HISCOX ASSURANCES | Penser à tout, et surtout à vous

Communiqué de presse

5 tendances qui vont marquer la cybersécurité en 2022

Paris, le 8 février 2022 – **En ce début d'année, Hiscox, assureur spécialiste, expert du cyber-risque, identifie 5 tendances qui vont marquer l'année 2022.**

« *Comme en 2021, nous nous attendons à ce que de nouvelles failles cyber apparaissent en 2022. Le cyber-risque fait désormais partie du quotidien des entreprises et c'est pourquoi la vigilance doit être de mise. D'autant plus que des réflexes simples et la mise en place d'outils permettent de se prémunir efficacement d'un nombre important de cyberattaques* », **déclare Craig Dunn Responsable du Cyber, chez Hiscox Europe.**

1. Les ransomwares évoluent, mais la réglementation commence à devenir effective

Les risques liés au ransomware vont perdurer en 2022. Comme observé en 2021, les techniques de ransomware vont évoluer, avec l'apparition d'outils plus perfectionnés pour exfiltrer les données sensibles dans le cadre d'attaques dites de "double extorsion".

En réponse aux menaces croissantes auxquelles elles sont confrontées, les entreprises (sous l'impulsion des régulateurs, de conseils d'administration plus informés et des cyberassureurs) seront contraintes de mieux segmenter leurs réseaux, de sécuriser leurs sauvegardes et d'améliorer leur résilience.

Les régulateurs continueront à se concentrer sur les échanges de crypto-monnaies, afin de rendre plus difficile l'encaissement de gains illégaux. En 2022, une régulation significative pour lutter contre les ransomwares pourraient être mise en place. Par exemple, la divulgation obligatoire des attaques de ransomware ou la divulgation du paiement d'une rançon, ainsi qu'une réglementation des normes de cybersécurité.

2. Les vulnérabilités de la supply chain seront fortement exposées

En 2022, les attaques visant les vulnérabilités de la supply chain, notamment contre les fournisseurs de services gérés (MSP) utilisés comme porte d'entrée pour les ransomwares, vont se perpétuer. Elles permettent aux attaquants d'accéder plus facilement ou plus largement à une ou plusieurs victimes. Elles sont au moins de trois sortes :

- Attaque d'un fournisseur ou partenaire connu,
- Attaque ciblant un fournisseur "invisible" : fournisseur tiers ou bibliothèque open source utilisée par l'entreprise elle-même ou l'un de ses partenaires,
- Attaque ciblant une entreprise en tant qu'échelon de la chaîne d'approvisionnement d'une entité plus importante. Il est désormais courant de voir des petites entreprises (disposant de moins de moyens) prises pour cible comme point d'entrée pour atteindre de plus grandes structures, généralement mieux protégées.

Il est très probable que les cyber pirates se tournent vers l'exploitation des vulnérabilités des logiciels open-source. Notamment parce qu'ils sont largement utilisés et qu'ils ont été conçus à une époque où internet était moins exposé aux cyberattaques et que la sécurité n'était pas la préoccupation première des concepteurs. La récente découverte de la faille log4j, qui touche les application web Java et a provoqué la mise en arrêt par mesure de sécurité de plusieurs sites d'informations et de services, est un bon exemple de ce type de vulnérabilité critique.

3. Les enjeux sociaux et environnementaux impactent la sphère cyber

En 2021, de nombreux groupes d'activistes, tel qu'Extinction Rebellion, ont mené des actions sous la forme d'événements physiques : manifestations, occupation de lieux, blocages d'autoroutes... Les prochaines années pourraient marquer l'entrée de cet activisme dans la sphère numérique. Les membres les plus radicaux de ces mouvements pourraient lancer des cyberattaques contre des entreprises très polluantes. Dans le prolongement naturel de ce phénomène, des activistes privés de droits pourraient s'emparer de moyens virtuels pour protester contre la position d'une entreprise ou d'un gouvernement sur certains sujets.

Par ailleurs, outre l'activisme cyber auxquelles elles sont exposées, les entreprises concernées par des activités hautement polluantes auront de plus en plus de mal à souscrire à une cyber assurance. A titre d'exemple, de nombreux assureurs, dont **Hiscox**, se sont engagés à ne plus assurer les nouvelles entreprises impliquées dans l'extraction, le transport et la production d'électricité à partir du charbon. Il y a fort à parier que cette tendance se démocratisera dans les années à venir.

4. La menace des cyberguerres interétatiques se renforce

Si les tensions géopolitiques autour de l'Ukraine montrent que l'ombre de conflits armés pèse encore sur l'ordre mondial, l'utilisation de la cyberguerre ouverte pourrait être une des modalités des démonstrations de force étatiques. C'est pour cette raison que la Lloyd's a introduit une série de nouvelles mesures d'exclusion afin de fournir plus de clarté aux clients, courtiers et assureurs quant aux cyberattaques qui seront couvertes et celles qui ne le seront pas en cas de guerre. Bien que la formulation de ces exclusions puisse sembler intimidante à première vue, elles répondent de manière adéquate à la complexité des réseaux informatiques transnationaux et à la concurrence interétatique du XXI^{e} siècle. C'est pourquoi **Hiscox** a d'ores-et-déjà inclus l'une de ces exclusions dans ses contrats.

Si les tensions entre la Chine, l'Europe, la Russie et les États-Unis continuent de croître, il est possible que des actes de cyberguerre renforcent l'hostilité entre les nations. Cela pourrait conduire à davantage d'attaques à grande échelle contre les infrastructures nationales, mais aussi renforcer les risques d'escalade dans les relations conflictuelles entre Etats.

5. Les exigences en matière de cybersécurité continuent de croître

Dans un contexte de transformation numérique soutenue par la crise sanitaire actuelle, les normes en termes de cybersécurité ne cessent de s'accroître. Ainsi, l'utilisation de la double authentification pour se connecter à ses comptes d'entreprise et l'usage d'un VPN, qui étaient encore l'apanage des grandes firmes il y a quelques années, sont devenus la norme dans les entreprises. Même à titre personnel, les Français, encouragés par le recours au télétravail généralisé, sont de plus en plus nombreux à vouloir se protéger et protéger leurs données de toute fuite éventuelle.

A propos d'Hiscox en France

Hiscox, assureur spécialiste depuis 1901, est établi en France depuis 25 ans où il assure près de 100 000 particuliers et professionnels. Assureur historique de l'Art et des biens d'exception pour la clientèle privée, Hiscox a su ensuite développer son expertise dans le domaine des assurances professionnelles avec une gamme spécialisée couvrant aujourd'hui près de 500 métiers de services. Distribué via des courtiers spécialisés, des partenaires banquiers ou assureurs, Hiscox a été pionnier de l'assurance en ligne et via conseillers pour les entrepreneurs et indépendants. L'entreprise est aujourd'hui leader de l'assurance des métiers de l'informatique et du digital et a développé une offre cyber parmi les plus complètes du marché. C'est la connaissance et la compréhension des métiers de ses clients et de leurs risques, la mobilisation des meilleurs experts avant pendant et après les sinistres qui permettent à Hiscox de construire des couvertures adaptées à leurs besoins. Hiscox a l'ambition de changer l'expérience de l'assurance pour ses clients et l'objectif de protéger au mieux ce qui compte pour eux.

https://www.hiscox.fr

Contacts presse
Weber Shandwick : hiscox@werbershandwick.com
Pia Manière – 07 61 44 68 42
Benjamin GANDOUIN – 06 98 75 99 36