LIVRE BLANC

5 FAÇONS DE GERER LES RISQUES LIES A LA MOBILITE ET A L'INTERNET DES OBJETS

Réduire les risques réseau par des politiques de sécurité

aruba
a Hewlett Packard Enterprise company

TechTarget | Custom Media

INTRODUCTION

Aujourd'hui, les professionnels sont plus mobiles que jamais. Dans le même temps, au bureau ou à l'extérieur, la connectivité ne fait que s'accroître. Selon Gartner, d'ici 2020, plus de 21 milliards d'appareils connectés seront en circulation dans le monde.[1] D'autres experts déclarent qu'à la même échéance, plus de personnes disposeront d'un téléphone mobile que de l'eau courante et d'une voiture, tandis que le trafic Internet franchira la barrière du zettaoctet.[2]

En clair, c'est clore le débat sur la sécurité BYOD. En effet, les entreprises savent depuis longtemps que pour rester concurrentielles, elles doivent se montrer suffisamment flexibles pour permettre aux utilisateurs de se connecter librement à plusieurs appareils, qu'ils soient personnels ou fournis par le service informatique. La majorité des entreprises sont parvenues à cette flexibilité par une approche mesurée, en définissant les conditions dans lesquelles un utilisateur a accès à des données sensibles sur son appareil. Ces conditions portent, entre autres, sur l'état de l'appareil, les procédures d'authentification utilisées ou encore le degré de sensibilité des données concernées. Les entreprises qui affichent une certaine maturité élaborent ces exigences sur la base d'évaluations solides des risques, et les codifient par le biais de politiques officielles. Ces politiques sont destinées à protéger le réseau et les données, tant lors de leur acheminement qu'en statique, sur des terminaux mobiles et IoT.

Mais à l'ère de la connectivité mobile permanente et de l'Internet des objets, il ne s'agit que de la première étape d'une véritable gestion des risques. L'efficacité des politiques de sécurité dépend entièrement de la manière de les mettre en œuvre. Et malheureusement, nombre d'entreprises ne disposent ni de la technologie, ni des processus permettant de réellement transformer les politiques de sécurité en actions cohérentes, à savoir par le biais de workflows d'application efficaces et automatisés. Pour vraiment atténuer le risque d'atteintes aux données liées à la mobilité et à l'IoT, les entreprises doivent réfléchir aux cinq mesures suivantes.

RIEN N'EST PLUS IMPORTANT QUE DE SAVOIR QUI ET QUEL APPAREIL EST EN TRAIN DE SE CONNECTER

A un instant T, la majorité des entreprises sont incapables de quantifier les risques parce qu'elles manquent de visibilité ou de contrôle sur les connexions au réseau. Sans cette capacité essentielle, il leur est difficile de faire appliquer des politiques au sein du réseau, de repérer des indicateurs de compromission et de déterminer leur degré de vulnérabilité face à de nouvelles menaces provenant des applications et utilisateurs mobiles ou de l'IoT.

Pour inventorier tout ce qui se connecte au réseau ou tente de le faire, les entreprises ont besoin de procédures automatisées, notamment pour identifier :

- Qui se connecte
- Comment et avec quel appareil
- Quelles ressources sont accessibles de l'appareil
- Quels risques apportent cet appareil ou cette autorisation d'accès aux données

LA VISIBILITE DES APPAREILS DOIT ALLER DE PAIR AVEC LE CONTROLE DU RESEAU

Si différents outils d'administration dédiés permettent aux entreprises d'examiner efficacement l'état de sécurité des appareils, ces outils ont toutefois leurs limites. En effet, les outils d'administration de terminaux ou d'appareils mobiles ne permettent pas d'intervenir sur le réseau, et ne constituent, à ce titre, qu'un des éléments d'une stratégie solide de sécurité mobile.

Les entreprises doivent être en mesure de non seulement inventorier les appareils qui se connectent au réseau, mais aussi de restreindre les accès en fonction de l'état desdits appareils. Elles doivent pouvoir examiner des informations contextuelles relatives à l'appareil, notamment déterminer l'état de ses paramètres d'autorisation, s'il a été rooté, si sa protection contre les logiciels malveillants est bien à jour et s'il présente d'éventuels signes de compromission.

Et la visibilité de ces éléments contextuels constitue une première étape essentielle. L'étape suivante consiste à associer à cette dernière, un moyen efficace de contrôler le réseau en fonction de la situation de l'appareil et des politiques de sécurité en vigueur. Pour mieux protéger leurs ressources réseau et empêcher les attaques provenant d'appareils à risque, les entreprises ont besoin d'un contrôle automatisé des accès afin de s'assurer que les appareils qui ne satisfont pas aux exigences de leur politique ne puissent pas se connecter tant qu'ils ne sont pas mis en conformité.

