Six étapes pour une meilleure cybersécurité - Conseils d'experts

Selon Stephen Burke, PDG de Cyber Risk Aware, l'équilibre entre la technologie, le personnel et la planification est essentiel à la réussite d'une stratégie

Selon le cabinet de recherche et de conseil Gartner, les dépenses mondiales en matière de sécurité de l'information devraient atteindre 123,8 milliards de dollars américains en 2020. Mais avec l'augmentation de la cybercriminalité - une augmentation qui a été largement amplifiée par la crise du coronavirus en grande partie à cause du passage au travail à domicile en masse et à une plus grande utilisation des appareils personnels - les organisations du monde entier vont encore perdre des trillions.

Si ces chiffres énormes révèlent quelque chose, c'est que l'investissement dans la technologie est loin d'être une panacée pour lutter contre la cybercriminalité. Au contraire, la meilleure façon de minimiser les risques, de réduire les vulnérabilités en matière de sécurité et de se préparer efficacement à d'éventuelles cyberattaques et violations de données est d'adopter une approche holistique qui équilibre les rôles de la technologie, du personnel et de la planification, tout en identifiant et en corrigeant les failles de chacun.

La cybersécurité est un sujet important en 2021 pour les organisations de toutes tailles. Les chefs d'entreprise doivent faire preuve d'audace. Ils doivent prendre des décisions plus intelligentes, tant en termes d'investissement dans des solutions technologiques innovantes que d'installation de processus qui protègent les données, aussi bien internes que celles des clients, et s'adaptent à la croissance numérique.

La plupart des entreprises pourraient - et devraient - améliorer leur cybersécurité, et cela doit venir d'en haut. Songez que l'erreur humaine a été à l'origine de 90 % des violations de données au Royaume-Uni en 2019, selon les analystes de cybersécurité CybSafe - et les chiffres sont comparables à l'échelle mondiale.

Stephen Burke, fondateur et directeur général de Cyber Risk Aware, une société de formation à la sensibilisation à la sécurité basée en Irlande, explique à Crowe que les chefs d'entreprise qui veulent prendre des décisions plus intelligentes en matière de cybersécurité doivent réaliser qu'il y a bien plus à prendre en compte que la dernière technologie ou le maintien d'un département informatique solide. En fait, c'est la culture et l'attitude de l'entreprise vis-à-vis de la cybersécurité qui comptent le plus.

En exclusivité pour The Art of Smart, M. Burke identifie six étapes clés pour établir un programme de cybersécurité efficace et inclusif.

1. Identifier les risques pertinents

Les risques de cybersécurité sont généralement liés aux éléments clés d'une organisation. « Le temps, le personnel, les ressources et l'argent étant limités, il n'y a que peu de choses sur lesquelles vous pouvez vous concentrer », reconnaît M. Burke. « Tous les risques ne sont pas pertinents pour toutes les entreprises ; il s'agit d'identifier ce qui pour vous sont les risques clés et les données qui doivent être traitées. »

2. Engager l'ensemble de l'organisation

La création d'un comité de pilotage informatique qui couvre la partie principale de l'entreprise, et l'identification des es risques associés aux systèmes ou aux données dans chaque département, améliorera la cybersécurité.

« Vous devez faire participer l'ensemble de l'entreprise - vous ne pouvez pas le faire tout seul », explique M. Burke. « Faites participer les gens de manière significative, en les associant aux risques encourus et en utilisant le langage de l'entreprise, et enregistrez ce dont l'entreprise devrait se préoccuper. »

3. Évaluer l'efficacité des contrôles existants

« Lorsque vous appliquez un contrôle, qui peut être un contrôle technique, sur un processus ou des personnes, il ramène [le risque] à un niveau résiduel », explique M. Burke. Il est donc important d'identifier les contrôles existants et de mesurer leur efficacité.

Il poursuit : « Cela permet ensuite de savoir dans quoi nous devons investir pour réduire le niveau de risque, afin que l'entreprise puisse dire : "Voilà ce que nous avons fait, nous avons vu ce risque, nous avons appliqué ces contrôles et nous sommes satisfaits du niveau que nous atteignons".

