Pas de ciel sans nuages ... pas d’IT sans cloud!

Avril 2024, Sandro Jaques

De même que les cyberattaques sont inéluctables, la question n'est pas de savoir si, mais quand vous irez dans le cloud. Comment pouvez-vous utiliser le meilleur des solutions cloud et naviguer de la manière la plus sûre possible dans ces environnements en constante évolution? Découvrez ici les principes à suivre pour maximiser les avantages des solutions cloud de Microsoft tout en protégeant de manière proactive vos actifs numériques et vos données confidentielles.

Pouvez-vous éviter le cloud?

Ces dernières années, Microsoft a beaucoup investi dans sa technologie cloud Azure et dans l'intégration de Microsoft 365. On voit clairement - que cela nous plaise ou non - que les solutions de sécurité efficaces de dernières générations sont proposées en priorité dans des environnements cloud et qu'il est très compliqué d'obtenir les services correspondants «on premise».

Ce phénomène est aujourd'hui si marqué que la Confédération et l'Armée suisse ne pourront probablement pas éviter de migrer vers ces services dans les années à venir si elles veulent continuer à répondre aux besoins des utilisateurs finaux.

L’évolution suggère que toutes les entreprises passeront (devront passer) tôt ou tard au cloud. Il s'agit donc de tirer le meilleur parti des solutions de cloud et d'évoluer de la manière la plus sûre possible dans ces environnements en constante évolution, car la responsabilité d'une utilisation sûre incombe toujours aux organisations.

Quel est le niveau de sécurité actuel du cloud?

Les technologies Cloud sont livrées avec une sécurité de base ; néanmoins, elles ne peuvent pas être considérées comme sûres en soi. Les environnements cloud sont mouvants et complexes, leurs fonctions, les rôles, et les droits évoluent constamment. Ceci conduit par inadvertance ou méconnaissance à des configurations qui n’appliquent pas toutes les bonnes pratiques de sécurité.

Nos clients ne savent pas toujours quelles informations ils ont le droit de mettre dans le cloud en regard des bases légales qui leur sont applicables ou des règles internes nécessaires à la protection des secrets commerciaux. Avec qui mes données dans le cloud sont-elles partagées ? Où mes données sont-elles sauvegardées ?

Cloud: les 12 erreurs les plus fréquentes que nous avons relevées

Les constatations issues des Assesments M365 Security de Redguard mettent en évidence des risques majeurs, tels que le partage involontaire de données confidentielles, la vulnérabilité des comptes privilégiés et les risques d'usurpation d'identité.

- De nombreuses données, parfois confidentielles, sont envoyées dans le Cloud Microsoft sans connaissance et consentement de l'utilisateur et des administrateurs du tenant M365 du fait que certaines options avancées d'Office 365 ne sont pas spécifiquement désactivées (paramètres).
- La compromission d'un compte privilégié dans Entra ID peut conduire à la compromission de tous les actifs d'une société du fait que de nombreuses sociétés synchronisent et utilisent les mêmes comptes privilégiés entre l'Active Directory et Entra ID.
- Aucune identification des Devices n'est mise en place dans les "Conditional Access", cela permet alors un accès à toutes les ressources de l'environnement lors de l'usurpation d'un compte utilisateur.
- Les "Conditional Access" ne sont pas configurés de telle manière à ce que le niveau de risque de l'utilisateur ou de la connexion soit évalué avant l'accès aux données (Entra ID Protection).
- Une mauvaise gestion des autorisations d'invitation des utilisateurs externes (Guest users) engendre une perte de la maîtrise dans les partages de données avec des entités externes.
- Lorsque les logs et les alertes ne sont pas configurés correctement, les analyses forensiques sont ralenties tout comme la reprise des activités de l'organisation lors d'une cyberattaque réussie.
- L'activation de « Anyone links » dans OneDrive peut conduire à des fuites de données confidentielles.
- Les fonctionnalités DLP, pourtant incluses dans les licences E3, ne sont que très rarement utilisées afin d'éviter le transfert de données confidentielles et sensibles dans les espaces Sharepoint, via Teams et par mail ou leur stockage dans OneDrive.
- Les outils permettant d'avoir une visibilité sur les utilisateurs, les groupes et leurs autorisations, tels que les "Access Review", ne sont que très rarement configurés.
- Les outils tels que les "CIS Benchmark", permettant de vérifier et de disposer d'un guide de mise en conformité de Azure AD et M365, ne sont que très rarement connus.
- L'autorisation d'utiliser les méthodes d'authentification « legacy » dans les environnements On-premise peut permettre aux collaborateurs de contourner l'utilisation des moyens modernes d'authentification plus sûrs et met à risque le périmètre de sécurité extérieur de l'entreprise.
- L'activation des politiques de partage des calendriers et des contacts dans Exchange Online peut conduire à des fuites d'informations confidentielles de la société.

