Transformation digitale : pas de succÃ¨s sans cybersÃ©curitÃ© intÃ©grÃ©e
SÃ©curitÃ©
PostÃ© par : JulieM
PubliÃ©e le : 14/3/2022 15:00:00

Salesforce a rÃ©cemment pris des mesures importantes pour renforcer ses protocoles de sÃ©curitÃ©, en exigeant de tous les utilisateurs qu'ils mettent en Å□uvre une authentification multifacteur (MFA) pour accÃ©der Ã ses produits, ses solutions et ses plateformes.

Cette exigence vient complÃ©ter des initiatives lancÃ©es par dâ□□autres gÃ©ants de la technologie, tels que Google et Twitter, et intervient alors que des cyberattaques sophistiquÃ©es continuent de cibler les entreprises de toutes tailles et de tous secteurs.

Selon Charles Cao, Directeur des OpÃ©rations et de la stratÃ©gie chez Conga, cette accÃ©lÃ©ration de mesures prises par les acteurs intervenants dans les processus de digitalisation est nÃ©cessaire dans un contexte oÃ¹ les cyber-risques sont trÃ¨s Ã©levÃ©s pour les organisations, qui doivent placer la cybersÃ©curitÃ© au premier plan :

Â« Depuis deux ans maintenant, nous avons observÃ© une accÃ©lÃ©ration importante de la transformation digitale au sein des entreprises pour rÃ©pondre Ã lâ□□Ã©volution des besoins des clients. Ces changements majeurs et rapides ont permis aux organisations de maintenir, voire de booster leur activitÃ© face Ã une sociÃ©tÃ© en pleine mutation. Pour beaucoup dâ□□entreprises, le digital a donc gÃ©nÃ©rÃ© un nombre important dâ□□opportunitÃ©s business.

En parallÃ¨le, ces transformations ont exposÃ© les organisations Ã de nouvelles menaces auxquelles elles font dÃ©sormais face. Elles doivent composer avec de nouveaux modes de travail, des collaborateurs dispersÃ©s, entre travail au bureau et Ã distance, et ainsi la nÃ©cessitÃ© dâ□□Ã©valuer les risques liÃ©s Ã la prolifÃ©ration des appareils connectÃ©s, professionnels et personnels.

De ce fait, le volume des donnÃ©es sensibles et critiques en circulation a considÃ©rablement augmentÃ©, tout comme la surface dâ□□attaque. Si l'on ajoute Ã cela des rÃ©glementations et des exigences de conformitÃ© plus strictes, les entreprises doivent impÃ©rativement prendre conscience de la valeur stratÃ©gique de la cybersÃ©curitÃ© en tant que facteur de pÃ©rennitÃ© et de croissance.

Pour relever ces dÃ©fis, la cybersÃ©curitÃ© doit ainsi Ãªtre intÃ©grÃ©e Ã la conception et Ã l'Ã©laboration de la stratÃ©gie de transformation digitale. Elle ne doit en effet pas Ãªtre traitÃ©e comme une simple rÃ©flexion une fois le processus engagÃ©. Aujourd'hui, les organisations ont commencÃ© Ã reconnaÃ®tre la nÃ©cessitÃ© d'Ã©tablir une stratÃ©gie de sÃ©curitÃ© solide et de la mettre en Å□uvre avec succÃ¨s.

Les dirigeants comprennent en effet de plus en plus qu'ils doivent aller au-delÃ de la simple conformitÃ© et s'assurer qu'ils disposent des capacitÃ©s nÃ©cessaires pour assurer le fonctionnement de l'entreprise et la sÃ©curitÃ© des donnÃ©es. Cette derniÃ¨re est essentielle pour protÃ©ger la propriÃ©tÃ© intellectuelle mais Ã©galement pour Ã©tablir une relation de confiance avec les collaborateurs, les partenaires et les clients.

Cela passe notamment par lâ□□adoption dâ□□outils capables dâ□□identifier les activitÃ©s malveillantes, de rÃ©pondre aux attaques et de s'en remettre rapidement afin de minimiser l'impact sur les opÃ©rations commerciales. Les organisations ont Ã©galement besoin de solutions

flexibles et Ã©volutives pour vÃ©rifier que les utilisateurs sont bien ceux qu'ils prÃ©tendent Ãªtre. Lâ□□objectif est notamment de restreindre lâ□□accÃ¨s aux ressources de lâ□□entreprise et de protÃ©ger les identitÃ©s afin de rÃ©duire le risque liÃ© Ã la perte de donnÃ©es et aux accÃ¨s non autorisÃ©s.

Outre les technologies, les organisations ont Ã©galement un rÃ´le important Ã jouer en matiÃ¨re de sensibilisation auprÃ¨s des collaborateurs. Lâ□□humain est en effet bien souvent le maillon faible de la chaine. Une stratÃ©gie solide ne peut rÃ©ussir si les employÃ©s ne sont pas formÃ©s aux questions de cybersÃ©curitÃ©, aux politiques de l'entreprise et au signalement des incidents.

MÃªme les meilleurs outils de protection ne sont pas infaillibles lorsque des collaborateurs commettent des actions malveillantes, intentionnelles ou non. L'Ã©ducation et la sensibilisation aux politiques de l'entreprise et aux bonnes pratiques, par le biais de formations rÃ©guliÃ¨res et de simulations, sont le meilleur moyen de rÃ©duire la nÃ©gligence ainsi que le risque de compromission.

Si la transformation digitale est aujourdâ□□hui incontournable pour les entreprises, la cybersÃ©curitÃ© lâ□□est tout autant au regard des cybermenaces actuelles. Le cyber-risque est omniprÃ©sent et aucune organisation nâ□□est Ã lâ□□abri. La question nâ□□est en effet plus de savoir si une attaque se produira, mais bien quand ; raison pour laquelle il est primordial dâ□□intÃ©grer la sÃ©curitÃ© Ã sa stratÃ©gie de digitalisation.

Câ□□est un enjeu crucial pour la pÃ©rennitÃ© des activitÃ©s, mais aussi un vÃ©ritable atout concurrentiel alors que la moindre cyberattaque peut avoir des consÃ©quences majeures dâ□□un point de vue Ã©conomique et financier, mais aussi en termes de rÃ©putation. Â»