La cybersécurité des effectifs à distance contre les nouvelles attaques par phishing

Malgré les circonstances difficiles liées à la propagation du Covid-19, la technologie a permis de maintenir certaines activités qui, sans elle, auraient dû être interrompues. Toutefois, la migration du travail de bureau vers le travail à distance a dû se faire parfois de manière précipitée. Depuis les entreprises françaises s'efforcent de mettre en place les mesures nécessaires qui n'ont pas pu être établies auparavant, soit par manque de temps ou de budget.

Si la reprise a été amorcée le 11 mai dernier avec la première étape du déconfinement, puis suivie par le stade 2 le 2 juin dernier, de nombreuses organisations ont pris le parti de continuer en télétravail, au moins partiellement, et ce pour toute la période estivale ; une situation qui exige une réorganisation et une meilleure sécurisation de l'environnement des employés, quel que soit l'endroit.

La décentralisation de la sécurité

Les progrès considérables qui ont été réalisés en matière d'outils de collaboration et d'accès à distance, ainsi que la sophistication accrue des dispositifs, ont permis aux employés de s'adapter au travail à distance à l'échelle de l'entreprise. Toutefois, malgré les nombreux bénéfices tirés du télétravail par les entreprises, les plus réfractaires ne manqueront pas de souligner la décentralisation des pratiques de sécurité.
Les équipes IT ont déjà subi le stress lié à l'accompagnement d'une main-d'œuvre qui a dû brusquement basculer vers le travail à distance. A présent, il est primordial que les employés soient dotés d'outils de sécurité adéquats et comprennent pourquoi il est important de les utiliser correctement, afin de garantir la sécurité des données de l'entreprise et la protection des actifs.

De nombreux employés travaillent encore sur des appareils moins sécurisés lorsqu'ils sont à distance, ainsi que sur des réseaux moins sûrs que ceux de leur entreprise. Cette situation ne fait qu'accroître la pression déjà ressentie pour limiter les risques en matière de sécurité et renforcer les défenses de tous les dispositifs et de toutes les applications. Malheureusement, les cybercriminels opportunistes exploitent l'incertitude et la vulnérabilité de cette période qui reste délicate.

Des menaces sophistiquées et de mauvaises pratiques en matière de mots de passe

La multiplication des attaques par phishing – par lesquelles les employés peuvent être amenés à fournir des informations telles que des identifiants de connexion –, combinée aux mesures de sécurité moins efficaces des employés, impose la mise en place d'une authentification forte et de pratiques de sécurité solides. Toutefois, un trop grand nombre d'organisations se fient encore uniquement aux mots de passe pour accéder à leurs appareils, à leurs applications et à leurs

réseaux alors qu'ils comportent toute une série de faiblesses inhérentes : ils peuvent être faciles à deviner, réutiliser et, bien sûr, ils peuvent faire l'objet de phishing. Malgré le risque encouru, ce type de comportement est très répandu.

Une récente étude du Ponemon Institute menée auprès de professionnels et d'employés du secteur IT en France a révélé que 39 % des personnes réutilisaient les mots de passe de leurs comptes professionnels et, plus inquiétant encore, que 51 % partageaient parfois ou fréquemment leurs mots de passe avec leurs collègues.

Les pratiques d'authentification renforcée devraient privilégier la convivialité, car l'adoption de nouvelles technologies et approches sera plus efficace si elles sont pratiques et faciles à utiliser. Que les employés travaillent à distance ou non, ceux-ci ont besoin d'un moyen simple et sûr pour créer, stocker et gérer des mots de passe, et des clés de sécurité matérielles intégrées à des gestionnaires de mots de passe professionnels peuvent les y aider.

La clé de l'authentification

L'authentification multifacteur (MFA) offre un niveau de sécurité supplémentaire inestimable pour les réseaux IT d'entreprise. De plus, dans un contexte particulier où les employés utilisent régulièrement les réseaux domestiques – qui sont généralement moins sécurisés que les réseaux professionnels – la MFA permet de s'assurer que l'accès aux applications et aux systèmes de l'entreprise est parfaitement protégé.

