Ransomware : comment protéger les institutions publiques ?

La médiatisation de ces cyberattaques et de leurs conséquences joue un rôle de sensibilisation pour la sécurité des données, non seulement auprès de la population, mais aussi et surtout auprès des institutions publiques visées. Une récente étude a révélé que certains acteurs n'ont pas signalé ce type d'incidents, malgré l'obligation légale de le faire. Le nombre réel d'attaques est donc certainement plus élevé que ce que l'on pense.

Il est grand temps d'agir. Mais nombreux sont ceux qui peinent à instaurer des mesures de protection efficaces et qui n'anticipent pas leur défense. La raison : ils disposent de trop peu d'informations sur les méthodes des hackers et n'ont pas la stratégie adéquate pour réagir.

Une étude récemment menée a également révélé que si 65 % des sondés français estiment disposer d'un plan clair et pouvoir ainsi se remettre rapidement d'une attaque de ransomware, près d'un tiers (32 %) ne testent pas leur plan de reprise. Et parmi les bons élèves, près de la moitié (43%) ne le testent qu'une fois par an voire moins.

La meilleure protection reste pourtant la prévention. Il faut prendre les mesures appropriées pour contrer l'attaque avant même qu'elle n'infecte le système. Les services du gouvernement qui traitent des informations sensibles devraient, par exemple, disposer de puissants pare-feu et solutions anti-spams pour limiter leur exposition aux adresses IP malveillantes.

Il est également possible d'aller plus loin, notamment en tenant les systèmes d'exploitation à jour et en instaurant des processus standardisés réunissant les correctifs, les mises à jour et les différents antivirus. Cependant, il ne suffit pas de déployer ces mesures. Il faut ensuite les tester et les optimiser en permanence pour assurer une protection continue des données.

Sensibiliser les employés à la cybersécurité

Les attaques de phishing qui tentent de voler les données personnelles d'un destinataire d'email sont particulièrement préoccupantes. Malheureusement, ces dernières sont également en augmentation, alors que les emails des employés deviennent de plus en plus vulnérables. En cas d'attaque, l'ouverture d'une pièce jointe dans un email supposé « légitime » peut en effet activer la propagation du virus à l'ensemble du système.

Pour limiter ce type d'incidents, il est essentiel d'éduquer le principal public concerné : les employés. Ils doivent donc être sensibilisés à la manière de protéger leur ordinateur d'une éventuelle attaque et à celle d'identifier un email suspect. Les méthodes des hackers ne cessent d'évoluer pour contrer les systèmes de sécurité. Il est donc primordial de tenir le personnel informé et de le former régulièrement.

Déployer des solutions de sécurité

Il existe une multitude de solutions de sécurité sur le marché qui couvrent aussi bien la détection de virus, la génération de mots de passe sécurisés ou le contrôle des points d'entrée et de sortie du cloud. Le choix de la solution la plus appropriée dépend des besoins de chaque entreprise.

Toutefois, il est important d'établir d'abord une stratégie de sécurité globale, sur la base de laquelle elles seront ensuite sélectionnées. L'entreprise doit veiller à ce qu'il n'y ait pas de patchwork mais un système global qui ne laisse aucune place aux lacunes.

Limiter les dommages et les temps d'interruption

Même les meilleurs plans peuvent échouer. Par conséquent, si toutes les mesures préventives et les systèmes de sécurité viennent à dysfonctionner, il faut veiller à ce que les données soient aussi sécurisées que possible et puissent être restaurées de manière fiable. Ceci est le seul moyen d'assurer des dommages et des temps d'arrêt minimes en cas d'attaque – un aspect particulièrement important compte tenu de la sensibilité des informations détenues par les institutions publiques.

Assurer l'efficacité du plan de reprise 25 % des professionnels sondés estiment que la récupération des données pourrait prendre des jours voire des semaines, ce qui illustre la nécessité absolue d'un plan de reprise efficace. Ceux-ci doivent intégrer des logiciels de sauvegarde et de reprise après sinistre reconnus.

Même si des images de sauvegarde locales peuvent être suffisantes pour protéger les données, il est recommandé d'aller plus loin et de les répliquer hors site, dans un cloud public ou privé, pour éviter que les ransomwares ne les cryptent. Cela permet de garantir que les fichiers sont toujours sécurisés et faciles à récupérer.

Payer n'est pas une solution

Lors d'une attaque de ransomware, il est important de rester calme et de ne pas payer. Le versement d'une rançon encourage les hackers à continuer et leur confirme à quel point la cible est vulnérable, pouvant alors provoquer de nouvelles attaques.

Les administrations, autorités et institutions publiques doivent être conscientes de la menace que représente la cybercriminalité. Ils doivent ainsi faire tout leur possible pour protéger leurs systèmes et leurs données et, en cas d'attaque réussie, veiller à ce que le public soit informé de manière ciblée et contrôlée. Il est également essentiel d'empêcher les hackers d'utiliser ces attaques pour ébranler la confiance dans les systèmes et les structures sociales existants.

Ainsi, plus les institutions publiques adopteront rapidement une telle approche de restauration et de reprise, plus elles seront à même d’assurer la continuité de leurs activités en 2020 et au-delà.