Retour au bureau : redéfinir les politiques d'accès privilégiés sur son réseau

Avec l'accélération des campagnes de vaccination contre la COVID-19, les entreprises préparent progressivement leur retour au bureau. Dans un environnement de plus en plus hybride où les collaborateurs peuvent se connecter en tout lieu et à tout moment, les cybercriminels disposent d'une plus grande surface d'attaque et de nombreuses nouvelles vulnérabilités à exploiter.

En prévision de ce retour au bureau – mais qui sera désormais largement combiné à des jours de télétravail – les entreprises doivent impérativement repenser leurs politiques d'octroie et de gestion des accès à privilèges sur leur réseau, afin de protéger leurs données et leurs collaborateurs en cas de nouvelle faille de données.

Les inconvénients d'un accès trop permissif

Plus les collaborateurs ayant accès aux comptes à privilèges sont nombreux, plus les attaquants ont d'opportunités d'infiltrer les systèmes de l'entreprise. Nous assistons d'ailleurs depuis un an à des fuites massives de données résultant d'attaques utilisant les informations d'identification.

Comme en témoignent les escroqueries par phishing sur Twitter ou encore les attaques contre SolarWinds, les hackers savent très bien que les informations d'identification à privilèges permettent d'accéder facilement aux données d'une entreprise de l'intérieur.
À l'heure où elles vont adopter de plus en plus un modèle de travail hybride combinant bureau et télétravail, les entreprises doivent identifier les autorisations d'accès supplémentaires accordées dans le cadre du télétravail et redéfinir les politiques d'accès à privilèges pour minimiser les risques.

Si les accès à privilèges restent indispensables pour effectuer certaines tâches, la plupart des entreprises ont tendance à accorder pendant trop longtemps des privilèges trop étendus.

Un rapport publié récemment par la société ForcePoint révèle que près de la moitié des utilisateurs à privilèges accèdent aux données sensibles/confidentielles par simple curiosité. Fait encore plus inquiétant, ils sont presque autant à subir une pression pour partager leurs droits d'accès au sein de l'entreprise. En donnant aux utilisateurs un accès plus étendu que nécessaire pour effectuer leurs tâches, les entreprises offrent un plus grand champ d'action aux attaquants.

Voici quelques bonnes pratiques à mettre en œuvre pour renforcer la sécurité des identités à mesure que les collaborateurs réinvestissent les bureaux :

1 – Sensibiliser les employés à l'importance de mots

de passe forts

Les équipes de sécurité doivent mettre l'accent sur la protection des informations d'identification. Les mots de passe sont indispensables, et plus ils sont forts (ou sécurisés), plus il est difficile pour les pirates d'accéder aux comptes des collaborateurs.

Les entreprises devraient investir pour former les collaborateurs aux règles de base de la sécurité des mots de passe, les encourager à créer des mots de passe uniques et complexes pour chaque système, s'assurer que les mots de passe des comptes d'entreprise/professionnels ne sont pas identiques à ceux des comptes personnels, et utiliser des applications d'authentification pour accroître le niveau de protection.

2 – Adopter l'authentification multifacteur

L'authentification multifacteur va de pair avec les mots de passe forts. Les équipes de sécurité doivent intégrer l'authentification multifacteur comme condition minimale requise. L'authentification multifacteur utilise diverses méthodes pour sécuriser les comptes et les utilisateurs, des codes PIN aux clés physiques en passant par la vérification biométrique.

Même lorsqu'un mot de passe a été découvert, l'authentification multifacteur peut protéger les données de l'entreprise en empêchant les cybercriminels d'y accéder. Grâce à cette couche de sécurité supplémentaire, ces derniers auront bien moins d'opportunités de pénétrer le réseau de l'entreprise.

3 – Adopter une stratégie Zero Trust et de moindre privilège

Le modèle Zero Trust élimine les autorisations vulnérables (c'est-à-dire les accès inutiles et excessifs) en faveur d'une attribution plus précise de droits spécifiques. Comme son nom l'indique (Zero Trust peut être traduit par « Confiance zéro »), ce modèle implique de ne faire confiance à personne. La sécurité Zero Trust est plus efficace lorsqu'elle est associée à un modèle d'accès basé sur le moindre privilège qui attribue aux utilisateurs (en particulier ceux nécessitant des autorisations élevées) uniquement les droits nécessaires à l'accomplissement de leurs tâches quotidiennes.

Au moment d'accorder des autorisations élevées, les équipes de sécurité doivent s'assurer que ces droits sont limités dans le temps et qu'ils offrent juste ce qui est nécessaire, ni plus, ni moins. Les entreprises ont tendance à accorder un accès privilégié plus longtemps que requis.
Les collaborateurs peuvent alors abuser de ces privilèges qui sont autant de portes ouvertes sur le réseau pour les pirates. Les équipes techniques doivent mettre en œuvre des solutions flexibles qui simplifient la gestion des autorisations et en permettent une attribution plus précise.

4 – Opter pour la sécurité axée sur les identités

Pour passer à un modèle hybride, de nombreuses entreprises choisiront de migrer leurs opérations dans le Cloud. Et malgré la difficulté de répliquer toutes les mesures de sécurité pendant cette transition, les entreprises pourront atteindre l'objectif Zero Trust en mettant les identités au cœur de leur stratégie. Pour ce faire, les équipes de sécurité doivent s'appliquer à établir un modèle d'identité unifié qui normalise la définition de l'identité dans l'ensemble de l'entreprise, en tenant compte de l'accès sécurisé et des identités numériques des utilisateurs, mais aussi de toutes les applications et données. Elles doivent également adopter des solutions qui leur permettent d'identifier et de révoquer rapidement, le cas échéant, les accès non autorisés au sein du réseau.

À l'heure où les entreprises se préparent au monde du travail de demain, du télétravail aux modèles hybrides, les équipes chargées de la sécurité doivent redéfinir la liste des utilisateurs qui bénéficient d'un accès privilégié et la durée de ces droits qui doivent à tout prix être limités dans le temps. En investissant dans la sécurité axée sur les identités, les entreprises pourront mettre en place une architecture Zero Trust et de moindre privilège qui protégera efficacement leurs données et leurs collaborateurs.