MARSH

Victime d'un ransomware ? Comment aller de l'avant ?

Les progrès technologiques s'accélèrent et transforment radicalement nos métiers. En parallèle, les expositions des entreprises au risque cyber continuent de croître, ce qui représente la possibilité de pertes économiques substantielles. Les dernières recherches et analyses de Marsh ont été présentées dans le rapport "Le nouveau visage des sinistres cyber" qui s'appuie sur des données sinistres de Marsh Continentale Europe, sur l'expérience et l'expertise de Wavestone et CMS, pour mettre en avant des solutions pratiques de gestion du risque cyber et **particulièrement des ransomwares**.

Grâce à une experience forte dans ce domaine, Marsh est en mesure de proposer de **bonnes pratiques pour aider les entreprises à mieux comprendre, mesurer et gérer** le risque de ransomware.

1. Comprendre : de quoi parlons-nous ?

Les attaques par ransomware visent à prendre en otage les données d'une entreprise (en les chiffrant ou en menaçant de les rendre publiques par exemple) - Ce type d'attaque est devenu très populaire dans le monde entier, y compris en Europe. En 2019, nous avons enregistré une hausse de 100% des demandes d'indemnisation dans le cadre d'attaque ransomware.

Les attaques sont de plus en plus **fréquentes**, aidées par de nouveaux types de logiciels malveillants, dont des ransomwares

La **gravité** opérationnelle et financière augmente nettement : les rançons, les coûts accessoires et les temps d'arrêt des activités sont en hausse de manière exponentielle

Le phishing , un sujet lié à la **COVID - 19 les emails** ciblent les travailleurs à distance.

Avec plus de personnes travaillant dans des environnements moins sécurisés, les attaques ont plus de succès.

Sur la base de l'ensemble des sinistres cyber analysés par Marsh, **67%** des attaques **sont malveillantes**

Le nombre de sinistres ransomware a **doublé** en 2019.

Durée d'interruption de l'activité
Une attaque cyber "simple" :
1 semaine pour une reprise totale de l'activité

Une attaque cyber "complexe" :
3-4 semaines avant la récupération de l'infrastructure de base
6 semaines avant la récupération des données

Source: The Changing Face of Cyber Claims, 2020

MARSH & McLENNAN COMPANIES

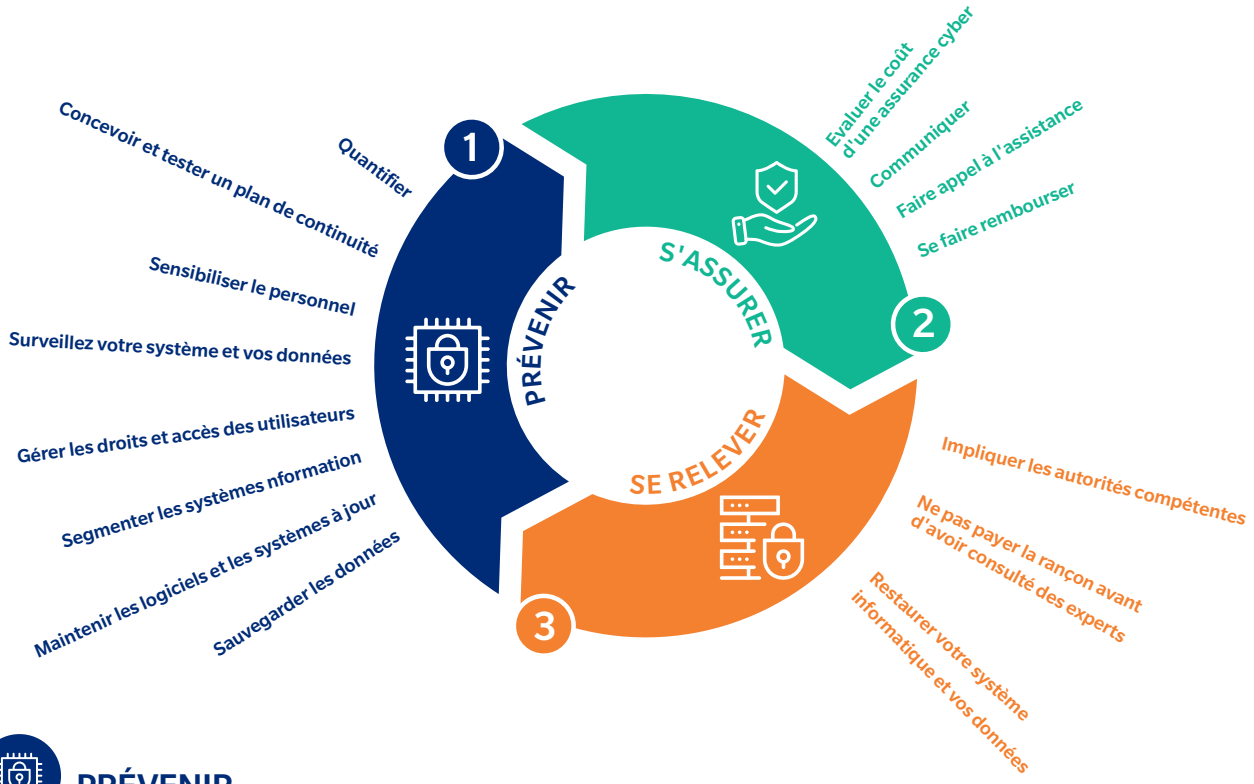
2. Mesurer : combien coûte une attaque ?

