

Informationen über den Cyberangriff auf Prinsotel am 16. Mai

1. Allgemeine Beschreibung und Zeitpunkt des Vorfalles

Am 16.05.24 um 8.15 Uhr entdeckten wir in der Zentrale von Prinz Hoteles SA in der C/Ter 27 in Palma, die die PRINSOTEL-Hotels (La Dorada, La Pineda, Alba, Mal Pas und La Caleta) verwaltet, einen Malware-Angriff (Ransomware), der alle Server des Unternehmens blockierte und ankündigte, dass sie unsere Daten verschlüsselt hätten.

Ein Cybersecurity-Expertendienst wurde beauftragt, die Eindämmung, Sanierung und forensische Analyse zu verwalten. Nach der Analyse der von dem Angriff betroffenen Geräte konnten wir nachweisen, dass ein Teil der entwendeten Daten exfiltriert und ein Teil in verschiedenen cyberkriminellen Gruppen veröffentlicht wurde.

2. Beschreibung der betroffenen personenbezogenen Daten und Informationen

Bitte beachten Sie, dass das Technologieunternehmen, das uns nach dem Vorfall begleitet hat, in der Lage war, unter den gestohlenen Daten zu verifizieren: personenbezogene Daten von Kunden und Nutzern von PRINSOTEL, insbesondere: Name, Vorname, Adresse, Personalausweis, Reisepass, Telefon, E-Mail. Andererseits waren auch Unternehmensdaten von PRINSOTEL betroffen. **In keinem Fall gibt es Hinweise darauf, dass Finanzdaten oder Passwörter gestohlen wurden.**

3. Zusammenfassung der bisher durchgeführten Maßnahmen zur Eindämmung möglicher Schäden

Sobald PRINSOTEL davon erfuhr, setzte es einen Reaktionsplan um, der die Einbindung eines technischen Expertenteams vorsah, um die Quelle der Sicherheitslücke zu identifizieren und den Angriff einzudämmen, was sofort der Guardia Civil (zur Weiterleitung an die zentrale technologische Ermittlungsbrigade der nationalen Polizei) sowie der spanischen Datenschutzbehörde mitgeteilt wurde.

PRINSOTEL richtete einen Krisenausschuss aus Fachleuten ein, um den Vorfall einzudämmen und die gesamte Kommunikation mit den Betroffenen zu leiten, damit diese jederzeit über den Vorfall informiert waren. Der Vorfall wurde inzwischen behoben und Prinsotel hat einen detaillierten Aktionsplan, um ähnliche Situationen in Zukunft zu vermeiden.

Sobald PRINSOTEL am 26. Juni von der Exfiltration erfuhr, schickte es den betroffenen Kunden und Nutzern per E-Mail detaillierte Informationen über den Vorfall mit ausführlichen Handlungsanweisungen, um zu verhindern, dass sie direkt von betrügerischem Verhalten betroffen sind.

Der Vorfall ist derzeit unter Kontrolle, und Prinsotel hat einen detaillierten Aktionsplan aufgestellt, um ähnliche Situationen in Zukunft zu vermeiden. Zu den weiteren Maßnahmen dieses Aktionsplans gehört die Einrichtung eines Dienstes zur Überwachung und Verwaltung von Sicherheitsvorfällen durch ein SOC, das die wichtigsten Sicherheitssysteme des Unternehmens mit dem definierten SIEM integriert. Dieser Dienst wird Folgendes umfassen: (i) Überwachung von Perimetersystemen, AD, IDS/IPS, kritischen Servern, EDR und anderen. Ebenso wird dieser Dienst in der Lage sein, das EDR-System der Organisation zu verwalten, (ii) wird Prinsotel einen Schwachstellenmanagementdienst für die digitalen Systeme von Prinsotel (Server, Endpoints usw.) und eine Frühwarnung vor Bedrohungen bieten, mit dem Ziel, die kontinuierliche Sicherheit der Organisation zu stärken, und (iii) wird auch sichere Härtingsrichtlinien für bestehende Systeme umfassen.

4. Kontakt mit dem Datenschutzbeauftragten von PRINSOTEL

Für zusätzliche Fragen oder weitere Einzelheiten wenden Sie sich bitte an den Datenschutzbeauftragten unter dataprotection@prinsotel.es.

5. Ausübung der Datenschutzrechte

Sie können Ihre Datenschutzrechte unter der angegebenen E-Mail-Adresse ausüben: das Recht auf Zugang, Berichtigung, Löschung oder Übertragbarkeit Ihrer personenbezogenen Daten oder das Recht, einer bestimmten Verarbeitung Ihrer Daten zu widersprechen oder sie einzuschränken.

Weitere Informationen über die Verarbeitung Ihrer Daten (Zwecke der Verarbeitung, Datenkategorien, Herkunft und Empfänger der Daten, Aufbewahrungsfristen usw.) können Sie in unserer Datenschutzerklärung unter <https://www.prinsotel.com/es/politica-privacidad/> nachlesen.

6. Empfehlungen für Maßnahmen nach dem Vorfall

Infolge des Angriffs ist es unsere Pflicht, Ihnen einige Richtlinien zur Verfügung zu stellen, um die Sicherheit Ihrer personenbezogenen Daten zu gewährleisten:

1. Wir werden Sie **nie** und unter keinen Umständen auf elektronischem Wege nach Ihren Bankdaten fragen. Wenn Sie einen Anruf oder eine Nachricht erhalten, in der Sie um diese Art von Informationen gebeten werden, geben Sie diese NIEMALS weiter.
2. Wenn Sie PRINSOTEL-Werbung per E-Mail, SMS oder über soziale Netzwerke erhalten, **überprüfen Sie immer die Identität** des Absenders und klicken Sie im Zweifelsfall nie auf einen Link, dem Sie nicht vertrauen.
3. **Seien Sie vorsichtig bei Anrufen in unserem Namen** oder von einem unserer Hotels. Vergewissern Sie sich, dass es sich um einen Anruf von einem bekannten Anbieter handelt und geben Sie niemals private Daten an.

