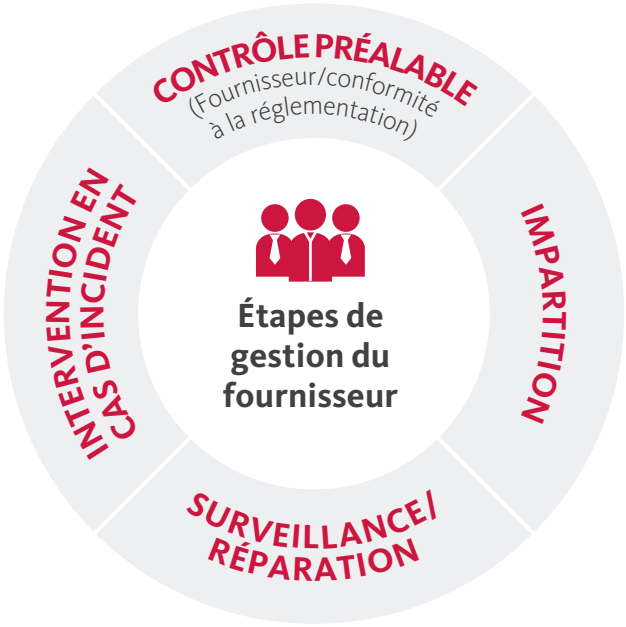
Gestion des fournisseurs : comment protéger vos données

OSLER

Donner à vos fournisseurs l'accès à vos systèmes et données peut être essentiel à la réussite de votre organisation, mais cela peut aussi comporter des risques importants. La gestion efficace de ces risques exige un ensemble de contrôles préalables, de surveillance, de protections contractuelles et d'interventions en cas d'incident.



Études de cas

Un fournisseur d'évaluation du crédit a traité les demandes de crédit au nom d'un grand fournisseur de services de téléphonie cellulaire.

Les attaquants ont eu accès aux bases de données du fournisseur de services et ont obtenu les dossiers de 15 millions de clients de l'entreprise de télécommunications.

Certaines données étaient chiffrées, mais on a craint que le chiffrement ait pu être compromis.

Les attaquants ont eu accès au réseau d'un grand détaillant en passant par un fournisseur.

En recourant à l'hameçonnage, les attaquants ont installé des logiciels malveillants dans les ordinateurs du fournisseur afin de saisir les données d'ouverture de session dans le réseau interne du détaillant.

Le logiciel malveillant était bien connu et aurait pu être détecté par un logiciel de sécurité très répandu. En date d'octobre 2015, le détaillant avait engagé des frais de 290 millions de dollars, dont un montant de 116 millions de dollars en règlement de recours collectifs.

De nombreux grands détaillants ont confié les services d'impression de photos en ligne à un fournisseur.

Les attaquants ont eu accès aux systèmes du fournisseur et ont déployé un logiciel malveillant conçu pour saisir des renseignements personnels et des données de cartes de crédit appartenant à des clients.

Au début de 2016, des recours collectifs avaient été intentés aux États-Unis et au Canada, et le fournisseur de services avait engagé des frais différentiels de 18 millions de dollars à la suite de l'incident.

Liste de vérification : vos contrats tiennent-ils compte des éléments suivants?

- ☑ Le contrôle des données de votre organisation qui sont stockées ou traitées par le fournisseur, y compris la façon de les utiliser, la façon d'y accéder, et la durée de leur conservation.
- ☑ Le retour, le transfert ou la destruction des données de votre organisation.
- ☑ La divulgation de renseignements personnels et d'autres données à des personnes chargées de l'application de la loi.
- ☑ La notification à un client de l'obligation juridique de divulguer des renseignements personnels (à moins que la loi ne lui interdise de le faire).
- ☑ Le recours à des sous-traitants, ce qui peut signifier de leur donner accès à des données ou de leur en transférer.
- ☑ L'utilisation, par le fournisseur, des données de votre organisation à son propre profit.
- ☑ L'obtention d'un consentement avant d'utiliser des renseignements personnels à des fins de marketing ou de publicité.
- ☑ La divulgation d'une liste de pays où les renseignements personnels peuvent être stockés ou traités.
- ☑ La notification à votre organisation de la violation de données et de la divulgation de renseignements nécessaires à votre organisation pour remplir ses obligations en matière d'avis.
- ☑ Les délais à respecter pour aviser d'une violation de données.
- ☑ La consignation du type, du moment et des conséquences d'une violation de données.
- ☑ La divulgation de renseignements sur les processus et les procédures que le fournisseur utilise pour protéger les renseignements personnels et d'autres données.
- ☑ Les paramètres de l'accès restreint et de l'utilisation des données.
- ☑ La séparation logique des données des autres clients du fournisseur.
- ☑ La limitation de l'accès aux données pour ne l'accorder qu'à ceux qui en ont besoin pour effectuer leur travail.
- ☑ L'enregistrement chronologique des données d'accès dans le journal d'audit de sécurité.
- ☑ L'authentification et les contrôles d'accès appropriés (p. ex. authentification à facteurs multiples).
- ☑ Le recours au chiffrement pour protéger les données en circulation et les données inactives.
- ☑ Les procédures pour assurer la continuité des activités et prévenir la perte de données en cas de panne de courant.
- ☑ La conformité avec les normes de sécurité reconnues à l'échelle internationale (p.ex. ISO 27001, 27002 et 27018), y compris la confirmation de la conformité par un vérificateur indépendant.
- ☑ L'imputation des coûts d'enquête et de mesures correctrices à la violation des données.
- ☑ L'imputation des risques de réclamation par des tiers.
- ☑ L'existence d'une couverture d'assurance appropriée.
- ☑ D'autres droits d'audit afin de vérifier la conformité.
- ☑ Les mesures correctrices en cas de non-conformité, telles qu'une injonction.