« Faites participer les gens de manière significative, en les associant aux risques encourus et en utilisant le langage de l'entreprise, et enregistrez ce dont l'entreprise devrait se préoccuper. » - **Stephen Burke**

4. Aborder le facteur humain - l'éducation sensibilise

On oublie souvent à quel point il est important d'investir dans le personnel, et pas seulement dans celui du service informatique. L'éducation de tous les membres du personnel sur la façon d'améliorer la cybersécurité et l'établissement de protocoles en cas de violation des données sont des activités vitales.

« Vous devez évaluer où se trouvent les vulnérabilités de votre personnel, donc un programme de sensibilisation à la cybersécurité humaine est une étape clé », explique M. Burke. « [Ces programmes] permettent d'évaluer où se situent les lacunes du personnel en matière de connaissances, d'évaluer la propension des courriels de phishing et de cibler la formation sur les personnes qui ont besoin d'aide. »

5. Trouvez et renforcez vos faiblesses techniques

Si vous parvenez à détecter les difficultés techniques et à les résoudre en conséquence, vous traitez une grande partie du problème.

« L'une des principales menaces actuelles concerne la collecte de données d'identification : il s'agit de voler les noms d'utilisateurs et les mots de passe des gens », explique M. Burke. « Ils sont à vendre et de nombreux cybercriminels ont donc accès à presque tous les mots de passe. Mais si vous mettez en place l'authentification multifactorielle, vous sécurisez 99 % de la récolte de certificats. »

6. Formulez un plan et testez-le

Les entreprises doivent se préparer à l'éventualité de cyberattaques en élaborant un plan de réponse aux incidents. Ce plan présente des avantages tant pratiques que juridiques et permet de prendre des décisions plus avisées. Un plan de réponse aux incidents implique d'identifier qui va prendre les décisions au nom de l'organisation en cas de violation de la sécurité. Le plan doit également indiquer comment les membres du personnel communiqueront si les systèmes de l'entreprise sont en panne, et aborder des questions telles que les aspects juridiques, éthiques et moraux du paiement de rançons.

M. Burke commente : « Le président Dwight D. Eisenhower a dit : «Les plans sont inutiles, mais la planification est indispensable.» Ce qu'il veut dire, c'est qu'il faut tester le plan. Si vous n'effectuez pas régulièrement des exercices de simulation de votre plan, vous n'en trouverez pas les lacunes. » Ne pas les combler pourrait s'avérer coûteux pour votre organisation, tant sur le plan financier qu'en termes de réputation.

Comment penser comme un cybercriminel

Il est essentiel de connaître son ennemi et de déterminer les vulnérabilités éventuelles de son entreprise, explique Jim Gee de Crowe UK

Crowe a une approche unique de la protection contre la cybercriminalité : elle se met dans la peau du cybercriminel, utilise des techniques similaires à celles des délinquants en ligne et s'infiltre sur le dark web. Étant donné qu'un rapport Crowe de juillet 2019 a calculé que la fraude est susceptible de coûter aux particuliers et aux entreprises 5 100 milliards de dollars américains par an - les pertes ayant augmenté de 56 % au cours de la dernière décennie - il est potentiellement plus coûteux de ne pas utiliser tous les moyens disponibles pour lutter contre cette menace importante.

« Nous effectuons une analyse de vulnérabilité externe, qui examine les vulnérabilités que les cybercriminels pourraient voir dans une organisation s'ils voulaient déterminer s'ils doivent consacrer du temps à l'attaquer plutôt qu'une autre », explique Jim Gee, National Head of Forensic Services chez Crowe UK.

Parallèlement à l'analyse externe, Crowe procède à une vérification interne des vulnérabilités. Ce processus est similaire aux premières étapes d'un test de pénétration, ou d'une cyberattaque autorisée, mais sans exploiter les faiblesses à l'intérieur de l'entreprise.

« Ces dernières années, nous avons développé des identités qui nous permettent d'aller sur les marchés et les forums du dark web, où la plupart des cybercrimes et des fraudes sont organisés », explique M. Gee. « Nous pouvons voir ce qui est discuté, ce qui est vendu et cela nous permet de rechercher des preuves des discussions qui ont lieu sur l'attaque

d'organisations particulières et sur des courriels et mots de passe compromis. »
Étant donné que les cyberattaques se classent au premier rang des risques mondiaux d'origine humaine, selon le rapport 2020 sur les risques mondiaux du Forum économique mondial, et que la cybercriminalité pourrait coûter 11,4 millions de dollars US chaque minute en 2021, il est clairement essentiel pour les entreprises de renforcer leurs défenses.

