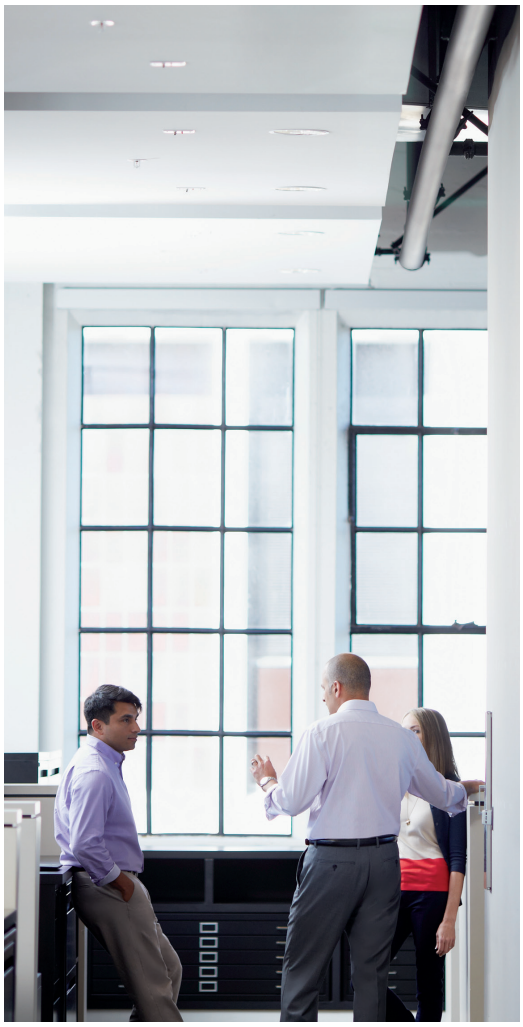
Cinq questions qu'un dirigeant devrait toujours se poser concernant son équipe de sécurité

Office

Microsoft



Les violations de données sont plus qu'un problème de sécurité. Une attaque d'envergure peut avoir une incidence sur votre clientèle, les relations avec vos partenaires, vos cadres, vos bénéfices et vos recettes. Des violations de données d'historique ont coûté leur emploi à plusieurs cadres, entraînant d'importantes pertes de revenus et occasionnant divers dommages à l'image de marque. Une enquête menée en 2014 par Experian et Ponemon Institute auprès de 700 consommateurs concernant l'image de marque a révélé que les violations de données étaient considérées comme les faits les plus dommageable pour l'image de marque, dépassant les catastrophes environnementales et un service à la clientèle insatisfaisant.[1] Dans un monde où les violations de données sont devenus monnaie courante, quelles mesures prendre pour limiter les dégâts ?

Les infractions signalées en 2015 étaient au nombre de 781, en léger recul par rapport aux 783 cas signalés en 2014.[2]

[1] Experian : Conséquences d'une énorme violation de données
[2] Rapport sur les violations de données, Identity Theft Resource Center (ITRC), 2015 Data Breach Report

Le coût total moyen consolidé d'une violation de données en 2015 était de 3,8 millions d'USD, en augmentation de 23 % par rapport à 2013.

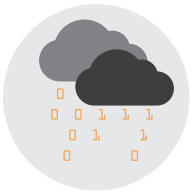
IBM 2015, Étude sur le coût des violations de données

Les failles de sécurité touchent l'ensemble de votre organisation. Cela signifie que les dirigeants doivent unir leurs forces à celles des responsables de la sécurité pour protéger l'organisation.

Si les responsables de la sécurité, les responsables de la sécurité des informations et les analystes en sécurité constituent la première ligne de défense contre les pirates informatiques, ils ne devraient pas être considérés comme l'unique et dernière ligne de défense. Les directeurs financiers, généralement responsables de la gestion des risques financiers auxquelles une organisation est exposée, devraient s'intéresser aux risques liés à la cybersécurité. Et d'autres dirigeants qui n'ont pas les mesures de sécurité dans leurs attributions peuvent également agir en faveur de l'amélioration de la sécurité globale de leur organisation.

- Les responsables techniques peuvent conseiller les responsables de la sécurité et les responsables de la sécurité des informations concernant les logiciels de sécurité implémentés au sein de l'organisation, mais ils devraient également se concentrer sur les caractéristiques de sécurité de toute technologie mise en œuvre.
- Les responsables du marketing les responsables des relations publiques doivent se soucier des risques potentiels d'une violation des données pour l'image de marque, en élaborant un plan de communication pour faire face à toute attaque afin de préserver le chiffre d'affaires.
- Les responsables des ressources humaines doivent être conscients des conséquences qu'une violation interne de données pourraient avoir sur le plan de la confiance des employés, en mettant l'accent sur la protection des informations confidentielles qu'ils gèrent.
- Les PDG et les membres du conseil d'administration doivent être conscients des effets qu'une cybersécurité défectueuse peut avoir sur l'évaluation de l'organisation, et prioriser la sécurité sur leur feuille de route.

