Conseils en matière de cybersécurité

Comment protéger votre entreprise face à la hausse des cyberattaques lors de la COVID-19

VICTOR

Les changements rapides apportés par la COVID-19, notamment le déplacement d'une grande partie des Canadiens pour travailler à distance, ont amené de nombreuses entreprises à mettre en œuvre de nouveaux processus commerciaux et de nouvelles mesures de cybersécurité, car le nombre de cyberattaques continue à augmenter.

Certaines entreprises ont même mis en œuvre des solutions technologiques pour combler d'éventuelles lacunes en matière de sécurité et assurer la sécurité de leurs employés lorsqu'ils travaillent en ligne. Ce type de mesures de sécurité ne sera pas différent pour le monde des affaires après la COVID-19. Les entreprises devront continuer à veiller à ce que leurs activités soient protégées contre les cyberattaques.

Se préparer au monde post-pandémique

Alors que les mesures de distanciation sociale deviennent moins répandues, les organisations devront adapter leurs activités à cette « nouvelle normalité ».

Cela nécessitera une évaluation approfondie des contrôles de cybersécurité et des processus opérationnels. Pendant la période de reconstitution de la pandémie, les changements apportés pour faire face à la pandémie devront peut-être être remplacés par des solutions plus sécurisées et permanentes.

Nous pouvons prévoir qu'à mesure que les Canadiens se remettent de la pandémie, sur le plan technologique, le monde des affaires post-COVID-19 pourrait ressembler à cela :

- Augmentation et institutionnalisation du travail à distance
- Une croissance significative de l'utilisation des outils de collaboration en ligne
- Augmentation des cyberattaques en raison du travail à distance
- Une évolution vers des services et applications gérés « dans le nuage »
- Une plus grande attention accordée aux pratiques de gestion de risques

Les entreprises et leurs employés devront garder ces facteurs à l'esprit lorsqu'ils travailleront dans le monde des affaires post-COVID-19. Voici cinq domaines clés à prendre en compte lors de l'élaboration d'un nouveau plan de cybersécurité.

Solutions de travail à distance

1

Anticipez une augmentation permanente du travail à distance. En gardant cela à l'esprit, considérez ce qui suit :

- Mettez en place des processus de connectivité sécurisée pour les employés sur leur poste de travail (par exemple, l'authentification multifactorielle pour les RPV et les systèmes d'information critiques)
- Gérez l'accès de votre personnel à distance en fonction des exigences de sécurité de l'entreprise et de la facilité d'utilisation pour les employés
- Mettez en œuvre des solutions de gestion des appareils mobiles pour traiter l'utilisation d'appareils technologiques (c'est-à-dire les téléphones portables, les ordinateurs portables, etc.) fournis par l'entreprise, ou d'appareils technologiques personnels approuvés par l'entreprise, à des fins professionnelles
- Appliquez les mises à jour de logiciels aux appareils technologiques fournis par l'entreprise aux employés
- Examinez de près les protocoles de bureau à distance, qui permettent l'accès à distance aux systèmes et serveurs Windows et peuvent inciter les pirates informatiques à tenter d'obtenir un accès non autorisé aux fichiers de l'entreprise
- Mettez en place des contrôles d'accès au réseau pour authentifier et valider l'accès des employés lorsqu'ils utilisent les appareils technologiques de l'entreprise, et appliquez les politiques de sécurité technologique avant de les autoriser à se connecter aux réseaux internes ou distants de votre entreprise

Services nébuleux

2

Les services nébuleux peuvent offrir des avantages considérables en termes de coût, d'efficacité, de résilience et de sécurité potentielle par rapport aux plateformes numériques hébergées pour la sauvegarde et l'application des informations commerciales. Toutefois, les services nébuleux devraient être adoptés et gérés de manière stratégique.

- Adoptez des stratégies formelles pour l'utilisation des services nébuleux
- Dressez un inventaire de l'utilisation du nuage dans votre entreprise
- Définissez des politiques pour la conservation des informations commerciales et les conditions requises pour l'utilisation des services nébuleux, la sauvegarde des données et la sauvegarde locale, en particulier pour les renseignements sensibles et/ou confidentiels
- Assurez-vous que votre fournisseur de services nébuleux dispose de protocoles de sécurité solides pour protéger les renseignements sensibles et/ou confidentiels de votre entreprise
- Assurez-vous d'avoir installé un logiciel dans le nuage qui surveille les activités d'accès et applique les politiques de sécurité
- Surveillez l'utilisation du nuage au sein de votre entreprise et appliquez les politiques de cybersécurité correspondantes pour vous protéger contre les virus technologiques, les logiciels malveillants ou toute activité suspecte

Outils de collaboration sécurisés

3

Si la communication par courrier électronique, les outils de productivité de bureau et la vidéoconférence ont été essentiels pendant la pandémie, les entreprises peuvent choisir d'innover en adoptant et en utilisant des outils de collaboration sécurisés supplémentaires. Voici quelques mesures de sécurité de base à prendre en compte lors de cette opération :

