ATEMPO
preserving data ecosystems

Protection moderne des données

Comment assurer la continuité d'activité de tous vos environnements

DATA PROTECTION

An Atempo Tech Paper

Aujourd'hui, les entreprises font face à plusieurs défis : crises économiques, pandémies, évolution des réglementations, cybercriminalité grandissante...

De plus en plus sophistiqués, les ransomware ciblent particulièrement les sauvegardes et les postes administrateur. Face à la recrudescence des attaques de type hameçonnage ciblé basé sur l'IA et à la démocratisation du travail hybride, il est important d'adopter les bonnes pratiques pour éviter les intrusions. Les attaques se multiplient et deviennent de plus en plus complexes. La cybercriminalité en tant que service se transforme en un véritable modèle économique.

En raison de son adoption massive, Microsoft 365 n'échappe pas à cette menace. Selon Gartner, en 2025 dans le monde, plus de 75% des sociétés IT auront eu à faire face à une ou plusieurs cyberattaques. Ces attaques peuvent être :

Externes : les hackers accèdent au réseau via des identifiants volés ou des piratages logiciels. Leurs motivations sont souvent financières, économiques ou politiques,

Internes : elles sont plus simples à perpétrer car les attaquants ont déjà accès au réseau.

En 2021, une entreprise est visée par un ransomware toutes les **11 secondes** (Cybersecurity Ventures)

D'ici 2025, jusqu'à **40%** des entreprises seront équipées de solutions de défense contre les ransomwares (Gartner)

En 2021, le coût de la cybercriminalité est estimé à **6 000 milliards**. de dollars, contre 9 400 milliards de dollars pour le Covid-19 (Cybersecurity Ventures World Bank)

44% des attaques sont perpétrées par phishing et liens malveillants (Tendances de la Data Protection 2022).

Afin de se prémunir de ces risques dans les environnements hybrides, il est nécessaire d'intégrer la sécurité à chaque étape du développement de la solution. Pour qu'un logiciel de sauvegarde soit "Secure by design", il convient de répondre à quelques exigences .

LES ENTREPRISES DOIVENT DÉVELOPPER LA CULTURE DU ZÉRO TRUST

Chez Atempo, les équipes de sécurité sont impliquées durant toute la conception de la solution et leur mission est de minimiser les risques. Elles participent activement à la mise en place des normes ISO 27001 et aux processus d'amélioration continue.

Leur rôle est également de suivre les tendances en matière de cybersécurité, les rapports relatant des dernières attaques, le suivi des flux RSS d'organisations telles que l'ANSSI, ou encore la participation à des évènements autour de la sécurité informatique.

UNE SOLUTION DE SAUVEGARDE « SECURE BY DESIGN »

L'intégration de la sécurité dès la conception est une approche du développement logiciel et matériel qui vise à rendre les systèmes résistants aux vulnérabilités et aux attaques grace à des mesures comme l'analyse de l'architecture, les tests d'intrustion continus, les authentifications et le respect des bonnes pratiques en matière de programmation.

Pour les solutions de sauvegarde web, telles que les solutions Atempo, les équipes respectent les principes fondamentaux de sécurité de l'OWASP (l'Open Web Application Security Project) établis pour aider les développeurs à créer des applications web hautement sécurisées.

Récemment, l'actualité a mis en lumière une attaque particulièrement dévastatrice contre une société IT affectant plus de 2 000 organisations. Les criminels avaient alors profité d'une vulnérabilité dans l'outil de gestion informatique. Cet exemple montre que les MSPs sont une cible importante pour les ransomware car les attaquants ont accès aux réseaux des clients. Le "Secure by design" est donc incontournable pour un fournisseur de solutions.

SYSTÈME D'EXPLOITATION LINUX

Les OS Linux représentent une cible bien moins exposée aux failles que les OS Windows.

Linux étant open source, le code peut être facilement modifié pour éviter les problèmes de sécurité. De la conception même de l'OS (gestion de la mémoire, séparation de l'espace mémoire utilisateur/noyau, la mémoire virtuelle, gestion des log), tout est developpé pour rendre les systèmes Linux plus sûrs. Les solutions Atempo sont intégralement conçues pour fonctionner avec Linux. Pour garantir un haut niveau de sécurité, il est indispensable d'appliquer les dernières versions logiciel et patchs correctifs.