« La COVID-19 a engendré une augmentation massive de la cybercriminalité », poursuit M. Gee. « La question n'est pas de savoir si une organisation sera attaquée, mais quand. » Pour que la réponse soit efficace, les organisations doivent comprendre les trois choses suivantes, suggère-t-il.

1. Il faut utiliser la technologie pour être aussi bien protégé que possible, mais il faut aussi être prêt à gérer une attaque si elle se produit, être capable de reconstruire et d'atténuer les dommages - l'approche doit être globale.

2. Il s'agit d'entreprises de cybercriminalité qui prennent des décisions commerciales pour déterminer quelles sont les meilleures organisations à attaquer en termes de ressources nécessaires et de bénéfices potentiels.

3. La cybercriminalité n'est pas comme les autres phénomènes que nous cherchons à gérer en tant que risques ; elle n'est pas statique mais extrêmement dynamique, changeant continuellement et évoluant comme un virus. Cela signifie que ce que les organisations font pour se protéger doit également évoluer et changer pour refléter les dernières manifestations du problème.

Points de vue de Crowe

Nadeem Maniar, Fraud & Forensic Director, Crowe UAE

« Chacun d'entre nous est soit une cible, soit une victime de la cybercriminalité. L'erreur humaine a causé 90 pour cent des violations de données cybernétiques au Royaume-Uni en 2019, selon l'Information Commissioner's Office - et les chiffres sont comparables dans le monde entier. Les marchés numériques du Moyen-Orient se sont développés avec un taux de croissance annuel de 12 % et, en conséquence, le coût des violations de données augmente à un rythme alarmant. En août 2020, The National [un journal du Moyen-Orient] a indiqué que le coût d'une violation de données en Arabie saoudite et dans les Émirats arabes unis avait augmenté de 9,4 % au cours de l'année écoulée. Ces incidents coûtent aux entreprises étudiées dans la région 6,53 millions de dollars US par violation en moyenne, ce qui est supérieur à la moyenne mondiale de 3,86 millions de dollars US par violation. La meilleure

défense est une bonne attaque. Les bons systèmes et contrôles, une sensibilisation opportune, les dernières techniques et un partenaire professionnel expérimenté comme Crowe peuvent vous aider, vous et votre organisation, à réduire le risque de cybercriminalité. »

Bibliography:
UK Information Commissioner's Office (ICO), 2019.
Association of Certified Fraud Examiners, 2020. Fraud In The Wake Of COVID-19: Benchmarking Report.
IBM Security, 2020. Cost Of A Data Breach Report.

Geert-Jan Kroll, Technology Advisory Partner, Crowe Peak (Pays-Bas)

« Avec l'entrée en scène du crime organisé, la cybercriminalité est devenue l'une des plus grandes économies illégales du monde, atteignant 10,5 trillions de dollars US par an d'ici 2025 - contre 3 trillions de dollars US en 2015. Le coût d'un seul incident est souvent assez élevé pour que les entreprises fassent faillite en moins de six mois. Avec la technologie et l'automatisation, les cybercriminels ont besoin de moins de compétences pour menacer des entreprises et chercher des vulnérabilités à exploiter. Avec l'apparition quotidienne de nouvelles techniques et méthodes, le paysage des menaces change constamment. Il peut donc être assez difficile de protéger vos actifs numériques et votre entreprise contre la cybercriminalité. Je pense que le paradigme de la cybersécurité devrait passer de la prévention à une approche plus cyclique. Cela signifie que les entreprises devraient appliquer le principe de «l'hypothèse de la violation», selon lequel elles supposent que, tôt ou tard, elles seront touchées par une violation ou un incident de sécurité. Outre la protection de leurs actifs numériques, les entreprises doivent mettre en œuvre des mesures liées à la détection des incidents, à la réaction et à la reconstruction afin de pouvoir agir en conséquence une fois l'incident survenu. Les chefs d'entreprise devraient adopter la conviction que chaque entreprise est une cible lucrative pour les cybercriminels et qu'en pratiquant une bonne cybersécurité, ils peuvent réduire considérablement le risque d'être victime de la cybercriminalité. La cybersécurité est une question de personnes, de processus et de technologie. Ainsi, c'est l'attitude d'une entreprise vis-à-vis de la cybersécurité et sa culture qui comptent le plus. »