Comment sécuriser mes activités dans le cloud?

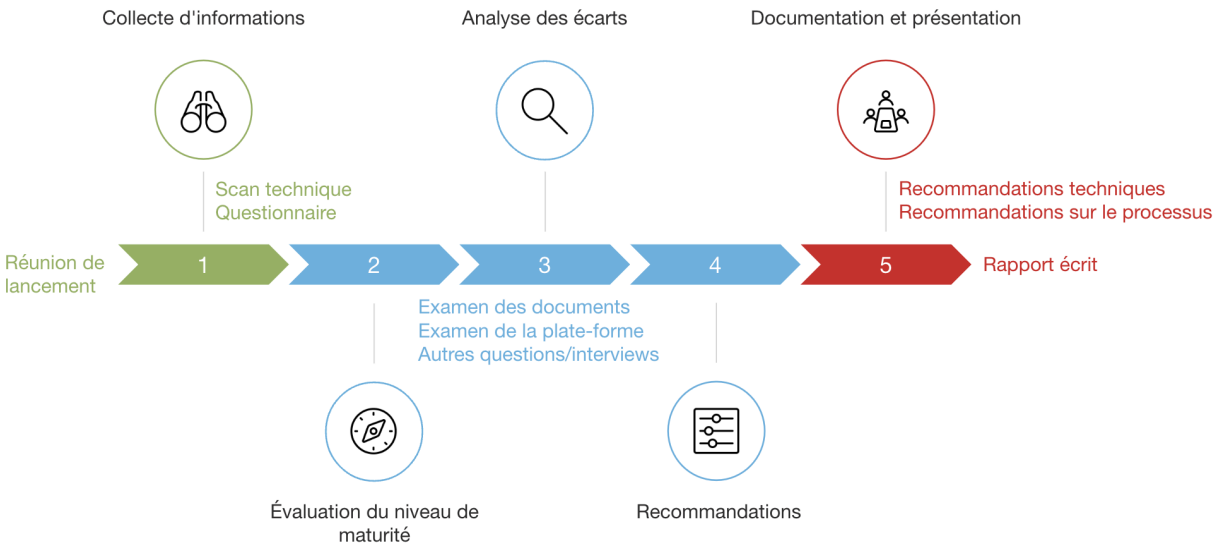
La sécurité des données dans le cloud va au-delà de la simple mise en œuvre des solutions de base, elle nécessite une compréhension approfondie des bases légales, des règles internes et des bonnes pratiques de sécurité.

Une gestion maîtrisée des autorisations, la configuration sécurisée des outils, la surveillance des logs, et une utilisation proactive des fonctionnalités de sécurité proposées par l'éditeur sont autant d'éléments cruciaux.

Les entreprises doivent également accorder une attention particulière à la formation et à la sensibilisation des utilisateurs pour éviter les erreurs de configuration qui pourraient compromettre la sécurité.

Voici les mesures à prendre:

- J'effectue une analyse de risque initiale et je définis un plan de mesure avant la migration de mes données dans M365.
- J'effectue un audit de mon environnement Entra ID et M365, tel que le M365 Security Assessment de Redguard:



- Je mets en œuvre les meilleures pratiques en matière de sécurité dans le cloud: https://www.cisecurity.org/insights/blog/foundational-cloud-security-with-cis-benchmarks
- Je comprends les attaques dans le cloud et j'agis en lien avec ces connaissances pour me protéger plus efficacement: https://attack.mitre.org/matrices/enterprise/cloud/
- Je désire maîtriser mon architecture de sécurité M365: https://learn.microsoft.com/en-us/security/benchmark/azure/overview

En fin de compte, naviguer de manière sûre et efficace dans les environnements de cloud computing exige un engagement continu à appliquer les meilleures pratiques de sécurité, une connaissance approfondie des outils disponibles et une adaptation constante à l'évolution des menaces et des risques. En nous choisissant comme partenaire, vous pouvez compter sur l'expertise acquise au fil des ans par près de 100 spécialistes qui disposent d'une expérience dans de multiples secteurs d'activités . Inscrivez-vous dès maintenant et faites-vous conseiller sans engagement.