ÉTUDE DE CAS

e-Scooter

FORMATION CERTIFIED
ISO/IEC 27001 LEAD IMPLEMENTER

Table des matières

I. Historique de la société

e-Scooter est une société privée, dont le siège social est situé à Paris, en France. Elle fournit des services de partage de trottinettes électriques depuis 2017. Constatant l'utilisation croissante de trottinettes motorisées électriques aux États-Unis, Marc Leroux a fondé sa société visant à introduire l'usage des trottinettes électriques dans toute l'Europe. Dans un premier temps, *e-Scooter* a lancé son système de partage de trottinettes à Paris, 750 trottinettes électriques ayant été testées pour la première fois, puis étendues à d'autres grandes villes européennes, comme Londres, Madrid, Berlin, Rome, et Istanbul.

L'utilisation des trottinettes électriques dans ces villes a augmenté à mesure que les gens préféraient utiliser des modes de transport rapides et pratiques. La possibilité de localiser et de garer des trottinettes à n'importe quel coin et les faibles frais pour les services rendaient l'expérience encore plus agréable pour les clients. Pour pouvoir utiliser l'un des scooters électriques de l'entreprise, les clients ont dû télécharger l'application *e-Scooter*. Grâce à l'application, les clients pouvaient localiser le scooter le plus proche et le déverrouiller en scannant son QR code. Le prix de départ pour déverrouiller le scooter était de 1 $, ajoutant 20 centimes par minute au prix final.

En outre, les clients ont apprécié la flexibilité offerte par *e-Scooter* pour payer les services de l'entreprise*. e-Scooter* a permis à ses clients de payer à la fois en ligne et en espèces. Pour ceux qui préféraient les transactions numériques, les clients avaient la possibilité de saisir leurs informations personnelles et d'effectuer des paiements directement via leurs comptes bancaires via l'application e-Scooter. Alternativement, pour ceux qui ont préféré payer en espèces, *e-Sooter* a intégré un système de paiement basé sur le numéro de téléphone dans l'application. Ainsi, en quelques étapes seulement, les clients pouvaient entrer leur numéro de téléphone et être redirigés vers un site Web affichant les localisations voisines où ils pouvaient facilement effectuer des paiements en espèces.

e-Scooter a développé son service de paiement en coopération avec *Bankit* (une entreprise qui propose des logiciels personnalisés spécialisés pour les entreprises de technologies financières). Tous les services que *BankIT* a offerts à *e-Scooter* étaient disponibles dans une seule plateforme qui gère le processus de paiement, y compris la sécurité nécessaire au fonctionnement d'une telle plateforme.

e-Scooter privilégie la sécurité et la durabilité, le bien-être de ses employés, et la mise en place de pratiques écologiques. Grâce à ces pratiques, l'entreprise a réussi à toucher des millions d'utilisateurs à travers l'Europe et à devenir un concurrent de

premier plan dans l’industrie du partage de scooters dans le monde pour atteindre une valeur nette de 200 millions de dollars.

II. Événements récents

Alors que l'entreprise a connu une croissance rapide de son chiffre d'affaires au cours des années, sa pression pour se démarquer sur le marché et fournir des services qualitatifs à ses clients s'est également accrue. Pour diminuer les coûts de production, maximiser les capacités de production, et augmenter les profits, la direction générale d'*e-Scooter* a décidé d'externaliser la production des trottinettes électriques à *LING*, une société privée en Chine.

Bien que l'entreprise ait apporté des changements prometteurs, elle a continué d'être confrontée à de nouveaux enjeux et défis qui nécessitaient des solutions innovantes pour conserver sa position de leader dans l'industrie du partage de trottinettes. L'un des enjeux était l'abandon des trottinettes par les clients dans des zones comme les lacs ou les rivières, ce qui rendait la récupération des trottinettes très difficile. Cela posait des préoccupations environnementales, mais rendait également le processus de récupération des scooters chronophage et coûteux pour l'entreprise.

