

Bloquer les connexion depuis une plage d'adresses IP

Bloquer l'accès à Office 365 à partir d'une adresse IP

Introduction

De plus en plus de collaborateurs travaillent en dehors des locaux de leur entreprise, depuis l'étranger, ou simplement lors de déplacements ponctuels. Afin d'assurer la sécurité et l'identité des utilisateurs, il est impératif de mettre en place des stratégies de sécurité. Nous verrons dans cet article comment faire cela avec Azure AD.

Prérequis

Avons de commencer, veuillez vérifier que vous disposez d'un abonnement ainsi que des licences utilisateurs « *Azure AD Premium P2* » .

Mise en place

Cliquer dans un premier temps sur votre Azure Active Directory. Puis dans la catégorie « **Sécurité** », allez dans « **Accès conditionnel** ».

Une nouvelle fenêtre apparaît. Cliquez sur « **Nouvelle stratégie** ».

Dans cet exemple, nous souhaitons bloquer toutes les connexions pour l'utilisateur testazure en dehors des IP de sa société. Dans le champ « **Utilisateurs et groupes** », on spécifie le(s) utilisateur(s) qui seront affectés par la stratégie.

Nous pouvons également sélectionner « **Tous les utilisateurs** », puis dans l'onglet « **Exclure** » granuler en fonction de la stratégie. Dans le champ « **Applications cloud** », vous déterminez quelles seront les applications accessibles ou non. Si vous souhaitez que l'individu malveillant n'ait accès à aucune applications, choisissez l'option « **Toutes les applications cloud** ».

Le champ « **Conditions** » comprend plusieurs onglets. Remarque : La stratégie s'activera si et seulement si la situation remplit **toutes les conditions**. Si vous laissez les onglets en statut « **Non configuré** », il ne prendra pas en compte cet élément. L'onglet « **Risque de connexion** » est présent grâce à la souscription de la licence P2. Il permettra l'automatisation de la sécurisation d'accès. Activer la condition en cliquant sur « **Oui** » puis « **Moyen** ». Vous trouverez les correspondances des niveaux de risques en cliquant sur le lien suivant :

<https://docs.microsoft.com/fr-fr/azure/active-directory/active-directory-reporting-risk-events>.

Cliquez sur l'onglet « **Emplacements** ». Ici, nous voulons bloquer l'accès au compte partout dans le monde sauf dans les locaux. Pour cela, activer la condition en cliquant « **Oui** » et on inclut l'option « **Tous les emplacements** ».

On exclut alors de cette stratégie notre adresse IP des locaux. Pour cela, aller dans l'onglet « **Exclure** ». On coche la case et on clique sur « **Configurer tous les emplacements approuvés** ».

Une nouvelle fenêtre s'ouvre. On spécifie une plage d'adresse à exclure, ou bien une seule adresse en /32. Puis cliquez tout en bas sur « **enregistrer** ».

Vous pouvez désormais fermer la fenêtre puis retourner sur le portail Azure et cliquer en bas « **Terminer** ». Dans le champ « **Application clientes** », cochez les deux applications clientes. Cliquez sur « **Terminer** » pour finaliser le champ « **Condition** ».

Pour finir, dans le champ « **Octroyer** », choisissez naturellement « **Bloquer l'accès** » et « **Demander un des contrôles sélectionnés** ». Pour finir, cliquez sur « **Activé** » pour mettre en marche la stratégie, puis « **Enregistrer** ».

Notez que la mise en place de la stratégie peut ne pas être instantanée. Prévoyez quelques minutes avant la prise en compte.

Surveillance avec le module Identity Protection

Identity Protection est disponible après souscription d'une licence « *Azure AD Premium P2* ». Il permet de protéger les identités des utilisateurs, et d'empêcher proactivement l'accès aux identités compromises. Cela est possible grâce aux algorithmes de Machine Learning utilisé par Azure AD prévenant ainsi des dangers potentiels. Pour utiliser Azure Identity Protection, il faut dans un premier temps aller dans le Market Place, puis taper « Identity Protection » et cliquer sur le service. Il faudra épingler le service au tableau de bord. (Veuillez ensuite rafraîchir la page). S'affiche alors sur votre tableau de bord Azure Identity Protection. Cliquez dessus. On observe 3 fenêtres dans l'onglet « **Vue d'ensemble** ». La première fenêtre correspond à l'environnement des risques liés aux utilisateurs. Par exemple si les identifiants d'un utilisateur ont été volés. La deuxième fenêtre indique le niveau de risque des événements des sessions qui peuvent être anormale ou issu d'un environnement non-identifié. On remarque qu'il y'a 3 niveaux de criticité : **Haute**, **Moyenne** et **Faible** Enfin, la dernière fenêtre correspond aux failles de notre environnement pouvant être exploitées.

Si un des utilisateurs de l'organisation possède le niveau de criticité « Haute », on peut par exemple forcer la réinitialisation de son mot de passe.

Vérification

Afin de vérifier, on pourra tenter de se connecter à partir d'une autre adresse IP en dehors de la société. (Pour cela, j'utilise un VPN afin de simuler une IP externe). On remarque bien que l'accès n'est pas autorisé.

Conclusion

Il est donc primordial de sécuriser nos accès à Office365 ou autres applications en cas de vol d'identités. Identity Protection nous permet d'ajouter une couche supplémentaire de protection et de gérer les différents cas possibles comme la connexion simultanée dans deux pays à un intervalle de temps quasi-nul et par conséquent obliger une réinitialisation du mot de passe par exemple. En fonction de votre environnement, vous pourrez donc définir plusieurs stratégies permettant d'accroître considérablement la sécurité d'accès aux ressources de l'entreprise.

