MONETARY AND CAPITAL MARKETS

Série spéciale sur la COVID-19

Les notes de la série spéciale sont rédigées par des experts du FMI dans le but d'aider les pays membres à faire face aux conséquences économiques de la COVID-19. Les opinions exprimées dans ces notes sont celles de l'auteur ou des auteurs et ne représentent pas nécessairement les points de vue du FMI, de son conseil d'administration ou de sa direction.

Travail à distance et cybersécurité en période de pandémie[1]

En raison de la pandémie de COVID-19, de nombreuses entreprises et autorités de réglementation du secteur financier ont adopté des modalités de télétravail qui supposent un accès à distance à des systèmes et à des données parfois sensibles. L'adoption massive du travail à distance pendant une période prolongée, et les inévitables facteurs de vulnérabilité qui en découlent, laissent présager la multiplication des cyberattaques, parfois sous des formes nouvelles. Si elles ne l'ont pas encore fait, les entreprises du secteur financier devraient mettre en place des contrôles de sécurité rigoureux en matière d'accès à distance. De même, si ce n'est pas déjà fait, les autorités de réglementation du secteur devraient élaborer des lignes directrices supplémentaires, fondées sur les normes techniques et les bonnes pratiques internationales.

I. SOURCES POTENTIELLES ACCRUES DE VULNÉRABILITÉ

La plupart des entreprises du secteur financier utilisent déjà des systèmes d'accès à distance aux données, mais les capacités installées ne permettent pas forcément à la majorité des employés de s'en servir en même temps, ce qui a pour effet d'accroître les risques pour la sécurité. Les départements informatiques sont soumis à une pression pour améliorer rapidement les capacités en perfectionnant ou en remplaçant les systèmes existants, ce qui leur laisse peu de temps pour effectuer des tests de sécurité poussés. Certaines failles dans les infrastructures et les protocoles d'accès à distance peuvent passer inaperçues et servir de cibles lors de cyberattaques.

Le recours aux technologies d'informatique « en nuage » (*Cloud computing*) se développe à mesure que les besoins augmentent. En raison de contraintes temporelles et financières, les risques pour la sécurité que pose l'utilisation du *Cloud computing* peuvent ne pas avoir été correctement évalués, et les mécanismes de contrôle existants risquent de ne pas être pleinement efficaces dans ce nouvel environnement de travail. Si certains fournisseurs de *Cloud computing* sont réputés disposer d'infrastructures sûres, les risques n'en disparaissent pas pour autant, car les entités utilisatrices de ces services retiennent toujours une part de

[1] Pour plus d'informations, les autorités des pays membres sont invitées à prendre contact avec Nigel Jenkinson (njenkinson@IMF.org), chef de la division supervision et réglementation financières du département des marchés monétaires et de capitaux du FMI.

responsabilité en matière de sécurité des données, notamment parce qu'il leur incombe de bien paramétrer les mécanismes qui en contrôlent l'accès.

Les employés peu habitués à travailler à distance et déjà sous pression à cause de la pandémie sont des victimes idéales pour les auteurs de cyberattaques, qu'il s'agisse d'hameçonnage ou de manipulation psychologique à des fins d'escroquerie. Ces dernières semaines, de plus en plus de cyberattaques ont été perpétrées selon le mode opératoire suivant : les auteurs cherchent à exploiter notre intérêt bien naturel pour toute information liée à la COVID-19 pour nous amener à réagir de d'une certaine façon, par exemple en incitant les victimes à cliquer sur des liens malveillants ou à télécharger des pièces jointes ou des applications porteuses d'un virus informatique.

Deux facteurs principaux augmentent le risque que de telles attaques réussissent : le manque de sécurité des points d'accès et les failles dans les protocoles d'authentification pour l'accès à distance. À titre d'exemple, les ordinateurs portables ou autres appareils mobiles sur lesquels les correctifs de sécurité les plus récents n'ont pas été installés sont considérés comme des points d'accès non sécurisés. Les procédures d'authentification qui se limitent à la saisie d'un mot de passe, sans moyen de vérification supplémentaire, présentent des faiblesses dans la sécurisation des accès à distance. Cela dit, il reste essentiel que les mots de passe utilisés remplissent des critères de sécurité stricts.

Au cours de la pandémie, il se peut que certaines tâches relatives aux systèmes et aux données sensibles, qui d'ordinaire ne peuvent être effectuées en dehors des locaux, comme par exemple les opérations de trésorerie, soient accomplies à distance. Les contrôles existants ne suffiront pas forcément à protéger les fonctions, les systèmes et les données critiques.

Les mesures techniques et les politiques en matière de sécurité de l'information sont essentielles pour réduire les risques de cybersécurité liés à l'accès à distance. Bien qu'elles ne soient pas spécifiques à l'accès à distance, des politiques strictes de sécurité de l'information (notamment le contrôle de l'accès aux données et des règles étendues en matière d'enregistrement et de suivi des données) sont fondamentales pour garantir la sécurité de l'accès à distance. Certaines entreprises n'ont pas su pleinement mettre en œuvre de telles mesures, et sont donc davantage susceptibles d'être la cible d'une attaque pendant la pandémie.