Un autre problème était que les scooters se faisaient facilement voler en raison de leur poids léger et parce que l'alarme ne se déclencherait pas si quelqu'un prenait le scooter et ne le déverrouillait pas. Après avoir été volée, la planche des trottinettes électriques serait remplacée par une autre planche et leur GPS serait retiré afin que l'entreprise ne puisse pas les localiser.

En outre, parce que l'entreprise utilisait des autocollants QR pour permettre aux clients d'utiliser les trottinettes électroniques, le risque de cyberattaques était assez élevé. En effet, les attaquants pouvaient facilement remplacer les codes QR du scooter électronique par des autocollants composés de codes QR fabriqués et comprenant des URL malveillantes. Ces URL redirigeraient alors les utilisateurs vers un autre site Web qui leur imposait de fournir leurs informations personnelles et financières, par conséquent, en volant leurs données.

L'entreprise a mis en place des mesures de protection contre les attaques par déni de service distribué (DDoS), sachant l'impact que de telles attaques pourraient avoir sur la disponibilité et l'expérience utilisateur de son application. En outre, la direction générale a décidé de mettre en place un système de gestion de la sécurité de l'information (SMSI) basé sur les exigences de la norme ISO/IEC 27001.

III. La mise en œuvre du SMSI

Après avoir initié la mise en œuvre du SMSI, la société a établi le domaine d'application du SMSI et la politique de sécurité de l'information. De plus, Lenny, le gestionnaire du projet, a entrepris certaines activités pour comprendre le contexte de l'entreprise et a mené une analyse des écarts et une évaluation du risque. Les résultats de l'évaluation du risque ont notamment mis en lumière les causes profondes des problèmes qui se posaient.

Sur la base des conclusions, *e-Scooter* a demandé au département de production de *LING* de concevoir une enceinte plus sécurisée pour la carte mère des scooters, sans vis visibles, ce qui rend difficile pour les acteurs malveillants d'altérer les composants internes, et d'installer davantage de capteurs pour détecter le vol et les dommages aux scooters, améliorant encore la sécurité. Par ailleurs, pour encourager une utilisation responsable et la responsabilisation, *e-Scooter* a exhorté ses utilisateurs à prendre une photo de leur scooter après l'avoir stationné et à le télécharger via l'application.

Une autre étape que l'entreprise a franchie a été de demander aux trottinettes de balayer leur emplacement et les données pertinentes (p. ex., le niveau de la batterie) toutes les 60 secondes vers les serveurs *d'e-Scooter*. Pour conserver un enregistrement immuable des métadonnées de chaque scooter, les données ont été stockées en toute sécurité dans une blockchain privée. La blockchain comprenait des informations sur le dernier utilisateur du scooter, la durée d'utilisation, le trajet emprunté et des informations personnelles, accessibles uniquement au personnel autorisé au sein de l'entreprise. Pour assurer la sécurité des données de la blockchain en cas de dommages sur ses serveurs internes, *e-Scooter* a décidé d'utiliser un service blockchain proposé par *NQS*. *NQS a* fourni une solution blockchain facile à construire et évolutive qui a permis *à e-Scooter* de mettre en œuvre facilement une forme rapide, centralisée, immuable et vérifiable de suivi de sa flotte de trottinettes.

En outre, *e-Scooter* a mis en œuvre la mesure 5.29 *Sécurité de l'information pendant la perturbation* de l'annexe A de la norme ISO/IEC 27001 afin de renforcer sa capacité à gérer et à se remettre des incidents, d'assurer la continuité opérationnelle et de renforcer sa résilience globale face aux perturbations. Enfin, pour régler le problème avec les codes QR, l'entreprise a décidé de sceller les codes QR derrière une couche plastique afin que les codes ne puissent plus être supprimés.

