WICHTIG - Zuletzter Cyber-Vorfall

Die FTI Group wurde vor kurzem Opfer eines Cyberangriffs, der zur Verschlüsselung bestimmter Server und Dateien im Netzwerk der Gruppe führte. Meeting Point Hotel Management Malta Limited, das Unternehmen, das das LABRANDA Riviera Hotel & Spa in Mellieha, Malta, verwaltet, war eines von mehreren Unternehmen auf der ganzen Welt, die von diesem Angriff betroffen waren.

Die Angreifer hatten damit gedroht, die Daten zu veröffentlichen, über die sie angeblich verfügten. Zu diesem Zeitpunkt war es unmöglich festzustellen, ob dies der Wahrheit entsprach oder nicht. Es hat sich nun herausgestellt, dass die Täter tatsächlich damit begonnen haben, die Daten einiger Unternehmen der FTI-Gruppe, darunter auch die von LABRANDA Riviera Hotel & Spa, online zu veröffentlichen. Aus diesem Grund hielten wir es für ratsam, diese Mitteilung zu veröffentlichen - trotz der Tatsache, dass eine gruppenweite Untersuchung noch im Gange ist.

Zuallererst möchten wir Ihnen versichern, dass wir alles in unserer Macht stehende tun, um die möglichen Folgen für die Betroffenen so gering wie möglich zu halten.

Unabhängig davon, ob Sie von einer möglichen Veröffentlichung oder nur von einer Verschlüsselung betroffen waren, möchten wir Ihnen einige Informationen über den Vorfall zur Verfügung stellen, damit Sie verstehen können, was passiert ist, in welchem Ausmaß Sie möglicherweise betroffen waren, wie wir reagiert haben und welche zusätzlichen Schritte wir zum Schutz Ihrer Daten unternommen haben.

Was ist passiert?

Am 28. Oktober 2021 wurden wir von unseren Kollegen im Ausland auf einen Vorfall aufmerksam gemacht, der die internen IT-Systeme der FTI Group betraf, auf denen auch wir Daten speichern. FTI leitete umgehend Reaktionsprotokolle ein, leitete eine Untersuchung mit Hilfe von externen Cybersicherheits- und Forensik Experten ein und führte Pläne zur Aufrechterhaltung des Geschäftsbetriebs ein, um die Unterbrechungen für uns und unsere Kunden zu minimieren und die kontinuierliche Sicherheit unserer Systeme zu gewährleisten. FTI arbeitete mit Experten zusammen, um den Vorfall vollständig einzudämmen und zu beheben sowie Empfehlungen zur Stärkung unserer Sicherheitslage gegen potenzielle zukünftige Bedrohungen zu geben. Die Arbeit daran läuft seit dem 28. Oktober 2021 auf Hochtouren.

Die FTI-Fraktion gab sofort eine Pressemitteilung heraus, in der sie die Öffentlichkeit darüber informierte, dass wir (als Gruppe) angegriffen worden waren.

Außerdem wurden am 28. Oktober 2021 und ab dem 1. November 2021 in regelmäßigen Abständen konzernweite Mitteilungen an die Mitarbeiter in aller Welt verschickt.

Ohne den Abschluss der Untersuchung abzuwarten, haben wir vorsichtshalber den maltesischen Datenschutzbeauftragten (IDPC) mit den uns zu diesem Zeitpunkt vorliegenden Informationen über die Situation informiert. Die Meldung wurde am 31. Oktober 2021 bestätigt.

Seitdem haben die laufenden Ermittlungen begonnen, um aufzudecken, welche Daten von LABRANDA Riviera Hotel & Spa von den Tätern infiltriert worden sind.

Um welche Informationen ging es?

Wir möchten betonen, dass wir keine Hinweise darauf haben, dass alle bei uns gespeicherten personenbezogenen Daten missbraucht wurden oder werden. Vielmehr gibt es starke Hinweise darauf, dass nur ein Teil der bei uns gespeicherten Daten gestohlen wurde.

Die Hauptkategorien der betroffenen Personen sind unsere Mitarbeiter - sowohl die derzeitigen als auch die früheren. Einige unserer Kunden und Dritte (hauptsächlich Lieferanten und Partner) waren ebenfalls betroffen, allerdings in weitaus geringerem Umfang. Nach dem, was wir bisher gesehen haben, beschränken sich die Angaben zu Lieferanten und Partnern auf Unterschriftsdaten, wenn sie in Vertretung eines Unternehmens handeln.

Bei den personenbezogenen Daten unserer Mitarbeiter, die von dem Vorfall betroffen sind, könnte es sich um alle Daten handeln, die uns im Rahmen des Arbeitsverhältnisses zur Verfügung gestellt oder von uns erzeugt wurden, z. B. die Personalakte des Mitarbeiters. Wenn Sie bei uns beschäftigt waren oder sind, könnte dies Ihren vollständigen Namen, Ihre Telefonnummer, Ihre E-Mail-Adresse und Ihre Privatanschrift, Ihr Geburtsdatum, Ihre Bankverbindung für die Gehaltsabrechnung, Ihre Sozialversicherungsnummer/Identifikationsnummer und Ihren Lebenslauf (sofern dieser noch in den Akten vorhanden war) umfassen. Wenn Sie uns auch Kopien Ihrer Ausweispapiere zur Verfügung gestellt haben, können diese ebenfalls betroffen sein. In einigen sehr begrenzten Fällen können auch Fotos in Ihrer Personalakte und von dienstlichen Veranstaltungen enthalten sein.

