Restreindre l'accès aux systèmes mainframe pour renforcer leur sécurité

Les systèmes mainframe restent essentiels aux activités des entreprises : selon une enquête récente de Forrester, 72 % des applications destinées aux clients sont en effet « totalement ou fortement dépendantes » du traitement mainframe.

Actuellement, 64 % des entreprises exécutent plus de la moitié de leurs applications critiques sur leurs systèmes mainframe, contre 57 % en 2018. Mais ce n'est pas tout. IBM indique que 80 % des données d'entreprise à l'échelle mondiale sont stockées ou générées par ces systèmes.
Malgré cela, beaucoup d'entreprises peinent encore à sécuriser leur mainframe. Selon IBM, 85 % d'entre elles considèrent la sécurité mainframe comme une priorité lors de leurs prises de décisions, mais 67 % avouent qu'elles n'y pensent qu'occasionnellement ou rarement.Compte tenu de l'importance vitale des systèmes mainframe pour les entreprises, le renforcement de la sécurité est exigé par diverses règlementations comme le RGPD, le CCPA ou le PCI DSS. Celles-ci requièrent des contrôles de sécurité que nous allons aborder ici.Ces règlements visent à protéger les utilisateurs et leurs données. La norme PCI DSS exige par exemple le recours à l'authentification multi-facteurs (MFA) dans certains scénarios concernant les données des titulaires de compte, le chiffrement, le masquage des données et des pratiques spécifiques pour l'application des correctifs de sécurité.

Le RGPD exige la protection des données en transit et au repos. Il vise principalement à restreindre l'accès aux informations personnelles identifiables (PII) pour que seules les personnes ayant un motif légitime puissent les consulter. Le CCPA repose sur les mêmes principes fondamentaux que le RGPD.

Les données sensibles doivent bénéficier d'une sécurité renforcée

Face à ces exigences réglementaires et à la multiplication des failles de sécurité, il est clair que les systèmes contenant des données sensibles doivent bénéficier d'une protection renforcée. Les identifiants de compte compromis s'imposent comme la faille de sécurité la plus courante. Les entreprises doivent donc rendre l'accès plus difficile pour éviter ces incidents.

Aujourd'hui, il est absolument essentiel d'appliquer les contrôles de sécurité d'entreprise aux systèmes mainframe. Les organisations doivent au moins déployer les capacités suivantes : contrôle des accès, confidentialité des données, durcissement des endpoints.

L'authentification multi-facteurs (MFA) est l'une des solutions les plus efficaces pour contrer les tentatives d'accès non autorisées. En effet, il ne suffit pas d'avoir le mot de passe de l'utilisateur pour se connecter. En plus de ces contrôles d'accès, les entreprises peuvent chiffrer et masquer leurs données sensibles pour garantir leur confidentialité et leur sécurité. Dans l'éventualité où un

système serait compromis, l’entreprise est assurée que les cybercriminels ne pourront pas voir ses données sensibles chiffrées et masquées.