Office 365 : évitez les pièges les plus fréquents sur le plan de la sécurité

VOTRE INFRASTRUCTURE AD LOCALE EST-ELLE LE MAILLON FAIBLE DE VOTRE ENVIRONNEMENT ?

Le guide des professionnels de l'informatique

POUR SÉCURISER UNE INFRASTRUCTURE ACTIVE DIRECTORY LOCALE AU SEIN D'UN ENVIRONNEMENT HYBRIDE

Quest

INTRODUCTION

Chaque mois, plus de **60 MILLIONS DE CLIENTS PROFESSIONNELS UTILISENT LA SUITE OFFICE 365**. L'engouement pour cette plateforme ne cesse de croître, et pour cause. Les entreprises peuvent réduire la complexité de leur infrastructure, ainsi que les coûts de licence et de maintenance, tout en optimisant leurs capacités de stockage. Par ailleurs, la plateforme Office 365 permet aux collaborateurs de travailler à distance sur tout type d'appareil, de gagner en extensibilité et d'assurer la continuité de l'activité.

Néanmoins, lorsqu'ils décident de migrer d'un environnement Active Directory (AD) local pour adopter un annuaire basé dans le Cloud, tel que le module Azure AD de l'environnement Office 365, il n'est pas rare que les décideurs s'attardent sur une même question : la sécurité. Personne ne peut ignorer que les failles de sécurité portent préjudice aux résultats financiers d'une entreprise (et, de fait, dégradent son image).

En 2016, une étude du Ponemon Institute a révélé qu'une fuite de données coûtait en moyenne 4 millions de dollars par incident.

INTRODUCTION (suite)

Sur le plan de la sécurité, quelle doit être la nature de vos doutes ? Microsoft s'engage sur un contrat de niveau de service à 99,9 % avec garantie financière pour la plateforme Office 365. Pour autant, le contrôle des modifications, la gouvernance des accès et la politique de sécurité des données relèvent toujours de la responsabilité des clients. Et la montée en puissance des environnements AD hybrides ne fait qu'aggraver la situation. À bien y réfléchir, 75 % des clients Office 365 qui comptent plus de 500 utilisateurs envisagent de synchroniser leur environnement AD local avec une solution Azure AD et de créer, ainsi, un environnement AD hybride.

Or, ce type de scénario peut conduire à des situations périlleuses et à un manque d'efficacité très handicapant. La moindre négligence lors de la configuration de l'environnement AD local se répercute automatiquement dans l'environnement Azure AD. Les entreprises sont à la fois confrontées aux problèmes de sécurité de l'environnement AD natif et de la plateforme Azure AD. De ce fait, l'envergure de l'infrastructure qu'elles doivent protéger contre les risques de fuites de données et de menaces internes est doublée.

INTRODUCTION (suite)

Sécurisez les données

Pour sécuriser les données stockées dans un environnement hybride, vous devez prendre les moyens nécessaires pour sécuriser votre environnement AD local, que ce soit avant, pendant ou après la migration. Le présent e-book offre un certain nombre de recommandations pour préparer la synchronisation de l'environnement AD local avec la plateforme Azure AD, ainsi que pour protéger les données au cours du processus de migration. Il décrit, en outre, les bonnes pratiques à adopter pour garantir un environnement hybride plus sécurisé.

AVANT LA MIGRATION : METTEZ DE L'ORDRE DANS VOS AFFAIRES

De nombreuses entreprises se reposent sur l'hypothèse selon laquelle les fuites et autres pertes de données sont des coûts à prendre en compte dans le budget d'exploitation et mettent en place des stratégies pour limiter au maximum ce risque. Avant d'entreprendre une migration, les données stockées au sein de l'environnement AD local doivent être recensées en détail et consolidées pour éliminer les éléments obsolètes et superflus. À ce stade, vous devez avoir trois objectifs :

- **Affiner votre cible** : conservez uniquement ce dont les utilisateurs ont besoin et éliminez les données qui ne sont plus utiles sur le plan commercial ou à des fins de conformité ; les données obsolètes ne servent à rien si ce n'est à accroître les risques de menaces et de non-conformité.
- **Passer les comptes des utilisateurs au crible** : éliminez les identifiants en double et les comptes inactifs, associez l'UPN aux noms de domaines destinés à l'environnement Office 365 et corrigez les droits d'accès temporaires accordés aux utilisateurs pour tester les fonctionnalités Office 365.
- **Renforcer les protocoles d'accès** : identifiez les mots de passe faibles et demandez aux utilisateurs finaux de les renforcer, effectuez une mise à jour des droits des administrateurs afin de refléter la réalité des équipes en place et mettez à jour les droits d'accès aux données utilisateur.