Obwohl wir verschiedene Vorsichtsmaßnahmen ergreifen, um die von uns verarbeiteten personenbezogenen Daten auf ein Minimum zu beschränken, z. B. durch Schwärzen der Krankenakten von Mitarbeitern, um die Offenlegung medizinischer Informationen zu vermeiden, und durch die Bearbeitung von Gästebeschwerden/-anfragen anhand der Zimmernummer und nicht anhand des Vor- und Nachnamens des/der Gäste(s), kommt es zwangsläufig vor, dass bestimmte Personen identifizierbar sind. In diesem Zusammenhang wurden zwar nur sehr wenige Fälle gefunden, aber einige medizinische Daten (z. B. allgemeine chronische Erkrankungen wie Rückenschmerzen und Asthma) könnten von den Tätern infiltriert worden sein.

Wir möchten unseren Kunden versichern, dass sich unser Buchungssystem in einem separaten Netzwerk befindet und dass die Menge der gestohlenen Kundendaten daher von begrenzter Natur ist.

Wie haben wir auf den Vorfall reagiert?

Um Ihre Daten bestmöglich zu schützen und das Risiko ähnlicher Vorfälle in der Zukunft zu begrenzen, hat die gesamte FTI-Gruppe unmittelbar nach Bekanntwerden des Vorfalls umfangreiche Maßnahmen zur Schadensbegrenzung eingeleitet, darunter die Isolierung unseres Netzwerks, die Verbesserung unserer Fähigkeiten zur Erkennung von Eindringlingen und die Stärkung unserer Reaktionsmechanismen. Wir stehen außerdem in engem Kontakt mit den zuständigen Datenschutz- und Ermittlungsbehörden, um die Behandlung des Vorfalls mit ihnen zu koordinieren und ihnen unsere volle Unterstützung anzubieten.

Was könnte mit Ihren Daten passieren/welche Risiken bestehen insbesondere für Sie?

- die Angreifer oder Dritte, die Ihre Daten erlangt haben, könnten Ihnen E-Mails mit Schadsoftware im Anhang schicken. Wenn Sie die Anhänge einer solchen E-Mail öffnen, könnte Ihr Endgerät mit Schadsoftware verseucht werden.
- die Angreifer oder Dritte Sie kontaktieren könnten, um Sie mit den gestohlenen oder veröffentlichten Daten zu erpressen (insbesondere wenn Sie ein betroffener ehemaliger oder aktueller Mitarbeiter von uns sind).
- wenn die Angreifer Kopien Ihrer Ausweise erlangt haben, ist es möglich, dass mit diesen als Vorlage illegal gefälschte Ausweiskopien erstellt werden. Uns sind nur wenige Kopien von Personalausweisen und Reisepässen bekannt, die von den Angreifern infiltriert wurden, und bisher scheinen keine derartigen Dokumente von Kunden betroffen zu sein.
- unter Verwendung des Namens, der Kontodaten und der E-Mail-Adresse sowie der Informationen, die Sie uns mitgeteilt haben (z. B. Ihre Hobbys und Interessen), können die Angreifer Identitätsdiebstahl begehen. Waren könnten auf Ihre Kosten und Gefahr zum Nachteil der dort gespeicherten Zahlungsquellen anderswo bestellt werden. Dies gilt insbesondere, wenn Sie dasselbe Passwort für verschiedene Shopsysteme verwenden.

Was können Sie tun?

Generell empfehlen wir Ihnen, wachsam gegenüber Phishing-Versuchen und dem Risiko von Identitätsdiebstahl und Betrug zu sein. Es gibt verschiedene Maßnahmen, die Sie ergreifen können, um Ihre persönlichen Daten zu schützen, einschließlich der unten aufgeführten:

- schützen Sie Ihre persönlichen Daten und melden Sie jede ungewöhnliche Aktivität den zuständigen Behörden (und/oder uns, wenn Sie ein Mitarbeiter sind)
- verwenden Sie komplexe Passwörter und ändern Sie diese häufig
- bewahren Sie Ihre Passwörter an einem sicheren Ort auf
- vermeiden Sie das Öffnen von E-Mail-Anhängen, die verdächtig aussehen
- Überwachen Sie Ihr Bankkonto und melden Sie Ihrer Bank jede ungewöhnliche Aktivität.

Die Sicherheit Ihrer Daten hat für uns höchste Priorität. Wir können Ihnen versichern, dass wir alles in unserer Macht Stehende getan haben und weiterhin tun werden, um die ständige Widerstandsfähigkeit unserer Systeme zu gewährleisten und zu verhindern, dass sich ein derartiger Vorfall wiederholt.

Wir bedauern aufrichtig, dass nicht nur wir, auf die der Angriff verübt wurde, sondern auch unsere Mitarbeiter und Kunden in diese äußerst unangenehme Lage geraten sind. Wir sind uns darüber im Klaren, dass diese Mitteilung einige Bedenken und weitere Fragen aufwerfen könnte. Sollten Sie daher weitere Fragen zu dieser Mitteilung haben, können Sie sich gerne an uns wenden: guestrelations.rivierahotel@labranda.com.

Wir danken Ihnen für Ihre Mitarbeit und Unterstützung,

Das Management