**Les PME Suisse face aux menaces cyberattaques** 28/02/2024

En 2022, les cyberattaques ont engendré des pertes financières colossales, s'élevant à 8 440 milliards de dollars à l'échelle mondiale. Pour 2024, les estimations indiquent que ce montant pourrait dépasser les 11 500 milliards de dollars. La Suisse n'a pas été épargnée par cette tendance alarmante, avec une augmentation de plus de 60 % des attaques visant les entreprises helvétiques. Parmi les secteurs les plus touchés, le domaine de la santé a été particulièrement vulnérable, suivi par les secteurs de la finance/banque et du gouvernement/défense.

En 2021, malgré le dépôt de 2 600 plaintes pour des actes de cybercriminalité, les experts estiment que seulement 10 % des incidents ont été signalés. En Suisse, seule une PME sur deux dispose d'une stratégie de sécurité informatique, sensibilise son personnel aux bonnes pratiques et effectue des audits de sécurité réguliers. Cette situation préoccupante a atteint un niveau critique, à tel point que même les grandes compagnies d'assurance remettent en question la viabilité de couvrir les entreprises contre les risques cybernétiques.

Les cybercriminels exploitent de plus en plus l'intelligence artificielle (IA) pour mener des attaques sophistiquées contre les entreprises. Voici quelques méthodes utilisées :

1. **Phishing amélioré par l'IA** : Les cybercriminels utilisent des algorithmes d'apprentissage automatique pour personnaliser les e-mails de phishing, augmentant ainsi leur taux de réussite en ciblant les utilisateurs de manière plus convaincante.
2. **Attaques par force brute améliorées** : L'IA est utilisée pour accélérer les attaques par force brute en analysant les schémas de création de mots de passe et en générant des listes de mots de passe probables.
3. **Attaques ciblées basées sur l'IA** : Les cybercriminels utilisent l'IA pour cibler des attaques en analysant les données sur les employés et les infrastructures informatiques des entreprises.
4. **Malware intelligent** : L'IA est utilisée pour développer des logiciels malveillants plus sophistiqués et plus difficiles à détecter.
5. **Attaques DDoS améliorées** : Les pirates utilisent l'IA pour coordonner et amplifier les attaques DDoS, rendant leur contrôle plus difficile.

L'attaque récente de Winbiz en novembre dernier, qui a paralysé 45 000 entreprises et 1 000 fiduciaires pendant plusieurs semaines, souligne l'urgence pour les PME suisses de renforcer leur posture de sécurité. Il est impératif de développer des politiques de sécurité des systèmes d'information et de les mettre en œuvre de manière proactive.

En conclusion, les PME suisses doivent prendre conscience de l'importance cruciale de protéger leur patrimoine informationnel. La cybersécurité ne peut plus être négligée et doit être considérée comme une priorité absolue pour assurer la pérennité et la stabilité des entreprises dans un environnement numérique en constante évolution.