Diligent

10 QUESTIONS

à poser dans l'évaluation de la sécurité des portails pour conseils

Lorsque des organisations engagent un fournisseur de portails pour conseils, elles lui confient la sécurité des documents sensibles et la mise en place d'un système de gestion d'accès à ces documents. Cette responsabilité va au-delà de spécifications techniques. C'est la raison pour laquelle il est essentiel pour les conseils, secrétaires d'entreprises, conseillers généraux et responsables de l'information d'être sereins et d'avoir confiance en la sécurité offerte par le fournisseur de leur portail pour conseils.

Voici donc 10 questions que les organisations devraient poser à tout fournisseur potentiel de portails pour conseils :

1 Le fournisseur investit-il de manière substantielle dans la recherche et le développement pour la cybersécurité ?

Les menaces de cybersécurité évoluent sans cesse - non seulement en raison des avancées technologiques, mais aussi à cause des changements qui s'opèrent dans les bas-fonds du cyberespace. Des pirates isolés ont ouvert la voie à des organisations sophistiquées capables de causer des perturbations à l'échelle mondiale. Un fournisseur de portails pour conseils doit pouvoir démontrer qu'en recherche et développement, il prend les mesures qui lui permettent de garder une longueur d'avance sur les nouvelles menaces.

2 Le fournisseur fait-il preuve de transparence quant à ses processus de sécurité ?

Le fournisseur doit être clairement capable d'expliquer ses dispositifs de sécurité physique (protection des serveurs, routeurs et autres équipements), ses processus de sélection de nouveaux employés, ses contrôles internes, sa surveillance du système (s'il subissait un piratage, comment l'apprendrait-il ?) et tout historique des violations de sécurité et de leur résolution.

3 Le fournisseur répond-il aux normes industrielles les plus exigeantes ?

En tant que gestionnaires externes d'informations confidentielles, les portails pour conseils répondent à des normes de sécurité comparables à celles des départements informatiques les plus exigeants dans bon nombre de secteurs industriels. Les principales accréditations incluent : un historique des audits annuels positifs SOC/SSAE 16 (couvrant la manière dont les fournisseurs rapportent leurs contrôles internes) et de la certification ISO 27001 pour la sécurité (conformité des systèmes de gestion relatifs à la sécurité des informations du fournisseur de logiciels avec les normes internationales, par opposition à la conformité de leurs centres d'hébergement de données).

4 Le fournisseur autorise-t-il des tests d'intrusion externes ?

La plupart des fournisseurs de portails mènent des tests d'intrusion dans le cadre de leur contrôle de qualité. Les portails répondant à des normes de sécurité élevées mèneront ces tests de manière presque continue plutôt qu'annuelle pour suivre l'évolution des menaces. Ils doivent également autoriser les clients et prospects à mener leurs propres tests de sécurité et d'intrusion (ou à engager eux-mêmes des tiers) pour effectuer des tests indépendants. Si cette démarche démontre leur niveau élevé d'assurance, elle constitue aussi une reconnaissance que la sécurité est en fin de compte un travail d'équipe.

5 Le fournisseur s'appuie-t-il sur des plateformes ou des logiciels tiers ?

De nombreux portails sont développés sur la base de plateformes disponibles commercialement ou utilisent des composantes externes prêtes à l'emploi pour certains éléments de leur logiciel. Toutefois, ces éléments tiers apportent leurs propres vulnérabilités de sécurité, ce qui attire les pirates, précisément parce que ces plateformes sont très répandues et ne sont pas développées pour répondre aux exigences d'un portail pour conseils. Au lieu de cela, les portails pour conseils doivent être développés entièrement avec des éléments de sécurité intégrés à tout niveau dans la conception de l'application.

6 Quel niveau de sécurité physique le fournisseur utilise-t-il ?

Si les informations numériques sont souvent perçues comme quelque chose d'intangible, elles sont en fait sauvegardées sur des serveurs bien réels. Ces installations d'hébergement de données doivent être protégées par des gardes sur site, des télévisions en circuit fermé et plusieurs niveaux de sécurité du périmètre. Il faut abriter les serveurs eux-mêmes dans des cages sécurisées, où les données hébergées de chaque organisation sont physiquement séparées les unes des autres. Et leurs clés cryptographiques doivent être protégées par des appareils endurcis et inviolables.

AICPA SOC | ISO 27001 CERTIFIED BY BRIGHTLINE | Télécharger dans l'App Store | Disponible sur le Windows Store

Diligent est une marque de Diligent Corporation, déposée aux États-Unis. Toutes les marques tierces sont la propriété de leurs propriétaires respectifs. ©2015 Diligent Corporation. Tous droits réservés.

7 Quel est le niveau de redondance des données ?

Les données font-elles l'objet d'une copie de sauvegarde ou les centres principaux de données basculent-ils sur des centres de secours ? Les fournisseurs de portails pour conseils doivent disposer d'endroits distants, géographiquement éloignés les uns des autres pour assurer que tout événement susceptible d'impacter un endroit n'en affectera pas d'autre. De plus, la redondance des informations doit être supportée par des renseignements donnés en temps réel, 7 j/7, 365 j/365, sur la performance des données.

8 Est-il possible de restreindre l'accès au portail à un appareil en particulier ?

Lorsque les membres du conseil se trouvent à différents endroits du globe et voyagent fréquemment, le besoin de sécuriser leurs appareils mobiles est capital. L'accès de l'utilisateur peut-il être restreint à l'un des appareils qui disposent d'une connexion au portail ? Existe-t-il également une option pour désactiver l'accès via le navigateur ? Des solutions d'autorisation d'appareils permettent aux organisations d'empêcher l'accès à partir d'appareils inconnus et non fiables. Il en résulte un contrôle plus strict des droits d'accès et des lieux.

9 Le fournisseur permet-il d'adapter le niveau de sécurité du portail ?

Chaque solution de sécurité implique un compromis entre confort et sécurité. Par conséquent, un niveau de sécurité ne convient définitivement pas à toutes les organisations. Au lieu de cela, un portail pour conseils doit être capable d'adapter certaines fonctions aux besoins de sécurité spécifiques de l'organisation et permettre, par exemple, différents niveaux de complexité du mot de passe, des politiques de blocage d'accès et des options d'exportation et d'impression des documents de conseil depuis le portail.

10 Les questions de sécurité du portail sont-elles prises en charge par l'assistance à la clientèle ?

Peu importe le niveau de sécurité d'un portail, la surveillance humaine est nécessaire pour garantir que tous les problèmes sont gérés dans les temps. Par exemple, un directeur qui saisit à plusieurs reprises son mot de passe de manière erronée et dont l'accès au système est bloqué doit recevoir immédiatement un coup de fil de l'assistance qui lui fournira de l'aide et vérifiera l'origine de ses tentatives infructueuses.

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

Courriel : info@diligent.com
Appelez le : +33 (0)1 56 60 58 58
Visitez : www.diligent.com

C0083_FR