Sécurité des données : avez-vous envisagé d'externaliser ?

Peu d'organisations sont capables d'investir dans toutes les technologies, ce qui dans la plupart des cas, nécessite quotidiennement de prioriser soigneusement les besoins en sécurité en parallèle des autres couts qui pèsent sur des budgets limités.

Et ce n'est pas facile. Avec de nombreux sujets qui requièrent leur attention, les responsables de la sécurité de l'information (RSSI) sont souvent confrontés à des décisions délicates. Par exemple, certaines entreprises optent pour la protection avancée contre les menaces (EPP/EDR) afin de lutter contre la vague continue de brèches de sécurité Pour d'autres, la sécurité et les tests des applications sont une exigence réglementaire et, par conséquent, souvent non négociable. La liste est longue : la croissance des programmes BYOD (amener votre propre matériel), par exemple, a élargi les vecteurs d'attaque pour les cybercriminels, et la prévention de la perte de données reste une préoccupation majeure dont il faut tenir compte.

Par conséquent, les RSSI ont l'habitude d'explorer toutes les options qui peuvent leur permettre d'atteindre leurs objectifs de sécurité tout en respectant le budget disponible. Une possibilité gagne en popularité dernièrement : externaliser la gestion de la sécurité, partiellement ou dans son intégralité. En optant pour un service de sécurité managé, les entreprises peuvent bénéficier d'expertises en sécuritéet déléguer les problèmes liés au déploiement, à l'administrationet à la surveillance des applications à un tiers de confiance.

Cette approche offre de nombreux avantages potentiels : elle peut accélérer le retour sur les investissements de sécurité, améliorer l'efficacité de la sécurité, et ce tout en réduisant les frais généraux et les budgets d'investissement. Bien que la mise en œuvre de la sécurité en tant que service ne soit pas une nouveauté sur le marché, la sophistication des options disponibles et le « rapport protection/coût » de plus en plus favorable renforcent son intérêt pour un large éventail d'entreprises.

Déploiement en interne ou services de sécurité gérés ?

Si les services gérés ne sont pas nécessairement adaptés à chaque organisation ou industrie, nombre de ses défenseurs et utilisateurs considèrent qu'ils peuvent offrir une sécurité de niveau entreprise pour une fraction de l'investissement requis pour déployer la même solution en interne. Ces avantages relèvent d'un éventail d'options qui éclairent souvent le processus décisionnel lors de l'examen d'une stratégie de sous-traitance :

1. Accès à des experts en sécurité

Dans l'ensemble de l'industrie de la cybersécurité, les ressources les plus rares, même pour ceux qui possèdent des budgets plus importants, sont les compétences et l'expérience. Les

professionnels de la sécurité qui déploient, gèrent, surveillent les activités et réagissent aux incidents pour minimiser les dommages sont extrêmement rares dans tous les secteurs, ce qui en fait des ressources précieuses (et souvent onéreuses).

Toutefois, travailler avec un fournisseur de services managés permet aux organisations d'accéder à leur expertise, comme stipulé dans leur accord de niveau de service. Cela peut être un avantage majeur, en particulier pour les organisations au budget limité qui ne peuvent pas se permettre d'avoir leurs propres ressources de sécurité internes.

2. Déploiement flexible

Pour certains, les préoccupations liées à la sensibilité des données incluses dans les rapports de sécurité obligent à conserver leur infrastructure sur site. Mais pour les situations où l'exécution de logiciels en interne n'est pas pratique et que la sous-traitance de la responsabilité n'est pas souhaitable, un modèle hybride a émergé : l'hébergement sur site de services de sécurité gérés. Dans cette approche, le vendeur fournit et gère les solutions utilisées dans le programme de sécurité tandis que le client gère l'infrastructure dans son propre environnement informatique.

Toutes les données restent chez le client tandis que les responsabilités de gestion du programme sont prises en charge par le fournisseur MSSP (Managed Security Service Provider). De cette manière, les organisations disposant de la bande passante informatique suffisante peuvent sous-traiter en toute sécurité les opérations de sécurité à leur(s) partenaire(s) de services managés. En procédant ainsi, les dépenses d'investissement initiales sont minimisées et les préoccupations associées aux données qui quittent les locaux sont éliminées.

3. Accélération de la rentabilité

Malgré la pression omniprésente de réduire le délai de rentabilisation, le déploiement de nouvelles solutions logicielles en interne n'est pas toujours simple. Les équipes internes doivent apprendre à travailler avec de nouveaux logiciels, à gérer correctement leur implémentation et à former leurs collègues (entre autres nombreuses priorités). De plus, l'impact des retards inattendus dus au manque de familiarité avec les outils peut également ralentir le délai de valorisation.

L'utilisation d'un fournisseur de services de sécurité managés peut permettre d'économiser une grande partie du temps de configuration et des coûts associés au déploiement. En outre, les changements d'infrastructure peuvent être minimisés ou entièrement éliminés et les experts du produits assument la responsabilité de l'installation, de la formation et du déploiement auprès de tous les employés concernés. Cela se traduit donc par une mise en œuvre et un délai de rentabilisation plus rapides.

Comment commencer

Le choix d'un fournisseur de services de sécurité managés nécessite un examen attentif et prendre la bonne décision dépendra de plusieurs paramètres. Les organisations disposant de temps, de budgets et de ressources, ou d'une infrastructure complète déjà en place, peuvent trouver que le déploiement sur site reste plus sensé.

D’un autre côté, si la diminution du délai de rentabilisation, la réduction des frais généraux informatiques et une expertise supplémentaire en matière de sécurité sont des priorités plus urgentes, un fournisseur de services managés (ou de services gérés hybrides) peut offrir un moyen très efficace de garantir un avenir sûr.