Darüber hinaus möchten wir Sie mit diesem Dokument vor allen möglichen Betrugsversuchen infolge des Vorfalls warnen, wie z. B. Phishing, Spear Phishing, Vishing, Smising, Pharming, Whaling ... usw., damit Sie sich vor diesen bösartigen Handlungen schützen können.

Diese Arten von Angriffen oder Betrügereien werden im Folgenden detailliert beschrieben, damit Sie ein anomales Verhalten erkennen und solche Aktionen verhindern können:

- **Phishing:** Phishing ist eine Social-Engineering-Technik, bei der E-Mails verschickt werden, die die Identität von Unternehmen oder öffentlichen Einrichtungen vortäuschen und personenbezogene Daten und Bankdaten des Benutzers anfordern. Über einen in der E-Mail enthaltenen Link wird versucht, den Benutzer auf eine betrügerische Website umzuleiten, auf der er seine Kreditkartennummer, Ausweisnummer, sein Passwort für den Zugang zum Online-Banking usw. eingeben muss.

Diese betrügerischen E-Mails enthalten oft das Logo oder das Markenbild des Unternehmens, können grammatikalische Fehler enthalten und versuchen manchmal,

Dringlichkeit und Angst zu vermitteln, um den Benutzer dazu zu bringen, die angeforderten Aktionen durchzuführen.

Eine Phishing-E-Mail kann auch einen Anhang enthalten, der mit bösartiger Software infiziert ist. Das Ziel dieser Schadsoftware ist es, den Computer des Benutzers zu infizieren und vertrauliche Informationen zu stehlen.

- **Spear Phishing:** Angreifer erstellen gefälschte E-Mails, Webseiten und sogar Kurznachrichten, die authentisch aussehen und von den Nutzern Anmeldedaten verlangen. Auf diese Weise gelangen Betrüger in den Besitz von Anmeldedaten für Online-Shops, soziale Netzwerke oder Cloud-Speicherplätze. Im schlimmsten Fall gelangen sie sogar in den Besitz von Bankinformationen oder Kreditkartendaten. Die Betrüger wissen, dass viele Nutzer die Passwortsicherheit nicht ernst nehmen und dasselbe Passwort für verschiedene Dienste verwenden. Auf diese Weise kann eine einfache Phishing-Website genutzt werden, um an sensible Daten zu gelangen, die auf dem digitalen Schwarzmarkt einen hohen wirtschaftlichen Wert haben.
- **Vishing:** Der Begriff Vishing setzt sich aus den Wörtern Voice und Phishing zusammen, weshalb es auch manchmal als Voice-Phishing bezeichnet wird. Bei dieser Technik nutzen die Angreifer die VoIP-Technologie (Voice over IP), um zahlreiche billige oder kostenlose betrügerische Anrufe zu tätigen und so an Codes, Passwörter oder Bankdaten des oft ahnungslosen Opfers zu gelangen.
- **Smishing:** Der Begriff Smishing ist eine Kombination aus SMS und Phishing. Ähnlich wie beim Phishing geben sich die Cyberkriminellen, die diese Nachrichten verschicken, als Vertreter eines vertrauenswürdigen Unternehmens oder einer Organisation aus, aber statt E-Mails verwenden sie SMS (Short Message Service). Diese mobilen Nachrichten dienen entweder dazu, das Opfer zur Preisgabe von Kontodaten aufzufordern oder Malware und Trojaner auf dem Gerät des Opfers ohne dessen Wissen zu installieren.
- **Pharming:** Pharming, eine Kombination aus den Wörtern "Phishing" und "Farming", ist ein dem Phishing ähnlicher Online-Betrug, bei dem der Website-Verkehr manipuliert und sensible Informationen gestohlen werden. Dabei handelt es sich um eine Art von Social-Engineering-Cyberangriff, bei dem Kriminelle Benutzer, die auf eine bestimmte Website zugreifen wollen, auf eine andere, gefälschte Website umleiten. Diese "gefälschten" Websites versuchen, die personenbezogenen Daten und Anmeldeinformationen des Opfers wie Passwörter, Sozialversicherungsnummern, Kontonummern usw. abzufangen, oder versuchen, Pharming-Malware auf dem Computer des Opfers zu installieren.
- **Whaling:** Ein Whaling-Angriff ist eine Methode, mit der Cyberkriminelle vorgeben, eine leitende Position in einem Unternehmen einzunehmen, um leitende Angestellte oder andere wichtige Personen innerhalb des Unternehmens direkt anzugreifen, um Geld zu stehlen, vertrauliche Informationen zu erlangen oder sich zu kriminellen Zwecken Zugang zu ihren Computersystemen zu verschaffen. Whaling, auch als CEO-Betrug bekannt, ähnelt insofern dem Phishing, als es Methoden wie Website- und E-Mail-Spoofing einsetzt, um das Opfer unter anderem dazu zu bringen, vertrauliche Informationen preiszugeben oder Geld zu überweisen.

Es tut uns sehr leid, dass wir in diese Situation geraten sind, aber Sie sollten wissen, dass Ihre Sorgenfreiheit für uns an erster Stelle steht und wir die Situation schnell und effizient in den Griff bekommen haben.

Prinsotel arbeitet bereits an dem nach dem Vorfall erstellten Aktionsplan und insbesondere an der Umsetzung verstärkter Sicherheitsmaßnahmen, um ähnliche Situationen in Zukunft zu vermeiden.