Dans le cadre de la mise en œuvre du SMSI, *e-Scooter* a effectué un audit interne au cours de laquelle l'auditeur interne a examiné le processus d'évaluation du risque mené par Lenny. L'auditeur a examiné l'analyse du risque documentée et discuté des vulnérabilités identifiées avec le département de production de *LING*. L'auditeur a

estimé que la réponse de l'entreprise aux résultats de l'évaluation du risque était adéquate. Notamment, la décision *d'e-Scooter* de concevoir une enceinte plus sécurisée pour la carte mère et de mettre en place des capteurs supplémentaires pour prévenir le vol et les dommages a montré son dévouement à la gestion proactive des risques. L'auditeur interne a également évalué l'efficacité de la mise en œuvre de la blockchain, concluant qu'elle offrait une couche supplémentaire de protection contre les dommages potentiels aux serveurs internes.

En outre, les mesures de sécurité mises en place par l'entreprise pour protéger les données des clients, telles que l'encouragement des utilisateurs à prendre des photos de trottinettes garées et l'étanchéité des codes QR derrière une couche plastique, ont démontré l'engagement d'*e-Scooter* à protéger les intérêts des clients et à garantir une utilisation responsable.

Tout en évaluant le programme de formation et de sensibilisation de l'entreprise, l'auditeur interne a découvert que *l'e-Scooter* n'avait dispensé de formation en sécurité de l'information qu'à l'équipe de développement logiciel. L'auditeur a estimé que le manque d'activités de formation et de sensibilisation pour les autres employés pouvait entraîner d'importantes vulnérabilités au sein des opérations de l'entreprise, comme le fait que les employés ne réussissent pas à prévenir les violations de la sécurité de l'information ou à répondre aux cyberattaques.

IV. Architecture des systèmes informatiques et description du réseau

e-Scooter dispose de deux serveurs dans son infrastructure réseau interne. Le premier est le serveur DB utilisé pour stocker les données de l'entreprise, telles que les informations stockées par le département des ressources humaines, le service de comptabilité, etc. Le second est utilisé par l'équipe de développement du logiciel pour accéder au code source des versions précédentes de l'application, ainsi qu'au code de la version actuelle. Grâce à ce serveur, l'équipe de développement logiciel passe en revue l'ancien code lors de l'ajout de nouvelles fonctionnalités et teste tout code avant le lancement.

e-Scooter dispose également de deux serveurs cloud. Le serveur principal est utilisé pour gérer les opérations back-end de l'application, gérer le trafic généré par les utilisateurs et stocker les données des utilisateurs. L'autre serveur cloud est le serveur cloud de la blockchain, qui stocke toutes les informations qui sont transmises par les capteurs des trottinettes à la blockchain. Ce service de blockchain cloud est proposé par *NQS,* et il communique avec le serveur de développement interne d'*e-Scooter* via une interface API.

L'équipe de développement logiciel d'*e-Scooter* apporte des modifications fréquentes à la base de données de développement, car elle est utilisée quotidiennement. Lorsqu'une version finale de l'application est prête à être testée avec des données réelles provenant de la base de données de blockchain, une demande est adressée au directeur de la sécurité de l'information pour obtenir une confirmation sur l'utilisation des données stockées dans la blockchain. L'accès aux données est donné au cas par cas, car il n'existe pas de méthode formelle établie. Cependant, à condition que certains changements de maintenance soient faits quotidiennement, les développeurs n'ont pas besoin de l'approbation du directeur de la sécurité de l'information. Ces changements comprennent les mises à jour de la version finale de l'application qui n'ont rien à voir avec les données de la blockchain.

Comme indiqué dans la politique de sécurité de l'information de l'entreprise, les développeurs doivent fréquemment sauvegarder leur code dans la base de données. Toutefois, cette pratique est fortement négligée par l'équipe de développement. Une fois l'application testée, l'approbation du directeur de la technologie est requise avant que la nouvelle version de l'application ne soit téléchargée sur le serveur cloud. Les nouvelles versions de l'application sont généralement accompagnées de mises à jour du back-end du serveur cloud. Lorsque des modifications surviennent, ce serveur et ses bases de données s'arrêtent pendant une période pouvant aller jusqu'à 10 minutes. Les utilisateurs sont informés que l'application est en cours de maintenance pendant cette

période. Ces modifications sont apportées lorsque le trafic de l'application est le plus faible, généralement entre 04 h 00 et 05 h 00.

