Repenser la sécurité pour les mobiles et le cloud

La transformation numérique est d'abord une transformation des usages. Portés par une mobilité omniprésente et un Cloud synonyme d'agilité et productivité, ces nouveaux usages soulèvent autant de nouveaux challenges en matière de sécurité. Les entreprises doivent repenser leur approche en se dotant de protections à même d'offrir une réponse complète qui s'étend des smartphones au Cloud et des identités aux données.

Le Cloud et la mobilité ont, définitivement, fait exploser l'ancestrale sécurité périmétrique qui protégeait jusqu'ici les infrastructures des entreprises. Parallèlement, l'ingéniosité et la complexité des attaques ainsi que la multiplicité des malwares et des attaques de phishing sur tous les environnements ont rendu plus complexe encore la protection des systèmes et des données. « Il faut, aujourd'hui, repenser la sécurité dans son intégralité et la mettre au cœur de l'entreprise » explique Laurent Cayatte, PDG de Metsys. « De l'utilisateur aux dirigeants, il faut une prise de conscience. Chacun doit comprendre que la sécurité est essentielle si l'on veut pouvoir travailler sereinement sans être effrayé par des risques omniprésents de vol d'identité, de données, ou autres. La confiance que l'on place dans le Cloud, dans la mobilité et plus généralement dans l'IT en dépend. ».
C'est pourquoi des partenaires ont aujourd'hui élaboré, autour de solutions techniques comme Microsoft Enterprise Mobility & Security Suite (EMS), de nouveaux programmes d'accompagnement afin d'aider les entreprises à imaginer et concrétiser une sécurité de bout en bout pour protéger les utilisateurs, les identités, les appareils mobiles, les données et les infrastructures tout en redonnant de la confiance et de la sérénité à l'IT.

1 Protéger les identités

Pour Laurent Cayatte, « la sécurité de bout en bout commence par une gestion hybride et fluide des identités. Hybride parce qu'il faut protéger à la fois les identités On Premises (pour se connecter à son PC comme aux applications de l'entreprise) et dans le Cloud (notamment pour se connecter à tous les services SaaS utilisés par l'entreprise). Fluide, parce qu'il est surtout essentiel de ne pas perturber l'utilisateur avec des processus d'authentification trop contraignants et nombreux. ».

Cette protection des identités est un travail de fond qui débute par un audit approfondi de vos Active Directory « On Premises » et Cloud (Azure Active Directory est la clé de voûte d'Office 365 et de la plupart des services en ligne de Microsoft). Les services EMS liés à Azure AD Premium permettent une étude précise et une surveillance avancée des comptes à privilèges et des usages. Ils aident, non seulement, à réduire le nombre de ces comptes mais aussi à affiner précisément les droits octroyés tout en limitant leur champ d'action.
Au-delà de l'audit, des mesures concrètes doivent être mises en œuvre pour sécuriser les accès. EMS fournit une solution d'authentification multi-facteurs pour renforcer les sécurités dès qu'un doute existe ou qu'un accès nécessite des mesures renforcées. Elle offre aussi un portail en libre-service de réinitialisation des mots de passe, ce qui contribue à notablement soulager le support. En outre, l'intégration de Microsoft Identity Manager permet d'automatiser et optimiser le workflow de création, surveillance et suppression des comptes utilisateurs avec tous les accès « on premises » et cloud qui en découlent.

2 Fluidifier les accès

« La protection des identités ne doit pas se faire au détriment de l'expérience utilisateur, sinon cela ne fonctionnera pas » rappelle Laurent Cayatte. Les mots de passe sont vécus par les utilisateurs comme une contrainte. Avec EMS, les entreprises peuvent définir des identifiants uniques pour accéder à toutes les ressources internes et dans le Cloud. Son approche SSO (Single Sign On) permet d'utiliser un même identifiant pour s'authentifier auprès de plus de 2800 services en ligne et applications en mode SaaS.
Combinée aux surveillances de l'activité des comptes, aux rapports avancés et aux fonctions d'authentification

multi-facteurs, **cette approche SSO contribue à fluidifier l'expérience utilisateur quel que soit l'ordinateur ou l'appareil mobile qu'il utilise.** Cependant, des partenaires sont essentiels pour accompagner l'entreprise dans la maîtrise de cet ensemble technologique et la mise en place des bonnes pratiques.

