Pourquoi la pandémie a modifié nos valeurs en matière de cybersécurité

« En cette période si particulière » doit être l'une des expressions les plus utilisées mais les moins utiles du moment.

En revanche, ce qui est certainement vrai, c'est que nous cherchons à retrouver de la stabilité dans de nombreux aspects du monde de l'entreprise, du maintien de l'emploi à celui du chiffre d'affaires. Nous essayons de mieux comprendre pour mieux nous préparer à l'avenir. Cette stabilité passe par les professionnels de la sécurité, ceux dont le travail consiste à protéger les données et les actifs technologiques d'une entreprise et à les maintenir fonctionnels pour tous les employés.

Internet est inondé de discussions sur les plus grandes menaces de cybersécurité de 2020, les voies les plus rapides vers la résilience, le coût des sanctions de mise en conformité, les violations de données et l'importance vitale de veiller à ce que les investissements dans la transformation numérique ne soient pas bloqués. Ce qui est moins clair, c'est la manière dont nous pourrions créer une valeur culturelle durable pour maintenir la sécurité, et le facteur humain de ces mesures pratiques. Quels sont donc les éléments qui influencent cette nouvelle culture de la sécurité ?

Phase de phishing

Lorsque les choses n'ont pas de sens, nous sommes enclins à chercher des informations pour les aider à en avoir plus. La tentation est grande pour les employés, qui travaillent désormais à distance, de visiter et de s'inscrire à des sources d'information nouvelles ou non fiables.

Le phishing est l'une des méthodes les moins chères et les plus efficaces pour atteindre des objectifs à grande échelle. Il n'est donc pas surprenant qu'il soit l'une des principales causes de violation de données. Cependant, les pirates informatiques améliorent leur jeu grâce à une myriade de techniques avancées. Les professionnels du phishing ciblent de nombreuses applications professionnelles SaaS et continuent à utiliser les informations personnelles partagées sur de nombreux sites de médias sociaux pour créer des messages interpersonnels de plus en plus authentiques.

En conséquence, ces attaques sont de plus en plus difficiles à identifier, même pour les utilisateurs les plus avertis. Il est essentiel de sensibiliser le personnel, non seulement par la communication, mais aussi par des démonstrations pratiques d'escroquerie et la mise en place de systèmes d'alerte simples et efficaces.

Laisser la « backdoor » ouverte

Comme la plupart des employés sont à la maison, les équipes de sécurité essaient de les équiper au mieux pour assurer leur propre sécurité à distance. Cela signifie que les gens sont plus susceptibles de commettre des erreurs, de transmettre des données à des sources non fiables, de ne pas suivre les protocoles de mise à jour et d'accumuler des vulnérabilités non corrigées.

Les serveurs cloud mal configurés, les environnements multi-noyaux ou encore les API non sécurisées laissent tous les systèmes vulnérables aux pirates. En outre, les employés sont plus susceptibles de télécharger des outils SaaS non sécurisés sans l'approbation du service informatique. Il n'est pas surprenant que plus d'une organisation sur cinq soit confrontée à un cyber-incident provenant d'une ressource informatique non autorisée.

Dans le cadre de l'évolution de la culture de la sécurité, la sécurité doit devenir la responsabilité de chacun, ce qui nécessite un changement de mentalité pour que nous n'apportions pas les vulnérabilités chez nous, et encore moins au bureau.

Évolution des rôles

Des recherches publiées plus tôt dans la pandémie ont indiqué que 47 % des équipes de sécurité se sont vues réaffectées à des tâches informatiques générales, et 90 % travaillent à distance à plein temps. Cela est bien sûr préoccupant car ces équipes sont inévitablement débordées de responsabilités et la menace d'une attaque pourrait être accrue. Cependant, cela pourrait être une chose positive, en aidant à évangéliser la cybersécurité à travers une réflexion informatique plus large, surtout que des investissements comme dans le DevSecOps continuent à briser le cloisonnement des idées.

La capacité à déployer les bons spécialistes de la sécurité là où ils sont nécessaires, tout en surveillant leur intégration dans le reste de l'équipe informatique, sera un atout pour sortir de la pandémie. Le fait d'établir des priorités en ce qui concerne le lieu de travail de ces professionnels pourrait également permettre d'automatiser certaines tâches à long terme.

Déficit de talents en matière de cyber-compétences

Nous ne voulons pas nous retrouver avec un manque de talents, qui est déjà un problème croissant dans l'industrie. Le manque croissant de cyber-compétences a fait que les organisations manquent de talents adéquats pour assurer les fonctions de sécurité nécessaires pour rester en sécurité – et cela inquiète de nombreux RSSI.

Le manque de connaissances techniques et d'expérience est l'une des raisons les plus citées pour justifier ce manque de talents dans la cybersécurité. Une culture d'entreprise inadaptée est également un frein important. Au sein de la communauté des RSSI, le consensus est assez clair pour affirmer que ce problème va s'aggraver, surtout au cours des cinq prochaines années, mais – comme beaucoup de changements qui se produisent actuellement – cela pourrait avoir été accéléré par la récente crise.

Ce n'est donc pas le moment de perdre de vue ces rôles clés, mais plutôt d'utiliser leur réaffectation pour renforcer et aider à déployer l'idée selon laquelle la sécurité est une valeur fondamentale de l'entreprise.

Le futur RSSI

Le RSSI doit étendre son rôle sur toute la chaîne de commande – autant pour la prise de décision auprès de la direction que pour les opérations sur le terrain. En adoptant un management vers le haut, les RSSI sont fermement ancrés dans le conseil de décision et il leur appartient souvent de combler le fossé entre les domaines dans lesquels ils savent qu'ils doivent protéger leurs entreprises et ceux dans lesquels leurs pairs estiment qu'il faut investir.

Pour gérer l'ensemble de la main-d'œuvre et mener une opération 24 heures sur 24 et 7 jours sur 7, il faut être capable d'identifier un incident de sécurité parmi une multitude de faux positifs et d'alertes de faible priorité. À l'avenir, les RSSI devront faire face à une main-d'œuvre encore plus flexible, ce qui les obligera à être plus agiles que jamais face aux menaces.

Malgré les difficultés et les défis rencontrés par nos entreprises au cours des derniers mois, il est apparu que la sécurité ne peut être reléguée au second plan. Le moment est venu pour nos équipes de cybersécurité de nous aider à faire en sorte que la sécurité, la stabilité et la sûreté de fonctionnement – au sens pratique comme au sens humain – soient placées au cœur des valeurs communes de l'entreprise.