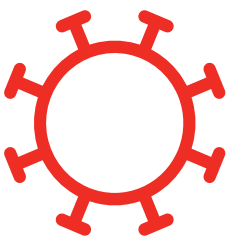
HISCOX
CYBERCLEAR®

Top 5 des menaces 2024

Alors que 2022 avait connu une accalmie sur le front des ransomwares, dans un contexte géopolitique agité, 2023 a subi une résurgence marquée du phénomène, couplé à une augmentation des occurrences de vol de données et de l'extorsion. Les conditions économiques difficiles et l'augmentation du coût de la vie ont également renforcé les inquiétudes concernant la criminalité financière, première motivation des cyberattaques selon le *Rapport Hiscox 2023 sur la gestion des cyber-risques*, tandis qu'avec la croissance de modèles tels que ChatGPT, facilitant la rédaction d'emails de phishing convaincants, les employés se sont plus que jamais retrouvés en première ligne. Quels risques les entreprises doivent elles avoir en tête pour 2024?

1 Les ransomwares d'exfiltration en augmentation

Au lieu de crypter les fichiers des victimes, certains cybercriminels optent pour la menace de communication de données et exigent des rançons en échange de la non-divulgation de celles-ci. Selon le rapport Hiscox 2023 sur la gestion des cyber-risques, 46 % des entreprises de plus de 250 employés ont payé une rançon afin de protéger les données de leurs clients, et 42 % des entreprises de moins de 250 employés ont déclaré qu'ils avaient versé une rançon dans le but de protéger leurs données confidentielles. Un nombre moins important d'entreprises ont payé pour redevenir opérationnelles. Moins de la moitié des entreprises ayant payé une rançon (46 %) ont récupéré toutes leurs données.

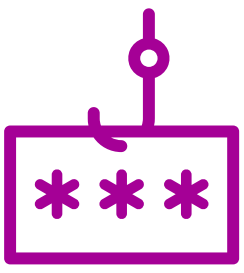


2 Les fraudes au virement (Payment Diversion Fraud), un défi croissant

Selon les données du rapport Hiscox, une entreprise sur trois a été victime d'une fraude au virement. Ce type de fraude arrive désormais en tête des conséquences d'une cyberattaque. Il consiste en des tactiques de manipulation ou de tromperie pour inciter les employés à rediriger des paiements légitimes vers des comptes frauduleux. La formation des employés aux comportements à adopter et réflexes à avoir en matière d'attaques d'ingénierie sociale telles que le phishing par mail ou par SMS (smishing) est une étape essentielle pour garantir la cybersécurité.

3 Les malwares gagnent en sophistication pour échapper à la détection

Depuis l'adoption généralisée des technologies EDR basées sur le comportement, on observe un déclin de l'efficacité des malwares traditionnels (logiciels malveillants, virus). Pour autant, une évolution se dessine : les malwares adoptent désormais des tactiques qui ne déclenchent pas d'alertes, comme l'utilisation de logiciels commerciaux à des fins malveillantes (par exemple, les logiciels d'accès à distance et de transfert de fichiers). Cette tendance des malwares devrait se poursuivre et donner naissance à des formes de malwares encore plus sophistiqués et insaisissables.



4 L'essor de l'IA : une épée à double-tranchant

Les grands modèles de langage (LLM) accélèrent la courbe d'apprentissage des acteurs malveillants, en les aidant à créer des malwares sophistiqués et personnalisés, à utiliser des outils de piratage et à composer des e-mails d'hameçonnage cohérents et convaincants. Des outils tels que WormGTP, spécialement conçus pour les activités des « black hats », les hackeurs malintentionnés, soulignent leur impact. Cependant, tout n'est pas noir : si l'IA offre des possibilités aux hackeurs, elle peut aussi jouer un rôle crucial dans le développement et le déploiement de logiciels de sécurité innovants et dans le renforcement des défenses existantes contre des menaces en évolution permanente. L'IA contribue à l'automatisation de la détection des menaces dans les systèmes de messagerie et les réseaux en analysant les activités et le comportement des utilisateurs pour y déceler des signes d'intention malveillante

5 « Hacktivisme » politique : un besoin d'encadrement face au risque de déstabilisation

Le Comité international de la Croix-Rouge (CICR) a publié le tout premier ensemble de règles d'engagement pour les hackeurs civils impliqués dans des conflits, mettant en garde contre une recrudescence des cyberattaques patriotiques, en particulier à la suite de l'invasion de l'Ukraine et maintenant du conflit entre Israël et le Hamas. Des groupes aux motivations idéologiques ont perturbé et perturberont divers secteurs, notamment les banques, les entreprises, les hôpitaux, les réseaux de chemins de fer et les services gouvernementaux de leurs opposants idéologiques et de leurs alliés. La menace que représentent ces groupes est un risque important ; étant donné que divers groupes de chaque côté des conflits se livrent à des cyberattaques, il est possible que cela se répercute sur des organisations non impliquées. Même si tous les « hacktivistes » n'adhèrent pas à ces règles, celles-ci établissent un cadre éthique et juridique qui permet de condamner les actions inacceptables, d'encourager un « hacktivisme » responsable et de préserver les normes éthiques essentielles au sein de la communauté des « hacktivistes ».

22662 01/24