La recrudescence des attaques contre l'industrie automobile nuit non seulement aux sociétés, mais aussi aux clients et aux employés

Il y a quelques jours, Renault UK a confirmé que certaines données de clients avaient été volées lors d'une cyberattaque contre l'un de ses fournisseurs tiers. Selon le constructeur automobile, le nom, l'adresse, la date de naissance, le sexe, le numéro de téléphone, le numéro d'identification du véhicule et les informations relatives à l'immatriculation des véhicules de ses clients ont été volés.

« Il s'agit d'un incident dangereux, car les données compromises se prêtent parfaitement aux attaques par hameçonnage et à l'usurpation d'identité. Les fraudeurs peuvent facilement se faire passer pour des représentants de Renault, des policiers ou même des avocats proposant de se joindre à un recours collectif contre la société et offrant une indemnisation substantielle. Il arrive fréquemment que des utilisateurs poursuivent en justice une société qui n'a pas assuré la sécurité de leurs données, en particulier aux États-Unis. Parfois, voyant une bonne occasion de parvenir à un accord, les avocats recherchent eux-mêmes les personnes qui ont été victimes d'une infraction. Cependant, les fraudeurs se font parfois passer pour des avocats qui proposent d'obtenir une indemnisation. De cette façon, ils cherchent à vous extorquer encore plus de données ou d'argent », met en garde Ignas Valancius, responsable de l'ingénierie chez NordPass, une société spécialisée dans la cybersécurité.

Il souligne que le cas de Renault n'est pas un événement isolé. Cette année, l'industrie automobile a été secouée par une série de cyberattaques et de violations de données.

« Il semble que les acteurs malveillants testent la maturité de la cybersécurité au sein de l'industrie automobile. Les pertes, la menace qui pèse sur la continuité des activités des petits fournisseurs et la nécessité pour les constructeurs automobiles de repenser leurs processus font l'objet de nombreuses discussions. Cependant, une cybersécurité insuffisante n'est pas seulement un problème pour les sociétés : les données des clients et des employés sont également volées », explique l'expert.

Infractions récentes très médiatisées

Récemment, des cybercriminels ont piraté Miljödata, un fournisseur suédois de logiciels de RH très populaire, volant par la même occasion les données personnelles des employés de Volvo North America. La même semaine, le géant international Stellantis, qui compte dans son portefeuille des marques telles que Jeep, Peugeot et Fiat, a révélé que les coordonnées de ses clients avaient été divulguées. Cet incident est également lié à la compromission d'une plateforme d'un prestataire de services tiers.

Les constructeurs allemands ont également essuyé quelques revers cette année. Au début du mois de septembre, il a été annoncé que les données de BMW avaient été piratées par le groupe de ransomware Everest. Au début de l'année 2025, Volkswagen a été victime d'une grave faille de sécurité qui a entraîné la divulgation des données personnelles d'environ 800 000 propriétaires de véhicules électriques. Sans oublier une autre affaire particulièrement controversée : l'attaque contre Jaguar Land Rover (JLR).

Pendant ce temps, aux États-Unis, des pirates ont infiltré la société Motility, spécialisée dans les logiciels destinés aux concessionnaires automobiles, pour dérober les données personnelles de près de 800 000 personnes avant de chiffrer les systèmes de la société. Au cours de cette même période, une fuite majeure provenant d'une plateforme de conformité des conducteurs a exposé les numéros de sécurité sociale et les permis de conduire de plus de 10 000 chauffeurs routiers texans.

Gare au phishing

Ce ne sont là que quelques exemples parmi les plus visibles de cette offensive incessante. L'industrie automobile continue de faire face à de nombreux défis, avec des dizaines d'incidents mineurs survenus cette année en plus des exemples mentionnés ci-dessus. Il semble que les marques de luxe aient été les cibles principales des groupes de pirates en 2025, compromettant ainsi des personnes fortunées. Il est probable que nous assistions prochainement à des attaques de harponnage et à d'autres types d'attaques ciblées, d'autant plus que les récentes infractions feraient partie d'une campagne plus large menée par des groupes d'extorsion », explique M. Valancius.