Il existe deux types de ransomware :

- **Ransomware non-ciblé.** Envoyé au hasard à des millions d'adresses électroniques, touchant principalement les PME et les particuliers. Le mécanisme est simple et le montant de la rançon est limité (environ 300 €, en bitcoin) mais le retour sur investissement pour les hackers est énorme, considérant le nombre de personnes qui payent la rançon. Dans ce cas, c'est le volume qui compte.
- **Ransomware ciblé.** Ces attaques beaucoup moins nombreuses sont préparées bien à l'avance par les hackers, généralement grâce à de l'ingénierie sociale. Les grandes entreprises sont prises pour cible (chiffre d'affaires > 500 M) et les hackers déclenchent l'attaque au pire moment possible pour l'entreprise. Les rançons peuvent alors atteindre plusieurs dizaines de millions d'euros.

3. Gérer, prévenir, assurer, se relever

Les conseils suivants peuvent vous aider à vous protéger contre ces réelles menaces



PRÉVENIR

1. **Sauvegarder les données :** l'objectif de la plupart des ransomwares est de vous empêcher d'accéder à vos données et de payer pour les récupérer. Il est essentiel pour votre entreprise d'effectuer des sauvegardes régulières et de les conserver en sécurité. Testez régulièrement la fiabilité de vos sauvegardes !
2. **Maintenir vos logiciels et vos systèmes à jour :** votre système d'information est vulnérable et ses points faibles sont utilisés par les hackers pour propager le virus et chiffrer vos données. En faisant les mises à jour, y compris celles de votre logiciel antivirus, vous êtes davantage protégé.
3. **Segmenter les systèmes d'informations :** certains composants de vos données et de vos systèmes d'information sont plus critiques ou sensibles que d'autres. Assurez-vous que ces éléments sont bien protégés afin que les hackers ne puissent pas y accéder facilement.
4. **Gérer les droits et accès des utilisateurs :** tous les salariés ou partenaires ne devraient pas accéder de la même façon à votre système. La bonne administration et un bon entretien des accès sont clés.
5. **Surveillez votre système et vos données :** afin que vous puissiez détecter le plus rapidement possible tout comportement anormal sur vos systèmes - ce qui signifie des temps de réaction plus rapides et une meilleure prévention des dommages.
6. **Sensibiliser le personnel :** faites de votre personnel votre meilleure arme contre les menaces ! Les ransomwares commencent souvent lorsqu'un membre de l'équipe ouvre une pièce jointe corrompue ou atterrit sur une page web malveillante.
7. **Concevoir et tester un plan de continuité d'activité :** les attaques sont déstabilisantes. La meilleure façon de faire face est encore de se préparer, notamment en mettant en place des plans et des procédures de gestion des incidents, et ainsi éviter l'échec.
8. **Quantifier :** la connaissance est clé, cherchez à savoir combien une attaque cyber pourrait vous coûter. Cette démarche vous aidera à gérer le risque au niveau du conseil d'administration et à le transférer à des tiers tels que les assureurs.

