IMPORTANT - Récent incident cybernétique

Le groupe FTI a récemment été victime d'une cyberattaque qui a entraîné le cryptage de certains serveurs et fichiers sur le réseau du groupe. Meeting Point Hotel Management Malta Limited, la société qui gère le LABRANDA Riviera Hotel & Spa à Mellieha, Malte, est l'une des nombreuses entités dans le monde qui a été touchée par cette attaque.

Les auteurs de l'attaque avaient menacé de publier les données dont ils prétendaient être en possession. A ce stade, il était impossible de déterminer si cela était vrai ou non. Il s'avère maintenant que ces auteurs ont effectivement commencé à publier, en ligne, les données de certaines entités du Groupe FTI, dont celles de LABRANDA Riviera Hotel & Spa. C'est pour cette raison que nous avons jugé prudent de faire cette communication publique - malgré le fait qu'une enquête à l'échelle du groupe soit toujours en cours.

Avant tout, nous tenons à vous assurer que nous faisons tout ce qui est en notre pouvoir pour limiter au maximum les conséquences potentielles pour les personnes concernées.

Que vous ayez été affecté par une éventuelle publication ou seulement par le cryptage, nous souhaitons vous fournir quelques informations sur l'incident afin que vous puissiez comprendre ce qui s'est passé, dans quelle mesure vous avez pu être affecté, comment nous avons réagi et quelles mesures supplémentaires peuvent être prises pour protéger vos données.

Que s'est-il passé ?

Le 28 octobre 2021, nous avons été alertés par nos collègues étrangers d'un incident affectant les systèmes informatiques internes du groupe FTI, sur lesquels nous stockons également des données. FTI a rapidement mis en place des protocoles de réponse, lancé une enquête avec l'aide d'experts tiers en cybersécurité et en médecine légale, et mis en œuvre des plans de continuité des activités afin de minimiser les perturbations pour nous et nos clients et d'assurer la sécurité continue de nos systèmes. FTI a travaillé avec des experts pour contenir et corriger complètement l'incident, ainsi que pour fournir des recommandations pour renforcer notre position de sécurité contre les menaces potentielles futures. Ce travail est en cours à pleine vitesse depuis le 28 octobre 2021.

Le groupe FTI a immédiatement publié un communiqué de presse pour alerter le grand public sur le fait que nous avions été attaqués (en tant que groupe).

Des communications à l'échelle du groupe ont également été envoyées aux employés du monde entier le 28 octobre 2021, et à partir du 1er novembre 2021 à intervalles réguliers.

Sans attendre les résultats de l'enquête, et par précaution, nous avons immédiatement notifié la situation au commissaire maltais à l'information et à la protection des données (IDPC) avec les informations dont nous disposions à ce moment-là. Nous avons accusé réception de cette notification le 31 octobre 2021.

Depuis lors, l'enquête en cours a commencé à révéler quelles données du LABRANDA Riviera Hotel & Spa ont été exfiltrées par les auteurs de l'infraction.

Quelles sont les informations concernées ?

Nous tenons à souligner que nous n'avons aucune preuve que toutes les données personnelles stockées chez nous ont été ou sont utilisées à mauvais escient. Au contraire, il y a de fortes indications que seule une partie des données stockées chez nous a été volée.

Les principales catégories de personnes concernées sont nos employés - actuels et passés. Certains de nos clients et tiers (principalement des fournisseurs et des partenaires) ont également été touchés, mais dans une mesure bien moindre. D'après ce que nous avons vu jusqu'à présent, les détails des fournisseurs et des partenaires se limitent aux détails des signataires lorsqu'ils agissent en représentation d'une entreprise.

Les données personnelles de nos employés qui ont été affectées par l'incident pourraient être toutes les données qui nous ont été fournies ou que nous avons générées au cours de la relation de travail, par exemple le dossier personnel de l'employé. Si vous étiez ou êtes employé par nous, il peut s'agir de votre nom complet, de votre numéro de téléphone, de votre adresse électronique et de votre adresse personnelle, de votre date de naissance, de vos coordonnées bancaires à des fins de paie, de votre numéro de sécurité nationale/identité et de vos CV (s'ils sont encore dans le dossier). Si vous nous avez également fourni des copies de vos documents d'identité, ceux-ci peuvent également être affectés. Dans certains cas très limités, il peut également s'agir de photos figurant dans votre dossier personnel et d'événements liés au bureau.

