Les données de santé des animaux d'élevage face aux risques cyber

Pascaline BOSSARD
Experte cybersécurité – Life science

Un secteur hautement stratégique mais non abordé en termes de cybersécurité et de protection des données.

Si la sécurité des données de santé humaines est un sujet fortement évoqué et traité, le pendant chez les animaux d'élevage est un domaine quasiment inconnu du grand public. Les enjeux sont certes différents mais les deux sont pourtant étroitement liés : 70 % des maladies infectieuses humaines ont une origine animale (source OMSA).

En France, les animaux d'élevage (dit de rente) font l'objet d'un suivi sanitaire strict, coordonné par la filière du diagnostic vétérinaire.

Il est un maillon essentiel de la santé publique et de la souveraineté alimentaire. La notion de sécurité alimentaire peut être représentée par le concept « from farm to fork », de la ferme à la fourchette. Le diagnostic vétérinaire est le maillon de la chaine qui fait le lien entre l'agriculture et l'agroalimentaire, garant par les analyses réalisées au quotidien de la qualité du lait ou de la viande qui sortent des élevages pour être transformés avant d'être consommés. Soumis à l'instabilité géo politique mondiale, à des contraintes environnementales de plus en plus importantes, à des besoins de traçabilité toujours plus poussés… son environnement est en constante évolution, avec un facteur d'accélération ces dernières années.

Les analyses réalisées servent des objectifs économiques, sanitaires et réputationnels sur les marchés.

Chaque jour, des milliers de données relatives à la santé des animaux ou à la production de lait sont générées pour permettre à la filière de fonctionner efficacement, et ce depuis de nombreuses années. A titre d'exemple, le secteur laitier représente à lui seul 120 millions d'analyses chaque année[1]. On peut parler de big data. Ces données sont indispensables au quotidien pour les différents intervenants de la filière. La dépendance accrue aux systèmes numériques expose le secteur à des risques de cybersécurité. Cela nécessite une réelle compréhension des enjeux cyber afin de préparer sa protection de manière adaptée en tenant compte des menaces spécifiques à ce secteur.

Comme pour les données de santé humaine, les données de santé animale sont riches, stratégiques et sensibles. Leur compromission entraîne des risques majeurs.
Risque sanitaire : un blocage des systèmes de suivi de troupeau peut fausser un diagnostic, retarder la détection des maladies ou compromettre la gestion des traitements.

[1] Rapport annuel d'activité du CNIEL- 2023

Risque économique : la perte de traçabilité - qu'il s'agisse de données de troupeau ou d'archives de filière - ou l'indisponibilité d'outils essentiels au diagnostic peut provoquer l'arrêt brutal d'une activité et générer des pertes considérables.
Risque de réputation : avec la sensibilité connue du grand public sur les sujets sanitaires, une fuite de données sensibles ou une campagne de désinformation peuvent altérer la confiance des consommateurs et nuire aux filières.

Quel est le niveau de maturité face aux risques et menaces encourus ?

Au-delà des attaques d'opportunités pour des raisons financières avec demande de paiement de rançons, nombre d'acteurs malveillants peuvent avoir des intérêts dans la déstabilisation de la filière, qu'il s'agisse d'hacktivistes/activistes ou d'acteurs étatiques. En France, l'élevage est un secteur économique important. La France est le 6ème exportateur mondial de produits agricoles et agroalimentaires. Au niveau Européen, la France est un des leaders sur le marché : premier pour la production de viande bovine, second en tant que producteur laitier ; elle détient le 3ème cheptel porcin. Ce qui en fait un acteur clé pour le pays, mais aussi la communauté européenne et donc une cible pour les entreprises ou états concurrents.

Des menaces spécifiques au secteur pèsent sur la disponibilité des données, leur intégrité, leur confidentialité et leur traçabilité avec des impacts plus ou moins importants. Cela est amplifié par l'utilisation d'outils métiers dont certains ne sont pas au standard de sécurité attendu. L'arrivée des objets connectés dans les élevages est aussi un facteur à prendre en compte dans le développement de la surface d'attaque.