« Les données personnelles identifiables des clients et des employés sont considérées comme les plus sensibles. De telles fuites présentent un risque important d'usurpation d'identité. Cela peut entraîner divers problèmes, allant de crédits à votre nom à l'utilisation de vos données d'identité ou de carte bancaire pour accéder à des sites pédopornographiques sur le dark web », ajoute l'expert en cybersécurité.

Comment se protéger

Selon Valancius, en exploitant les données des employés, les cybercriminels peuvent mettre la main sur davantage de secrets d'entreprise. Ils peuvent donc s'intéresser à certains employés en particulier, notamment ceux qui occupent des postes à responsabilité.

Les clients et les employés des sociétés victimes d'une violation peuvent vérifier si leurs adresses e-mail ou leurs mots de passe ont été divulgués grâce à l'Analyse des fuites de données. Cet outil peut alerter les utilisateurs en temps réel si leur adresse e-mail ou leurs informations de carte bancaire ont fait l'objet d'une fuite de données.

« Je recommande également vivement de mettre à jour vos mots de passe et d'activer l'authentification multifacteurs partout, si ce n'est déjà fait. Gardez un œil sur votre compte afin de détecter toute activité inhabituelle et tout e-mail de hameçonnage. Soyez vigilant, même si les e-mails semblent provenir de sources légitimes, comme des constructeurs

automobiles ou la police. Si vous recevez de tels messages, faites preuve d'une extrême prudence, car les liens peuvent mener à des pages conçues pour vous voler encore plus de données. Si vous n'êtes pas sûr de l'authenticité d'un e-mail ou d'un message, il est préférable de ne pas cliquer sur le lien. Accédez directement au site de cette société ou organisation, identifiez-vous (ou contactez-la directement par téléphone) et vérifiez si le message est authentique. « Ne cliquez sur aucun lien et ne communiquez pas vos données à des inconnus qui vous appellent », conseille Valancius.

Selon l'expert en cybersécurité, les grandes entreprises devraient également faire preuve de davantage de prudence. Il est essentiel de renforcer la sécurité des données, en particulier lors de la collaboration avec des fournisseurs et partenaires tiers, car l'expérience montre que de nombreux cyberincidents proviennent de plateformes tierces.

« Les sociétés doivent mettre en place des stratégies de cybersécurité adéquates et former régulièrement leurs employés et partenaires afin d'assurer une bonne gestion des mots de passe et une vigilance numérique plus vaste. Il est également essentiel de contrôler l'accès aux systèmes de la société par les fournisseurs, les vendeurs et autres tiers. Les meilleures pratiques en matière de cybersécurité stipulent que les agents tiers ne doivent pas avoir un accès permanent aux systèmes d'une société. Toutes les demandes et connexions externes doivent toujours être traitées au cas par cas et protégées par une authentification à deux facteurs. Si le partage de données en temps réel est nécessaire, il ne doit se faire que par le biais d'un VPN ou d'autres outils chiffrés », conseille M. Valancius.

À PROPOS DE NORDPASS

NordPass est un gestionnaire de mots de passe pour les entreprises et les particuliers. Il est basé sur des technologies de pointe pour une sécurité optimale. Développé pour être abordable, simple et convivial, NordPass permet aux utilisateurs d'accéder à leurs mots de passe en toute sécurité sur les ordinateurs, les téléphones et les navigateurs. Tous les mots de passe sont chiffrés sur l'appareil, afin que seul l'utilisateur puisse y

accéder. NordPass a été créé par les experts à l'origine de NordVPN, l'application de sécurité et de confidentialité avancée à laquelle font confiance plus de 14 millions de clients à travers le monde. Pour plus d'informations : nordpass.com/fr/.