II. RECOMMANDATIONS

Si ce n'est pas encore le cas, les autorités et les entreprises doivent assurer rapidement la mise en œuvre complète des bonnes pratiques et des normes techniques internationales en matière de sécurisation du travail à distance. Certaines normes techniques sont spécialement consacrées aux vérifications qu'il convient d'effectuer en cas de télétravail (par exemple les normes NIST 800-46 Rev 2 ou BSI IT-Grundschutz Compendium), tandis que d'autres portent sur des contrôles génériques qui peuvent également s'appliquer au travail à distance (comme la norme COBIT 2019[2], ou la série de normes ISO 27000). Voici quelques éléments essentiels que les entreprises et les autorités devraient traiter en priorité : i) authentification renforcée des utilisateurs et des appareils[3] et méthodes de cryptage solides ; ii) sécurité des appareils utilisés pour l'accès à distance ; iii) suivi de la sécurité des réseaux.

[2] Par exemple, les contrôles BAI09.02, DSS05.02, DSS05.03 et DSS05.06

[3] Il est fortement recommandé de faire intervenir deux méthodes de vérification pour permettre à un utilisateur de s'authentifier. Les appareils aux deux extrémités d'une connexion doivent être authentifiés, par exemple au moyen de certificats numériques.

Les services d'accès à distance et les profils des utilisateurs ne doivent être activés que lorsque c'est nécessaire. En l'absence de besoin réel, il faut désactiver l'accès à distance, afin de réduire les possibilités d'attaque.

L'utilisation de plateformes de *cloud computing* doit être subordonnée à une évaluation détaillée des risques. Selon les résultats de cette évaluation, et en fonction du caractère critique des systèmes et des données transférées sur telle ou telle plateforme, il convient de mettre en place des mécanismes de contrôle de sécurité efficaces en tirant pleinement parti des possibilités offertes par la plateforme utilisée (comme le contrôle d'accès aux actifs, la gestion des identités et des accès, ainsi que l'enregistrement et la surveillance).

Les téléconférences doivent être organisées sur des plateformes approuvées et protégées contre tout accès non autorisé. Dans la mesure où nombre d'informations sensibles sont transmises et partagées dans le cadre de téléconférences, il est essentiel de procéder à une évaluation des risques avant de déployer un tel dispositif à grande échelle, de manière à assurer que les informations soient suffisamment sécurisées. En outre, il conviendrait d'authentifier les personnes participant à une téléconférence en se servant de moyens à la fois techniques et procéduraux, par exemple en utilisant des codes PIN et en vérifiant que les participants connectés ont bien été invités à la conférence virtuelle en question.

De nouvelles campagnes de sensibilisation à la cybersécurité devraient être lancées à l'intention de tous les employés. C'est du maillon le plus faible de la chaîne que dépend la solidité de l'ensemble, aussi tous les employés doivent être rendus conscients du niveau de menace accru que représentent l'hameçonnage et les réseaux sociaux pendant la pandémie. Les services d'assistance doivent rapidement prêter main forte aux utilisateurs en cas de suspicion d'incidents de sécurité.

Des contrôles rigoureux portant sur les configurations d'un bout à l'autre de la chaine de connexion à distance devraient être mis en œuvre afin d'empêcher toute intervention malveillante. Ainsi, les employés ne devraient pas bénéficier de droits d'administration sur les ordinateurs portables appartenant à la société[4], des configurations de sécurité renforcée et des solutions de sécurité actualisées pour les points d'accès devraient être mises en place, les paramètres de sécurité de la connexion devraient être définis conformément aux bonnes pratiques et être verrouillés, et l'infrastructure d'accès à distance de la société devrait être étroitement contrôlée. Une bonne pratique consiste à effectuer des scans de sécurité sur les appareils utilisés pour le télétravail, et d'en faire une condition nécessaire pour l'accès à distance.

Les entreprises doivent mettre en place des contrôles de sécurité supplémentaires pour les travaux sensibles qui ne sont pas censées s'effectuer à distance en temps normal. Ainsi, les utilisateurs chargés de telles tâches ne devraient pouvoir se connecter qu'au moyen d'appareils appartenant à l'entreprise et contrôlés par elle, paramétrés pour une sécurité maximale, et sur lesquels les correctifs de sécurité les plus récents ont été installés. Par ailleurs, les données sensibles ne devraient pas pouvoir être stockées localement[5].

Les autorités de supervision devraient insister sur le fait que le télétravail multiplie les risques pour la cybersécurité, lesquels demandent à faire l'objet de contrôles renforcés. Les autorités compétentes

[4] Lorsque les employés utilisent leurs ordinateurs personnels dans un contexte professionnel, et que ces derniers ne peuvent pas être convenablement vérifiés par l'entreprise, il est fortement recommandé que les employés concernés se voient attribuer des comptes utilisateurs sans privilèges.

[5] L'utilisation obligatoire de terminaux correctement configurés, ou de serveurs de rebond, permet de restreindre efficacement le stockage local des données.

pourraient mettre en place de nouvelles directives relatives à ces risques, ou bien, le cas échéant, rappeler les dispositions existantes, et fournir davantage d'informations si nécessaire, par exemple en s'inspirant du contenu de la présente note[6]. Il conviendrait que les dirigeants des entités concernées soient conscients qu'en l'absence de directives permettant d'anticiper les risques, ou si les pratiques de gestion des risques des entreprises ne sont pas adaptées, un certain nombre de vérifications essentielles feront défaut ou seront inefficaces, et qu'il sera difficile d'y remédier dans les circonstances actuelles. Le renforcement des contrôles internes et du suivi des activités des employés et l'organisation de campagnes de sensibilisation peuvent en partie remédier à cette carence.

[6] Pour en apprendre davantage sur les meilleures pratiques de vigilance en matière de cyber-risque, voir la publication du FMI « Cybersecurity Risk Supervision », accessible ici : https://www.imf.org/en/Publications/Departmental-Papers-Policy-Papers/Issues/2019/09/23/Cybersecurity-Risk-Supervision-46238.