Si l'authentification à deux facteurs (2FA) – basée sur des mots mémorisables ou des mots de passe uniques (OTP) par SMS – est une méthode connue de nombreux utilisateurs qui y ont recours pour accéder à des services à titre privé, elle peut également être exposée au phishing, entre autres menaces. La MFA de base, fondée sur un logiciel qui envoie un code par SMS ou par email, constitue une avancée par rapport à la simple connexion au moyen d'un nom d'utilisateur, mais elle n'est pas la plus optimale.

Du point de vue de l'utilisateur, la saisie de codes peut être une source d'erreurs et risque d'allonger le processus de connexion. Ils se lassent bien souvent des étapes longues et peu pratiques associées à l'authentification, lesquelles réduisent leur productivité et entravent leur travail. Les outils d'authentification multifacteur matériels, tels que les clés de sécurité, offrent un autre moyen de renforcer la sécurité de l'authentification en prouvant que la personne qui accède au dispositif ou à l'application est bien celle qu'elle prétend être.

Les clés de sécurité peuvent également résoudre le problème souvent négligé que constitue la sécurité des téléphones portables, laquelle se voit également renforcée en ces temps de travail à distance. Bien que de nombreux employés accèdent régulièrement aux applications à des fins professionnelles depuis leur téléphone, 62 % des organisations françaises ayant répondu à l'enquête de Ponemon ont déclaré qu'elles ne pensaient pas que les mesures nécessaires avaient été prises pour protéger les informations sur les téléphones portables. Cette lacune en matière de sécurité devrait être résorbée afin d'éviter des incidents susceptibles de causer des dommages.

Une protection accrue

Parmi les autres méthodes de protection des données d'entreprise manipulées par les employés qui travaillent à distance figurent le chiffrement de bout en bout et les réseaux privés virtuels (VPN). Le chiffrement peut être utilisé seul ou en combinaison avec un VPN, mais il est généralement limité à un service ou à une application particulière. Un VPN protège les données entre les appareils et les serveurs, mais pour le reste, celles-ci sont exposées aux risques liés à Internet. Afin de fournir un niveau de sécurité supplémentaire, il est possible de configurer certains VPN de manière à ce qu'ils fonctionnent avec une clé de sécurité pour y autoriser l'accès à distance.

Les environnements cloud facilitent la transition vers le travail à distance sans compromettre la collaboration. Les solutions de gestion des accès et des identités permettent aux entreprises de déterminer qui consulte quoi, quand et pourquoi, et elles leur donnent une vue d'ensemble du réseau et de son utilisation. Pour les employés qui travaillent à distance, l'identification unique est très pratique, mais si leurs droits d'accès sont compromis, celle-ci peut se révéler inefficace pour empêcher l'accès à de multiples applications et sources d'information. Là encore, l'authentification à plusieurs facteurs limite le risque que des données tombent entre de mauvaises mains et que des cyberattaquants accèdent à toute une série de services.

Faciliter la transition des travailleurs

Dans la mesure où les employés doivent s'adapter à des environnements de travail en dehors du bureau, ils n'accordent pas nécessairement la priorité à la sécurité ni à des méthodes d'authentification solides. Pour les équipes en charge de la sécurité, le bouleversement soudain et profond des habitudes de travail, ainsi que la dispersion géographique des employés et l'utilisation potentielle de toute une série de dispositifs non standard, constituent un défi de taille pour le maintien d'une cybersécurité forte et sûre.
Il est important de combler toute faille de sécurité éventuelle engendrée par ces nouvelles méthodes de travail pour éviter que les données et les actifs de l'entreprise ne soient mis en danger. Le développement de protocoles d'authentification qui vont au-delà de la simple combinaison nom d'utilisateur/mot de passe, et des faiblesses qui y sont inhérentes, contribuera à renforcer les défenses contre toute une série de cybermenaces.

Les méthodes d'authentification multifacteur plus poussées, telles qu'une application d'authentification mobile ou une clé de sécurité matérielle, renforcent la sécurité sans pour autant perturber indûment les utilisateurs. Il s'agit là d'un point important, car en cette période de télétravail, les employés ont l'impression parfois d'être isolés du support IT et ils doivent avoir confiance dans les équipements et les processus qui leur sont fournis pour travailler. Les protocoles d'authentification doivent convenir aux employés, tout en offrant un niveau de protection adéquat pour les réseaux, les systèmes et les données.