Exclusions de cyberassurance : quatre exemples de mises à niveau qu'une police pourrait ne pas couvrir en cas de brèche

13 septembre 2022

Le présent article est le deuxième d'une série de trois. Les autres articles portent sur l'assurance contre les pertes d'exploitation et la façon de réduire les frais de *cyberassurance*.

La gestion d'une brèche de sécurité informatique est une expérience pénible et coûteuse. S'il y a un côté positif, c'est qu'un incident peut mettre au jour les vulnérabilités à corriger pour une entreprise. Habituellement, les polices de cyberassurance ne couvriront pas le coût de ces améliorations ou n'en couvriront qu'une partie. En effet, la cyberassurance est conçue pour remettre les systèmes d'une organisation dans l'état où ils étaient avant une attaque, et non pour couvrir les mises à niveau.

Dans le présent article sur les exclusions de cyberassurance, nous donnons quatre exemples de mises à niveau qui pourraient ne pas être entièrement couvertes, ainsi qu'un aperçu de la manière dont les assureurs et les assurés négocient habituellement ces questions.

Exemple 1 : Mettre à niveau les logiciels et le matériel

Après une brèche de sécurité, les professionnels en intervention en cas d'incident informatique et en reprise des activités pourraient recommander des mises à niveau du système. À titre d'exemple, on suggère souvent aux entreprises de passer d'un serveur Microsoft Exchange local au nuage Office 365. Après une attaque par rançongiciel, on pourrait aussi vous recommander de passer à la version la plus récente d'un logiciel si vous n'êtes pas en mesure de restaurer complètement vos systèmes à partir d'une sauvegarde.

La position de l 'assuré : C'est le moment idéal pour mettre à niveau nos logiciels afin d'être plus solides et plus attrayants pour les assureurs.

La position de l ’assureur : La police ne couvre pas les mises à niveau qui impliquent une augmentation des coûts, le passage à un modèle par abonnement ou des frais de formation du personnel.

Le conseil de juristes spécialisés en cyberassurance : Les assurés doivent presque toujours assumer le coût des mises à niveau de leurs logiciels et de leur matériel. Il existe cependant une exception si la mise à niveau est la seule option possible. Les organisations doivent ajouter le coût des mises à niveau régulières à leur budget informatique afin d’assurer leur sécurité et d’améliorer leurs chances d’obtenir et de conserver une cyberassurance.

Exemple 2 : Renforcer la détection et la gestion des incidents sur les terminaux

Après une atteinte à la sécurité, il est courant de mettre en place des logiciels de détection et de gestion des incidents sur les terminaux pendant une courte période afin de surveiller l’activité du réseau et de repérer les logiciels malveillants.

La position de l ’assuré : Nous devrions maintenir le contrat avec notre fournisseur de logiciels de détection à plus long terme pour renforcer nos défenses. Nous tenons à ce que la situation ne se reproduise pas.

La position de l ’assureur : Votre politique de cyberassurance couvre l’effacement de la présence de l’auteur de la menace dans votre système. Les logiciels de détection et de gestion des incidents sur les terminaux sont uniquement couverts dans le contexte de la réponse immédiate suivant une brèche de sécurité. Les contrats permanents visant à prévenir les menaces ne sont pas couverts.

Le conseil de juristes spécialisés en cyberassurance : Le renforcement de la détection et de la gestion des incidents sur les terminaux constitue une amélioration de la sécurité tournée vers l’avenir. Cette mesure figure d’ailleurs dans notre liste de vérification de la cyberhygiène, au même titre que les mises à niveau régulières des logiciels et du matériel. Bien qu’il s’agisse d’une excellente idée, les organisations ne peuvent pas inclure les coûts connexes dans leur réclamation de cyberassurance.

Exemple 3 : Simplifier l ’infrastructure du réseau

Au fil du temps, l’infrastructure informatique d’une entreprise peut devenir un labyrinthe d’intégrations personnalisées, d’angles morts, de vieux serveurs et de fournisseurs de services décentralisés. Ce phénomène est particulièrement fréquent lorsque des entreprises fusionnent. Une cyberattaque peut causer des ravages sur ces systèmes.

La position de l ’assuré : Notre réseau est comme le monstre de Frankenstein. Nous ne l’aurions jamais bâti de cette façon si nous l’avions fait à partir de zéro. Il sera beaucoup plus long d’essayer de recréer ce désordre que de faire correctement les choses la deuxième fois, et le temps, c’est de l’argent. Notre compagnie d’assurance devrait couvrir les coûts et nous permettre de reprendre nos activités plus rapidement, et peut-être même pour moins cher!