En ce qui concerne la protection des ressources organisationnelles les plus importantes, quelles questions tout dirigeant devrait-il poser à son équipe de sécurité ?



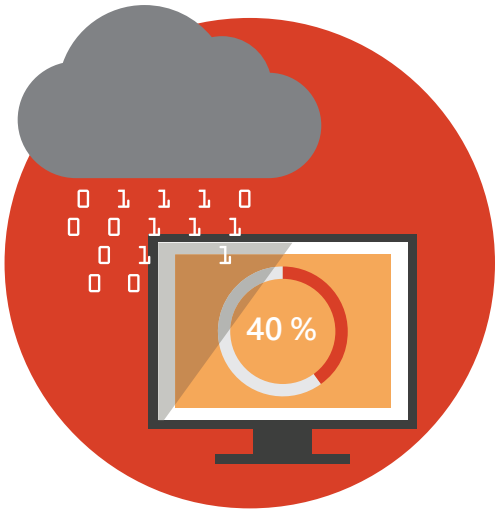
QUESTION 1

Combien de fois constatez-vous l'utilisation de services cloud non approuvés ?

Dropbox. Google Drive. MediaFire. Egnyte. Votre organisation ne soutient probablement pas l'usage de clouds privés, mais il est probable que votre équipe de sécurité ait déjà constaté leur présence.

Les clouds « clandestins » (options de synchronisation et de partage de fichiers privés non prises en charge ou sécurisées par l'infrastructure informatique d'une organisation) se glissent au sein des organisations. Selon une étude réalisée par Symantec en 2013, 77 % des organisations étaient confrontées à des situations de clouds clandestins.[3]

Pour résoudre ce problème, les équipes de sécurité devraient discuter avec les responsables techniques afin de pouvoir recommander un service cloud approuvé par l'organisation. A partir de là, d'autres membres de la direction peuvent peser sur le choix de la solution la plus utile pour leurs employés et partenaires. Discuter avec les équipes de sécurité concernant l'implémentation de solutions cloud prises en charge par l'organisation. Des solutions de niveau entreprise, telles que Microsoft OneDrive Entreprise, permettent aux employés d'enregistrer, de partager et de manipuler des documents sans compromettre la sécurité des données.



40 % des organisations confrontées à des situations de cloud clandestin ont constaté l'exposition de données confidentielles.[3]

[3] Étude de Symantec : Éviter les coûts masqués du cloud

"Le fait qu'Office 365 soit soutenu par Microsoft revêt une importance considérable. Je n'aurai plus à changer de fournisseur parce que je fais confiance à Microsoft pour s'occuper à notre place de notre messagerie électronique et d'autres services."

Paraic Nolan
Directeur financier
Big Red Book

QUESTION 2

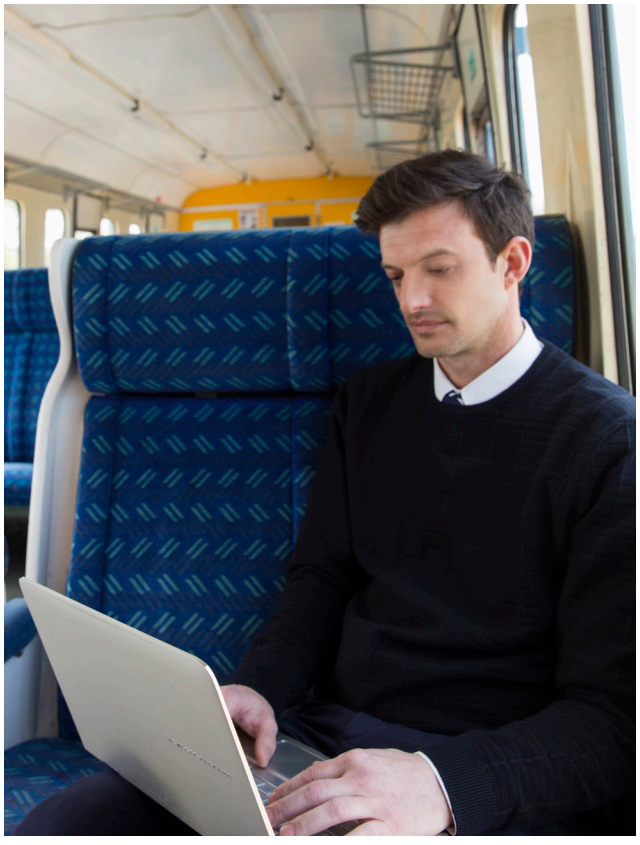
Nous protégeons-nous contre les menaces internes ?