Conseil à l'attention des professionnels de l'informatique

Pour éliminer les doublons, exécutez l'outil Microsoft IDFix afin d'identifier et de corriger les erreurs d'objet dans l'environnement Active Directory local avant de synchroniser les utilisateurs, les contacts et les groupes dans l'environnement Microsoft Office 365.

MIGRATION : SURVEILLEZ LES DONNÉES DE PRÈS

Après avoir géré le surplus de données et les comptes en double, résolu les problèmes d'accès et respecté les protocoles de sécurité, l'heure est à la migration vers l'environnement Office 365. Si le travail le plus ardu a déjà été accompli, restez vigilant tout au long du processus de migration pour garantir la sécurité des données. Les administrateurs informatiques doivent mettre en place un système d'audit, de reporting et d'alertes de modifications en temps réel durant le processus de migration afin d'assurer la sécurité des données. Ci-après trois points à observer :

- **Accès** : pour les accompagner dans leurs projets de migration, les entreprises ont souvent recours à des consultants indépendants. Elles sont donc amenées à accorder des droits d'accès temporaires à des intervenants extérieurs.
- **Obligations légales de conservation** : il n'est pas rare que des données en transit doivent être conservées à des fins légales (e-mails archivés ou fichiers Outlook.pst) ; il est donc capital de mettre en place une chaîne de contrôle rigoureuse pour limiter au maximum les risques sur le plan juridique ou de la conformité.
- **Problèmes** : en cas d'anomalies constatées au niveau des données en transit (données consultées par des utilisateurs sans autorisation), réagissez immédiatement pour résoudre le problème. S'agissant des données stratégiques, « mieux vaut prévenir que guérir » dans tous les cas de figure.

Conseil à l'attention des professionnels de l'informatique

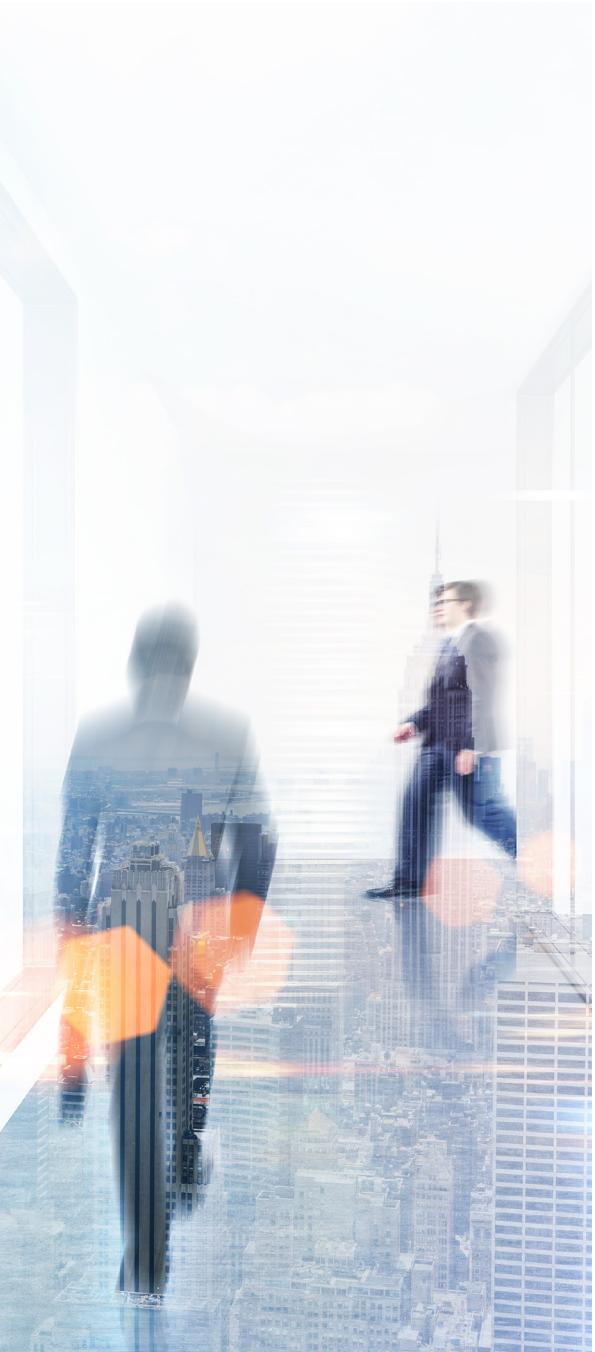
Une migration vers un environnement Office 365 est également l'occasion de remettre à plat l'offre de vos fournisseurs. Chaque prestataire doit vous proposer des solutions pour gérer les données sensibles durant le processus de migration afin de garantir l'intégrité de vos données tout au long de leur cycle de vie. Dans le cas contraire, le prestataire n'a pas suffisamment le souci de défendre vos intérêts.

