La cyber-assurance, un marché d’avenir ?

Pour faire de la cyber-assurance le prochain pilier majeur de l'industrie, la technologie doit permettre de sécuriser les données, détecter failles et mesurer le risque. Florian Graillot fait le point.

Le marché de la cyber-sécurité devrait passer à 232 milliards de dollars en 2022, contre 138 milliards de dollars en 2017, selon MarketsandMarkets. Notamment à cause des menaces qui augmentent en permanence: 1 091 violations de données en 2016 (+40% sur un an) et 1 579 en 2017 (+45% sur un an) selon l’Identity Theft Resource Center. Ces chiffres devraient continuer à augmenter, car le nombre d’internautes va passer à 6 milliards d’ici 2022, contre 3,8 milliards en 2017, selon Cyber Security Ventures. En considérant qu’il est impossible d’éviter complètement les cyber-menaces, nous nous intéressons à 3 secteurs principaux de la cyber-assurance : la sécurisation des données, la surveillance des failles de sécurité, et l’évaluation des cyber-risques.

Sécuriser les données autant que possible

À la suite des milliers de failles qui se sont produites ces dernières années, plus de 700 millions de données ont été volées en 2016 et 2017 selon Wikipédia. Avec le développement du stockage dans le Cloud, plusieurs startups se sont positionnées sur un stockage sécurisé pour mieux protéger les données qu’elles hébergent. En France, *Lena Cloud* ou *SecureSafe* en Suisse fournissent ce type de service avec plusieurs niveaux de sécurité : du chiffrement, à la surveillance des fuites, ou la surveillance des menaces en continu. *Amazon*

Web Services offre aussi plusieurs options pour sécuriser le stockage, notamment le service « Macie » qui utilise le Machine Learning pour identifier les données sensibles et surveiller la façon d'y accéder afin d'identifier toute menace. Du côté infrastructure, *Seclab* a développé une technologie brevetée pour sécuriser les interconnexions réseau avec de nombreux cas d'usage dans l'IoT, la SmartCity ou les Voitures Autonomes.

Le chiffrement des données reste un sujet majeur lorsque l'on considère que des violations de données se produiront inévitablement. En Europe, de nombreuses startups se concentrent sur ce domaine. *BoxCryptor*, en Allemagne, ou *AxCrypt*, en Suède, ont développé des solutions pour chiffrer les fichiers directement où ils sont stockées. Le principal enjeu, cependant, est de gérer le chiffrement et la sécurité en continu car de nombreuses applications reposent sur le partage et les flux de données : téléconsultation, stockage dans le Cloud, collecte de données IoT, messagerie, API, etc. Au Royaume-Uni, *Psyphr* ou *Hush* en Espagne, proposent d'intégrer leurs solutions directement dans l'environnement client avec des outils dédiés à la surveillance des risques. En France, *Tanker* a développé un SdK de chiffrement complet approuvé par l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) pour sécuriser n'importe quelle application dans laquelle il est intégré.

Du point de vue de l'assurance, la protection des données est un point clé. Le premier exemple dans ce domaine est le partenariat entre Aon, Allianz, Cisco et Apple pour offrir une solution dédiée de cyber-sécurité / cyber-assurance. Les solutions matérielles Cisco et Apple ont été sélectionnées comme étant particulièrement sûres, donnant accès à des primes plus attractives.

Surveiller les failles de sécurité

Selon PwC France, 76% des PME françaises ont déjà fait face à une cyber-attaque. Il est donc clé d'être informé en cas d'intrusion ou vol de données. Au-delà des logiciels anti-virus qui identifient des signatures connues, la technologie doit aider à identifier les activités anormales sur les réseaux dans un environnement où les menaces sont en évolution permanente. Il est important d'avoir connaissance d'une faille de sécurité avant, pendant ou après qu'elle se soit produite, car c'est la première étape pour renforcer la cyber-protection. Cela sera encore plus important avec l'application de la RGPD (Règlement Général sur la Protection des Données) à partir du 25 mai 2018, car les entreprises gérant des données personnelles devront signaler toute violation au régulateur, au maximum 72h après qu'elle se soit produite.

Plusieurs startups répondent à ce besoin en alliant service et technologie. En France, *CyRating* propose d'évaluer le niveau de cyber-risque pour les organisations notamment en les comparant au marché. Au Royaume-Uni,

DynaRisk se concentre sur le B2C pour fournir aux clients un score de sécurité s'appuyant sur plus de 50 facteurs de risque. Chacune utilise ses propres algorithmes pour interpréter les données recueillies auprès de leurs clients (types de données, usage, infrastructure, …)

Pour aller plus loin, des startups utilisent la technologie pour surveiller en continu les menaces. En France, *AIsid*, et CyberSprint aux Pays-Bas ont développé des solutions de surveillance des menaces directement sur les infrastructures. C'est une façon à la fois d'anticiper le risque en identifiant les failles qui pourraient être corrigées, et de s'informer en cas d'attaque.

