre facteur à ne pas négliger : les membres des conseils eux-mêmes qui, par leurs habitudes de travail inadaptées, s'exposent aux cybercriminels. En choisissant d'accéder à des documents, de les stocker et de les distribuer d'une manière certes commode, mais peu sûre, ils prennent le risque que leurs données tombent dans de mauvaises mains et échappent ainsi à leur contrôle. Les courriels, les fichiers PDF et les systèmes de stockage en nuage, par exemple, sont probablement beaucoup moins sûrs que les méthodes employées par l'organisation.

Les membres des conseils d'administration et le personnel doivent rester vigilants dans leur approche des technologies de communication. Mais les idées reçues sur la technologie et les méthodes de travail utilisées peuvent également nuire aux pratiques professionnelles les plus sécurisées.

LES TROIS IDÉES REÇUES SUR LA SÉCURITÉ

Pour éviter que e travail des membres des conseils d'administration soit préjudiciable à la sécurité de votre conseil, il est essentiel que vous soyez conscient des idées reçues suivantes :

1. Le courrier électronique est sûr

Si la messagerie électronique peut être pratique, rapide et facile pour communiquer des informations confidentielles, elle n'est tout simplement pas adaptée à cet usage ; avec les courriels, vous n'avez aucun moyen d'empêcher la réexpédition du contenu. De plus, il est difficile d'annuler un message expédié, de sorte que, dès qu'un courrier électronique est envoyé, vous perdez effectivement le contrôle de l'information.

2. La protection par mot de passe est un gage de sécurité

S'il n'est pas déraisonnable de considérer que l'ajout d'un mot de passe à un PDF rend celui-ci inaccessible aux utilisateurs non autorisés, une recherche basique dans n'importe quel moteur de recherche montre comment contourner la sécurité d'un PDF. Effectuez cette recherche sur Google et vous trouverez plus de 2 300 000 résultats vous expliquant avec quelle saisissante facilité vous pouvez ouvrir illégalement ce type de document prétendument sécurisé. La vérité, c'est que la technologie PDF n'est pas sûre et que vous ne devriez pas vous y fier.

3. Le stockage interne des données est plus sûr

L'idée reçue la plus dangereuse est peut-être celle sur le stockage des données, selon laquelle les données stockées en interne sont plus sûres que celles stockées auprès d'un fournisseur externe. En vérité, c'est souvent le contraire ; par exemple, dans le cadre de solutions internes, l'organisation compte sur ses propres administrateurs pour accéder aux données et les gérer, mais comme 55 % des attaques sont perpétrées par des personnes internes à l'entreprise, cet accès peut s'avérer catastrophique.[3] Par ailleurs, d'un point de vue technique et opérationnel, les programmes et infrastructures de sécurité de l'organisation peuvent être insuffisants pour protéger les données des menaces actuelles. À l'inverse, un fournisseur de solutions SaaS tel que Diligent restreint l'accès aux seuls utilisateurs autorisés ; notre équipe n'a pas accès aux données des clients. Par ailleurs, nous disposons de politiques et procédures de sécurité intégralement contrôlées et offrons des fonctions de sauvegarde et récupération de données en cas de sinistre, de même qu'un système de surveillance de la sécurité bien supérieur aux capacités de la plupart des autres organisations.

2 Global Risk Insights, septembre 2015. "globalriskinsights. com/2015/09/how-strong-are-the-middle-easts-cybersecurity-net-works/
3 « IBM 2015 Cyber Security Index » (Indice de cybersécurité IBM 2015) et « IBM X-Force Threat Intelligence Quarterly Q2 – 2015 » (Renseignement sur la menace IBM X-Force - 2e trimestre 2015) https://securityintelligence.com/ the-threat-is-coming-from-inside-the-network/

ÉVALUATION DE LA SÉCURITÉ

Les leaders qui souhaitent évaluer les pratiques de leur conseil en matière de cybersécurité peuvent se poser trois questions simples :

Où les données du conseil sont-elles enregistrées ?

Toute évaluation de la sécurité doit commencer par examiner qui contrôle les données. Si l'on ignore où se trouvent les informations et que l'on est incapable de contrôler leur destination, la solution est très peu sûre.

C'est pourquoi l'envoi électronique de documents de conseil au format PDF n'est pas une solution sécurisée. Les fichiers peuvent être envoyés accidentellement par des membres du conseil à d'autres personnes étrangères à celui-ci, ou stockés dans des messageries électroniques personnelles mal sécurisées sur des systèmes que les fournisseurs eux-mêmes considèrent comme peu sûrs.

