Ransomwares : Faut-il payer ou pas ?

Les ransomwares, ou logiciels de rançon, sont des programmes malveillants qui chiffrent les données d'un utilisateur ou d'une organisation, rendant l'accès à ces données impossible sans une clé de décryptage fournie par l'attaquant. Pour débloquer leurs fichiers, les victimes se voient souvent demander de payer une rançon, généralement en cryptomonnaie pour masquer l'identité de l'auteur.

Les ransomwares peuvent se propager par différents moyens, tels que des e-mails de phishing, des téléchargements de logiciels infectés ou des vulnérabilités dans des systèmes non mis à jour. Une fois infiltrés, ils peuvent causer des dommages considérables, tant financiers que réputationnels, aux victimes.

En France, le nombre d'attaques par ransomware a considérablement augmenté ces dernières années. Selon le rapport de l'ANSSI (Agence nationale de la sécurité des systèmes d'information), les entreprises, mais aussi les collectivités et même les particuliers, sont de plus en plus ciblés.

- France : En 2022, l'ANSSI a enregistré une augmentation de 20 % des signalements d'incidents liés aux ransomwares par rapport à l'année précédente. Des secteurs critiques comme la santé, l'éducation et les services publics sont particulièrement vulnérables.
- Union Européenne : À l'échelle de l'UE, des études estiment que près de 1 entreprise sur 5 a été victime d'une attaque par ransomware. Les pertes financières résultant de ces attaques peuvent atteindre plusieurs millions d'euros, sans compter les coûts indirects liés à la perte de productivité et à la récupération des données.

Les auteurs de ransomwares sont souvent des groupes organisés, opérant au sein de réseaux criminels structurés. Ils peuvent être basés dans différentes régions du monde, notamment en Russie, en Asie et en Europe de l'Est.

Voici quelques caractéristiques des criminels derrière ces attaques :

- Formation et expertise : Beaucoup d'attaquants possèdent des compétences techniques avancées, leur permettant de développer des logiciels sophistiqués et de contourner les systèmes de sécurité.
- Motivations financières : L'objectif principal est généralement financier. Les rançons demandées peuvent varier de quelques centaines à plusieurs millions d'euros.
- Systèmes de partenariat : Certains groupes proposent même des « services de ransomware » à d'autres criminels, permettant ainsi à des individus moins expérimentés de mener des attaques.

Face à l'augmentation des ransomwares, la question de payer ou non la rançon est complexe. Payer ne garantit pas toujours le décryptage des données et peut encourager les criminels à poursuivre leurs activités. Les entreprises doivent donc renforcer leur cybersécurité et envisager des stratégies de réponse aux incidents pour minimiser les risques.

Du point de vue des assurances, quel est leur point de vue à ce sujet ? Proposent-elles toujours des possibilités de rembourser ?

En France, la question de l'indemnisation des rançons dans le cadre des attaques par Ransomware est complexe et a récemment été clarifiée par des évolutions législatives. Depuis l'adoption du projet de loi d'orientation et de programmation du ministère de l'Intérieur (LOPMI), l'indemnisation des rançons par les assureurs est conditionnée à un dépôt de plainte par la victime dans les 24 heures suivant l'attaque et avant tout paiement de la rançon. Cette mesure vise à dissuader le versement de rançons tout en garantissant un cadre légal pour les entreprises qui souhaitent être couvertes[1].

[1] https://www.howdengroup.com/fr-fr/rapport-assurance-cyber-2024-risque-resilience
https://formation.lefebvre-dalloz.fr/actualite/cyber-rancons-quelle-indemnisation-des-assurances

Les compagnies d'assurance comme AXA proposent des solutions spécifiques pour les cyber-risques, incluant la couverture des pertes d'exploitation et les frais de gestion de crise, mais elles appliquent des critères stricts pour l'indemnisation, notamment en fonction de la conformité des entreprises aux normes de cybersécurité comme le RGPD. Par ailleurs, des initiatives telles que la réduction des primes pour les entreprises mettant en place des mesures préventives (ex. : sauvegardes régulières, audits) encouragent les bonnes pratiques en cybersécurité[2].

Enfin, le débat autour du remboursement des rançons reste actif. Certains experts estiment que leur couverture pourrait alimenter les cybercriminels, tandis que d'autres affirment qu'elle est nécessaire pour aider les entreprises à se relever après une attaque. Le secteur évolue également grâce à l'intégration de nouvelles technologies (IA, analyses prédictives) pour limiter les risques et prévenir les incidents avant qu'ils ne surviennent[3] [4].

---

[2] https://www.axa.fr/pro/assurance-materiel-informatique/assurance-cyber-risques.html
https://www.servyr.com/dossier-special-cyber-assurance-en-2024-tendances-defis-et-opportunites/

[3] https://formation.lefebvre-dalloz.fr/actualite/cyber-rancons-quelle-indemnisation-des-assurances

[4] https://www.servyr.com/dossier-special-cyber-assurance-en-2024-tendances-defis-et-opportunites/