LA CYBERSÉCURITÉ À L'HEURE DE COVID-19 : LES CLÉS POUR ÉPOUSER LE TÉLÉTRAVAIL EN TOUTE SÉCURITÉ

11 mars 2020 | Michael Sentonas | Point de vue d'un dirigeant

La déclaration officielle de pandémie mondiale par l'Organisation mondiale de la santé aujourd'hui souligne ce que nous sommes tous en train de réaliser : la maladie COVID-19, causée par une variante du coronavirus, va provoquer un bouleversement social et économique sans précédent à l'ère moderne. Nos clients nous font d'ores et déjà savoir qu'ils sont confrontés à des difficultés imprévues et de taille tandis qu'ils cherchent des solutions pour répondre aussi rapidement que possible aux directives d'entreprise enjoignant les employés à déserter les bureaux et les campus d'entreprise pour travailler depuis leur domicile. Face à l'abandon des bureaux à l'échelle mondiale, le maintien de la sécurité présente des risques importants pour la plupart des entreprises.

LES DÉFIS DE L'ADOPTION RAPIDE D'UN MODÈLE DE TRAVAIL À DISTANCE

Selon le dernier rapport de l'International Workplace Group, 50 % des employés du monde entier travaillent hors de leur siège principal au moins 2,5 jours par semaine. COVID-19 contraint toutefois un nombre croissant d'entreprises, voire toutes, à adopter immédiatement un modèle de travail à distance. Outre la pression que cet abandon des bureaux fait peser sur les équipes informatiques, les architectures de réseau et même les fournisseurs d'équipements, les entreprises font face à de véritables défis en termes de cybersécurité.

Six facteurs clés pouvant contribuer à assurer la cybersécurité des télétravailleurs :

- **Vérifiez que vous disposez d'une politique de cybersécurité à jour qui couvre le travail à distance.** Peut-être avez-vous déjà mis en place des politiques de sécurité robustes, mais il est important de les réviser régulièrement et de s'assurer qu'elles restent adéquates tandis que votre entreprise passe à un modèle où un plus grand nombre de personnes travaillent à domicile qu'au bureau. Les politiques de sécurité doivent couvrir la gestion des accès en télétravail, l'utilisation des appareils personnels et des considérations actualisées en matière de confidentialité des données dans le cadre de l'accès des employés aux documents et autres informations. Il est également important de prendre en compte l'augmentation de l'utilisation de l'informatique de l'ombre et des technologies cloud.
- **Prévoyez la connexion d'appareils personnels au réseau de votre entreprise.** Les employés en télétravail peuvent utiliser des appareils personnels pour effectuer des tâches professionnelles, en particulier s'ils ne peuvent pas avoir accès à un appareil fourni par l'entreprise en raison du ralentissement des chaînes logistiques. Les appareils personnels devront avoir le même niveau de sécurité que les appareils d'entreprise, et vous devrez également tenir compte des implications pour la confidentialité de la connexion d'appareils personnels au réseau d'entreprise.
- **Des données sensibles risquent d'être consultées via des réseaux Wi-Fi non sécurisés.** Les employés qui travaillent à domicile risquent d'accéder à des données d'entreprise sensibles par le biais de réseaux Wi-Fi domestiques qui ne seront pas dotés des mêmes contrôles de sécurité (tels que des pare-feu) que ceux utilisés dans les bureaux d'entreprise. Le nombre de connexions à distance augmentera considérablement, ce qui nécessitera de se concentrer davantage encore sur la confidentialité des données et de traquer les intrusions depuis un plus grand nombre de points d'entrée.

- **La visibilité et l'hygiène de cybersécurité seront critiques.** Il n'est pas rare que l'hygiène de cybersécurité des appareils personnels laisse à désirer. Le télétravail peut entraîner une perte de visibilité sur les appareils et la façon dont ils ont été configurés, patchés et même sécurisés.
- **Une sensibilisation continue est cruciale, car les escroqueries conçues pour exploiter la crise du coronavirus se multiplient.** L'Organisation mondiale de la santé (OMS) et la Commission fédérale du commerce (FTC, Federal Trade Commission) des États-Unis ont déjà mis en garde contre les attaques par phishing et les campagnes d'escroquerie en cours sur le thème du coronavirus. Une sensibilisation continue des utilisateurs finaux et une communication permanente sont extrêmement importantes, et il convient de s'assurer que les télétravailleurs peuvent contacter rapidement les services informatiques pour obtenir des conseils. Les entreprises doivent également envisager la mise en place de mesures de protection de la messagerie électronique plus strictes.
- **Les plans de gestion de crise et d'intervention sur incident doivent pouvoir être exécutés par des utilisateurs distants.** Un cyberincident qui survient alors qu'une entreprise fonctionne déjà dans des conditions inhabituelles a beaucoup plus de chances de devenir incontrôlable. Des outils de collaboration à distance performants, notamment des ponts de conférence hors bande, des plateformes de messagerie instantanée et des applications de productivité, peuvent permettre à une équipe géographiquement dispersée de créer un « centre de crise virtuel » pour la gestion des interventions. Si les plans de votre entreprise reposent sur l'accès physique ou sur l'envoi de techniciens pour des tâches spécifiques (par exemple, la création d'une nouvelle image disque ou le remplacement de machines compromises), il peut être prudent d'explorer d'autres méthodes ou de vous orienter vers des ressources locales.

