Avis d'expert – Comment adopter une stratégie Anywhere/ Anytime /Anydevice, tout en assurant la conformité et la sécurité des données ?

11 septembre 2020

Nicolas Cheymol

Nous avons demandé à Nicolas Cheymol, Enterprise Solution Architect et Practice Leader sur les solutions de gestion et sécurisation des périphériques chez Exakis Nelite, de développer la question pour les lecteurs de Solutions Numériques.

Depuis 10 ans, le nombre d'utilisateurs souhaitant accéder à leurs données d'entreprise en mobilité augmente exponentiellement. La réponse logique fut de fournir des PC portables, un accès VPN et éventuellement un téléphone professionnel. Avec l'avènement des smartphones, tous les utilisateurs sont équipés et habitués à consulter leurs courriels personnels et une partie grandissante, souvent non éligible à un téléphone professionnel, veut pouvoir à minima consulter et envoyer des courriels depuis son téléphone.

Un certain nombre d'entreprises travaillant sur des accords de télétravail, de *flex office* ou répondant simplement aux besoins des utilisateurs ont initié le remplacement de 90 % des postes de travail fixes par des PC portables. Depuis le mois de mars, cette stratégie s'est étendue pour organiser le télétravail. Le télétravail massif a forcé les entreprises misant sur une protection périmétrique à revoir leur copie, et souvent, en prenant des risques, afin de fournir un service aux utilisateurs leur permettant de travailler à distance.

Il existe aujourd'hui un panel large de solutions protégeant la donnée tout en permettant à l'utilisateur d'y accéder. Ces solutions ne couvrent pas le premier risque lié à l'identité des utilisateurs qui, si compromise, ouvre l'accès à de nombreuses attaques.

Protéger l'identité

La protection de l'identité se fait sur deux axes : l'authentification multi-facteur et la gestion de risque.
L'authentification multi-facteur ne veut pas dire nécessairement OTP (*One Time Password*) il peut simplement s'agir d'un périphérique connu de l'entreprise (PC, smartphone, Clé FIDO, smartcard, certificat etc.). La gestion du risque lié à l'identité nécessite une solution utilisant le Machine Learning et l'Intelligence Artificielle, afin de détecter si un utilisateur est compromis en fonction de son comportement. Et ainsi, mener les actions nécessaires : ouverture d'incident, blocage de la connexion, réinitialisation du mot de passe.

Contrôler les accès

Une fois vos identités protégées, il est nécessaire de protéger la donnée. Soit en l'empêchant de sortir de l'entreprise sur des périphériques non gérés et fournir des accès distants via des solutions de virtualisation qui répondent à certains besoins mais présentent des limitations d'usages. Ou bien alors en conteneurisant les applications et permettant ainsi par exemple la lecture, l'écriture de courriels sur des téléphones ou tablettes personnels tout en s'assurant que la donnée est chiffrée et l'application protégée par un code PIN.
Afin de s'assurer d'un comportement différent en fonction de la situation des règles d'accès conditionnel doivent être mises en place assurant ainsi une expérience optimale et une sécurité accrue.

Protéger les données

La donnée est au cœur des enjeux des entreprises, la perte ou le vol de données peuvent être catastrophique. La protection de la donnée via des mécanismes de sauvegarde est courante et généralement bien gérée. Il n'est pas rare que l'attaque via ransomware cause des pertes de données critiques car non sauvegardées sur les systèmes adéquats, ou suite à une détection de l'attaque trop lente compte tenu des règles de rétention. La classification des données permet ainsi de détecter de telles failles avant qu'il soit trop tard.

Une donnée, même critique et confidentielle, peut nécessiter un partage en externe avec des partenaires, des sous-traitants etc. Empêcher le partage aux utilisateurs présente des risques économiques forts pour l'entreprise. Les utilisateurs trouvant des moyens de contournement afin de continuer à partager en déclassifiant la donnée, la partageant via clé USB, papier ou autre méthode de shadow IT. La protection des fichiers via une méthode de chiffrement et une authentification à l'accès permet de s'assurer que même une fuite de fichier ne permettra pas à cette donnée d'être accessible par un tiers.

Accompagner les utilisateurs

La protection de l'identité, le contrôle d'accès ainsi que la classification et protection des données doit se faire avec un bon accompagnement des utilisateurs qui permet d'améliorer l'image du service informatique et la visibilité des services fournis afin de se prémunir du shadow IT.

L'exposition des applications à travers une solution sécurisée ne suffit pas pour répondre à l'ensemble des besoins ou à vous protéger de l'ensemble des vecteurs d'attaque. Il est important de fournir des solutions simples d'utilisation, de former les utilisateurs, protéger leur identité ainsi que classifier et chiffrer les documents sensibles.

À LIRE ÉGALEMENT