Vous y connaissez-vous en ransomware?

Face à la menace des ransomware, les entreprises doivent faire évoluer leurs pratiques et tenir compte des caractéristiques de leur organisation. Pour une protection efficace, les chefs d'entreprise doivent se poser et répondre à plusieurs questions importantes.

Les auteurs

Philipp Leo est associé directeur chez Leo & Muhly Cyber Advisory et Lieutenant-colonel dans le cyber commandement de l'armée suisse.

Öykü Isik est professeur de stratégie numérique et de cybersécurité à l'IMD.

Fabian Muhly est associé directeur chez Leo & Muhly et chercheur en criminologie à l'Université de Lausanne.

L'avertissement est arrivé dans un e-mail resté dans un dossier de spam, sans être ouvert et négligé. En ce lundi matin ordinaire, les applications informatiques ne fonctionnaient pas et les documents ne pouvaient pas être ouverts, de quoi inquiéter. Un e-mail, rédigé dans un anglais approximatif et adressé à un chef d'entreprise allemand, demandait une rançon pour décrypter les fichiers de sa société. C'est ainsi qu'a commencé, dans un élevage de chevaux de course dans le sud de l'Allemagne, un épisode de ransomware en 2014. Il ressemble à de nombreuses autres situations d'urgence et offre des leçons sur la façon de gérer. Ne disposant pas de sauvegarde de données et n'étant pas préparé, le propriétaire de ce haras a accepté la situation, négocié pour faire baisser le prix et finalement organisé le règlement d'un paiement en bitcoins – reprenant finalement le contrôle de ses opérations quotidiennes.

Chaque organisation ciblée est différente, avec des limites financières, des contraintes opérationnelles et des définitions uniques de la quantité de clients, de ventes, de capital ou de données qu'elle peut se permettre de perdre. Certaines organisations pensent, à tort, que leur cyberassurance peut les aider. A mesure que les risques se multiplient, il en va cependant de même des primes d'assurance avec des couvertures changeantes. Plusieurs grands assureurs, dont AXA, pourraient ne plus couvrir les rançons, mais seulement le coût de la perte d'activité. Les assureurs renoncent notamment à proposer une assurance pour ce type de cybermenaces, car ils ne peuvent pas en évaluer durablement les risques financiers. Un nombre croissant d'attaques étant considérées comme financées par des États – comme les attaques NotPetya de 2017 qui ont coûté des milliards de pertes –, certains assureurs tentent de les classer comme des actes de guerre, ce qui les libère de toute responsabilité.
Face à des menaces qui évoluent rapidement, les meilleures pratiques doivent suivre le rythme. Les questions suivantes vous aideront à protéger vos données et votre organisation.

A quelle vitesse?

Le groupe de ransomware REvil n'a eu besoin que de deux heures pour installer un logiciel sur les serveurs Kaseya en 2021. Et la portée, tout comme la vitesse, ne fait qu'augmenter. L'essor des services managés avec des ressources cloud et de l'informatique à la demande fournis par des entreprises tierces a compliqué les choses. Les prestataires de services offrent des cibles pour des attaques qui peuvent paralyser des centaines de leurs clients en aval, ce qui augmente la pression pour payer rapidement les demandes de ransomware ou risquer d'affecter d'énormes réseaux d'organisations.

Dans quel délai une entreprise peut-elle transférer ses données critiques sur un serveur sauvegardé à l'abri des pirates afin de pouvoir poursuivre ses activités? Un système paralysé peut-il être retiré rapidement pour éviter la propagation du cryptage ou des logiciels malveillants? Ces chiffres sont-ils prouvés ou des suppositions?
Quels sont les délais et les autorisations nécessaires pour obtenir une quantité spécifique de bitcoins – ou d'autres cybermonnaies – et quelles sont les démarches à effectuer? S'il faut du temps pour obtenir ces fonds avant de les transférer, ce délai peut donner à l'entreprise visée une précieuse marge de négociation.

Si les victimes tardent à demander l'aide de la police ou du service IT, elles risquent d'être punies par l'effacement des données ou l'escalade du déni de service. Les équipes de pirates s'attachent également à trouver et à désactiver les plans de sauvegarde ou de réponse dans le cadre des stratégies d'attaque, recherchant parfois explicitement les polices de cyberassurance dans le réseau de la cible pour adapter les demandes de rançon. D'autres groupes de ransomware ne chiffrent même pas les données mais font chanter leurs victimes en les menaçant de publier ou de vendre des données critiques.

Combien?

Votre équipe ou votre comité d'intervention a-t-il consulté les propriétaires, la direction locale ou le siège mondial pour savoir combien ils peuvent se permettre de perdre (ou de dépenser) en cas d'attaque? Mesurez-vous les temps d'interruption en heures, en jours ou en gigaoctets de données? La cyberassurance couvrira-t-elle les pertes ou les perturbations? Certaines organisations identifiées comme payeurs, subissent des attaques répétées ou une deuxième demande de rançon plus importante de la part

