Les piratages ne sont pas près de faiblir

INTERNET L'Office fédéral de la cybersécurité vient de dresser un premier bilan de 2025, notant une intensification des attaques. Un expert avertit: les offensives, de plus en plus automatisées, vont augmenter cette année

ANOUCH SEYDTAGHIA

Pour les spécialistes de la Confédération, l'avenir n'est plus aux attaques de masse, mais à des actions personnalisées. *(ANTON VIERIETIN/ISTOCKPHOTO)*

Si 2025 a été une année compliquée sur le front de la cybersécurité en Suisse, 2026 s'annonce plus difficile encore. A lire le dernier rapport de l'Office fédéral de la cybersécurité (OFSC), les particuliers, mais surtout les entreprises, devront redoubler de vigilance ces prochains mois. Il y a en face une industrialisation des cyberattaques, en cours depuis des années mais qui se renforce grâce notamment à l'intelligence artificielle.

Au total, l'OFSC a reçu 65000 signalements de cyberincidents en 2025, un chiffre quasi stable par rapport à 2024. Ces annonces sont très variées, les principales portant sur les appels téléphoniques émanant prétendument de la police (26% des annonces), devant les tentatives d'hameçonnage (ou *phishing*, 19%) et les tentatives d'escroqueries à l'investissement en ligne via des publicités (9%). Bien sûr, il ne s'agit que d'un reflet de la situation effective, nombre de cyberincidents n'étant pas signalés, dont ceux qui causent des pertes financières.

Dommages prévus en hausse

Les entreprises sont clairement ciblées par les pirates. Ainsi, le nombre d'annonces pour des tentatives d'arnaque au CEO (aussi appelée «arnaque au président»), consistant à obtenir le versement rapide de fonds, est passé de 719 à 970. Le nombre de signalements d'attaque par rançongiciel (ou *ransomware*) est passé de 92 à 104. Attention, avertit l'OFSC: «Le nombre de cas ne donne toutefois aucune indication sur l'ampleur des dommages. Les cybercriminels se concentrent de plus en plus sur des cibles lucratives, si bien que les dommages subis par cas devraient augmenter à l'avenir. On constate en outre que désormais, les attaques par rançongiciel s'accompagnent presque toujours d'une fuite de données, ce qui accroît encore l'ampleur des dommages».

Concernant les tentatives d'hameçonnage, par SMS, WhatsApp ou e-mail, l'OFSC appelle aussi à la prudence, notant que «la tendance n'est plus aux attaques de masse mais aux attaques personnalisées. Les pirates prennent le temps de cibler individuellement leurs victimes. Apparemment, l'investissement en vaut la peine». C'est notamment le cas sur les sites de petites annonces, écumés par les pirates, qui parviennent à convaincre les victimes de faire des versements instantanés via Twint. Des virements souvent impossibles à récupérer.

Une vigilance absolue s'impose. «Nous nous attendons à une accélération significative de l'automatisation des cyberattaques, ce qui entraînera une augmentation du nombre de ces attaques. Ces attaques deviendront plus rapides, évolutives et personnalisées, principalement grâce aux avancées en intelligence artificielle (IA) générative et agentique, ainsi qu'à l'utilisation des deepfakes dans les attaques d'ingénierie sociale», prédit Cédric Nabe, associé chargé du département Risk Advisory pour la Suisse romande chez Deloitte.

L'IA pour contourner les mesures de sécurité

Pour l'OFSC, l'utilisation de l'IA par les pirates n'en est qu'à ses débuts. «L'année dernière, l'utilisation de l'IA dans les tentatives d'escroqueries à l'investissement en ligne via des campagnes publicitaires a été frappante. Des interviews qui paraissaient authentiques ont ainsi été générées avec des personnalités politiques connues, qui recommandaient une méthode prétendument secrète pour investir de l'argent avec des rendements élevés». De plus, «des premiers cas où des images compromettantes ont été créées à l'aide de l'IA afin de faire chanter des personnes ont aussi été signalés», avertissent les autorités.

> **«Les attaques deviendront plus rapides, évolutives et personnalisées»**
>
> CÉDRIC NABE, DU DÉPARTEMENT RISK ADVISORY SUISSE ROMANDE CHEZ DELOITTE

Attention aussi à la rapidité des attaquants. «L'IA agentique permettra de découvrir et d'exploiter les vulnérabilités à une vitesse et à un volume surpassant les capacités humaines. Par exemple, en 2025, nous avons déjà été confrontés aux premiers virus utilisant l'IA pour contourner les mesures de sécurité ou s'y adapter. Cette menace va s'intensifier en 2026», affirme Cédric Nabe. Comment tenter de s'en prémunir? «Cela passe par la détection des comportements anormaux, l'adoption de l'IA dans les mesures de sécurité, la sécurisation des identités (via l'authentification multifacteurs et la biométrie comportementale), des sauvegardes immuables, la segmentation réseau et la détection des deepfakes. La préparation à la gestion des incidents et des crises deviendra une compétence critique pour la survie des entreprises» répond le spécialiste.

Enfin, un autre type de cyberattaque sophistiquée a été détecté en 2025: les attaques via des machines, transportées dans des voitures, appelées «SMS Blaster». Ces appareils se font passer pour des antennes de téléphonie, et grâce à eux, les pirates ont pu envoyer des SMS frauduleux directement aux appareils situés à proximité. Les victimes ont reçu le message, appelant notamment au paiement d'une soi-disant amende, sans que leur numéro de téléphone soit connu des escrocs. Le lien contenu dans le message redirigeait vers une page de paiement d'apparence authentique qui récupérait les données de carte de crédit. Même si des arrestations ont eu lieu en Suisse, il est fort possible que de telles attaques se produisent à nouveau cette année. ▬