Liste de contrôle pour la protection des données inter-services

Maximisation de la valeur commerciale grâce à l'évaluation des besoins en matière de sécurité dans l'ensemble de l'organisation

Que vous soyez à la tête d'une entreprise de fabrication mondiale, d'un petit magasin de détail, d'un établissement de soins de santé, d'une école ou d'une organisation à but non lucratif, vous disposez d'informations sensibles dont les pirates peuvent tirer profit, et ces données se trouvent dans tous les coins et recoins de votre entreprise.

Lorsque vous étudiez une solution de protection des données, il est capital de garder à l'esprit les utilisateurs finaux et leurs cas d'utilisation. Cette liste de contrôle vous permet de vous assurer que les données les plus sensibles de votre organisation sont protégées, qu'elles soient en mouvement ou au repos, même lorsqu'elles ont quitté le réseau de votre organisation.

Services devant protéger leurs données

- **Équipe dirigeante : communications stratégiques et confidentielles.** L'équipe dirigeante est responsable de la gestion de l'entreprise et cette tâche inclut souvent des données hautement confidentielles qui doivent être protégées à tout prix. Il peut s'agir de la stratégie et des prévisions de l'entreprise, des communications internes, des présentations des parties prenantes ou des investisseurs, des documents destinés au conseil d'administration, et des informations relatives aux fusions et aux acquisitions.

- **Technologies de l'information et assistance :** identifiants, mots de passe et détails de l'architecture système. La capacité de fonctionnement de l'ensemble de l'organisation repose sur les technologies de l'information. Ce sont également ces technologies qui protègent les mots de passe, les contrôles d'accès, l'architecture système, les logiciels (y compris les correctifs) et les informations de comptes clients de l'entreprise.

- **Service juridique, gestion des risques et conformité :** détails contractuels et documentation sensible. L'American Bar Association recommande le chiffrement des communications avec les clients pour une bonne raison. Une fuite de données juridiques confidentielles, qu'elle résulte d'une erreur utilisateur ou d'une attaque malveillante ciblée, peut déboucher sur des amendes et des frais coûteux, en plus de nuire à la réputation de votre entreprise et d'éroder le sentiment de confiance de vos clients. De plus, à l'instar de l'équipe dirigeante, les services juridiques se voient confier des détails contractuels et des informations stratégiques confidentielles.

- **Service financier : informations bancaires internes et informations de paiement de clients.** Ces données peuvent inclure vos informations comptables internes, les cartes de crédit de l'entreprise et d'autres documents financiers sensibles, ou les données financières des clients. Par exemple, si vous traitez des transactions par carte de crédit pour des clients, les numéros de carte de crédit peuvent être vendus par lot sur le marché noir. Étant bien conscients que les banques surveillent de manière proactive les transactions suspectes, les pirates informatiques ciblent des emplacements de stockage d'informations de carte de crédit massifs pour rentabiliser leurs efforts.

- **Produit, innovation et R&D : propriété intellectuelle et secrets commerciaux.** Bien qu'elle soit plus difficile à chiffrer que les biens physiques, la propriété intellectuelle est l'un des actifs les plus précieux de votre entreprise, et vos concurrents aimeraient beaucoup s'en emparer. Les brevets, les caractéristiques et conceptions des produits, les ressources de recherche et développement, les plans de vente et marketing exclusifs et autres secrets commerciaux sont à la base du succès de votre entreprise. Les laisser aux mains d'espions industriels pourrait donner à vos concurrents l'occasion de voler des parts de marché durement gagnées et de vous faire revenir des années en arrière.

- **Ventes et marketing : listes de clients et appels d'offres.** Ces équipes sont en relation avec l'extérieur, mais gèrent quand même des données confidentielles qui doivent être protégées. Les études de marché, les plans de mise sur le marché des nouveaux produits, les listes de clients, les appels d'offres et les données sur les contrats clients sont souvent gérés par ces services et partagés en interne. En 2021, le système marketing de l'USAID a été victime d'une attaque : un pirate a pu envoyer des e-mails de phishing en apparence légitimes aux contacts de la base de données via un fournisseur tiers.

- **Ressources humaines : données financières et personnelles des employés.** Toute entreprise qui héberge des données personnelles confidentielles, comme des numéros de sécurité sociale, présente un attrait majeur pour les criminels qui cherchent à usurper l'identité de quelqu'un. Tous les documents fiscaux que vos nouvelles recrues doivent remplir représentent une manne financière pour les personnes malintentionnées et possédant un certain savoir-faire en matière de piratage. Lorsque des données salariales et d'autres informations liées aux RH se retrouvent entre de mauvaises mains, cela pèse sur les relations avec les employés et entraîne des défis au niveau du leadership que l'on préférerait éviter.

Pour faire en sorte que les données de votre entreprise restent entièrement sécurisées, il est essentiel d'offrir à chaque employé la possibilité de chiffrer et de protéger ses communications. De nombreuses organisations choisissent d'étendre la protection des données à l'ensemble de l'entreprise, notamment NEXT Insurance (client de Virtru), un leader du secteur des assurances axé sur le numérique. Récemment, NEXT a augmenté son utilisation de Virtru et a acheté des licences pour chaque employé de l'entreprise.

« Nous voulons que chaque personne ait la possibilité de protéger les fichiers qu'elle envoie », a déclaré Ram Avrahami, responsable des services informatiques et des systèmes d'information mondiaux chez NEXT Insurance. « Chaque employé de l'entreprise sera amené à partager des données confidentielles à un moment donné. Peut-être pas tous les jours, peut-être pas toutes les semaines, mais ce moment arrivera. Supposons, par exemple, que vous souhaitiez envoyer un message avec une pièce jointe devant être protégée, ou que vous envoyiez un e-mail contenant des informations confidentielles contenant des mots-clés de protection contre la perte de données (DLP). Nous voulons faciliter le chiffrement automatique de ce type d'e-mail. »