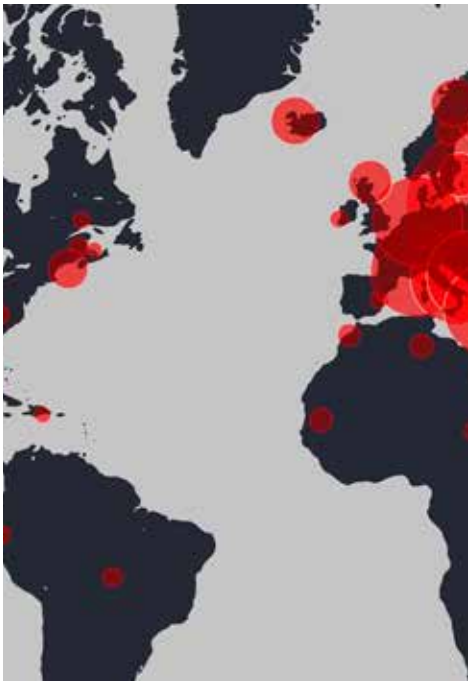
COVID-19 et cybersécurité

Guide de référence rapide pour les leaders et les responsables de la sécurité

COVID-19

La pandémie de COVID-19 a un impact important sur les entreprises et les employés en télétravail. En ce temps d'incertitude et de confusion, les auteurs de menaces cherchent activement par toutes sortes de moyens à exploiter la situation.



UN CLIMAT IDÉAL POUR LES CRIMINELS

En raison de la pandémie de COVID-19, les employés doivent travailler à distance pour protéger leur santé et leur sécurité tout en assurant la continuité des activités normales des entreprises. Les employés utilisent la messagerie texte et des plateformes de collaboration pour communiquer tandis que leur organisation doit composer avec la pénurie de licences de réseau privé virtuel (VPN) et les problèmes de bande passante. Cette mesure sans précédent pousse un grand nombre d'utilisateurs à travailler « en dehors du coupe-feu », ce qui entraîne un fardeau supplémentaire pour les mesures de cybersécurité comme la prévention des attaques par déni de service (DDoS), la sensibilisation à la sécurité, la fuite de données, la disponibilité et la surveillance du réseau.

Nous constatons actuellement une augmentation marquée de l'exploitation des vulnérabilités : escroqueries par hameçonnage, programmes malveillants intégrés aux cartes de suivi de la COVID-19 et augmentation des attaques par logiciels de rançon. Nous faisons ici un tour rapide de ce que vous devriez faire pour reprendre le contrôle de votre cybersécurité et vous défendre contre les auteurs de menaces.

QUE DEVRIEZ-VOUS FAIRE ?

Voici certaines mesures de sécurité dont vous devriez tenir compte lorsque vos employés doivent travailler en dehors du coupe-feu :

sensibilisez vos employés : informez-les que les cartes de suivi risquent d'être infectées de programmes malveillants et qu'il y a une recrudescence d'escroqueries par hameçonnage. Consultez le guide « Hygiène de cybersécurité pendant la pandémie de COVID-19 – Ce qu'il faut faire et ne pas faire : un guide à partager avec vos employés »;

mettez en place des mesures de prévention des fuites de données (établissez ou renforcez les règles de conduite entourant les communications au moyen des versions des plateformes de clavardage et de collaboration pour lesquelles vous n'avez pas de licence);

faites une surveillance rigoureuse afin de reconnaître les indicateurs d'une attaque aussi vite que possible;

assurez-vous que les antivirus et les protections contre les programmes malveillants sont à jour pour tous les points d'extrémité;

assurez-vous que les mises à jour et les correctifs sont appliqués à tous les points d'extrémité connectés à Internet et que ces derniers sont soumis à des analyses de vulnérabilité;

s'il est impossible d'appliquer un correctif ou de sécuriser un point d'extrémité, ce dernier devrait être doté de sa propre mesure de protection pour atténuer le risque;

vérifiez que la protection contre les attaques par déni de service (DDoS) fonctionne comme prévu; pour certaines organisations, les serveurs n'arrivent pas à soutenir l'augmentation du trafic légitime et deviennent indisponibles comme lors d'une attaque par déni de service;

si vous n'avez pas de solution de réponse en continu (24/7) aux incidents, vous devriez songer à vous en procurer une, du moins pour les prochaines semaines;

étendez les contrôles traditionnels (p. ex., les solutions de détection et de réponse aux points d'extrémité (EDR) et la collecte de journaux d'événements Windows) aux ordinateurs personnels des employés pour atténuer les risques. L'infrastructure de bureau virtuel (VDI) permet également de mieux prévenir les fuites accidentelles de données.

Pour toute question concernant la cybersécurité, écrivez à **globalcybersecurity@cgi.com.**