1 "Gartner: 21 Billion IoT Devices to Invade by 2020," InformationWeek, 10 novembre 2015
2 "Phones Will Drive Internet Traffic Past the Zettabyte Mark This Year," Recode, 3 février 2016

LE CONTEXTE UTILISATEUR ET ENVIRONNEMENTAL EST ESSENTIEL

Plus les contrôles d'accès mettent l'accent sur l'aspect contextuel, plus il est possible d'affiner les politiques d'autorisation. Certes, l'état de l'appareil est important, mais les informations relatives à l'utilisateur, au point d'origine de la connexion, voire à la date et à l'heure, le sont tout autant.

La mise en application de politiques doit pouvoir surveiller le contrôle des accès pour protéger les ressources réseau en fonction de critères tels que les utilisateurs, le lieu, la date et l'heure, etc. Parallèlement, les entreprises doivent pouvoir relier plusieurs appareils à un même employé et élaborer des processus de contrôle transparents qui ne perdent pas de vue le contexte utilisateur. Ce même contexte servira alors à surveiller le comportement tant des utilisateurs que des entités au sein du réseau.

A terme, l'automatisation du contrôle des accès devrait être optimisée en fonction de la tâche à accomplir, le contexte permettant de minimiser les risques associés à la mobilité.

NE NEGLIGEZ PAS LES CONNEXIONS CABLEES

La sécurité de la mobilité dépend en grande partie de celle des connexions sans fil de l'entreprise. Toutefois, ladite entreprise ne doit pas oublier l'importance des connexions câblées.

Les ports câblés non protégés des espaces publics de l'entreprise constituent bien souvent le talon d'Achille d'une stratégie de protection du réseau solide. Le problème se pose dès lors qu'un visiteur peut déambuler dans l'un de ces espaces, débrancher une imprimante ou le téléphone IP d'une salle de conférence, et le remplacer par un ordinateur portable pour bénéficier d'un accès ouvert et instantané.

ELABOREZ UN PLAN DE REMÉDIATION EFFICACE POUR TOUT SCENARIO

Si un contrôle des accès de grande qualité est indispensable,

il faut toutefois disposer d'un plan ou d'un workflow pour résoudre les problèmes quand les choses tournent mal. L'une des plus grandes erreurs des entreprises consiste à mettre en place une technologie qui contrôle les connexions des appareils au réseau, sans délivrer automatiquement aux utilisateurs un message leur expliquant pourquoi leur appareil s'est vu refuser la connexion. C'est ce type de négligence qui fait exploser le nombre de tickets d'incident, fait perdre du temps aux utilisateurs et irrite la direction.

Les contrôles d'accès que les entreprises mettent en place doivent donc s'accompagner d'un plan et d'un processus visant à rationaliser le workflow en aval du blocage d'un appareil. En d'autres termes, on déclenchera automatiquement, autant que faire se peut, des mesures de remédiation : informer les utilisateurs sur le problème à l'origine de la restriction ; impliquer le service d'assistance et le support informatique ; enfin, mettre à la disposition des utilisateurs une documentation ou toute autre ressource nécessaire pour les guider rapidement au fil du processus de remédiation.

L'AIDE QU'APPORTE ARUBA CLEARPASS

ClearPass offre les fonctionnalités nécessaires à la mise en œuvre de ces cinq mesures : visibilité, contrôle des politiques, automatisation des workflows et intégration avec les autres produits de sécurité. Ses caractéristiques sont notamment les suivantes :

- Gestion intégrée des profils. Il s'agit de collecter en temps réel des données telles que les catégories, les fournisseurs et les versions du système d'exploitation des appareils.
- Processus d'authentification. Ils permettent d'exploiter le contexte des appareils et des utilisateurs pour appliquer les contrôles.
- Partage de contextes. Il permet la collaboration avec des systèmes tiers. Ces systèmes comptent notamment les pare-feu, l'administration des terminaux et des appareils, l'analyse comportementale des utilisateurs et des entités, et des services informatiques qui fournissent des données précises sur les utilisateurs et les appareils en vue d'améliorer les workflows de remédiation.

Autant de fonctionnalités qui confèrent à l'entreprise le pouvoir de régir la manière dont les utilisateurs et les appareils exploitent les ressources internes, et ce indépendamment du rôle de l'utilisateur, du type d'appareil ou du point de connexion.

CONCLUSION: LA COMBINAISON GAGNANTE

Alors que les entreprises s'efforcent d'appliquer toutes ces mesures de réduction des risques liés à la mobilité, il n'existe aucune technologie miracle. Pour gérer toutes les dimensions du risque, elles ont besoin d'un système équilibré de contrôles. Il leur faudra donc combiner des contrôles d'accès réseau granulaires et une visibilité sur les connexions, d'une part, et des plateformes d'orchestration informatique dédiées à la remédiation, d'autre part.

Pour ce faire, les entreprises doivent déployer des solutions dans un souci d'intégration, en veillant à choisir des fournisseurs compatibles pour établir un maillage de sécurité commun et homogène.