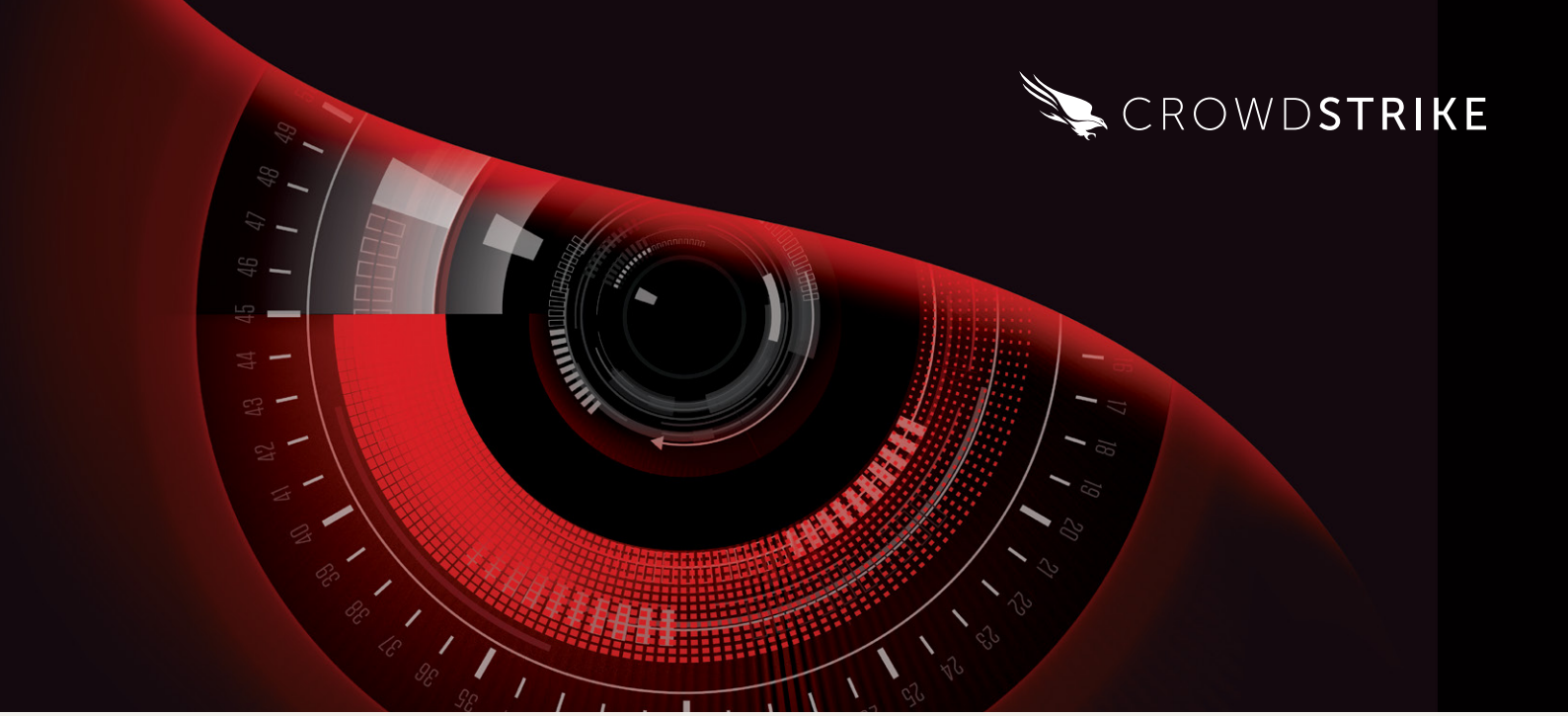
GARANTIR LA SÉCURITÉ DES TÉLÉTRAVAILLEURS

CrowdStrike est particulièrement bien placé pour aider les entreprises aux prises avec ce passage soudain au télétravail, et ce pour deux raisons. Tout d'abord, notre plateforme cloud et notre architecture à agent léger sont idéales pour prendre en charge et, plus spécifiquement, protéger les utilisateurs distants. Ensuite, en tant qu'entreprise, nous donnons personnellement l'exemple à cet égard : notre propre personnel compte de nombreux télétravailleurs géographiquement dispersés. Nous avons donc une connaissance institutionnelle approfondie de la prise en charge performante et sécurisée du travail à distance.