Figure 1 : Structure des applications cloud

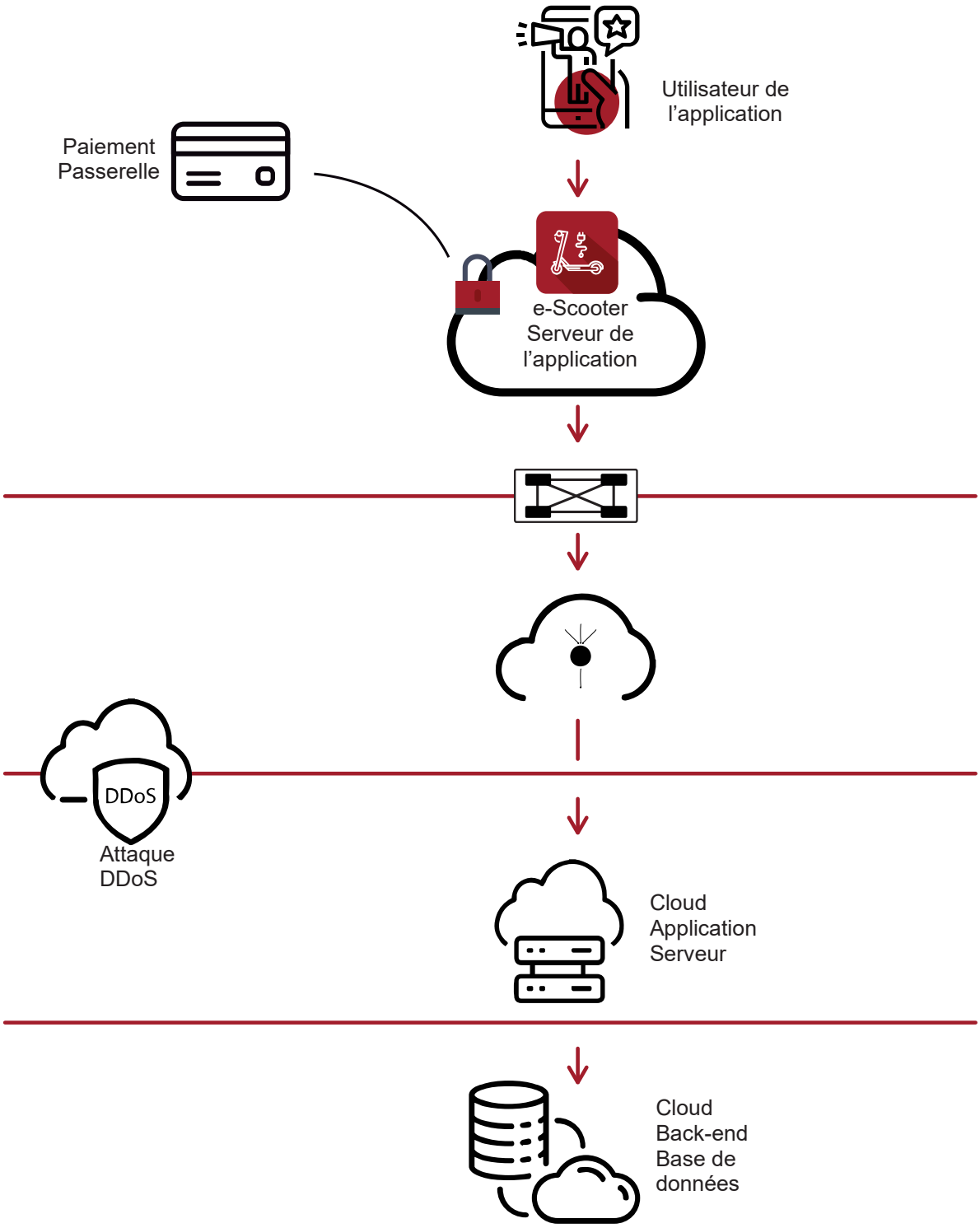

Figure 2 : Infrastructure locale