La position de l ’assureur : L’assurance couvrira habituellement les coûts nécessaires pour remettre les systèmes dans l’état où ils étaient. Toutefois, s’il n’y a pas de différence de coût entre les options, les mises à niveau pourraient être couvertes. Si le coût de la mise à niveau est plus élevé, l’assurance pourrait n’en couvrir qu’une partie.

Le conseil de juristes spécialisés en cyberassurance : Il peut être possible d’obtenir une couverture pour les améliorations réseau; les entreprises n’ont qu’à prouver que la mise à niveau sera financièrement avantageuse pour la compagnie d’assurance. Les organisations doivent évaluer le coût de deux scénarios : ramener le réseau à son état antérieur ou le simplifier. S’il s’avère moins cher de bâtir un nouveau réseau, il y a de fortes chances que l’assureur accepte de couvrir les coûts. Nous vous recommandons de présenter à votre assureur la comparaison des coûts et d’obtenir son approbation avant d’entreprendre une refonte de vos systèmes informatiques.

Exemple 4 : Rétablir la confiance des fournisseurs

Les brèches de sécurité informatique peuvent entraîner des problèmes de réputation, les entreprises ayant subi une attaque étant perçues comme des partenaires d’affaires à haut risque. Cela peut conduire les partenaires d’intégration à refuser l’accès aux réseaux ou aux bases de données partagés jusqu’à ce que l’entreprise soit en mesure de prouver qu’elle a amélioré sa cybersécurité.

La position de l ’assuré : Mes fournisseurs ont une liste de mises à niveau que je dois effectuer, et je ne peux pas reprendre mes activités avant que ce soit fait. Ces mises à niveau devraient être couvertes par les volets restauration ou pertes d’exploitation de notre police de cyberassurance.

La position de l ’assureur : Les mises à niveau exigées par les fournisseurs ne sont pas couvertes puisqu’elles ne concernent pas la restauration de l’ancien système.

Le conseil de juristes spécialisés en cyberassurance : La question est délicate. Les coûts correspondent-ils à la définition d’une restauration, à savoir qu’ils sont nécessaires à la reprise des activités? S’agit-il plutôt de mises à niveau nécessaires pour satisfaire à de nouvelles normes? (Les mises à niveau ne sont souvent pas couvertes par les polices de cyberassurance.) C’est aussi une question de cause. Les mises à niveau découlent-elles du cyberincident ou de l’imposition par le fournisseur de nouvelles normes plus strictes? Il va sans dire que la police ne couvrira pas les coûts des mises à niveau exigées par un fournisseur si aucun incident ne s’est produit. Dans une telle situation, l’assureur et l’assuré doivent reconnaître cette ambiguïté et tenter de parvenir à un accord.

Que doivent donc faire les entreprises?

Une police d’assurance habitation ne couvrira pas la construction d’un manoir si un petit bungalow est ravagé par un incendie. De la même façon, une police de cyberassurance ne couvrira pas l’amélioration de systèmes obsolètes après une cyberattaque.

Cela ne signifie pas pour autant que les organisations doivent se contenter de leur situation préalable à l’incident. En fait, si elles n’investissent pas dans leur

cyberhygiène, elles pourraient faire face à une augmentation du coût de leur couverture ou même se voir refuser toute cyberassurance.

Les organisations qui ont subi une brèche de sécurité et qui ont besoin de solutions rentables pour se rétablir devraient d'abord présenter leurs efforts de restauration comme étant moins coûteux que le rétablissement de l'état antérieur. En représentant les plus grands assureurs du monde dans le cadre de réclamations de cyberassurance complexes, nous avons appris que les compagnies d'assurance se montrent souvent très raisonnables si les améliorations proposées constituent la voie de reprise la plus rentable.

Si vous avez besoin d'aide pour déterminer les aspects d'une réclamation qui sont couverts ou comprendre les clauses de votre police de cyberassurance à la suite d'une brèche, n'hésitez pas à communiquer avec Eric Charleston ou Michelle Doody.

Par

Eric S. Charleston, Michelle Doody

Services

Cybersécurité, respect de la vie privée et protection des renseignements personnels, Contestation de réclamations d'assurance

---