Pourquoi Devriez-Vous Envisager D'Apprendre La Cybersécurité

3,12 millions. Il s'agit du nombre estimé de spécialistes de la cybersécurité nécessaire à l'échelle mondiale alors que les cybers attaques dans le monde ne cessent de croître en fréquence et en ampleur (Duffy, 2021). Ces derniers mois seulement ont vu certaines des plus grandes failles de sécurité de l'histoire, plus sur lesquelles plus tard. Le développement le plus important dans le récit de la cybersécurité récemment est que les derniers cas très médiatisés sont sortis du cadre des fuites de données privées des clients, auxquelles nous nous sommes franchement déjà habitués. Au lieu de cela, le distributeur de gaz américain Colonial Pipeline et l'un des plus grands producteurs de viande au monde JBS ont payé une somme combinée de plus de 15 millions de dollars aux pirates en quelques jours afin de rétablir leurs opérations après un arrêt forcé parce que les pirates avaient obtenu un accès et un contrôle complets sur leurs systèmes en ligne (Wood, 2021) (Fung, 2021). Ces cas représentent une forme différente de cyber attaque, qui entrave notre vie quotidienne d'une manière que les fuites de données, bien que dangereuses et effrayantes, ne pourraient jamais. Les pénuries de gaz le long de la côte sont des États-Unis, où Colonial opère principalement, ne sont que l'une des conséquences d'une tendance générale aux perturbations dues aux cyber attaques. D'où le besoin urgent de professionnels de la cybersécurité, alimenté également par la numérisation rapide, forcée et complètement non préparée des opérations commerciales dans le monde en raison de la pandémie.

Quand le monde s'est arrêté pendant un certain temps car nous avons été forcés de rester à la maison l'année dernière, tout ce qui pouvait aller online, l'a fait. Alors que les entreprises les plus célèbres telles que les géants de la technique Facebook ou Google ont été rapides à s'adapter et ont eu un passage relativement facile au monde online, toutes les entreprises n'étaient pas aussi

bien préparées ou disposaient de toutes les conditions nécessaires pour passer en douceur au format travail à domicile. Cette transition aléatoire signifiait que la cybersécurité était parfois négligée afin de maintenir l'entreprise en activité. Sans aucune préparation ni formation, les employés ont commencé à travailler online, de précieuses informations et documents privés ont été numérisés et stockés sur des plateformes online ou des nuages et trop peu d'attention ont été accordées à la sécurité de ces systèmes. Cela a fourni une bouée de sauvetage à de nombreuses entreprises et à leurs employés pendant les périodes les plus graves de la pandémie, mais cela a également ouvert la porte à des cybers attaques.

En mai, le Colonial pipeline susmentionné a été victime d'une attaque de ransomware, qui bloque l'accès de l'entreprise à ses fichiers et systèmes, qui ne peut être consulté que si l'entreprise paie une rançon aux attaquants. Il a finalement dû faire exactement cela: la société a payé 4,4 millions de dollars, une décision prise par son PDG quelques heures après l'attaque (Olenick, 2021). JBS a dû être encore plus généreux et a dû payer 11 millions de dollars. Du point de vue des entreprises, payer la rançon était probablement la décision la plus optimale qu'elle aurait pu prendre.

Les entreprises n'avaient pas beaucoup d'options. Essentiellement, cela se résumait au choix entre payer la rançon ou non. Comme les économistes aiment le souligner, un agent rationnel prend une décision basée sur les avantages marginaux et les coûts marginaux des alternatives. Bien que la direction puisse se rendre compte de l'erreur de sous-investissement dans la cybersécurité dans le passé, cette erreur a déjà été commise et aucune des alternatives actuelles ne peut changer cela. Ainsi, face au choix de redémarrer leurs opérations ou de devoir supporter un gel indéfini sans plan d'action sur la façon de rétablir la vie normale, les avantages de pouvoir travailler à nouveau l'emportent de loin sur les millions de dollars demandés par les pirates. Dans le grand

schéma des choses, cependant, de telles actions par l'entreprise victime peuvent servir d'incitation pour les attaques de ransomware à croître et à se multiplier, mais cela ne fait pas partie du processus de prise de décision de l'entreprise. Donc, tant que la cybersécurité n'est pas à un niveau beaucoup plus avancé partout, les attaques de ransomware seront dirigées contre des entreprises qui n'ont jamais soupçonné qu'elles pourraient être ciblées, et la plupart du temps, les attaquants obtiendront ce qu'ils veulent.

Les droits de propriété ont été une partie indispensable de l'existence humaine aussi longtemps qu'il y a une histoire enregistrée de celui-ci. Cependant, pendant la grande majorité de cette période, la définition des biens comprenait les biens corporels, ceux qui peuvent être vus, déplacés et entreposés dans un endroit sûr. Bien que conceptuellement assez proches, la sécurité physique et la cybersécurité sont, malheureusement pour la plupart des entreprises, deux services complètement différents qu'elles doivent acquérir pour que leur propriété soit sûre. Comme la propriété intellectuelle telle que les données et les documents que les entreprises stockent online devient de plus en plus précieuse que tous les actifs corporels qu'elles possèdent, la demande de spécialistes de la cybersécurité, “gardes du corps de la propriété intellectuelle”, si vous voulez, augmente plus rapidement que pour la plupart des autres professions, donc que vous envisagiez un changement de sphère ou que vous soyez indécis quant à ce que vous voulez faire de votre vie, une carrière dans la cybersécurité semble un bon pari pour l'avenir.

Les références

Duffy, C. (2021). *Wanted: Millions of cybersecurity pros. Salary: Whatever you want*. Retrieved from CNN Business: https://edition.cnn.com/2021/05/28/tech/cybersecurity-labor-shortage/index.html

Fung, B. (2021). *JBS says it paid $11 million ransom after cyberattack*. Retrieved from CNN Business: https://edition.cnn.com/2021/06/09/business/jbs-cyberattack-11-million/index.html

Olenick, D. (2021). *Colonial Pipeline CEO Confirms $4.4 Million Ransom Payment*. Retrieved from Data Breach Today: https://www.databreachtoday.com/colonial-pipeline-ceo-confirms-44-million-ransom-payment-a-16696

Wood, R. W. (2021). *Colonial Pipeline Paid $4.4 Million In Bitcoin Ransom. Is It Tax Deductible?* Retrieved from Forbes: https://www.forbes.com/sites/robertwood/2021/05/20/colonial-pipeline-paid-44m-ransom-can-you-deduct-ransom-on-your-taxes/?sh=2cef06487d87