Communiqué de presse

5 novembre 2026

Concessions automobiles : le cloud au coeur des enjeux de cybersécurité

Paris, novembre 2026 - Le Cybermois, le mois européen de la cybersécurité, rappelle chaque année l'importance de la cybersécurité. Mais la vigilance ne s'arrête pas en octobre. Nextlane, plateforme européenne dédiée à la distribution automobile, alerte sur les risques qui pèsent sur les données des concessions automobiles. Face aux systèmes vieillissants et aux ressources informatiques limitées, le cloud peut renforcer la sécurité, à condition d'être correctement conçu et supervisé. L'occasion pour Nextlane de rappeler les principaux enjeux et les bonnes pratiques à adopter.

Des concessions confrontées à des risques bien réels

Les concessions traitent de nombreuses données sensibles : pièces d'identité, dossiers de financement ou informations d'immatriculation. Leur perte ou leur indisponibilité peut paralyser l'activité et fragiliser la confiance des clients.

Les infrastructures hébergées sur site présentent également des risques : une panne ou une attaque peut affecter plusieurs services simultanément. La gestion des mises à jour, des accès et des sauvegardes nécessite une vigilance constante. Si les sauvegardes sont stockées au même endroit que les données d'origine, elles peuvent être compromises, avec des conséquences importantes sur la continuité de l'activité et la préservation du portefeuille client.

Les accès constituent enfin une porte d'entrée privilégiée. En 2025, le piratage de compte représentait 21 % des demandes d'assistance des entreprises et associations, contre 16 % pour l'hameçonnage[1]. D'où l'importance de sécuriser les accès et de sensibiliser les équipes.

Le cloud, un levier pour sécuriser et maintenir l'activité

Pour une concession, passer à un cloud managé, c'est d'abord ne plus dépendre de serveurs installés sur site, ni avoir à les entretenir.

« Chez de nombreux distributeurs, les systèmes informatiques se sont construits au fil du temps, avec des logiciels parfois anciens ou encore insuffisamment intégrés entre eux. Leur maintenance représente un enjeu important. Avec Nextlane Cloud Hosting, développé en partenariat avec AWS, la surveillance, la maintenance et les mises à jour de sécurité sont prises en charge par des équipes spécialisées. L'hébergement des données est exclusivement assuré dans des centres de données européens, sur un socle sécurisé et standardisé dès sa conception. Les distributeurs peuvent ainsi s'appuyer sur une infrastructure pensée pour leurs enjeux de sécurité. »,

– Matthieu Cévaër, VP Sales chez Nextlane

Le choix du cloud répond aussi à un enjeu de conformité. Au regard du RGPD, la concession reste en principe responsable des données de ses clients. Un hébergement maîtrisé, avec des accès sécurisés et des traitements encadrés, l'aide à limiter les risques, dans le respect des responsabilités de chaque partie.

Le cloud managé renforce enfin la continuité d'activité. Selon l'architecture retenue, applications et données restent accessibles même en cas de panne locale ou d'indisponibilité d'un site. Les équipes peuvent ainsi travailler à distance et les différents sites d'un groupe se coordonner plus facilement. Si l'incident touche les données elles-mêmes (suppression accidentelle, panne ou cyberattaque), des sauvegardes automatisées, externalisées et régulièrement testées assurent leur restauration.

Ce qui distingue l'approche cloud de Nextlane

Au-delà du choix d'un hébergement cloud, la manière dont l'environnement est structuré joue un rôle important dans la maîtrise des risques. Nextlane s'appuie sur une « Landing Zone », un socle sécurisé et standardisé. Le principe est comparable à l'aménagement d'une concession : avant d'installer le showroom, l'atelier ou le stock, il faut un site structuré, avec des accès contrôlés, des zones séparées et des règles de sécurité. Dans le cloud, la Landing Zone joue ce rôle : elle prépare et sécurise le terrain avant l'arrivée des applications et des données.

