Violations de données : l'approche « sur site » expose davantage

Les compromissions se multiplient à un rythme effréné, et rien ne laisse présager un ralentissement. Ainsi, selon l'ANSSI, les cyberattaques ont été multipliées par quatre en 2020 par rapport à l'année précédente. Cette croissance constante des cybermenaces repose sur deux piliers : le vol d'identifiants et l'absence de correctifs apportés aux logiciels.

Les limites de l'approche sur site

Le piratage de Microsoft Exchange Server illustre les défis que pose l'infrastructure sur site, en particulier en termes de gestion des correctifs. Parmi les difficultés, il y a notamment la maintenance d'une infrastructure vaste et diversifiée, la disponibilité de l'expertise nécessaire à cette fin, ainsi que le maintien d'une visibilité précise des actifs avec le niveau de détail requis pour traiter les vulnérabilités sur l'ensemble du réseau.

En outre, le temps entre la publication d'un correctif de sécurité et l'exploitation de la vulnérabilité ne cesse de se réduire. Selon une étude de FireEye, 58 % des vulnérabilités découvertes en 2018 et 2019 ont été exploitées le jour même. Plus inquiétant encore, 42 % des vulnérabilités ont été exploitées après la publication d'un correctif, dont 12 % dans la semaine suivant la publication et 15 % dans les deux à quatre semaines qui ont suivi.

Cela signifie que les cybercriminels ont très rapidement pris connaissance de la brèche, déployé leurs stratégies et réussi à attaquer une entreprise avant même que celle-ci ait eu la possibilité d'appliquer le correctif correspondant. En effet, les hackers savent très bien que les entreprises mettent du temps à appliquer des correctifs, ils en tirent donc profit.

La taille et la complexité de beaucoup d'entreprises expliquent ces longs cycles de déploiement des correctifs. Et même en cherchant à raccourcir ces délais, elles ne pourraient le faire que pour un sous-ensemble de leurs systèmes les plus critiques et les plus exposés. Sans compter que patcher sollicite une quantité importante de ressources, ainsi qu'un inventaire précis et détaillé du matériel, des logiciels et des bibliothèques provenant de tiers ; ce que la plupart des entreprises ont du mal à maintenir à jour.

Pour les organisations évoluant dans des secteurs fortement réglementés – tels que les services financiers, les soins de santé ou le secteur public – ce problème est en outre exacerbé par les exigences en matière de conformité.

Seulement, une rapidité d'exécution comporte aussi des inconvénients. Si les équipes IT agissent précipitamment pour corriger un exploit, le risque de compromettre d'autres systèmes ou même de perdre la disponibilité en ligne est élevé. Cela peut être évité en concevant un processus par étapes pour identifier les impacts négatifs potentiels, mais cette stratégie induit un niveau de maturité qui fait défaut à de nombreuses organisations encore actuellement.

Le « cloud-first » accélère la transformation numérique

En pratique, la taille et la maturité des infrastructures sur site sont généralement dérisoires par rapport aux offres des fournisseurs de services de cloud. Bien que la migration vers une solution basée sur le cloud présente des avantages, les entreprises doivent néanmoins effectuer des contrôles préalables pour s'assurer qu'elles n'héritent pas de problèmes différents ou plus graves.

Lorsqu'elle est bien réalisée et fait l'objet d'un examen approfondi, l'adoption du cloud permet aux organisations de tirer parti de la capacité, de la flexibilité, de la maturité et de l'investissement global réalisés par les fournisseurs de plateformes. L'accès à des mises à jour et correctifs automatisés, ainsi qu'à la surveillance et à l'intervention en temps réel — le tout sans nécessiter de ressources supplémentaires — constituent des facteurs clés qui contribuent à la popularité croissante du cloud, en particulier depuis le début de la pandémie.

Depuis un an, les entreprises ont en effet ravivé les plans de transformation numérique, qui devaient s'étaler sur des mois voire des années, et ont migré vers le cloud en quelques semaines pour soutenir une main-d'œuvre très dispersée et vulnérable.

Les dépenses mondiales en services de cloud public devraient ainsi augmenter de 18,4 % en 2021 selon Gartner, pour atteindre un total de 304,9 milliards de dollars.

L'assurance de l'identité

Face à l'évolution du paysage des menaces et aux répercussions considérables des violations, les entreprises devraient comparer les capacités des fournisseurs de services de cloud à leurs propres capacités pour évaluer les risques en cas de compromission réussie : est-ce que l'organisation dispose en interne notamment d'un système d'identité solide basé sur l'authentification unique (SSO) et d'une authentification multi-facteurs (MFA) résistante au phishing.

Ces deux points forment une base de sécurité solide, car permettent non seulement aux entreprises de rationaliser l'accès aux applications décentralisées entre les fournisseurs de services cloud, mais aussi d'assurer un haut niveau de confiance dans les systèmes, les appareils et les utilisateurs qui accèdent aux actifs de l'entreprise.

Cependant, toutes les solutions MFA ne sont pas logées à la même enseigne, le recours au SMS par exemple n'est pas exempt de failles du fait de la technique « Man in the middle ».
Même les technologies reposant sur l'usage d'un mobile et le mode Push notification peuvent être déjouées. Les clés de sécurité physique sont ainsi la seule méthode MFA qui, selon une étude de Google, protège à 100 % contre les attaques de phishing ciblées.