IRON MOUNTAIN®

TROIS FAÇONS DE RÉAGIR FACE À UN PIRATAGE INFORMATIQUE

Lorsque des infrastructures critiques sont attaquées, aucune donnée de l'entreprise n'est à l'abri. Découvrez comment votre entreprise peut se protéger contre les hackers, qu'ils sévissent dans votre pays ou à l'étranger.

Aucun secteur n'est à l'abri d'une cyberattaque. Rien qu'au cours de l'année écoulée, nous avons assisté à toutes sortes d'événements, que ce soit la mise hors service de gazoducs couvrant une grande partie des États-Unis ou des violations de données dans des hôpitaux du monde entier pendant la pandémie. Ce sont des faits réels et non pas de la fiction.

Les équipements informatiques qui géraient un gazoduc installé aux États-Unis ont été piratés le 29 avril 2021. Selon des experts en cybersécurité, le point d'entrée de cette attaque a été rendu possible à cause d'un « seul mot de passe compromis ». Même si c'est de cette manière que les pirates se sont introduits dans le système, la compagnie pétrolière avait laissé ses portes grandes ouvertes car elle n'avait pas déployé une authentification multifactorielle sur son compte VPN.

La véritable origine de ces attaques fait l'objet de débats nourris, mais qu'elles soient lancées depuis l'étranger ou depuis le pays ciblé, les entreprises doivent savoir comment protéger leurs actifs les plus sensibles, à savoir leur univers informationnel numérique.

Quelles leçons pouvons-nous tirer de ces incidents pour aider les entreprises à se protéger contre de futures attaques de piratage ?

LE SAVIEZ-VOUS ?

- Saviez-vous que vous pouvez contenir une violation en surveillant les différentes couches des défenses d'un réseau ?

CONSTAT :

- Le rapport d'enquête 2021 sur les violations de données publié par Verizon indique que 80 % de ces violations sont liées à des identifiants faiblement sécurisés ou bien réutilisés.

Y a-t-il vraiment une différence entre des pirates sévissant depuis l'étranger ou dans votre pays ?

En général, les pirates commandités par des États disposent de financements plus conséquents pour lancer des campagnes d'infiltration de systèmes informatiques vulnérables sur de longues durées. Dès lors, ces pirates prennent tout leur temps pour installer diverses « portes dérobées » destinées à étendre leur mainmise sur un réseau tout en échappant aux principales détections.

Malheureusement, la cybercriminalité par des acteurs étatiques est une forme de guerre numérique qui va perdurer. L'étude 2021 Nation States, Cyberconflict and the Web of Profit de HP indique que 75 % des experts estiment que la pandémie de COVID notamment a été l'occasion idéale pour que les adversaires de tel ou tel pays lancent des cyberattaques. Pire encore, plus de 40 % de ces incidents ont eu un impact à la fois physique et numérique sur le pays ciblé.

Motivations mises à part, les méthodes utilisées sont sensiblement les mêmes, que les acteurs opèrent dans le pays visé ou depuis l'étranger. La pratique qui consiste à armer des robots conversationnels (chatbots) à des fins d'hameçonnage commence à être utilisée. Lorsque des utilisateurs répondent à des messages, ils peuvent être influencés jusqu'à communiquer leurs informations de connexion.

Retenir les données d'une entreprise en otage n'a rien d'original. Mais le recours à des attaques par malware destructrices invite les entreprises à redoubler leurs efforts en matière de confinement et de protection.

Voici comment les entreprises peuvent réagir à des piratages informatiques :

RALENTIR LES PIRATES

Se contenter de maintenir des firewalls endurcis ne suffit plus pour protéger le périmètre d'une entreprise. Quiconque travaille dans la sécurité informatique sait qu'un firewall n'est plus adapté. Et si elle contribue largement à dissuader les utilisateurs de répondre à des emails suspects, la sensibilisation des employés n'est pas la parade à toutes les violations.

Prenez le temps d'organiser une formation robuste qui permettra à tous vos employés de prendre les précautions qui s'imposent en matière de cybersécurité. En procédant de la sorte, votre entreprise pourra éviter la plupart des écueils tels que cliquer sur un lien provenant d'un expéditeur inconnu ou bien partager des informations avec une personne ne disposant pas d'identifiants corrects. Si ces sessions de sensibilisation sont bien menées, elles permettront à vos employés d'être plus réactifs vis-à-vis de leur environnement numérique et donc de ralentir de potentiels acteurs malveillants.

CONFINEMENT DES ÉLÉVATIONS DE PRIVILÈGES

BeyondTrust, une entreprise de solutions de gestion des accès à privilèges (PAM) définit l'élévation de privilèges comme « une attaque visant à obtenir un accès illicite à des droits élevés, alias privilèges, au-delà de ce qui est nécessaire ou attribué à un utilisateur », que ce soit la prise de contrôle d'un compte, l'exploitation d'erreurs logicielles ou l'obtention de privilèges administratifs.

Si elles ne sont pas rapidement contenues, ces élévations de privilèges peuvent vite se transformer en véritables attaques par malware de type Wiper (essuie-glace) qui permettront aux pirates d'accéder à vos données afin de les supprimer ou de les écraser complètement.

C'est le genre de scénario qui s'est récemment déroulé un peu partout à travers le monde, que ce soit lors de l'attaque du système ferroviaire de l'Iran avec le malware Meteor Wiper ou de la tentative d'attaque de type Wiper avant les Jeux Olympiques de Tokyo au Japon.

Dans la plupart des cas, la surface d'attaque numérique est globale selon Chuck Everette, responsable de la promotion de la cybersécurité chez Deep Instinct. Attendre ne serait-ce que 60 secondes est trop long lorsqu'un cybercriminel est parvenu à obtenir un accès privilégié à votre système.

Étant donné la portée désormais mondiale des attaques contemporaines, prendre des mesures de confinement des élévations de privilèges s'avère crucial. C. Everett recommande donc que « l'entreprise sache où se trouvent ses données et ses actifs, qu'elle mette en œuvre les bonnes pratiques d'hygiène de la sécurité et qu'elle investisse dans des produits de pointe de supervision et de prévention de la cybersécurité » pour bénéficier d'une protection efficace.

SYNCHRONISER LE CONFINEMENT AVEC LA PROTECTION DES DONNÉES ET LA REPRISE APRÈS UN SINISTRE

Pour contrer des cyberattaques, il est indispensable de disposer de ressources de protection et de reprise des données.

Pour ce faire, des sauvegardes de données fréquentes et automatiques ainsi que des processus rapides de récupération du système permettront de restaurer vos données ainsi que les applications associées et le système d'exploitation sous-jacent. Envisagez aussi de stocker une copie inaltérable de vos données hors site et hors ligne, une copie qui ne pourra pas être piratée ni modifiée et qui vous permettra de récupérer des données propres et non infectées.

Qu'il s'agisse de sécurisation physique ou de chiffrement des sauvegardes stockées, plus particulièrement lors de leur transport sur le réseau ou en cas de sauvegarde à distance ou dans le Cloud, un plan de protection et de récupération des données est vital pour toutes les entreprises.

Qu'elles soient lancées depuis votre pays ou l'étranger, les attaques informatiques restent imprévisibles. Saurez-vous réagir si un pirate de données jette son dévolu sur votre entreprise ?