Bien que nous prenions diverses précautions pour minimiser les données personnelles que nous traitons, par exemple en rédigeant les dossiers de congé de maladie des employés pour éviter de révéler des informations médicales et en traitant les plaintes/requêtes des clients par numéro de chambre plutôt qu'en utilisant le nom et le prénom du ou des clients, il y a inévitablement des occasions où des individus spécifiques sont identifiables. À cet égard, bien que très peu de cas aient été trouvés, certaines données médicales (par exemple, des conditions chroniques génériques comme le mal de dos et l'asthme) peuvent avoir été exfiltrées par les auteurs.

Nous souhaitons rassurer nos clients sur le fait que notre système de réservation se trouve sur un réseau distinct et que, par conséquent, la quantité de données volées concernant les clients est limitée par nature.

Comment avons-nous réagi à l'incident ?

Afin de protéger au mieux vos données et de limiter le risque d'incidents similaires à l'avenir, l'ensemble du groupe FTI a mis en place des mesures d'atténuation importantes immédiatement après avoir pris connaissance de l'incident, notamment en isolant notre réseau, en améliorant nos capacités de détection des intrusions et en renforçant nos mécanismes de réponse. Nous sommes également en étroite communication avec les autorités compétentes en matière de protection des données et d'enquête pour coordonner avec elles le traitement de l'incident et leur offrir notre entière coopération.

Que pourrait-il se passer avec vos données/quels sont les risques pour vous en particulier ?

- les attaquants ou les tiers qui ont obtenu vos données pourraient vous envoyer des e-mails avec des logiciels malveillants en pièce jointe. Si vous ouvrez les pièces jointes d'un tel e-mail, votre appareil final pourrait être contaminé par un malware.
- les attaquants ou les tiers pourraient vous contacter afin de vous faire chanter avec les données volées ou publiées (en particulier si vous êtes un de nos employés concernés, passé ou présent).
- si les attaquants ont obtenu des copies de vos cartes d'identité, il est possible que des copies de cartes d'identité illégalement falsifiées soient créées en les utilisant comme modèle. Nous n'avons connaissance que de quelques copies de cartes d'identité et de passeports qui ont été exfiltrées par les attaquants et, jusqu'à présent, aucun de ces documents de clients ne semble avoir été affecté.
- En utilisant le nom, les détails du compte et l'adresse électronique, ainsi que les informations que vous avez partagées avec nous (par exemple, vos loisirs et vos intérêts), les attaquants peuvent commettre une usurpation d'identité. Des marchandises pourraient être commandées ailleurs à vos frais et risques au détriment des sources de paiement qui y sont stockées. Cela est particulièrement vrai si vous utilisez le même mot de passe pour différents systèmes de boutique.

Que pouvez-vous faire ?

D'une manière générale et pour des raisons de bonnes pratiques, nous vous encourageons à rester vigilant face aux tentatives de phishing, y compris tout risque d'usurpation d'identité et de fraude. Il existe plusieurs mesures que vous pouvez prendre pour protéger vos informations personnelles, notamment celles décrites ci-dessous :

- protéger vos informations personnelles et signaler toute activité inhabituelle aux autorités compétentes (et/ou à nous si vous êtes un employé)
- utilisez des mots de passe complexes et changez-les souvent
- conservez vos mots de passe dans un endroit sûr
- évitez d'ouvrir les pièces jointes d'un e-mail qui vous semblent suspectes
- surveillez votre compte bancaire et signalez toute activité inhabituelle à votre banque.

La sécurité de vos données est une priorité absolue pour nous. Nous pouvons vous assurer que nous avons fait, et que nous continuerons à faire, tout ce qui est en notre pouvoir pour garantir la résilience permanente de nos systèmes et empêcher que ce type d'incident ne se reproduise.

Nous regrettons sincèrement que non seulement nous, sur qui l'attaque a été perpétrée, mais aussi nos employés et nos clients aient été mis dans cette position extrêmement désagréable. Nous comprenons que cette communication puisse susciter des inquiétudes et des questions supplémentaires. Par conséquent, si vous avez d'autres questions concernant cet avis, n'hésitez pas à nous contacter à l'adresse guestrelations.rivierahotel@labranda.com.

Nous vous remercions de votre collaboration et de votre soutien,

La gestion