Stéphane de Jotemps, Directeur des Ventes du programme de corporate e-learning Skillsoft.

Rebâtir une cybersécurité post-Covid en 10 points

La crise du Covid-19 a impacté et remis en question les certitudes que les professionnels de la cybersécurité tenait pour acquises il y a encore un an et demi. Voici dix conseils pour une application optimale des leçons tirées de la crise.

Depuis plus d'un an, la crise de la Covid-19 défait systématiquement et une par une les fondations que nous tenions pour acquises et solides. Le mois de décembre a lui aussi contribué à ce contexte pesant et incertain lorsque plusieurs milliers de systèmes et dossiers furent menacés lors de l'attaque de SolarWinds.

Il est possible que, dans les deux cas, certaines des retombées soient dues à la fatigue ou à la complaisance. Quoi qu'il en soit, nous pouvons et devons faire mieux. La bonne nouvelle, c'est que nous pouvons atténuer les risques de cyberattaques en suivant quelques leçons essentielles que la COVID-19 nous a (ou aurait dû) nous apprendre. Nous avons appris des maladies infectieuses et des cyber-attaques sur le tas, et chacun d'entre nous doit aujourd'hui penser comme un épidémiologiste. La voie vers une cybersécurité prête pour l'avenir.

Examinons 10 leçons tirées de la lutte contre Covid-19 qui, si elles sont appliquées avec vigilance, pourraient améliorer la cybersécurité sur le lieu de travail :

Arrêtez de supposer que tout est sûr

Depuis trop longtemps, nous avons accepté les faiblesses de la chaîne d'approvisionnement en logiciels. Nous devons faire preuve de plus de diligence pour faire pression sur les entités de la chaîne d'approvisionnement afin qu'elles apportent la preuve d'un contrôle de sécurité approfondi.

Faites attention à ce que vous partagez

Faites attention aux hackers qui cherchent à accéder à des informations d'identification ou à des informations confidentielles. Protégez la propriété intellectuelle et les données contre les faux intrus.

Ne devenez pas un « super-spreader »

N'ouvrez pas les pièces jointes provenants d'emails d'inconnus. Ne transmettez jamais un message auquel vous ne faites pas confiance ou que vous ne pouvez pas vérifier complètement. Assurez-vous que les paramètres de confidentialité sont à jour et actifs.

Distance sociale

Segmentez les réseaux et les bases de données. Ne suivez pas la foule et n'utilisez pas de code tiers sans avoir effectué de tests de sécurité. Créez une distance dans la chaîne d'approvisionnement des logiciels.

Portez un masque

Les envahisseurs exploiteront les plus petites ouvertures et vulnérabilités. Couvrez les expositions avec des pare-feu solides et des programmes de détection des menaces en cours. Arrêtez les injections SQL nuisibles. Les formulaires web sont un point d'entrée privilégié pour les intrus qui souhaitent insérer des commandes SQL. Sans être détectés, les pirates peuvent accéder aux bases de données et y apporter des modifications malveillantes.

Donnez le bon exemple

Mettez en place un programme de champions de la sécurité. Les champions encouragent les connaissances en matière de sécurité, quantifient les risques

et modélisent les bonnes pratiques. Un programme assure un flux constant de défenseurs de la sécurité motivés.

Assainissez tout

Encodez et chiffrez toutes les données sensibles et les informations confidentielles. Intégrer la sécurité tout au long du cycle de développement des logiciels.

Faire le nettoyage de façon fréquente

Tenez-vous au courant des correctifs de sécurité et des nouvelles versions de logiciels. Les correctifs sont souvent la conséquence de vulnérabilités découvertes lors d'attaques, ce qui signifie que le difficile travail de détection a déjà été fait pour vous.

Vaccinez jusqu'à ce que l'immunité du groupe soit acquise

Tout le monde doit améliorer ses connaissances en matière de sécurité et poursuivre sa formation. La sensibilisation à la sécurité, tout comme les anticorps, peut ne pas durer longtemps. Accueillez la sécurité comme faisant partie du cycle de vie du développement. Commencez à transférer davantage la responsabilité de la sécurité vers le développement et vers les opérations de développement.

Attendez-vous à des variantes et des mutations plus sévères

Investir dans la transformation numérique et la modernisation des technologies. Modéliser les menaces et les réponses.

Nous devons également renforcer l'immunité en détectant les intrusions et en évaluant les vulnérabilités. Verrouiller les portes et fermer les fenêtres d'opportunité pour les envahisseurs en cassant les mauvaises habitudes. La demande de connaissances en matière de sécurité oblige les organisations prêtes pour l'avenir à développer des compétences dans tous les rôles et niveaux professionnels.

Stéphane De Jotemps, Directeur des Ventes du programme de corporate e-

---

Article écrit par STÉPHANE DE JOTEMPS