HISCOX

Alerte presse

Cybersécurité : les 5 tendances de 2023

Paris, février 2023 – Hiscox, assureur spécialiste de la protection cyber pour les petites et moyennes entreprises, dévoile 5 tendances de la cybersécurité qui marqueront 2023. Ces tendances fournissent des informations précieuses sur les menaces émergentes et nouvelles vulnérabilités permettant aux entreprises de mieux comprendre l'évolution des risques et de prendre les mesures préventives permettant de renforcer leur posture de sécurité.

« *Les conséquences de la guerre en Ukraine, les remous géopolitique et économiques qui en découlent, la montée de l'activisme cyber ont contribué à accroître encore la cybermenace pour l'année à venir. Face à cette situation, l'engagement des autorités et le déploiement de l'authentification sans mot de passe sont des motifs d'espoir, mais il demeure essentiel que les entreprises s'engagent activement face aux risques et menaces qui pèsent sur leurs systèmes informatiques et leurs données sensibles. C'est un processus continu qui nécessite une collaboration étroite entre acteurs – spécialistes de la sécurité, responsables des systèmes d'information, employés et utilisateurs, assureurs – afin de protéger les données, les infrastructures et la réputation des organisations* », déclare **Nicolas Kaddeche, Directeur Technique chez Hiscox France.**

1. Des menaces internes grandissantes au sein des entreprises

En 2022, les ménages et les entreprises du monde entier ont subi une inflation élevée, la hausse des coûts de l'énergie, des produits de grande consommation et des taux d'intérêts, la paralysie des chaines logistiques, une activité économique réduite... Ces difficultés vont se poursuivre voire se renforcer en 2023 et font craindre une hausse des attaques internes au sein des entreprises nourrie par les motivations suivantes :

- **Une motivation financière :** Lorsque les salariés peinent à payer leurs factures, ils sont davantage enclins à prendre des risques pour obtenir une compensation financière. Cela peut prendre la forme d'une corruption de salariés par des organisations criminelles, au moyen de pots-de-vin en échange de biens de propriété intellectuelle, d'un accès à distance, d'identifiants etc. Nous nous attendons également à une hausse des fraudes financières, car les salariés voient de plus en plus de raisons de commettre ces infractions à motivation financière.
- **Le mécontentement des salariés :** Face au ralentissement du marché de l'emploi et au fait que les augmentations de salaires ne couvrent pas l'inflation, certains salariés en colère pourraient décider d'exfiltrer les données d'une entreprise ou, dans des cas plus extrêmes, de les supprimer. La baisse de moral entrainera probablement aussi davantage d'incidents dus à la négligence.

2. Augmentation des attaques sur fond d'activisme

La guerre Ukraine-Russie se déroule aussi sur le front cyber. Si la Russie, considérée avant-guerre comme une cyber-puissance, n'a pas totalement atteint ses ambitions en la matière, l'Ukraine a pour sa part rassemblé une armée d'activistes forte de 210 000 membres, baptisée « l'Armée informatique d'Ukraine ». Même si la cause de l'Armée informatique est légitime, elle constitue un mauvais précédent pour les futurs activistes : une fois la guerre terminée, sur quoi cette armée jettera-t-elle son dévolu ?

Pour les autres formes d'activisme cyber, la question des limites morales se pose également. En 2022, par exemple, les actions pour le climat sont devenues plus fréquentes et plus spectaculaires, à l'image des aspersions de peinture sur les œuvres d'art ou des sit-in sur les routes. En 2023, ces tensions devraient s'accentuer, avec une possibilité accrue de recours aux cyber-attaques par les activistes.

3. Fracture et spécialisation des gangs de ransomware

La pression exercée par les autorités gouvernementales sur les groupes de ransomware a contribué à faire baisser les attaques de ce type dans certaines parties du monde en 2022, après un bond en 2021 : lorsque des

attaques par ransomware se sont produites, les entreprises ont refusé de payer, ou ont été empêchées de verser des rançons.

Pour continuer échapper aux autorités et continuer à perpétrer leurs actions, de nombreux groupes ont été contraint de recourir à l'anonymat. On a assisté en 2022 à une fracturation de groupes de ransomware notoire, sur le point d'être neutralisés, en petits groupes spécialisés, évoluant sous différents pseudonymes et s'attaquant à de nouvelles cibles. Cette tendance devrait se poursuivre car les gangs gagnent en stabilité à réaliser de petites actions clandestines ciblant des secteurs ou zones géographiques spécifiques. Les demandes de rançon élevées qui font la une des journaux et attirent l'attention des autorités ont également diminué l'année dernière, ce qui semble corroborer cette évolution. Pour 2023, Hiscox anticipe la poursuite de la baisse des demandes de rançon et des attaques moins fréquentes, les gangs fracturés disposant de moins de ressources et cherchant à naviguer sous les radars.

4. Déploiement accéléré de l'authentification sans mot de passe

Face à l'insuffisance des protections par mot de passe, l'adoption de l'authentification à plusieurs facteurs (MFA) a beaucoup progressé ces dernières années, devenant une exigence fondamentale pour la protection des services à distance et des comptes en ligne. Mi-2022, Apple, Microsoft et Google se sont engagés à soutenir davantage les normes promues par l'alliance FIDO (Fast ID Online), afin d'accélérer la mise en place des connexions sans mot de passe.

Cette connexion sans mot de passe représente le futur de l'authentification. Son adoption par les trois géants de la tech favorisera son déploiement car beaucoup d'entreprises ont recours à leurs technologies. Les dispositifs reposant sur la biométrie (reconnaissance faciale, empreintes digitales, etc.), intégrés dans tous les appareils conçus par ces sociétés, sont beaucoup plus difficiles à pirater et nécessitent un accès physique à l'appareil. Hiscox anticipe une adoption accélérée de l'authentification sans mot de passe en 2023 en raison de sa simplicité d'utilisation et des garanties de sécurité qu'elle offre.

5. Les câbles sectionnés, un risque accru pour l'infrastructure Internet

La cybersécurité est souvent cantonnée au numérique, mais les infrastructures physiques nécessaires au fonctionnement de l'Internet mondial peuvent également être la cible d'attaques. Récemment, le câblage de fibre optique entre les pays a montré des signes de fragilité alarmants. Ces câbles sous-marins constituent la faiblesse des communications Internet dans le monde et toute rupture pourrait être extrêmement préjudiciable à notre vie quotidienne et au fonctionnement des entreprises.

En 2022, ces câbles ont déjà subi de nombreuses attaques. Tous les incidents se sont produits dans des circonstances suspectes et leurs responsables n'ont pas été identifiés. Des attaques de ce type vont vraisemblablement se produire à nouveau car les câbles constituent des cibles faciles et de grande valeur. On ignore à ce jour si ces actes sont le fait d'États hostiles visant la connectivité Internet des pays ou d'activistes ciblant les infrastructures Internet.

Pour en savoir plus sur le risque cyber, son impact et sa prise en compte par les entreprises françaises et internationales, téléchargez le Rapport Hiscox 2022 sur la gestion des cyber-risques.


HISCOX

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

Contact presse :
Weber Shandwick : hiscox@webershandwick.com
Romain MERLE - 06 60 35 18 43