Après la migration : sécurisez vos activités tout en assurant leur croissance

La migration vers un environnement AD hybride constitue une opportunité unique (même si le processus s'avère fastidieux) de limiter les risques liés à la présence de données inutiles, de droits d'accès/autorisations obsolètes et de comptes d'utilisateurs en double au sein de votre environnement AD local. Après avoir « mis de l'ordre dans vos affaires », le moment est venu d'appliquer 4 bonnes pratiques préconisées à la suite d'une migration afin d'établir une méthodologie relative au cycle de vie. Le but ? Maintenir l'environnement tel que vous l'avez organisé :

1. Recenser en continu
2. Détecter et alerter
3. Corriger et limiter les risques
4. Analyser et restaurer

APRÈS LA MIGRATION : RECENSEZ EN CONTINU



1 Recenser en continu

Il est essentiel d'auditer votre environnement hybride pour comprendre à tout moment qui a accès aux autorisations, aux groupes à privilèges, aux groupes métier sensibles, aux stratégies de groupes (GPO) et aux données. Un recensement détaillé de l'environnement AD local et de la plateforme Azure AD doit vous permettre d'identifier facilement :

- Les domaines exposés aux attaques, les vulnérabilités et le profil de risque
- Les titulaires de droits d'accès aux données sensibles
- Le mode d'obtention des accès
- Les bénéficiaires de privilèges élargis au niveau de l'environnement AD, des serveurs et des bases de données SQL
- Les systèmes vulnérables aux menaces de sécurité

Conseil à l'attention des professionnels de l'informatique

Telle une caméra de sécurité qui fonctionne à tout moment « pour le cas où », il est capital de passer régulièrement en revue les individus qui ont accès aux données et le motif d'obtention de leurs droits. En effet, l'accès aux données sensibles doit être réservé aux individus qui en ont réellement besoin. Cela vaut autant pour des questions de sécurité que pour des obligations de conformité.

APRÈS LA MIGRATION : DÉTECTEZ ET ALERTEZ

2 Détecter et alerter

Identifier en temps réel les activités suspectes au sein d'un environnement AD hybride : telle est la solution pour limiter au maximum l'impact d'une attaque interne ou d'une fuite de données. Pour mettre en relation des données informatiques disparates émanant de nombreux systèmes et appareils, il convient de prendre des mesures de sécurité proactives de façon à détecter rapidement :

- Les autorisations et les activités anormales des utilisateurs
- Des activités suspectes sur des comptes à privilèges
- Des modifications qui peuvent être le signe d'une menace interne majeure
- Un signalement rapide d'intrusion
- Une attaque par force brute en cours

Il est également intéressant d'étudier des solutions qui contribuent à optimiser les outils d'audit natifs. Les outils d'audit des environnements AD natifs, Azure AD et Office 365 n'offrent pas le niveau de gouvernance et de visibilité nécessaire pour satisfaire aux obligations de conformité. Ils peuvent s'avérer problématiques du point de vue de leur fonctionnalité :