S'ASSURER

pour vous aider à traverser la crise et à contribuer à votre redressement financier

1. **Évaluer le coût d'une assurance cyber :** l'assurance cyber peut vous apporter une assistance rapide pendant et après l'attaque et vous permettre de demander une indemnisation pour vos pertes financières.
2. **Communiquer :** après un incident affectant votre sécurité, les entreprises doivent regagner la confiance de leurs clients, salariés et partenaires. Des spécialistes aident à reconstruire une réputation solide.
3. **Faire appel à l'assistance :** de nombreuses entreprises ne disposent pas des ressources internes ou de l'expertise nécessaires pour gérer un incident de sécurité. Des prestataires de services spécialisés vous aident à minimiser les dégâts et à reprendre vos activités le plus rapidement possible. L'analyse Forensics d'événements de grande ampleur peut vous aider à comprendre la cause profonde du succès de l'attaque, à prendre les mesures appropriées pour vous rétablir - et aussi à être plus robuste à l'avenir.
4. **Se faire rembourser :** l'assurance cyber permet d'atténuer les pertes financières d'une entreprise. Elle peut les aider à éviter un avertissement sur résultat - voire la faillite - à la suite d'attaques cyber sévères.

SE RÉTABLIR

améliorez-vous !

1. **Impliquer les autorités compétentes :** elles peuvent vous aider à enquêter et à vous remettre d'un incident. La plupart de nos clients se trouvant dans cette situation ont en effet décidé de porter plainte.
2. **Ne pas payer la rançon avant d'avoir consulté des experts :** il n'y a aucune garantie que les criminels vous remettent la clé de déchiffrement lorsque vous payez - ce sont des escrocs après tout ! De plus, si votre organisation est perçue comme étant prête à payer, cela encouragera probablement d'autres attaques, qu'elles soient du même groupe ou d'autres, et elles seront encore plus sophistiquées.
3. **Restaurer votre système informatique et vos données :** il est préférable de restaurer votre système et vos données à partir de sources fiables et de mettre à jour vos mots de passe. Il est essentiel de vérifier que les données que vous restaurez sont intactes. Tenez-vous informé afin d'être dans la meilleure situation possible : vous pouvez obtenir notre avis sur les sinistres que nous avons traités cette année en consultant notre rapport **"Le nouveau visage des sinistres cyber"**, qui rassemble des données provenant de toute l'Europe continentale.

A PROPOS DE MARSH

Marsh est leader mondial du courtage d'assurance et du conseil en risque. Avec plus de 35 000 employés dans plus de 130 pays, Marsh propose à ses clients entreprises et individuels des solutions de gestion des risques et de conseil basés sur des données.

Marsh est une filiale du groupe Marsh & McLennan Companies (NYSE : MMC), une société internationale de services professionnels qui fournit à ses clients des conseils et des solutions en matière de risques, de stratégie et de capital humain. Avec 76 000 collaborateurs dans le monde et un chiffre d'affaires annuel de 17 milliards de dollars, MMC aide ses clients à naviguer dans un environnement de plus en plus dynamique et complexe grâce à 4 entreprises leaders sur le marché : Marsh, Guy Carpenter, Mercer, et Oliver Wyman.

Suivez Marsh sur Twitter @MarshGlobal; LinkedIn; Facebook; et YouTube, ou abonnez-vous à BRINK.

Pour plus d'information sur l'assurance cyber et nos autres solutions Marsh, visitez notre site internet marsh.fr ou contacter votre chargé de clientèle.

LARI LEHTONEN
Responsable de l'activité cyber
+33 (0)1 55 46 37 45
lari.lehtonen@marsh.com

NHAT TRUONG
Practice leader, cyber risk consulting
+33 (0)1 41 34 19 48
nhat.truong@marsh.com