Cybersécurité : éviter les pièges d'un changement de solution

Les entreprises qui maîtrisent le processus de migration vers une nouvelle solution de sécurité professionnelle connaissent bien la difficulté (et le temps) associée à cette tâche, mais garder conscience des besoins de l'entreprise en matière de cybersécurité est un impératif commercial.

Seule une entreprise sur dix se déclare entièrement satisfaite de sa solution de sécurité actuelle.
Il est donc clair que la plupart des organisations se prépareront bientôt à adopter un nouvel outil ou une nouvelle solution de sécurité.

Selon les prévisions, les cyberattaques coûteront au monde 11,4 millions $ par minute en 2021. Les responsables de la cybersécurité subissent donc une énorme pression pour protéger les actifs les plus critiques de l'entreprise : ses données et sa propriété intellectuelle.
L'exécution d'un plan de migration est toutefois une entreprise importante à mener correctement. Toute défaillance expose l'entreprise à une interruption de ses activités.

Comment savoir s'il est temps de rompre avec votre fournisseur actuel de solutions de sécurité ? Vous trouverez ci-dessous plusieurs indicateurs à prendre en compte avant de définir et d'exécuter une stratégie de migration.

Les catalyseurs du changement

La décision de changer de fournisseur de solutions ne se prend pas à la légère. En parallèle, vous devez passer en revue vos partenariats existants pour déterminer s'ils ont dépassé leur date de péremption. Les solutions de votre fournisseur actuel affichent-elles des performances faibles ou dépassées ? S'appuient-elles sur d'anciennes technologies ?

Dans ce cas, la réputation de votre entreprise, les informations sur vos clients et d'autres actifs sont potentiellement en danger. Si votre solution actuelle ne suit pas le rythme des changements ou l'évolution des vecteurs de menaces, vous devez adopter une solution plus complète.

L'agilité est également une caractéristique essentielle à prendre en compte. Les entreprises sont aujourd'hui en constante évolution, de sorte que les solutions de sécurité des données qui adoptent une approche du type « configurer, oublier » ne sont plus viables.

Si les solutions en place entravent la capacité d'une entreprise à adopter un fonctionnement innovant et agile, il s'agit d'un problème existentiel. Un problème primant même sur les considérations concernant l'évolution des exigences de conformité réglementaire, qui obligent les organisations à réévaluer en permanence la solidité de leurs solutions de sécurité existantes.

Après avoir déterminé que les systèmes et solutions en place ne répondent plus à leurs besoinsactuels et futurs, les entreprises devront franchir le pas et choisir un nouveau vendeur ou fournisseur de solutions. Déterminer qui et pourquoi sera donc le prochain grand défi.

Définir sa stratégie de migration : étape 1

Une rapide recherche sur Google révèle une abondance de fournisseurs, qui proposent tous des solutions de sécurité adaptées aux besoins de chaque organisation. Choisir un fournisseur peut donc présenter des difficultés pour les entreprises. La solution consiste à passer outre le jargon marketing pour déterminer si le service proposé répond vraiment à leurs besoins.

Commencez par discuter avec vos homologues dans votre secteur d'activité. Demandez-leur quelles solutions ils utilisent. Appuyez-vous également sur les conseils des analystes pour obtenir une analyse détaillée des vendeurs et de leurs solutions.

Idéalement, la première étape consiste à prendre le temps de définir une demande de proposition (DDP) très structurée invitant les principaux fournisseurs à vous soumettre des plans formels. Vous devez également constituer une équipe de projet inter-services chargée d'affiner les besoins généraux de l'entreprise, d'évaluer les prestataires potentiels et de déterminer leur capacité à répondre à ces exigences.

Le processus de préparation de l'appel d'offres est essentiel. Il s'agit de définir toutes les exigences, en collaboration avec toutes les personnes concernées, et de vérifier leur cohérence avec la stratégie de l'entreprise. Élaborez un système de notation ou de pondération qui servira de base à la prise de décision, avec notamment un classement des capacités et des exigences souhaitées par ordre d'importance.

Dans le cadre de la méthodologie de sélection, assurez-vous d'élargir les points pris en compte dans le processus. La solution sera-t-elle intuitive pour les utilisateurs ? Comment le retour sur investissement sera-t-il mesuré ? La solution sera-elle suffisamment agile pour suivre le rythme du changement ?

Idéalement, les entreprises raccourciront leur liste à trois fournisseurs maximum et utiliseront le processus d'appel d'offres pour examiner leurs capacités plus en détail. Au cours de l'examen et de l'évaluation des fournisseurs, lancez un programme de démonstration de faisabilité très ciblé pour vous assurer que la solution choisie conviendra à votre environnement.

Définir sa stratégie de migration : étape 2

Après avoir choisi un prestataire, vous passerez à l'élaboration d'un plan de migration pour le déploiement. Ce plan commence par l'évaluation des besoins en données, mais aussi de la classification, de la logique commerciale et des dépendances internes, la définition d'un calendrier assorti d'un test pilote, puis l'élaboration d'une topologie du réseau en vue du déploiement.
Dans le cadre du processus de transition, fixez des étapes claires pour la gestion des versions, la validation, le transfert et la désactivation.

Ne vous arrêtez pas là ! Après avoir correctement exécuté le plan et lancé les éléments de la migration, allez encore plus loin pour optimiser votre retour sur investissement.
Cela nécessite une stratégie post-migration qui intègre des bilans fréquents avec le fournisseur de la solution, axés sur l'amélioration du déploiement et de la valeur ajoutée.

Les pièges courants et les moyens de les éviter

Plusieurs écueils peuvent faire échouer un programme de changement. Le plus évident : ne pas préparer de feuille de route de migration à long terme comportant des livrables précis et un plan d'implication et de communication avec toutes les personnes concernées.
L'absence d'un plan d'urgence au cas où les membres de l'équipe de migration quitteraient le projet en cours de route peut aussi représenter un obstacle. Citons également le déploiement d'une solution avant de la tester et d'impliquer les experts internes.

Une réflexion longue et sérieuse sur ce que vous devez réellement protéger est la mesure la plus importante que vous puissiez prendre pour garantir la réussite de votre projet de migration.
En définitive, le déploiement et la maintenance d'outils ne suffisent pas à assurer la sécurité de l'entreprise. En effet, une tonne d'outils à la pointe du marché ne garantissent pas la sécurité de l'entreprise s'ils ne sont pas intégrés correctement à la stratégie de sécurité globale.

Pour y parvenir, il faut comprendre comment fonctionne l'entreprise, identifier les données et applications essentielles pour apporter de la valeur ajoutée aux clients, et favoriser une stratégie solide de gestion des risques pour protéger ces actifs.

Migrer en toute sérénité

Il y a du vrai dans le dicton « Savoir, c'est pouvoir ». Pour toute nouvelle solution déployée, l'adoption d'une approche axée sur le risque commence donc par une compréhension approfondie des actifs les plus critiques à protéger en matière de données.

En posant les bonnes questions sur l'entreprise dès le début du programme de migration, on pourra déterminer la profondeur, l'étendue et le niveau de service requis, puis déterminer si le fournisseur de sécurité en question est à la hauteur du défi. Car, dans un monde où les frontières traditionnelles de la sécurité n'existent plus, le but du jeu consiste à minimiser les temps de détection à l'aide des processus et technologies de prévention des pertes de données les plus adaptés.