Lire cet article en ligne

Attaques par rançongiciels : les bonnes pratiques pour s'en prémunir et y faire face

Depuis plusieurs mois, les cyber-attaques par rançongiciels ne cessent de se multiplier. De récents exemples médiatiques montrent que toutes les organisations peuvent être touchées, privées ou publiques, et quelle que soit leur taille.

Dans ce cadre, cet article vous propose un rappel des bonnes pratiques à mettre en œuvre afin de limiter les risques et savoir réagir efficacement en cas d'attaque.

Avant tout, qu'est-ce qu'un rançongiciel (ou *ransomware* en anglais) ?

L'ANSSI (Agence nationale de sécurité des systèmes d'information) en fournit la définition suivante :

> « *Technique d'attaque courante de la cybercriminalité, le rançongiciel ou ransomware consiste en l'envoi à la victime d'un logiciel malveillant qui chiffre l'ensemble de ses données et lui demande une rançon en échange du mot de passe de déchiffrement* »***[1]***.

Ces derniers mois, les victimes de ces rançongiciels ont été nombreuses : parmi les plus emblématiques, on compte En France les entreprises *Sopra Steria, Bouygues Construction* ou plus récemment l'oléoduc américain *Colonial Pipeline*.

Les conséquences pour les entreprises peuvent être désastreuses : outre les potentielles pertes de données ou le paiement d'une rançon, les victimes doivent faire face à la désorganisation voire l'arrêt de leur activité et à une chute subséquente de leur chiffre d'affaires. Ceci sans compter le risque sérieux de dégradation de la réputation et les impacts négatifs sur les relations avec les clients et les partenaires.

Dans ce cadre, comment les organisations peuvent-elles se prémunir contre ces rançongiciels ? Et que faire si une attaque survient malgré tout ?

En août 2020, l'ANSSI, en partenariat avec la DACG (Direction des Affaires Criminelles et des Grâces), a publié un guide présentant un certain nombre de recommandations visant à limiter les risques et réagir de façon adéquate en cas d'attaque par rançongiciels[2].

Au regard de la recrudescence récente de ces attaques, voici un rappel succinct des conseils de l'ANSSI.

Mesures pour réduire le risque d'attaque

Intervenir en amont de toute attaque peut être une stratégie payante, qui peut permettre d'éviter les attaques ou, à tout le moins, de réduire les pertes. Ceci implique de mettre en place au sein de l'organisation les principes de cybersécurité ci-après listés[3].

- ***Sauvegarder les données***

Il est important d'organiser des sauvegardes régulières de l'ensemble des données de l'organisation.

Sachant que le rançongiciel peut également atteindre les sauvegardes, il est impératif de prévoir, au moins pour les données les plus critiques, des sauvegardes déconnectées du réseau informatique, par exemple grâce à des systèmes de stockage externes.

- ***Maintenir à jour les logiciels et les systèmes***

Pour limiter les vulnérabilités des systèmes d'information, il est essentiel d'installer rapidement et régulièrement les mises à jour des logiciels et systèmes utilisés qui contiennent des correctifs de sécurité.

- ***Utiliser et maintenir à jour les logiciels antivirus***

Les logiciels antivirus peuvent permettre d'éviter la compromission et le chiffrement des fichiers. Pour qu'ils restent efficaces, il est important de procéder à des mises à jour fréquentes.

- ***Cloisonner le système d'information***

Un rançongiciel a vocation à se propager sur l'ensemble du réseau informatique de l'organisation. Il est donc utile d'organiser un cloisonnement entre les différentes zones réseaux. Il est également possible de cloisonner et isoler les niveaux d'administration les plus hauts afin que ceux-ci soient difficilement atteignables par le rançongiciel.

- ***Limiter les droits des utilisateurs et les autorisations des applications***

Limiter les postes de travail disposant de droits d'administration est également une mesure importante à mettre en place. Il peut aussi être utile de prévoir certains postes d'administration sans accès à Internet.

- ***Maîtriser les accès à internet***

Les rançongiciels exploitant souvent les accès à Internet, la mise en œuvre d'une passerelle Internet sécurisée

permettant de bloquer les flux illégitimes est cruciale.

- ***Mettre en œuvre une supervision des journaux***

Il est important, afin d'assurer un suivi de la sécurité informatique de l'organisation, d'assurer une supervision des incidents grâce à la mise en place d'une politique de journalisation des évènements. Cette supervision peut permettre de détecter une éventuelle compromission et gagner du temps dans la compréhension des incidents.

