Gérer les identités et les droits d'accès : une nécessité en matière de cybersécurité

Très souvent mise en avant sous un angle purement technique, la cybersécurité doit également être abordée d'un point de vue organisationnel. À cet égard, les notions de gouvernance, de gestion des identités et des accès aux applications et au système d'information sont des points stratégiques. On notera que cette tendance s'accélère fortement avec le développement du cloud qui héberge la majorité des applications que nous utilisons au quotidien. La gestion des identités est tout sauf anecdotique ! Ainsi, selon une récente étude publiée par le cabinet d'étude Vanson Bourne, 92 % des entreprises ont du mal à gérer les identités.

Mais qu'est-ce que le SSO ?

Le SSO (Single Sign On) est un dispositif qui permet aux utilisateurs de s'identifier de manière unique pour accéder en toute sécurité aux applications et ressources auxquelles ils ont droit. Il s'agit d'une technologie qui a non seulement pour but de simplifier le travail des équipes opérationnelles, mais aussi de renforcer le niveau de sécurité de l'entreprise en adoptant une politique d'accès au SI industrielle. Nous sommes donc à la croisée des projets qui allient technologies et aspects organisationnels.

Une dimension avant tout organisationnelle

Un élément clé pour réussir son projet de SSO est de prendre de la hauteur, de créer un véritable référentiel d'accès au SI et plus globalement de mettre en place une gouvernance d'accès aux ressources digitales et applications de l'entreprise. C'est le prérequis indispensable pour concevoir un système efficace qui prendra en compte les spécificités organisationnelles de chaque entreprise. Il n'y a en effet pas de projet de SSO réussi sans approche sur mesure.

Comment le SSO sécurise les accès aux applications ?

Comme nous l'avons précisé, le SSO permet d'accéder à toutes les ressources digitales au travers d'une authentification unique. Ce point est stratégique quand l'on sait que nous accédons en moyenne à plus de sept applications par jour, qui nécessitent autant de mots de passe différents. Le risque est alors évident : des mots de passe trop simples, notés sur des post-its, etc. Autant de facteurs qui peuvent nuire très gravement à la sécurité du système d'information. Sans compter les risques liés à l'usurpation d'identité et à la difficulté de mettre en place des pistes d'audit d'accès au SI. Enfin, au niveau des équipes techniques et IT, le SSO permet aux administrateurs de ne plus avoir à gérer des politiques de réinitialisation constante de mots de passe (mots de passe perdus, etc.).

Ne pas négliger la gestion des accès et l'IAM (Identity and Access Management)

Ce point est également capital et contribue fortement à sécuriser au maximum l'accès à son SI, que ce soit en interne comme en externe (avec les partenaires). L'enjeu est de gérer finement les droits d'accès au SI et à telle ou telle ressource. Industrialiser cette étape est fondamental et permet de répondre à de nombreux cas d'usage comme la gestion des entrées et sorties des collaborateurs. Sur ce point, cela contribue notamment à s'assurer qu'un ancien collaborateur ne pourra plus se

connecter aux applications de l'entreprises ni à ses données.

Les projets SSO et IAM impliquent donc de travailler en étroite collaboration entre les départements IT et métiers. C'est à cette condition que la gestion des accès sera un succès opérationnel concret. À l'heure où le système d'information ne cesse de s'ouvrir (en interne et en externe) et où les entreprises multi-sites poursuivent leur croissance, le SSO et l'IAM vont jouer un rôle déterminant dans les politiques de cybersécurité. La question de la bonne gouvernance des accès n'est donc pas un simple gadget, mais un impératif stratégique.