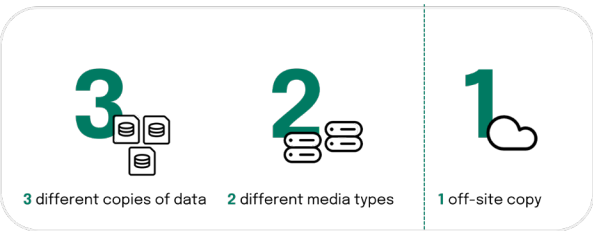
CONSTRUISEZ VOTRE SOLUTION DE SAUVEGARDE EN APPLIQUANT LES BONNES PRATIQUES EN MATIÈRE DE SÉCURITÉ

Pour configurer votre solution de sauvegarde dans les environnements hybrides, des bonnes pratiques doivent être respectées :

- Isolez votre service de sauvegarde et assurez-vous que votre serveur est inconnu de votre Active Directory pour éviter les ransomware. Faites en sorte que seuls les ordinateurs qui ont besoin d'accéder à vos environnements de sauvegarde peuvent le faire. Il est préférable que les communications restent sécurisées grâce au chiffrement du réseau entre le serveur et les différents nœuds de stockage.
- Chiffrez vos sauvegardes : bien géré, le chiffrement constitue un excellent moyen de défense. Limitez l'accès physique

- aux sauvegardes de données. Que vous choisissiez de stocker vos sauvegardes sur un serveur, un NAS, de la bande ou sur le Cloud, assurez-vous que l'accès est suffisamment contrôlé.

- Appliquez la règle du 3-2-1. Le principe consiste à disposer de 3 copies de vos données sur deux supports différents, dont une est conservée hors site pour garantir la reprise après sinistre. Dans la stratégie de sauvegarde, il est important d'appliquer la protection "Air-Gap». Les solutions Atempo sont conformes aux meilleures pratiques de l'industrie, s'adaptent aux spécificités de chaque entreprise et permettent de bâtir sa propre stratégie de sécurité en ajoutant un verrouillage d'objet ou le support des bandes WORM.



INCLUEZ LA SAUVEGARDE DANS LA STRATÉGIE DE REPRISE D'ACTIVITÉ

Les solutions Atempo vous aident à déployer votre plan de reprise d'activité en cas de sinistre et à préserver vos sauvegardes.

CONTRÔLEZ LES PRIVILÈGES

La solution de sauvegarde doit pouvoir définir précisément le contrôle d'accès basé sur les rôles pour permettre aux utilisateurs d'accéder à la solution et respecter le principe de moindre privilège qui précise qu'un utilisateur doit bénéficier d'un minimum de privilèges pour réaliser une tâche. Les solutions Atempo proposent l'authentification multifacteurs pour augmenter le contrôle de l'accès aux données par l'utilisateur.

RESPECTEZ LES NORMES FOURNISSEURS

La technologie Atempo garantit que les données sont protégées et restaurées en cas de sinistre, conformément aux normes des fournisseurs. Atempo respecte les recommandations de Microsoft en utilisant les dernières API conseillées pour sauvegarder et restaurer les données Microsoft 365. Les solutions Atempo utilisent les API Microsoft Graph alors que de nombreuses solutions utilisent encore EWS (Exchange Web Services) pour la sauvegarde et la restauration des données.

L'adoption des solutions de Data Protection Zero Trust s'est accélérée en réponse à la démocratisation du travail à distance. Malgré la flexibilité des nouvelles méthodes de travail, les organisations peinent à contrôler et sécuriser l'accès aux données et aux ressources réseau. La mise en place d'une stratégie Zero Trust permet d'augmenter le niveau de sécurité en contrôlant les accès, et ainsi réduire les connexions non autorisées aux localisations réseaux critiques.

La flexibilité des solutions Atempo permet d'améliorer la sécurité des connexions entrantes, de s'assurer du respect des bonnes pratiques et s'accompagne d'une innovation continue pour protéger et suivre de près vos données.

L'offre de protection des applications M365 est particulièrement efficace car elle permet une modularité des rétentions sur une variété de supports de stockage dont la bande pour effectuer des sauvegardes dites "Air-Gap".

Mise à jour : 02/09/2024