- Mettez en œuvre des protocoles de courrier électronique sûrs et un cryptage pour protéger contre les accès non autorisés
- N'envoyez pas de renseignements relatifs au travail à vos appareils technologiques personnels (téléphone portable, tablette, ordinateur portable, etc.) car cela pourrait compromettre des renseignements sensibles/confidentiels et les exposer à la cybercriminalité (c'est-à-dire aux mauvais acteurs)
- Lorsque vous utilisez des outils de vidéoconférence tels que Zoom ou WebEx, protégez votre vie privée en rendant la réunion privée et en appliquant un code d'accès pour éviter que des parties indésirables ne détournent votre réunion
- Limitez les fonctions de partage pendant la vidéoconférence afin de protéger les renseignements sensibles/confidentiels et d'empêcher la divulgation accidentelle de contenus non destinés au partage public
- Évitez de partager publiquement le lien du site Web de réunion par vidéoconférence, qui pourrait inviter des pirates informatiques potentiels ou des invités indésirables à votre réunion
- Utilisez un fournisseur de services qui privilégie les mesures de cryptage et de cybersécurité pour protéger votre vie privée et les renseignements de votre entreprise

Politique « Apportez votre propre appareil »

4

En raison de la crise de COVID-19, de nombreuses organisations ont autorisé leurs employés à utiliser leurs appareils technologiques personnels, notamment les ordinateurs portables, les téléphones portables et les tablettes, à des fins professionnelles. Les appels téléphoniques ont été acheminés vers des téléphones portables personnels, le courrier électronique a été mis à disposition sur des appareils personnels et les employés ont été autorisés à accéder à des applications basées sur le nuage à partir d'appareils personnels.

Toutefois, afin de protéger et d'atténuer les risques cybernétiques potentiels pour votre entreprise et vos employés, tenez compte des éléments suivants :

- Assurez-vous que votre entreprise a établi une politique sur la mise en œuvre et l'utilisation d'appareils technologiques personnels à des fins professionnelles (c'est-à-dire « Apportez votre propre appareil »)
- Vérifiez que la police d'assurance de votre entreprise prend en charge ce concept, car certains assureurs peuvent refuser l'utilisation d'un appareil personnel, sauf si celui est lié au réseau de votre entreprise
- Examinez les mesures mises en œuvre pendant la COVID-19 pour assurer la protection continue des réseaux commerciaux et des renseignements sensibles de votre entreprise
- Veillez à ce que les appareils personnels soient bien protégés par un logiciel de sécurité et un cryptage mis à jour
- Révisez et mettez à jour les profils RPV et les règles de pare-feu afin que les employés reçoivent les privilèges appropriés en fonction de leur rôle
- Sensibilisez les employés aux pratiques technologiques sécuritaires tout en utilisant leurs appareils technologiques personnels pour se prémunir contre les cyberattaques potentielles à la lumière de l'utilisation d'un appareil personnel

Plan d'évaluation et d'intervention en cas d'atteintes cybernétiques

5

Les entreprises devront mettre en œuvre un plan solide et actuel d'intervention en cas d'atteintes. C'est important pour faire face à l'impact potentiel d'une atteinte cybernétique sur la continuité des activités.

- Procédez à une évaluation des risques et mettez en œuvre des mécanismes de sécurité, tels que l'authentification multifactorielle, la signature unique et la déconnexion automatique des appareils non surveillés
- Effectuez régulièrement des audits de cybersécurité et des tests de vulnérabilité de vos systèmes informatiques et de vos appareils technologiques afin d'évaluer, de définir et de corriger les faiblesses et les lacunes en matière de sécurité
- Intégrez les enseignements tirés des opérations d'urgence provoquées par la COVID-19
    - S'il n'y avait pas de plan d'intervention en cas d'atteinte préexistant, la nécessité d'un tel plan devrait être évidente
- Rafraîchissez et mettez à jour vos plans d'intervention en cas d'atteinte et de reprise après sinistre pour tenir compte de la situation actuelle de votre entreprise et de la « nouvelle normalité »
- Assurez une formation et une sensibilisation régulières des employés à la sécurité contre les cybermenaces
    - Un personnel bien formé constitue votre meilleure ligne de défense contre les attaques
- Obtenez une police d'assurance contre les cyber-risques ou révisez votre police existante pour vous protéger contre les nouveaux défis de la cybersécurité et vous assurer que la police répond aux besoins de votre entreprise

Un nouvel accent sur la résilience

La COVID-19 a renforcé la nécessité pour les entreprises de revoir leur stratégie de cybersécurité afin de s'aligner sur les exigences de la « nouvelle normalité ». Cette récente crise a mis en évidence la nécessité de se préparer à de graves perturbations des activités et d'établir des plans d'urgence solides. La période de redressement et de préparation post-COVID-19 offre aux entreprises la possibilité de reconstruire et d'améliorer la résilience de leurs organisations et de mettre en place des pratiques commerciales solides pour l'avenir.

Pour plus d'informations, visitez assurancevictor.ca ou consultez les ressources supplémentaires suivantes :

- Assurance contre les cyber-risques de Victor
- Ressources sur la COVID-19
- Infographie : « Journée typique dans la vie d'un propriétaire d'entreprise »
- Vidéo animée : « Une journée dans la vie d'un propriétaire d'entreprise dans un cybermonde »

#COVID-19 #CyberAttaques #LaMenaceEstRéelle #SoyezPrudent

Visitez assurancevictor.ca pour en apprendre davantage.