SCÉNARIO DE RÉCLAMATION

Débâcle de la base de données

Une attaque par rançongiciel entraîne des complications imprévues pour un détaillant de produits domestiques

VICTOR

Au cours des deux dernières décennies, la technologie a transformé le mode de fonctionnement des entreprises, et la plupart d'entre elles dépendent de leurs systèmes informatiques d'une manière ou d'une autre. Même les entreprises traditionnelles, comme les magasins de vente au détail et les distributeurs grossistes, utilisent des systèmes informatiques et les données qu'ils contiennent pour assurer le fonctionnement quotidien de leurs activités. Si ces systèmes deviennent indisponibles ou cessent de fonctionner correctement à la suite d'une cyberattaque, cela peut avoir un impact négatif sur l'entreprise en question et entraîner un préjudice financier important.

Un assuré ainsi touché était un magasin de produits de bricolage et de rénovation de maisons dont les affaires étaient limitées à un seul magasin. Le magasin vend une large gamme d'articles domestiques, notamment des meubles et des abris de jardin, des équipements de jardin, des ustensiles de cuisine, des accessoires de salle de bains, et des outils et équipements de bricolage. Les clients peuvent acheter en magasin ou se faire livrer à domicile les articles les plus volumineux, sur demande. L'entreprise dispose d'un grand entrepôt relié au magasin de vente au détail qui est utilisé pour stocker les produits et qui peut ensuite être utilisé pour réapprovisionner les étagères ou, dans le cas d'articles plus volumineux, les faire sortir pour que les clients puissent les retirer ou les faire livrer.

Un employé tombe dans le piège

L'incident a commencé lorsqu'un employé a été victime d'un courriel d'hameçonnage. Le courriel indiquait qu'il y avait un état financier joint qui devait être vérifié. Même si le courriel ne s'adressait pas directement à l'employé, comportait de nombreuses fautes de grammaire et semblait provenir d'une adresse électronique suspecte, **la curiosité a eu raison de l'employé, qui a cliqué sur la pièce jointe**. Après avoir cliqué sur la pièce jointe, une variante du rançongiciel a été téléchargée sur le serveur de l'entreprise et a commencé à crypter les fichiers et les programmes du réseau, y compris les sauvegardes de l'assuré, qui n'avaient pas été stockées à l'extérieur.

Le serveur étant crypté, l'entreprise n'a pu accéder à aucun des systèmes qu'elle utilisait quotidiennement, notamment le système de gestion du point de vente et les informations relatives aux ventes, aux livraisons et à la gestion des stocks.

Ayant besoin de toute urgence de rétablir l'accès à ces systèmes et bases de données, l'assuré a signalé l'affaire à l'équipe de réclamations et d'intervention en cas d'incident cybernétique de Victor. Les sauvegardes de l'assuré ayant été cryptées par le rançongiciel, l'équipe de réclamations et d'intervention en cas d'incident a examiné les autres options disponibles. La première étape a consisté à déterminer quelle souche de rançongiciel avait été utilisée dans l'attaque en examinant la note de rançon et un échantillon des fichiers cryptés. Dans ce cas, le rançongiciel utilisé était une souche bien connue et bien établie, et l'équipe a pu trouver une clé de décryptage disponible gratuitement en ligne. À l'aide de la clé de décryptage, l'équipe a commencé le processus de décryptage des programmes et des fichiers de l'entreprise.

Dans la plupart des cas de rançongiciel, une fois que les données et les programmes de l'entreprise ont été décryptés et que le rançongiciel a été supprimé, l'entreprise peut continuer à utiliser ses systèmes informatiques normalement.

Cependant, les choses ne sont pas toujours aussi simples que cela. Malheureusement, les cybercriminels n'ont pas la même approche du contrôle préalable des produits que les entreprises respectueuses de la loi, et ceux qui créent des rançongiciels n'auront pas fait l'effort de tester la compatibilité de leurs souches de rançongiciels avec tous les types de fichiers ou de programmes imaginables. En conséquence, **les rançongiciels peuvent causer des dommages involontaires et parfois irréparables** aux fichiers électroniques et aux programmes informatiques.

Dans le présent cas, bien que la majorité des données de l'entreprise aient été accessibles après le processus de décryptage, une base de données contenant six mois d'informations relatives aux niveaux de stock et aux statuts de livraison a été corrompue. Malgré de nombreuses tentatives de reconfiguration et de restauration de la base de données, les fichiers ont été jugés irréparables, ce qui les rendait inaccessibles à l'entreprise.

