LA SÉCURITÉ DES DONNÉES : une affaire de technologie et de personnes

Rémy Magnac, responsable Sécurité, nous explique comment ***Digiposte*** appréhende l'enjeu stratégique de la protection et de la sécurisation des données. Entretien

Rémy Magnac

Qu'est-ce que Digiposte ?
Digiposte est la boîte aux lettres numérique de La Poste qui permet aux entreprises de dématérialiser des documents incontournables de la vie de leurs salariés et de sécuriser leur envoi et leur conservation côté collaborateur. Digiposte permet aussi aux particuliers de gérer leurs documents administratifs et les données personnelles sensibles associées en toute sécurité. Aujourd'hui, nous accompagnons près de 10 000 entreprises qui dématérialisent et déposent les bulletins de paie dans les coffres-forts numériques de leurs salariés. Nous avons aussi près de 6 millions d'abonnés (plus de 3 millions d'entre eux sont des salariés).
Au-delà de la conservation des fiches de paie, Digiposte permet aussi à ses abonnés de collecter des documents comme les relevés d'imposition, des factures type EDF/e-commerçant, leurs relevés bancaires mais aussi des documents émis par les organismes de santé (relevé Ameli, Mutuelle…). Il s'agit de données sensibles et confidentielles qu'il convient de sécuriser avec efficacité.

Et c'est le cas de Digiposte : nous sommes conformes aux normes d'archivage et de sécurité des données françaises (ISO 27001, AFNOR NF Z 42-013), aux décrets sur le coffre-fort numérique (décret n°2018-418 et décret n° 2018-853) et au Règlement général sur la protection des données (RGPD). Nous possédons aussi la certification HDS (hébergeurs de données de santé). À ce jour, nous sécurisons plus de 300 millions de documents pour le compte de nos abonnés.

Au sein de Digiposte, vous êtes responsable sécurité Digiposte. Quelles sont votre feuille de route et vos principales missions ?
J'ai deux missions principales afin d'assurer la sécurité de Digiposte. Premièrement, je suis en charge de concevoir et d'adapter le plan de sécurité de Digiposte en prenant en compte nos évolutions technologiques et l'apparition des menaces. L'enjeu est clé, il s'agit de pouvoir anticiper les menaces existantes et futures afin d'être en mesure de contrer d'éventuelles attaques. Par exemple, nous nous prémunissons bien évidemment contre les attaques de ransomware. Ces attaquants s'infiltrent dans les systèmes d'information, choisissent les documents et données qu'ils estiment avoir de la valeur et les chiffrent pour faire une demande de rançon en contrepartie du déchiffrement des données. Cette menace, nous l'avions déjà anticipée chez Digiposte il y a une dizaine d'années. La modification des données au sein des coffres-forts n'est tout simplement pas permise.
Ma deuxième mission consiste à contrôler le niveau et la qualité des dispositifs de sécurité. A cet effet, nous avons mis en place des tests automatisés, des audits plusieurs fois par an avant les mises en production, de la veille et de la surveillance active en direct du système d'information. Tout cela dans l'optique de prévenir le risque de cyberattaques, mais aussi pour adapter et faire évoluer notre système.

Quelles sont les dernières évolutions gouvernementales et réglementaires sur la protection des données et comment Digiposte se positionne-t-il sur ce sujet ?
Alors que le volume de données produites jour après jour ne cesse d'augmenter, les piratages sont plus fréquents, plus virulents et plus médiatisés. Plus que jamais la collecte, l'exploitation et le stockage des informations sont porteurs d'enjeux stratégiques notamment en termes de protection des données à caractère personnel. Cette dimension a pris encore plus d'importance depuis le début de la crise sanitaire. Le récent rapport d'activité de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) souligne clairement l'accélération et l'augmentation du risque et des menaces de toutes formes. Par ailleurs, le Plan France Relance de l'économie comporte, lui-aussi, un volet cybersécurité avec un budget notable de 136 millions d'euros sur 2 ans.
C'est pourquoi il est important d'asseoir la souveraineté numérique française. À notre niveau, nous essayons de contribuer à cet enjeu qui dépasse largement la question de la simple localisation du stockage en France ou Europe. Se pose également la question de la dépendance technologique à un nombre réduit d'acteurs, notamment les GAFA et les fabricants de semi-conducteurs, et de l'exposition à des lois étrangères, comme le CLOUD Act ou encore la législation chinoise, qui sont intrusives et posent un risque de contrôle… Face à cela, nous soutenons les initiatives des agences gouvernementales comme la qualification SecNumClouD ou l'agrément HDS pour les hébergeurs de données de santé. Sur un plan règlementaire, on peut aussi citer la Loi de programmation militaire.