Il en va de même pour les solutions « en nuage » : vos fichiers pourraient se trouver sur n'importe quel serveur sur le réseau de partage de fichiers et vous n'avez aucun moyen de savoir où ils se trouvent exactement. Le succès des solutions en nuage se base sur l'hypothèse qu'elles sont sûres alors qu'en fait, des cas graves de piratage tels que la divulgation de mots de passe ou de photos de célébrités confiés à des fournisseurs de services en nuage démontrent à quel point cette présomption de sécurité est infondée.[4]

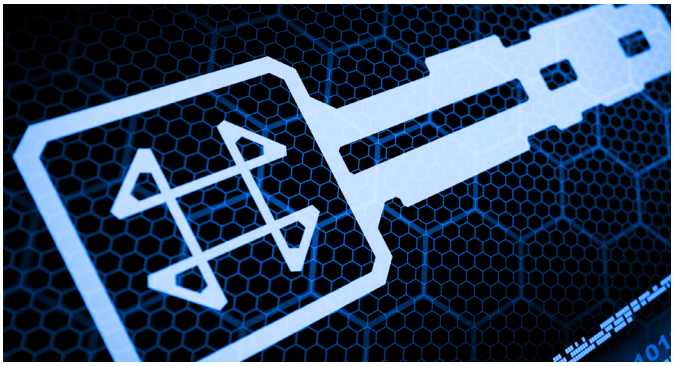
Bien que les portails hébergés pour conseils d'administration ressemblent à des systèmes en nuage et soient souvent appelés à tort systèmes de « stockage en nuage », ils sont très différents de ces derniers ; les portails hébergés pour conseils contrôlent de près la localisation de vos données et veillent à séparer les informations de chaque organisation qu'ils hébergent. Connaître la localisation des données et les mesures de sécurité qui leur sont appliquées assure un meilleur contrôle avec l'assurance de savoir qui accède aux informations.

Quelle est la solidité des serrures ?

S'il est crucial de connaître la localisation de vos données, il est tout aussi fondamental de veiller à ce que seuls des utilisateurs autorisés y accèdent. Un des moyens d'y parvenir est le chiffrement des données : celles-ci sont converties en une chaîne de 0 et de 1 dénuée de sens, de sorte que seules les personnes en possession de la bonne clé numérique sont en mesure de les déchiffrer.

Les dossiers de conseil au format papier ne sont pas protégés ; toute personne y ayant accès peut les lire. S'il est possible de chiffrer et protéger par mot de passe les fichiers PDF envoyés par courriel ou enregistrés sur des systèmes de partage de fichiers, cela signifie que les personnes qui distribuent et reçoivent ces documents doivent gérer les protocoles de mots de passe. Mais même dans ce cas, les documents PDF restent vulnérables aux attaques « de force brute » par des logiciels facilement accessibles.

Les portails hébergés hautement sécurisés utilisent généralement un chiffrement à 256 bits et comme le nombre de combinaisons possibles dépasse l'imagination, on peut légitimement dire que les pirates les plus déterminés auraient besoin d'une éternité pour casser le code, même avec la technologie la plus avancée.



Qui contrôle les clés ?

Quelle que soit la puissance du système de chiffrement, toute personne en possession de la bonne clé peut accéder aux informations, et toute personne qui détient le mot de passe nécessaire pour accéder à un fichier PDF est le propriétaire virtuel du document. Un mot de passe volé c'est des documents volés.

En revanche, un portail professionnel ne perd jamais le contrôle des documents. Contrairement aux mots de passe, les clés de chiffrement sont contrôlées par le système ; la personne qui se connecte ne verra que ce qu'elle est autorisée à voir et si un mot de passe est volé, l'administrateur peut simplement interdire l'accès par ce mot de passe.

Concernant les utilisateurs autorisés, les administrateurs peuvent limiter l'accès à certains documents, et donner accès pour autoriser la consultation de documents à un groupe d'utilisateurs particulier ; par exemple, un comité des rémunérations peut préférer ne pas partager ses informations avec l'ensemble du conseil d'administration.

L'administrateur d'un portail hébergé pour conseil peut également contrôler l'accès aux appareils en limitant l'utilisation d'appareils personnels et moins sécurisés par les membres du conseil et en imposant l'accès aux données avec les systèmes propres à l'organisation. De même, lorsque des documents sensibles ne sont plus nécessaires, l'administrateur peut effectuer un « nettoyage virtuel » en interdisant leur consultation. De façon similaire, l'accès peut être limité en fonction de l'utilisateur ou de l'appareil, ce qui s'avère utile lorsqu'un membre quitte le conseil et que des documents doivent être récupérés ou qu'un mot de passe a été volé.

MONTRER L'EXEMPLE EN MATIÈRE DE SÉCURITÉ

Il faut accorder la plus grande importance à la cybersécurité, en particulier à la sécurité des informations et données du conseil d'administration ; un portail sûr et intuitif qui gère toutes les informations du conseil, ainsi que la communication et la collaboration entre ses membres, permet d'améliorer la sécurité et les pratiques professionnelles.

L'incapacité d'un conseil d'administration à respecter des normes sécuritaires strictes peut ébranler le système de sécurité de l'organisation dans son ensemble, tandis qu'un conseil d'administration qui montre l'exemple accroît l'efficacité de son entreprise en matière de sécurité et lui permet de mieux résister aux menaces toujours plus nombreuses.

4 BBC News, http://www.bbc.co.uk/news/technology-29011850