Concrètement, les règles d'accès, de réseau, de supervision et de gouvernance sont définies en amont : les environnements sont isolés les uns des autres, les accès contrôlés et les politiques de sécurité appliquées de façon homogène. Une grande partie de cette configuration est automatisée, ce qui vise à limiter les écarts et les erreurs manuelles. Chaque concessionnaire bénéficie ainsi, dès le départ, des mêmes standards de sécurité, dans un environnement capable d'évoluer avec ses besoins.

Pour les distributeurs déjà dans le cloud, la question n'est pas seulement de savoir où sont hébergées leurs données, mais comment leur environnement est construit et supervisé. Chez les fournisseurs généralistes, la sécurité est partagée : le fournisseur protège l'infrastructure, mais la configuration, les accès et la supervision restent à la charge du client. Avec Nextlane Cloud Hosting, ces tâches sont assurées par des équipes spécialisées, dans un environnement conçu pour la distribution automobile.

Cybermois : les recommandations de Nextlane pour sécuriser les concessions

Pour Nextlane, le cloud managé renforce la cybersécurité des concessions, mais doit s'accompagner de bonnes pratiques pour limiter les risques.

1. **Exiger un environnement cloud sécurisé dès sa conception.** Le cloud ne garantit pas, à lui seul, un niveau de sécurité suffisant. La concession doit vérifier auprès de son prestataire que les environnements sont isolés, les accès encadrés, les activités supervisées et les configurations standardisées et automatisées pour limiter les erreurs humaines, dès la mise en place puis régulièrement.
2. **Généraliser la double authentification sur les outils professionnels** : logiciels de gestion de concession (DMS), messageries et portails constructeurs. Cette mesure ajoute une barrière supplémentaire lorsqu'un mot de passe est compromis.
3. **Réviser régulièrement les droits d'accès.** Dans un secteur où les mouvements de personnel et les mobilités entre sites sont fréquents, les comptes des collaborateurs qui partent doivent être désactivés rapidement pour ne pas devenir un point d'entrée.
4. **Sensibiliser les équipes à l'hameçonnage.** Accueil, administration des ventes et après-vente reçoivent chaque jour des messages de clients, de fournisseurs et de constructeurs. Ils doivent savoir repérer les courriels suspects, les pièces jointes inattendues et les usurpations d'identité, y compris lorsqu'elles sont facilitées par l'intelligence artificielle.
5. **Anticiper la gestion d'un incident.** Identifier les interlocuteurs à prévenir, définir les procédures de secours, déterminer les priorités de rétablissement et tester régulièrement la restauration des sauvegardes permettent de limiter l'improvisation lorsqu'une attaque ou une panne survient.

Pour Matthieu Cévaër, la protection des concessions repose sur la complémentarité entre technologie et vigilance humaine : « *Le cloud permet aux concessions de bénéficier d'une infrastructure sécurisée et de moyens techniques qu'elles ne pourraient pas toujours mobiliser seules. Mais la cybersécurité ne repose pas uniquement sur la technologie. La gestion des accès, la sensibilisation des collaborateurs et la préparation aux incidents sont tout aussi essentielles.* »

[1] *Source : bilan 2025 de Cybermalveillance.gouv.fr, publié en mars 2026.*

À propos de Nextlane

Nextlane est le leader européen de logiciels pour la distribution automobile. Son écosystème sécurisé, ouvert et intelligent permet aux concessionnaires et aux constructeurs de stimuler leur croissance et d'offrir une expérience client optimisée. La suite complète de Nextlane couvre l'ensemble du cycle de vente automobile, de la gestion des stocks de véhicules aux services après-vente, en passant par la comptabilité et la facturation. Avec plus de 700 collaborateurs dans 11 pays, Nextlane s'engage à digitaliser et simplifier l'ensemble du parcours automobile. Sa mission est de promouvoir l'excellence digitale dans l'industrie en créant un écosystème numérique fiable.

Pour plus d'informations, visiter le site www.nextlane.com/fr