Quels sont les enjeux que pose la gestion des données sur le plan technologique, notamment en termes de sécurisation ?

Les technologies sont primordiales pour assurer la sécurité des données. Nous nous intéressons aux nouvelles méthodes de chiffrements, au déploiement de l'authentification double facteur… À Digiposte, deux procédés importants sont mis en place. Premièrement, tous les accès à la salle des coffres sont contrôlés, tracés et horodatés. Le chiffrement nous permet de cacher le contenu des documents, seuls ceux ayant les clés de déchiffrement y ont accès. Nous avons aussi développé le produit afin d'assurer une sécurisation optimale de la connexion. Seul l'utilisateur connaît ses identifiants (ni Digiposte, ni l'employeur n'y ont accès). Nous avons mis en place un mécanisme de dispositif de confiance (« trusted device »).

Chaque fois que l'utilisateur se connecte via un nouvel appareil, celui-ci est d'abord reconnu et pour se connecter, l'utilisateur doit entrer un code unique et limité dans le temps reçu sur son e-mail. Une fois que le code a bien été entré et qu'on est assuré que c'est bien l'utilisateur qui se connecte, l'appareil est ajouté à l'historique d'appareils connus. L'utilisateur peut aussi choisir d'activer la double authentification par l'application et recevra, à chaque nouvelle connexion, un code unique à entrer pour s'identifier et accéder à son coffre. Nous effectuons aussi des campagnes de sensibilisation sur le format et la sécurisation des mots de passe (en accord avec les recommandations de la CNIL en la matière) et identifiants auprès de nos utilisateurs. Comme nous le savons, nombreux sont ceux qui utilisent le même mot de passe pour différents sites et applications. Nos utilisateurs ont des profils variés, ils peuvent être des non-initiés, des internautes occasionnels ou encore des passionnés de technologie ("geeks"). Nous avons une approche pédagogique lorsque nous communiquons auprès d'eux. Nous leur expliquons, au travers de nos newsletters , comment cette pratique facilite le bourrage d'identifiants (« credential stuffing ») si leurs données ont été récupérées par des acteurs malveillants. Dans cette démarche de sécurisation, nous avons aussi noué des partenariats avec des experts de la sécurité par exemple avec l'INRIA avec qui nous étudions de nouveaux algorithmes résistants à des attaques post-quantiques.

Quel est le positionnement éthique de Digiposte sur la gestion et la protection des données ?

La confidentialité est au cœur de l'ADN du groupe La Poste qui en a toujours été garant pour le courrier physique. Aujourd'hui, c'est très naturellement que cela se transpose à Digiposte. Autre point important que nous avons déjà mentionné, nous ne modifions et n'accédons pas aux documents déposés dans les coffres-forts.

En parallèle, le RGPD est venu normer le cadre autour de la protection des données et de leur confidentialité en France et en Europe notamment avec la nécessité d'avoir le consentement de l'utilisateur pour le recueil, l'exploitation et la conservation des informations personnelles. Enfin, le coffre-fort Digiposte est la propriété de son utilisateur, celui-ci est donc maître de ses données personnelles.

La Poste n'exploite pas les données des coffres forts numériques Digiposte, rappelons-le, le modèle économique La Poste ne repose pas sur la revente de données à des tiers. Même si les bulletins de paie sont déposés par l'employeur, c'est le salarié qui en est le propriétaire et qui le reste même s'il change d'entreprise.

Quels sont les enjeux économiques de la protection des données ?

La sécurité et la conformité réglementaire ont un coût économique très important. Face à cet enjeu, le groupe La Poste a choisi d'investir dans un service dédié à la lutte contre la cybercriminalité qui intervient à plusieurs niveaux : la veille technologique, la surveillance du dark web, l'analyse des tentatives d'attaques, l'automatisation de leur neutralisation, et le suivi des anomalies dans les plans de risques résiduels… Les analyses de risques en amont permettent au final la couverture des risques en assurant l'adéquation entre le risque métier et les moyens mis en œuvre pour les réduire. Elles facilitent la priorisation des sujets clés et du cœur de métier Digiposte tout au long de la démarche. Et pour relever ce défi, au-delà des moyens matériels, il faut bien évidemment des compétences et des talents. Ce sont nos experts qui nous permettent d'avancer sur ces sujets et de garantir un niveau de protection optimal. Au-delà des compétences internes, nous travaillons avec des cabinets spécialisés reconnus sur la place publique, par des auditeurs certifiés individuellement (certifications GIAC GPEN Pentester & ISO 27005 Risk Manager).