Les menaces internes sont généralement considérées comme l'un des risques les plus difficiles à prévenir. Avec le recours croissant aux sous-traitants, travailleurs indépendants et autres employés intérimaires, se défendre contre les menaces internes potentielles semble pratiquement impossible. En 2013, le FBI a estimé que les attaques malveillantes d'initiés internes avaient un coût d'environ 412 000 dollars par incident.[4]

Bien qu'il n'y ait pas de solution unique pour se protéger contre des menaces internes, les experts recommandent une approche concertée impliquant l'intervention de plusieurs membres de la direction. L'acquisition de talents devrait se concentrer sur de solides contrôles des antécédents de l'ensemble des employés et contractants, et les relations humaines peuvent aider à attirer l'attention sur les comportements singuliers de certains employés (par exemple, qui bâclent le travail ou se vantent des dommages qu'ils pourraient occasionner).[5] Les responsables financiers et techniques peuvent discuter de la possibilité d'implémenter des outils de surveillance du comportement en matière de sécurité afin d'identifier des cas où des employés accèdent à des fichiers qui ne les concernent pas, où des fichiers ou des informations sont enregistrés dans un emplacement externe, et où des employés se connectent à des heures anormales.

Fort heureusement, en cas de soupçon quant à l'existence de menaces internes, des solutions telles que Protection contre la perte de données (DLP) de Microsoft déployées dans OneDrive Entreprise, SharePoint Online, Exchange et Office 2016, permettent à vos administrateurs informatiques de prémunir votre organisation contre la perte de données sans épuiser les budgets prévus pour assurer la compatibilité.

Les administrateurs reçoivent des notifications si des informations confidentielles sont échangées, et ont la possibilité de se renseigner sur les données et l'accès de certains employés. De plus, la solution Protection contre la perte de données permet aux administrateurs d'examiner les données relatives aux incidents, et de générer des rapports ad hoc pour voir précisément où des informations peuvent avoir fuité.



[4] Fred Donovan, FierceITSecurity : La personne assise à côté de vous est-elle un initié malveillant ?

[5] George Silowash, Software Engineering Institute : Common Sense Guide to Mitigating Insider Threats (guide de bon sens pour l'atténuation des menaces internes) : 4ème édition

Vous ne devez pas vous défendre uniquement contre les virus et les logiciels malveillants, car 19 % des incidents de sécurité impliquent des initiés malveillants.

Fred Donovan, FierceITSecurity : La personne assise à côté de vous est-elle un initié malveillant ?

QUESTION 3

Disposons-nous d'un groupe de travail dédié à la cybersécurité ?

On apprend aux professionnels de la cybersécurité à se demander quand (pas si) une violation se produira. Planifier en matière de violation de données consiste à créer un groupe de travail au sein de l'organisation, qui désigne qui se charge de notifier l'attaque aux clients (responsable du marketing), qui assure la sécurisation du réseau (responsable technique, responsable de la sécurité et responsable de la sécurité des informations), et qui gère l'incidence juridique de la violation des informations (responsables des services juridique, clientèle et RH). Si la création d'un groupe de travail dédié la cybersécurité au sein d'une organisation soit considérée comme un pratique recommandée, la plupart des organisations ne disposent d'aucune équipe de ce type.

Selon un sondage réalisé par le service de sécurité des informations de Microsoft, parmi les cadres financiers d'entreprise, 63 % estiment qu'ils se contentent de réagir aux menaces de sécurité, 28 % qu'ils anticipent ces menaces, et 9 % qu'ils sont à la traîne.[6]

Qui faut-il impliquer ? Le groupe de travail sera en grande partie composé d'analystes de la sécurité et d'informaticiens. Mais il ne faut pas négliger l'importance du soutien des services chargés des questions juridiques, des finances, des investissements et des relations publiques. Toute personne potentiellement impliquée dans la résolution d'une violation de données doit faire partie d'un groupe de travail dédié à la cybersécurité et être prête à agir.