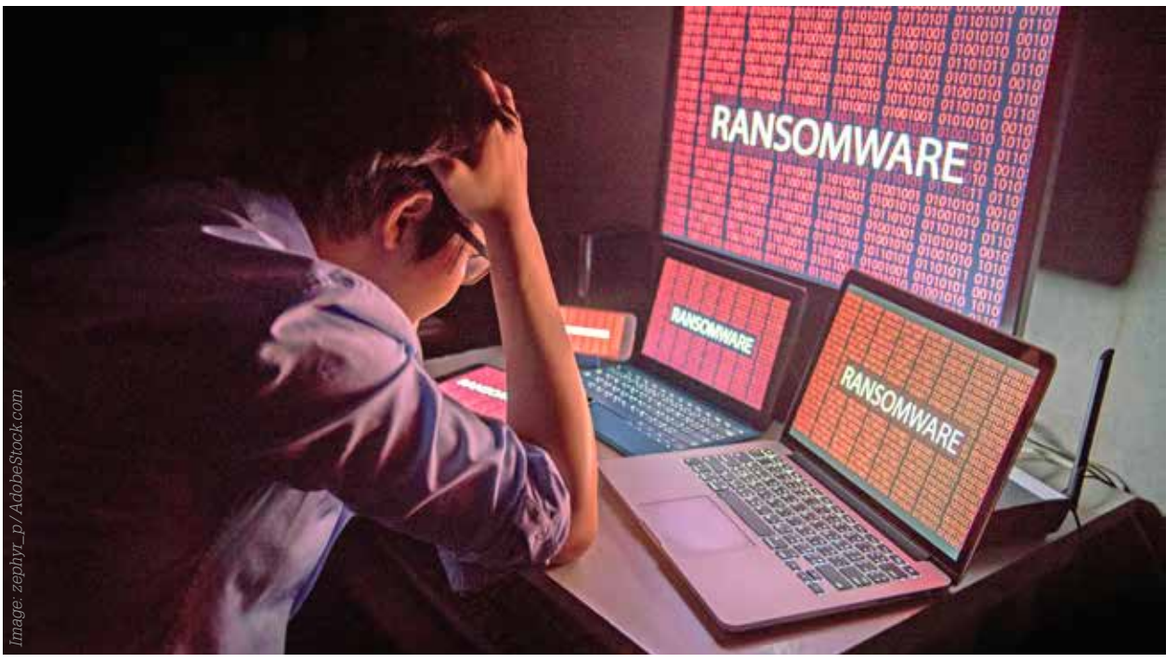

Image: zephyr_p/AdobeStock.com

des attaquants initiaux. Ces incertitudes rendent toute réponse difficile sans une préparation sérieuse.

Le paiement de la rançon ne représente qu'une partie du coût. La perte de productivité et de chiffre d'affaires, la récupération des données et l'atteinte à la réputation sont autant de conséquences possibles. Il s'agit de défis multidimensionnels qui influent sur la prise de décision tant dans les discussions de crise à court terme que dans la vision à plus long terme de l'organisation.

Chaque bureau, chaque site national présente des vulnérabilités et une sensibilité aux prix qui lui sont propres. Il n'existe pas de solution universelle, même au sein d'un même secteur ou d'une même entreprise.

L'avons-nous déjà fait?

Selon une étude réalisée par Veeam en 2021 auprès de plus de 3000 décideurs informatiques, 58% des sauvegardes de données échouent lors d'une tentative de restauration. Ainsi, disposer d'une réponse testée et éprouvée pour les systèmes IT permet une plus grande confiance dans la négociation avec les hackers.

Le rapport Verizon 2021 Data Breach Investigations Report suggère que 85% des cyberattaques réussies font appel à l'ingénierie sociale – par le biais de messages, d'appels téléphoniques et de sites web, et pas seulement par le biais du phishing par e-mail. Les données confidentielles divulguées ne sont parfois utilisées que bien plus tard, une fois combinées avec des détails lors d'attaques ultérieures. Vos collaborateurs partagent-ils ces expériences et savent-ils comment éviter ces manipulations?

Quelle a été votre expérience avec les forces de l'ordre ou les organisations similaires? Les enquêtes sur les attaques sont plus efficaces lorsque les autorités ont accès à des informations sur des incidents similaires et à des responsables coopératifs. Quelle est la politique locale et mondiale de votre entreprise en matière de divulgation aux partenaires, aux clients et aux autorités?

Sommes-nous prêts?

Malgré des investissements massifs dans la cybersécurité, de nombreuses organisations fonctionnent aujourd'hui différemment de ce qu'elles étaient avant la pandémie de COVID-19, avec des équipes distantes, des effectifs réduits et d'autres facteurs. Chaque organisation devrait connaître ses risques et sa réponse, tout comme elle le fait pour un exercice d'incendie, une urgence météorologique ou tout autre éventuelle interruption.

Connaître les normes de votre secteur pour définir les attentes des clients et des partenaires est un autre aspect de la préparation. Gérer activement les intérêts de vos clients et partenaires peut faire la différence sur le plan stratégique dans le maelström actuel des ransomwares.

Partager le message de sécurité avec les partenaires et les fournisseurs peut contribuer à créer une réponse communautaire où l'on veille les uns sur les autres. En outre, vos dépenses en matière de cybersécurité devraient continuer à augmenter à mesure que les méthodes des criminels évoluent.

En répondant aux questions posées dans cet article et en vous armant d'un plan doté de ressources adéquates, vous accélérerez votre temps de réponse en cas d'urgence, tout en réduisant l'incertitude et en éliminant les doublons.