La base de données corrompue entraîne des retards importants

Sans accès à la base de données, l'entreprise a rencontré de nombreuses difficultés. Le personnel du magasin n'était pas en mesure de vérifier la base de données la plus récente pour savoir si un article particulier était en stock. Ainsi, lorsqu'un client demandait si un article était disponible, la seule possibilité était qu'un membre du personnel contacte un membre de l'équipe de l'entrepôt et lui demande de parcourir l'entrepôt pour voir si l'article était disponible, ce qui entraînait des retards importants dans le service. **Le manque d'informations sur les niveaux des stocks signifiait également que l'entreprise ne disposait pas d'une vue d'ensemble précise des articles en rupture de stock et devant être commandés à nouveau auprès des fournisseurs**, ce qui a entraîné une pénurie d'articles populaires. En outre, sans accès aux informations relatives aux livraisons, l'entreprise a perdu la trace du statut de livraison de certains articles, ce qui a eu pour conséquence que les articles n'ont pas été livrés au client à temps ou, dans certains cas, qu'ils ont été livrés deux fois.

La seule façon de résoudre ce problème était de recréer manuellement l'inventaire du stock actuel. Pour ce faire, les employés devaient passer en revue chaque article en stock, à la fois dans l'entrepôt et dans le magasin, créer un numéro d'identification pour chaque article, puis le numériser dans la base de données. L'entreprise avait également besoin de mieux comprendre le statut de la livraison de tous les articles. Pour éviter les retards et les doubles livraisons, le personnel devait passer en revue toutes les ventes en cours et voir comment elles correspondaient aux copies sur papier des reçus de livraison pour établir quels articles avaient été livrés et quels articles étaient encore en attente de livraison.

Compte tenu de la taille du magasin et de la quantité de données sur les stocks et les ventes que cela impliquait, il s'agissait d'une activité considérable, et le personnel a dû faire des heures supplémentaires, mais même cela n'a pas suffi. L'entreprise a également dû faire appel à des entrepreneurs indépendants pour l'aider dans sa tâche. Au total, **il a fallu deux semaines à l'entreprise pour reconstruire entièrement cette base de données**. Cela a coûté 20 858 $ en heures supplémentaires des employés et en frais de personnel contractuel.

Bien que le magasin soit resté ouvert pendant toute la période de récupération, **les perturbations du service ont entraîné une réduction des ventes**. Pour le mois en question, l'entreprise avait prévu des ventes de 460 031 $, mais les ventes réelles pour le mois ne se sont élevées qu'à 353 611 $, soit un déficit de 106 420 $. En appliquant un taux de bénéfice brut de 20 % au déficit, la perte d'exploitation de l'assuré a été calculée à 21 284 $.

Le rôle de l'erreur humaine et autres leçons

Cette réclamation met en évidence quelques points essentiels. Tout d'abord, elle illustre le rôle clé de l'erreur humaine dans de nombreux incidents cybernétiques. Beaucoup d'entreprises refusent d'acheter des polices d'assurance contre les cyber-risques au motif qu'elles ont mis en place une bonne sécurité informatique. Mais **ce raisonnement ne tient pas compte du fait que la majorité des incidents cybernétiques sont le résultat d'une erreur humaine**. Dans le présent cas, l'incident a été déclenché par un employé qui a cliqué sur une pièce jointe malveillante. Les entreprises doivent veiller à ce que les employés soient informés des risques posés par les courriels d'hameçonnage et sachent comment les repérer.

Deuxièmement, elle montre qu'en cas d'incident lié à un rançongiciel, il ne suffit pas toujours d'effectuer le processus de décryptage pour que l'entreprise en question retrouve automatiquement l'accès à ses systèmes et à ses données. **En réalité, il peut y avoir toutes sortes de complications imprévues.** Dans ce cas, même si les données et les applications ont été décryptées à l'aide d'une clé de décryptage disponible gratuitement, le rançongiciel lui-même avait corrompu l'une des principales bases de données de l'entreprise, ce qui a eu un impact négatif sur les activités de l'assuré.

Troisièmement, elle démontre l'importance d'avoir une couverture de recréation de données dans une police d'assurance contre les cyber-risques. De nombreuses polices d'assurance contre les cyber-risques ne couvrent que les coûts de récupération ou de restauration à partir de sauvegardes, mais pas les coûts de recréation ou de réintroduction des données perdues à partir de zéro. Une partie importante de la réclamation de l'assuré provenait des **coûts de main-d'œuvre associés au personnel et aux travailleurs contractuels qui devaient numériser et ressaisir manuellement les données** pour s'assurer que l'inventaire des stocks était correct et à jour, et les courtiers devraient s'assurer que leurs clients disposent de cette importante couverture dans leurs polices.

Enfin, elle révèle que presque toutes les entreprises modernes sont exposées, sous une forme ou une autre, aux risques cybernétiques. Même si l'entreprise en question était un magasin de produits de bricolage et de rénovation de maisons qui ne dépendait pas uniquement de ses systèmes pour fonctionner, **l'entreprise dépendait toujours de ses systèmes informatiques et de ses données pour gérer efficacement le magasin et fournir un service efficace à la clientèle**. Lorsque certaines données de l'entreprise ont été corrompues, cela a eu un impact négatif sur l'ensemble des activités, et la mise en place d'une police d'assurance contre les cyber-risques a constitué un précieux filet de sécurité pour l'entreprise.

Visitez assurancevictor.ca/cyber pour en apprendre davantage.