Non soumis à des réglementations fortes et contraignantes (non inclus dans NIS1, non considéré comme organisme d'importance vitale, hors cadre du RGPD…), la maturité globale du secteur n'est pas au niveau pour faire face aux menaces et risques identifiés. Il y a une sous-estimation de ces derniers, avec une méconnaissance de l'importance de la valeur des données produites ou utilisées. Pourtant les attaques d'origine cyber sont déjà une réalité dans le secteur, en France et à l'étranger, ce qui tend à introduire le sujet mais de manière encore très timide. Nous pouvons ici illustrer les propos avec la cyberattaque subit par une coopérative agricole impactant près de 30 000 éleveurs dans 22 départements français en décembre 2024[2].

Le niveau de maturité est très différent selon les structures. De manière générale, il est assez faible au regard des enjeux. Contrairement à ce qui peut exister dans d'autres secteurs d'activités, il n'y a pas de coordination sur la cyberdéfense dans le secteur du diagnostic vétérinaire.

Combler les vulnérabilités pour réduire les risques.

Des actions sont à entreprendre du niveau le plus local à celui de l'état pour une montée en compétences de tous les acteurs. La modernisation des outils obsolètes (notamment étatique) est indispensable ou à minima, les isoler quand cela est possible. Toutes les technologies qui permettraient de sécuriser la filière existent sur le marché. Mais pour pouvoir installer les systèmes nécessaires de manière efficace, il faudra revoir les processus, notamment l'ultra segmentation des bases de données.

Une réelle prise de conscience est nécessaire par tous les acteurs afin de pouvoir faire progresser l'existant. Une sensibilisation à tous les niveaux

[2] « Ils nous ont contactés via une messagerie cryptée pour obtenir une rançon : cette cyberattaque rend la vie impossible aux éleveurs, France Info, 2 janvier 2025

semble indispensable afin de créer une réelle culture de la protection des données produites et échangées. La compréhension des enjeux et des besoins sera alors la meilleure des préventions. Contrairement à d'autres secteurs déjà imprégnés par la notion de cyber sécurité, par le bais de la formation ou de la réglementation, le secteur vétérinaire dans son ensemble n'aborde pas ou peu ces sujets. Par exemple, il n'y aucune formation sur la sécurité des données ou la partie juridique liés aux données dans les écoles vétérinaires ou les cursus scientifiques.

Le changement ne pourra se faire sans une gouvernance forte permettant de regrouper les acteurs autour des problématiques de sécurité des données. Le maillage actuel rend complexe la montée en compétence globale. La posture individuelle ne sera pas suffisante pour protéger toute la chaine. Placer l'intérêt commun au-dessus sera un levier indispensable pour aligner toute la filière sur des standards, comme cela a pu être fait dans la santé humaine par exemple. De l'union viendra la force, au sein de chaque métier d'abord puis au sein de l'éco système.

L'évolution du cadre réglementaire, notamment avec la transposition de NIS2 et du data act en 2025 devrait assoir des règles pour une partie des acteurs. Une réelle compréhension de ce cadre et surtout son application vont imposer la mise en place d'un certain nombre de processus accentuant la protection des données.

Quel avenir ?

L'exploitation des données produites par le diagnostic vétérinaire serait bénéfique à la fois pour l'efficacité de la surveillance sanitaire et pour la protection des nouvelles infrastructures. Un environnement où les données sont non seulement disponibles, intègres, mais aussi mieux sécurisées est indispensable. L'arrivée de l'IA avec des modèles permettant de réaliser des diagnostics en amont des analyses est déjà en train de s'établir ce qui va complexifier le système actuel.

Sécuriser la filière est une priorité avant que les données ne soient en dehors des organismes actuels et donc en dehors de leur contrôle.