Pourquoi les programmes de sécurité « Zero Trust » doivent intégrer la sauvegarde et la récupération des données ?

Etant donné l'environnement actuel qui est mondial, mobile, hybride, cloud et sans frontières, les approches traditionnelles en matière de sécurité ne peuvent plus fonctionner. La seule confiance accordée aux employés, aux clients et aux partenaires ne saurait être un gage de sécurité. La nouvelle injonction est désormais : « Ne faites jamais confiance, vérifiez systématiquement »

L'idée que des douves entourent les entreprises dans lesquelles les interactions à l'intérieur de leur château fort sont fiables et toutes les interactions extérieures ne le sont pas est dépassée. Il existe désormais une meilleure approche : le « Zero Trust ». C'est un antidote aux stratégies de sécurité obsolètes, car il exige des organisations qu'elles suppriment totalement la confiance de l'équation en limitant et contrôlant les accès.

Le « Zero Trust » consiste à évaluer le niveau de sécurité des utilisateurs en fonction de leur identité, localisation, de leur appareil et de leur comportement, afin de déterminer si les utilisateurs sont bien ceux qu'ils prétendent être. Le « Zero Trust » consiste également à accorder juste assez de privilèges, seulement au moment opportun, pour que les utilisateurs puissent effectuer les tâches et opérations nécessaires, et rien de plus.

Avec le « Zero Trust », seules les autorisations minimales sont accordées, juste au bon moment, pour accomplir une tâche précise. Ces autorisations sont ensuite révoquées immédiatement après l'achèvement de la tâche ou de la transaction. Une approche de sécurité de type « Zero Trust » authentifie et autorise chaque connexion, par exemple, lorsqu'un utilisateur se connecte à une application ou un logiciel à un ensemble de données via une interface de programmation d'applications (API).

Le Cigref, association des grandes entreprises et administrations publiques françaises, s'est récemment penché — dans un rapport — sur la question du Zero Trust, s'interrogeant sur sa pertinence et son implémentation. Pour le Cigref, le Zero Trust transforme une logique de réseau (interne/externe) en une logique applicative dynamique, doit faire l'objet d'une mise en application progressive aussi bien en interne qu'aux produits.

Le constat est le suivant : l'approche actuelle de la protection des systèmes et des informations ne procure pas suffisamment de sécurité. Les organisations doivent partir du principe que des acteurs malveillants s'introduiront inévitablement dans le système et qu'elles doivent tout faire pour minimiser leur surface d'attaque et protéger leurs données critiques en évitant qu'elles ne soient endommagées ou détruites.

Dans le cadre de cette stratégie de « Zero Trust », les organisations doivent également faire preuve d'une vigilance accrue en ce qui concerne leurs stratégies de sauvegarde et de récupération des

données. Le concept de vérification, d'authentification et d'enregistrement permanents de qui va où et fait quoi doit s'appliquer aux opérations régulières et à l'utilisation des applications. Il doit également s'appliquer aux processus de sauvegarde et de récupération des données. Par exemple, il est essentiel de savoir qui est à l'origine de la sauvegarde et où les données sont sauvegardées.

Il est également essentiel de s'assurer que les solutions utilisées pour la sauvegarde et la récupération des données, quelles qu'elles soient, intègrent des mécanismes d'authentification tels que l'authentification multifacteurs, les services d'identité et l'accès basé sur les rôles. Prenons l'exemple d'un employé qui a

besoin de récupérer les données de son ordinateur portable. Quelles sont les informations d'identification qui permettent à cet employé de restaurer la machine ? Quelles autorisations ont été accordées, et ces autorisations doivent-elles être modifiées pour refléter un nouvel ensemble d'exigences ? Si l'équipe informatique restaure un ordinateur portable installé il y a un an, qui garantit que personne d'autre n'a accès à cette machine ? Une approche de la sauvegarde et de la récupération des données basée sur la confiance zéro peut contribuer à résoudre ces questions tout en sécurisant davantage les données de l'entreprise.

La bonne nouvelle est que l'adoption du « Zero Trust » pour la sauvegarde et la récupération peut signifier l'extension des contrôles de sécurité qui existent déjà. Par exemple, l'application de l'authentification multifacteurs aux processus de sauvegarde et de restauration peut contribuer à établir une garantie de l'identité de l'utilisateur et à ajouter un niveau de protection plus élevé aux organisations.

Le stockage immuable doit également faire partie de toute initiative de « Zero Trust ». On parle d'immuabilité lorsque les données sont converties en un format permettant d'écrire une fois et de lire plusieurs fois. Le stockage immuable protège les données contre les attaques malveillantes en prenant continuellement des snapshots de ces données toutes les 90 secondes. Comme le stockage objet est immuable, il peut être restauré rapidement, même s'il a été victime d'un ransomware.

Les compromissions de données étant de plus en plus nombreuses et complexes, les entreprises doivent envisager de nouvelles approches pour renforcer leur protection contre les cybermenaces.

Le « Zero Trust » n'est pas une technologie ou une architecture spécifique. Il s'agit plutôt d'une nouvelle façon de penser qui peut aider les entreprises à mettre en place une protection plus résiliente contre les menaces et à atteindre un niveau de sécurité supérieur.