3 Sécuriser les appareils

La mobilité est un véritable défi pour la sécurité des données et de l'infrastructure. Non seulement parce qu'elle fait exploser la notion de périmètre défensif, mais également parce qu'elle introduit une diversité de terminaux et de plateformes (Windows, MacOS, iOS, Android, etc.) qui engendre mécaniquement une complexité supplémentaire. EMS intègre Microsoft Intune, une solution MDM avancée qui centralise, unifie et simplifie la gestion des appareils et de leur diversité.

Dès lors il devient possible de bloquer à distance l'accès à un appareil s'il a été volé, ou de l'effacer à distance. Il est aussi possible d'effacer à distance uniquement les données et applications de l'entreprise sans toucher aux données personnelles lorsque l'employé quitte l'entreprise. Les collaborateurs ont accès à un portail en libre-service qui leur permet d'enrôler leur propre appareil dans les stratégies de sécurité de l'entreprise sans faire appel aux techniciens de la DSI.

« Les différents modules d'EMS fonctionnent de pair et c'est ce qui fait la force de la solution » explique Laurent Cayatte. « En mixant Intune et Azure AD Premium, on peut faire de l'accès conditionnel aux applications pour empêcher qu'un utilisateur accède à telle application ou à telle donnée si son téléphone a été « rooté » par exemple, ou si l'on détecte que l'utilisateur semble s'être connecté à la fois en France et en Chine à quelques minutes d'écart ».

Cette notion d'accès conditionnel aux ressources et aux données est, aujourd'hui, fondamentale. Bien implémentée, elle contribue à considérablement rehausser le niveau de sécurité général.

4 Protéger les données coûte que coûte

« Dans un monde Cloud et mobile, la sécurité doit se focaliser sur la donnée et la protéger par tous les moyens imaginables » constate Laurent Cayatte. EMS incorpore plusieurs fonctionnalités pour sécuriser les données notamment au travers du service Azure Information Protection intégré à l'offre. **Il devient ainsi possible de classer et chiffrer automatiquement les documents confidentiels, de tracer le parcours de ces documents y compris hors des murs de l'entreprise et de simplifier à la fois l'accès et le partage de ces documents protégés et sécurisés sur tous les périphériques**. Bien évidemment EMS prend aussi en charge le chiffrement des emplacements de stockage ou encore l'émission de notifications lors du partage de documents sensibles.

En outre, un module comme Cloud App Discovery permet d'analyser les usages des services Cloud, de comprendre et découvrir les usages des utilisateurs et leurs mauvaises pratiques et de faire ainsi la chasse au Shadow IT et aux risques qu'il induit pour la sécurité des informations confidentielles.

5 Protéger une infrastructure devenue hybride

Bien évidemment, toute sécurité de bout en bout doit aussi s'étendre à la lutte contre les attaques de plus en plus sophistiquées des hackers, hacktivistes, cybercriminels, concurrents malveillants et autres organisations d'espionnage.

« Des services comme Microsoft Advanced Threat Analysis permettent d'identifier les attaques avant que les données ne soient menacées » souligne Laurent Cayatte.

Ils incorporent, en effet, des outils d'analyse comportementale à base de Machine Learning pour contrôler l'ensemble du trafic réseau et des accès, détecter les comportements déviants, et alerter des risques et attaques le plus tôt possible.

Un accompagnement indispensable.

Lister l'intégralité des modules fonctionnels et services d'EMS est un vrai challenge. Bien des entreprises clientes d'EMS en ignorent le potentiel réel d'autant que comme toute solution en partie Cloud elle s'enrichit sans cesse. « Des partenaires comme Metsys sont essentiels pour s'assurer que nos clients comprennent bien toute la richesse de l'offre et qu'ils puissent mettre en œuvre toute cette richesse afin de bénéficier d'une vraie sécurité de bout en bout » souligne Jean-Philippe Lesage, Cloud Solution Architect for Partners chez Microsoft France. Se faire accompagner de partenaires experts, est devenu indispensable. Ils aident les entreprises dans la formulation de leurs besoins, dans l'élaboration des scénarios d'usages qui les accompagnent ainsi que dans la mise en œuvre pratique des solutions.

METSYS

Gold
Microsoft Partner