- Système d'audit difficile à configurer
- Configuration d'une boîte de messagerie/d'un objet à la fois
- Incapacité à surveiller les règles d'audit en cas d'évolution ou de désactivation par d'autres administrateurs
- Incapacité à configurer automatiquement de nouvelles boîtes de messagerie/de nouveaux objets selon la stratégie d'audit souhaitée
- Absence d'alertes en temps réel, nombre limité d'actions basées sur les alertes
- Durée limitée de conservation des données auditées avant qu'elles ne soient définitivement perdues
- Difficulté d'interprétation des événements

APRÈS LA MIGRATION : CORRIGEZ ET LIMITEZ LES RISQUES

3 Corriger et limiter les risques

En cas de faille (ou d'erreur d'accès), vous devez déterminer les problèmes révélateurs d'un dysfonctionnement et les corriger immédiatement. Dès lors que vous disposez d'un processus de reporting pour détailler les événements qui surviennent tout au long du cycle de vie, vous êtes à même d'agir vite.

L'application automatique de stratégies de sécurité au sein de votre environnement AD hybride garantit une réduction du risque d'erreurs humaines et de leur éventuelle récurrence. Le processus doit veiller à ce que :

- Les dispositifs de contrôle autorisent l'accès aux utilisateurs répertoriés sur la liste blanche et refusent l'accès aux utilisateurs recensés sur la liste noire
- Les utilisateurs bénéficient des droits d'accès les plus faibles possible pour exercer leurs fonctions
- Les ressources sensibles soient protégées
- Les modifications effectuées sans autorisation puissent être corrigées manuellement et sans délai

Conseil à l'attention des professionnels de l'informatique

Les collaborateurs commettent fréquemment des erreurs susceptibles de mettre les données en danger. Proposez aux utilisateurs professionnels des programmes de formation complets qui couvrent les bonnes pratiques à adopter lors de la diffusion de données au sein et en dehors de l'entreprise. Cette formation doit être repensée tous les ans afin de mettre à jour les bonnes pratiques au fil des évolutions technologiques.

APRÈS LA MIGRATION : ANALYSEZ ET RESTAUREZ

4 Analyser et restaurer

En cas d'incident de sécurité, mieux vaut restaurer rapidement les données pour limiter les temps d'arrêt et la perte de productivité. Ce processus doit vous permettre d'analyser les données de sécurité de référence afin de déterminer la manière dont est survenu l'incident et sa cause. Ce processus doit, par ailleurs, vous aider à :

- Prévenir la répétition d'un incident
- Créer un système pour tester le plan de continuité d'activité sans occasionner de perturbations
- Déterminer le temps nécessaire pour effectuer une restauration manuelle à la suite d'un incident de sécurité au sein d'un environnement AD
- Concevoir la meilleure méthode pour rendre l'environnement AD de nouveau opérationnel

EN QUOI QUEST SOFTWARE PEUT VOUS AIDER ?

Parce qu'elles s'appuient sur un réseau d'experts et de partenaires de haut niveau, les solutions Quest contribuent à simplifier la migration, la sécurité et la gestion des environnements Office 365, Azure AD et AD hybrides. Dotée d'une expérience reconnue dans la gestion de projets de migration et de consolidation, la société Quest possède un portefeuille de solutions de bout en bout conçues pour vous aider à :

- Moderniser votre infrastructure AD pour assurer sa compatibilité avec les solutions Cloud
- Réduire les délais de migration et déploiement
- Protéger votre environnement contre les failles de sécurité
- Limiter les risques de non-conformité
- Automatiser les opérations de sauvegarde et de restauration
- Optimiser les coûts de licence afin de maximiser le retour sur investissement

S'appuyant sur près de 20 ans d'expérience dans la migration des plateformes Microsoft, la société Quest confère aux entreprises les moyens d'adopter un environnement Office 365 et Azure AD sans devoir s'engager dans des dépenses colossales, sans risques, sans craintes et sans incertitudes. Découvrez comment la société Quest **garantit la réussite de votre environnement hybride**.

Quest

Join the Innovation.