[6] Sondage sur la sécurité des informations de Microsoft, septembre-octobre 2015

84 % des organisations ne disposent pas d'un groupe de travail dédié à la cybersécurité.

Financial Executives Research Foundation : Rôle du responsable financier dans la cybersécurité

QUESTION 4

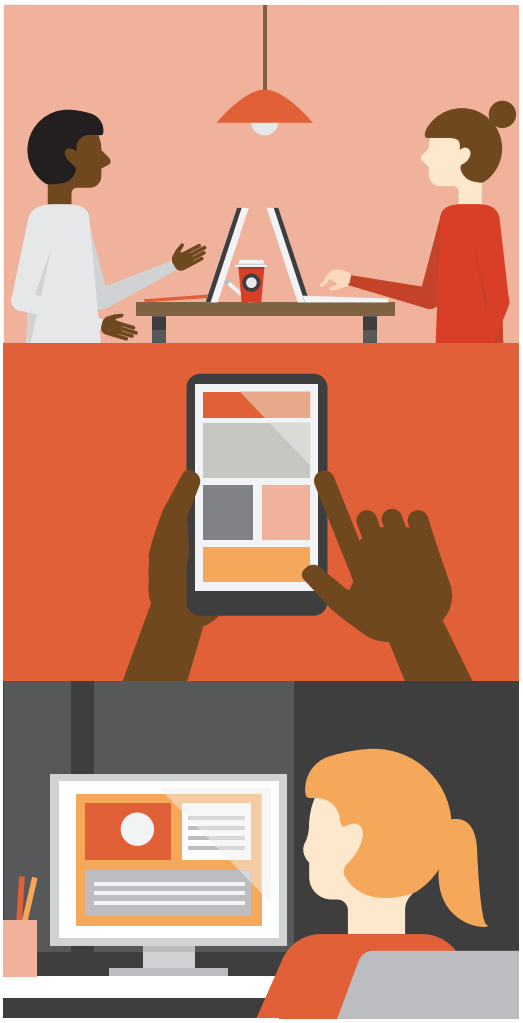
Notre stratégie BYOD est-elle sécurisée ?

Ces cinq dernières années, les stratégies BYOD ont explosé, qui permettent aux employés d'accéder en permanence à des fichiers de leur organisation sur leurs propres appareils. Toutefois, selon un rapport établi en 2014 par Check Point, plus de la moitié des responsables informatiques estimaient que les incidents de sécurité liés aux stratégies BYOD avaient coûté à leurs organisations plus de 250 000 dollars en deux ans.[7]

Il est possible de poursuivre des stratégies BYOD sans compromettre la sécurité ou exploser le budget. Interrogez les équipes de sécurité concernant les capacités d'authentification unique et la gestion des mots de passe libre-service résultant de l'offre actuelle. Des outils de gestion de la mobilité, telle la solution Enterprise Mobility Suite de Microsoft, permettent aux employés de rester connectés aux applications dont ils ont besoin sans compromettre la sécurité. Un rapport de Forrester sur l'impact économique de Microsoft Office 365 révèle que 28 % des utilisateurs en entreprise déclarent avoir constaté une amélioration de la sécurité des données mobiles résultant de la capacité d'Enterprise Mobility Suite à effacer à distance les données d'appareils perdus.[8]

[7] Infosecurity Magazine : Le coût des incidents liés aux stratégies BYOD dépasse 250 000 dollars

[8] Rapport Forrester : Impact économique total (Total Economic Impact™) de Microsoft Office 365, octobre 2014