Découvrez ci-dessous plusieurs fonctionnalités de la plateforme cloud CrowdStrike Falcon® qui vous permettront de migrer rapidement votre personnel du bureau vers le domicile en toute sécurité :

Exploitez l'évolutivité et le rapport coût-efficacité du cloud. L'architecture conçue spécifiquement pour le cloud s'adapte aux exigences des clients tout en offrant une immense capacité de stockage et une puissance de calcul considérable pour assurer une protection en temps réel, indépendamment du lieu de connexion de vos employés. Le recours à une architecture de sécurité cloud garantit que des ressources supplémentaires peuvent être mises en service selon les besoins. Par conséquent, il n'est pas nécessaire de planifier, préparer et mettre en service du matériel et des logiciels particuliers pour suivre la cadence et assurer la prise en charge d'un plus grand nombre d'utilisateurs distants.

Bénéficiez d'un niveau de sécurité optimal indépendamment de l'emplacement de vos employés. Une architecture de sécurité entièrement native au cloud vous permet de protéger toutes les charges de travail où qu'elles soient, y compris celles qui résident à l'extérieur du pare-feu, même si elles sont hors ligne. Vous bénéficiez en outre de fonctionnalités de sécurité en temps réel offrant un niveau d'efficacité optimal, ainsi que d'informations sur l'état de conformité. La traque des menaces sur tous les appareils, en particulier ceux qui ne sont pas connectés au réseau, est essentielle. Seule une solution native au cloud permet une traque des menaces simple et performante avec un accès instantané aux données depuis n'importe quel endroit.



Appuyez-vous sur une architecture de sécurité simple offrant une visibilité complète. Pour gérer la sécurité de façon proactive, il est indispensable de savoir en permanence qui utilise votre réseau et ce qui s'y passe. Il est essentiel d'avoir une visibilité complète sur chaque appareil qui se connecte au réseau, quel que soit l'endroit où la connexion est établie. Grâce à l'agent léger unique de CrowdStrike® Falcon, il n'est pas nécessaire de redémarrer pour installer la solution ; l'impact sur les performances d'exécution est minime ; l'expérience de l'utilisateur final n'est pas affectée par des mises à jour de signatures invasives ou des charges lourdes susceptibles de dégrader les ressources système lors des analyses ; et la protection des utilisateurs peut être assurée en quelques secondes. Les fonctionnalités de surveillance et découverte continues et complètes des charges de travail de la plateforme Falcon offrent aux équipes de sécurité une visibilité totale sur chaque appareil, à savoir les appareils sur site, les appareils professionnels et personnels des télétravailleurs, ainsi que les charges de travail cloud. Cette visibilité étend également la protection aux conteneurs et appareils mobiles.

Assurez une sécurité sans faille grâce à un service SaaS de protection des endpoints. Avec CrowdStrike Falcon Complete™, les clients peuvent confier l'implémentation et la gestion de la sécurité des endpoints, ainsi que l'intervention sur incident à l'équipe d'experts en sécurité chevronnés de CrowdStrike. Ils bénéficient ainsi instantanément d'un niveau de sécurité optimisé, sans devoir assumer la charge, la complexité et le coût de la gestion d'un programme complet de sécurité des endpoints, ce qui libère les ressources internes pour travailler sur d'autres projets. Entièrement gérée et infaillible, Falcon Complete est une solution unique de protection des endpoints qui met à la disposition des clients les personnes, les processus et la technologie nécessaires pour gérer tous les aspects de la sécurité des endpoints, de l'intégration et la configuration à la maintenance, la surveillance, la gestion des incidents et les mesures correctives, qu'il s'agisse d'une charge de travail sur site ou d'un travailleur distant.

CONCLUSION

La crise provoquée par COVID-19 risque de durer un certain temps. Les entreprises et leurs employés seront rapidement contraints de prendre des décisions difficiles, telles que généraliser le télétravail. L'introduction rapide du télétravail comporte des risques, mais la sécurité de vos réseaux, appareils et données ne doit pas nécessairement en faire partie.

Appelez votre représentant CrowdStrike pour obtenir des informations sur les programmes spéciaux destinés aux clients CrowdStrike qui doivent faire face à une augmentation massive du nombre d'utilisateurs distants. CrowdStrike est déterminé à aplanir les difficultés qui entravent la prise de décisions rapides et à garantir à tous les utilisateurs l'accès à la technologie et à l'expertise nécessaires pour travailler en toute sécurité, où qu'ils se trouvent.

NE MANQUEZ PAS UN WEBCAST IMPORTANT

Rejoignez les experts de CrowdStrike le mercredi 18 mars pour examiner les clés d'une prise en charge sécurisée des télétravailleurs. **Inscrivez-vous dès aujourd'hui.**

Autres ressources:

- Découvrez la **plateforme CrowdStrike Falcon.**
- Inscrivez-vous pour participer au webcast : **La cybersécurité à l'heure de COVID-19 :les clés pour épouser le télétravail en toute sécurité.**
- Visitez **la page web de Falcon Complete** pour en savoir plus sur la protection entièrement gérée des endpoints.
- **Bénéficiez d'une évaluation gratuite de la version complète de CrowdStrike Falcon Prevent™** et découvrez les performances d'une véritable solution antivirus de nouvelle génération face aux menaces actuelles les plus sophistiquées.