- ***Sensibiliser les collaborateurs***

L'attaque par rançongiciel intervient souvent à la suite d'une négligence de la part d'un membre de l'organisation victime, par exemple par l'ouverture d'une pièce jointe piégée. Il est donc important de former et sensibiliser les utilisateurs aux bonnes pratiques de sécurité numérique.

- ***Evaluer l'opportunité de souscrire à une assurance cyber***

Certaines compagnies d'assurance proposent désormais des contrats d'assurance cyber intégrant une couverture contre les attaques aux rançongiciels, comprenant assistance juridique et couverture financière des préjudices subis.

- ***Mettre en œuvre un plan de réponse aux cyberattaques***

Une attaque par rançongiciel peut déstabiliser considérablement le fonctionnement d'une organisation. Il est donc important de déterminer, en amont, un plan de réponse visant à assurer les modalités d'une continuité informatique en cas d'attaque.

- ***Penser sa stratégie de communication de crise cyber***

Les conséquences sur l'image et la réputation de l'organisation visée par une attaque par rançongiciel ne sont pas à négliger. Pour limiter ces impacts négatifs, il est important de préparer en amont une stratégie de communication de crise adaptée et efficace.

Mesures pour réagir en cas d'attaque

Les mesures préventives ne permettent pas toujours d'éviter les attaques. En cas d'occurrence, il est important de savoir comment réagir rapidement et efficacement pour limiter l'impact du rançongiciel.

- ***Adopter les bons réflexes***

En cas d'attaque, plusieurs actions doivent être immédiatement mises en œuvre dont notamment :

-Ouvrir une main courante pour tracer les actions et évènements liés à l'incident ;

-Isoler les équipements infectés en les déconnectant du réseau ; –

-Déconnecter les supports de sauvegarde non infectés ;

-Procéder à la mise en veille prolongée des machines dont les fichiers ont été chiffrés (une extinction électrique complète pouvant compromettre la récupération ultérieure de fichiers) et laisser éteint les équipements non démarrés.

- ***Piloter la gestion de la crise cyber***

Il est conseillé de réunir une cellule de crise au plus haut niveau de l'organisation pour coordonner la réponse à l'attaque et prendre les décisions stratégiques requises au niveau opérationnel, mais également en termes de communication interne et externe.

- ***Trouver de l'assistance technique***

En cas d'attaque, une assistance technique est indispensable. Si l'organisation ne dispose pas de ressources internes à cet effet, il est impératif de faire appel à des prestataires externes spécialisés dans la réponse à ce type d'incident de sécurité.

- ***Communiquer au juste niveau***

Pour déterminer les actions de communication à mener, il convient de mettre en œuvre un état des lieux technique, médiatique et social de l'attaque. Un accompagnement des collaborateurs pourra également être organisé par une communication interne adaptée.

- ***Ne pas payer la rançon***

Il est déconseillé de payer la rançon, puisque cela ne garantit en rien que les cybercriminels permettront le déchiffrement des systèmes. Au demeurant, les rançons financent les organisations cybercriminelles et les encouragent à multiplier ce type d'attaques.

- ***Déposer plainte***

Un dépôt de plainte auprès des services de police ou de gendarmerie est indispensable. Le dépôt de plainte permettra de réaliser une enquête qui pourra éventuellement fournir des éléments pour permettre de déchiffrer les données altérées. Outre qu'elle peut permettre l'identification et la condamnation des cybercriminels responsables, Il s'agit d'un préalable nécessaire à la réparation du sinistre subi par l'organisation.

- ***Restaurer les systèmes depuis des sources saines***

Les équipements infectés doivent faire l'objet d'une réinstallation du système et d'une restauration de données depuis les sauvegardes effectuées de préférence avant la compromission du système. Il est impératif de vérifier que les données restaurées ne sont pas infectées par le rançongiciel.

Pour obtenir un détail plus approfondi des recommandations de l'ANSSI et de la DACG, nous vous invitons à consulter leur guide « *Attaques par rançongiciels, tous concernés – Comment les anticiper et réagir en cas d'incident »,* disponible sur le site de l'ANSSI[4].

---

[1] https://www.ssi.gouv.fr/entreprise/principales-menaces/cybercriminalite/rancongiciel/

[2] https://www.ssi.gouv.fr/guide/attaques-par-rancongiciels-tous-concernes-comment-les-anticiper-et-reagir-en-cas-dincident/

[3] Ces règles sont issues du *Guide de l'hygiène informatique de l'ANSSI* disponible au lien suivant : https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/

[4] https://www.ssi.gouv.fr/guide/attaques-par-rancongiciels-tous-concernes-comment-les-anticiper-et-reagir-en-cas-dincident/