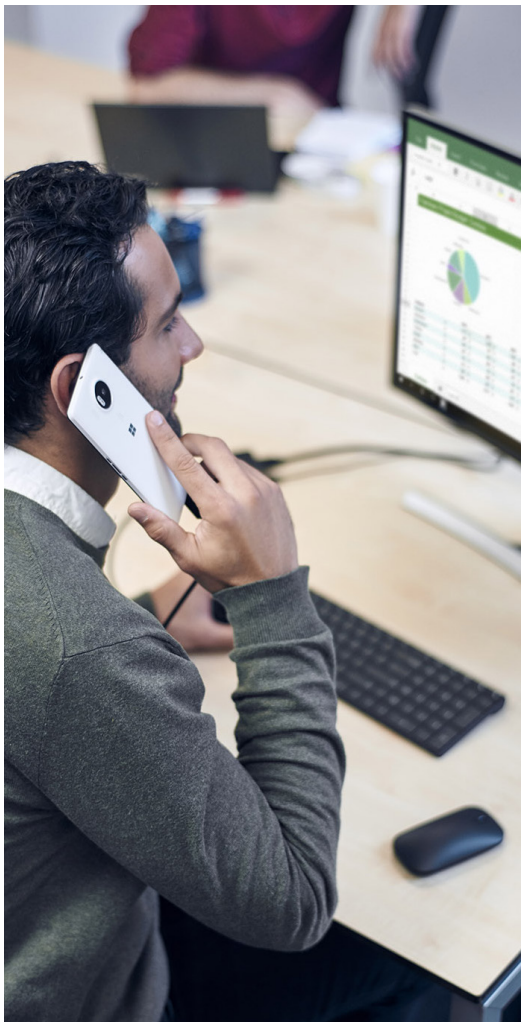
Par ailleurs, l'application Gestion des périphériques mobiles (GPM) intégrée dans Office 365 peut aider une organisation à sécuriser ses appareils mobiles à partir de n'importe quel endroit. Votre équipe informatique peut gérer les stratégies relatives aux appareils mobiles, et effectuer un effacement sélectif des données d'Office 365 quand un employé quitte votre organisation, faisant ainsi gagner du temps à vos services en charge de la gestion des ressources humaines, de l'informatique et de la sécurité.

"Nous devions sécuriser et gérer les appareils mobiles et smartphones utilisés en dehors du réseau d'entreprise, ainsi que les données qu'ils contenaient. La solution Enterprise Mobility Suite offre ces capacités, en un seul package économique."

Kris Mampaey
Directeur informatique
Willemen Groep

QUESTION 5

Vous sentez-vous limité par votre budget disponible pour la sécurité ou par la taille de l'équipe qui s'en charge ?



Les responsables de la sécurité de l'entreprise sont chargés d'embaucher des équipes opérationnelles en permanence, qui doivent gérer de multiples solutions de sécurité et des milliers d'alertes quotidiennes. Leurs budgets et allocations d'embauche sont-ils raisonnables ? Lors de l'examen de la durabilité de la sécurité d'une entreprise, la direction doit veiller à allouer un budget généreux au développement rapide de la sécurité, et évaluer la possibilité de réduire d'autres budgets pour répondre à ces besoins.

Qu'il s'agisse d'embaucher du personnel de gestion, d'engager des analystes supplémentaires ou de doper le budget informatique, déterminez les besoins de votre équipe dédiée à la sécurité, et apportez les changements nécessaires pour vous assurer qu'elle puisse travailler de manière optimale.

Les dépenses en cybersécurité ne ralentissent pas. Gartner a signalé que les dépenses en cybersécurité ont atteint le montant record de 75 milliards de dollars en 2015, et prévoit qu'elles atteindront les 170 milliards de dollars d'ici 2020.[9]

[9] Steve Morgan, Forbes : Le marché de la cybersécurité atteint le montant de 75 milliards de dollars en 2015 ; Il devrait atteindre les 170 milliards de dollars d'ici 2020

Fort heureusement, la plupart des outils que votre entreprise utilise déjà peuvent compléter votre plan de sécurité. Des solutions de synchronisation et de partage de fichiers prises en charge au sein de l'entreprise, telles que Microsoft SharePoint et OneDrive Entreprise, peuvent éliminer l'utilisation par les employés de clouds clandestins, tout en améliorant sensiblement la sécurité sous-jacente des fichiers partagés avec des partenaires et sous-traitants. La constitution d'un groupe de travail dédié à la cybersécurité, et la communication avec celui-ci, peuvent être facilitées par des outils de communication de bureau tels que le module de conférence web de Skype Entreprise et Exchange Online. Améliorez la sécurité de votre stratégie BYOD avec les applications mobiles disponibles pour une série de programmes Office sur des appareils Apple, Android et Windows. Plus important encore, tous ces outils sont à la portée de votre budget et probablement connus de vos employés grâce à Office 365.

Le moment est venu de parler avec votre équipe de sécurité.

Avons-nous géré notre utilisation du cloud clandestin ? ☐

Avons-nous sécurisé notre stratégie BYOD ? ☐

Que faisons-nous pour nous protéger contre des menaces internes ? ☐

Mon équipe de sécurité dispose-t-elle d'un budget suffisant ? ☐

Avons-nous constitué notre groupe de travail dédié à la cybersécurité ? ☐

Vous avez besoin d'autres conseil professionnels ?

Plongez dans l'esprit des novateurs dans les domaines des affaires et de la technologie avec la série en diffusion web Modern Workplace de Microsoft :

https://products.office.com/business/modern-workplace/webcast-series