La recherche de fuites de données est une autre façon de repérer les failles, une fois qu'elles se sont produites. En France, *CybelAngel* s'appuie sur l'intelligence artificielle pour explorer le Web (et le Dark Web) et rechercher des données sensibles qui auraient été volées. *LeakWatch* offre une solution SaaS pour identifier facilement les données compromises et exposées en ligne.

Certains assureurs se positionnent déjà sur cette tendance : AXA a investi aux États-Unis, chez *Security Scorecard*, qui analyse en direct les vulnérabilités selon 10 facteurs de risque pour sécuriser l'écosystème qui entoure toute organisation, et dans *Contrast Security* qui permet d'intégrer la surveillance et la correction des cyber-menaces nativement dans les applications. Les grands acteurs technologiques lorgnent également sur ce marché en pleine croissance :Google a récemment annoncé « Chronicle », une filiale dédiée à la cyber-sécurité pour aider les entreprises à surveiller les menaces en ligne.

Évaluer le risque

Selon Juniper Research, le coût des violations de données s'élèvera à 8 milliards de dollars entre 2017 et 2022, en raison des divers cyber-risques. L'année dernière, « WannaCry », un rançongiciel, a piraté plusieurs industriels, dont un constructeur automobile qui a dû cesser les activités de plusieurs de ses usines de production. Dans ce cas précis, le coût associé est assez facile à évaluer en estimant le nombre de voitures qui n'ont pas été produites en raison de cette interruption de production. Les grandes entreprises de technologie font face quant à elles, aux violations de données de leurs clients. Danc ces cas, il est plus difficile d'évaluer le coût d'une telle perte : les dommages sont-ils plus importants pour le client final ou pour la plateforme Web elle-même ? Les données volées sont-elles critiques pour les clients (nom, adresse, contact, détails de paiement…) ? Existe-t-il un impact pour la plateforme au-delà de la confiance et de la réputation ?

Du point de vue de l'assurance, il est essentiel d'évaluer le risque et de calculer le coût associé pour élaborer des polices de cyber-assurance pertinentes. Selon l'OCDE, le marché de la cyber-assurance représentait 3,5 milliards de dollars en termes de primes en 2016, avec un taux de croissance

de 30 % sur chacune des cinq années précédentes. Peu de startups se positionnent pour l'instant sur cette partie de la chaîne de valeur. En Suisse, *CyQuant* cible l'évaluation et la tarification des risques, en combinant technologie et compétences en modélisation des risques. Leur outil est destiné aux acteurs de l'assurance et de la réassurance qui auront de plus en plus besoin de la technologie pour les aider à évaluer le risque dans une industrie où les données historiques sont encore rares.

Au fur et à mesure que le marché de la cyber-assurance se développera, la technologie sera essentielle pour traiter d'énormes quantités de données en direct. C'est pourquoi de plus en plus de startups utilisent l'Intelligence Artificielle (et plus spécifiquement le Machine Learning) pour tirer parti des données comportementales. Au Royaume-Uni, *Darktrace* ou *Cybereason* et *Versive* aux États-Unis utilisent depuis longtemps ce type de technologie pour identifier les menaces inconnues.

Les cyber-menaces vont également augmenter avec l'essor de l'IoT : Juniper Research prévoit 46 milliards d'appareils connectés en 2022. Les objets connectés doivent d'ailleurs avoir à terme les mêmes capacités de mise à jour que les logiciels : chaque fois que les développeurs identifient des failles ou des menaces, ils les réparent et proposent aux utilisateurs de mettre à jour leurs logiciels. C'est un énorme défi pour les développeurs de l'IoT de pouvoir mettre à jour les logiciels intégrés dans les appareils connectés. Souvenons-nous des voitures connectés, piratées à distance il y a quelques années, obligeant les constructeurs à rappeler les véhicules pour procéder à une mise à jour de sécurité.

L'IDC (International Data Corporation) s'attend à ce que 265 trillions de gigaoctets de données soient créés mondialement en 2025 (contre 16 trillions de gigaoctets en 2017) dont 60% seront créés ou gérés par les entreprises. En Europe, le RGPD sera mis en application fin Mai et définira les bonnes pratiques pour les entreprises qui utilisent des données personnelles. Comme les entreprises doivent s'assurer que ces données ne sont pas compromises, la cyber-assurance va devenir un défi croissant et une exigence pour tous ces acteurs. Des startups offrent d'ailleurs aux entreprises un service pour mieux se conformer à la réglementation en s'appuyant sur la technologie. En Irlande, *ShhSystems* propose d'accompagner les entreprises dans le processus de mise en conformité et plus généralement de placer la sécurité au cœur de toute entreprise gérant des données. En France, *TwinPeek* se concentre sur la confidentialité des données à la fois pour les clients qui pourraient reprendre le contrôle de leurs données et pour les entreprises qui pourraient développer des fonctions natives de confidentialité dans leurs produits.