PRINSOTEL

Information about the cyberattack suffered in Prinsotel last 16 May

1. General description of the incident and timing

On 16-05-24 at 8:15 a.m. at the Headquarters of Prinz Hoteles SA, located at c/Ter 27 Palma, which manages the PRINSOTEL establishments (La Dorada, La Pineda, Alba, Mal Pas, and La Caleta), we detected a malware attack (ransomware) that blocked all the company's servers, announcing that they had encrypted our data.

We proceeded to contract an expert cybersecurity service, who were in charge of managing the containment, remediation, and forensic analysis processes. After the analysis carried out on the computers affected in the attack, we have also verified that part of the data that were hijacked has been exfiltrated and some have been published in different groups of cybercriminals.

2. Description of the affected data and personal data.

We inform you that the technology company that has assisted us after the incident has verified that the stolen data include: personal data of PRINSOTEL clients and users, specifically: name, surname, address, National Identity Document, passport, telephone, email. Additionally, it has also affected PRINSOTEL's corporate information. **In any case, there is no evidence that financial data or passwords have been stolen.**

3. Summary of the measures implemented so far to control the potential damage.

From the moment it became aware of this incident, PRINSOTEL set a response plan that involved the engagement of an expert technical team to identify the origin of the breach and contain the attack, which was immediately communicated to the Spanish Civil Guard (to be referred to the Central Technological Investigation Brigade of the National Police) and to the Spanish Data Protection Agency (AEPD).

PRINSOTEL created a crisis committee made up of expert professionals in order to contain the incident and manage all communications with those affected to keep them informed at all times of the incident. At present, the incident has been corrected and Prinsotel has a detailed action plan to prevent similar situations in the future.

As soon as PRINSOTEL became aware of the exfiltration, on 26 June, it sent affected clients and users, via email, detailed information about the incident, including detailed guidelines to prevent them from being directly affected by any fraudulent behaviour.

The incident is currently under control and Prinsotel has a detailed action plan to prevent similar situations in the future. The measures in this action plan include, among others, the implementation of a security incident monitoring and management service through a SOC that integrates the organisation's main security systems with the defined SIEM. This service will include: (i) the monitoring of perimeter systems, AD, IDS/IPS, critical servers, EDR, among others. Likewise, this service will be capable of managing the organisation's EDR system, (ii) it will provide Prinsotel with a vulnerability management service on Prinsotel's digital systems (servers, endpoints, etc.) and early warning of threats, with the aim of strengthening the organisation's continuous security, and (iii) it will also include secure hardening guides for existing systems.

PRINSOTEL

4. **Contact of PRINSOTEL's Data Protection Officer**

For any additional questions or further details about it, you can address the Data Protection Officer, contacting him through dataprotection@prinsotel.es.

5. **Exercise of data protection rights**

You can exercise the data protection rights that protect you: the right to access, rectify, delete, or request the portability of your personal data, or the right to object to or restrict certain processing of your data, at the specified email address.

You can obtain additional information on the processing of your data (purposes of processing, data categories, source and recipients of the data, retention periods, etc.) by consulting our privacy policy published at https://www.prinsotel.com/es/politica-privacidad/.

6. **Recommendations on how to act after the incident.**

As a result of the attack, it is our obligation to give you some guidelines to ensure the security of your personal data:

1. We will **never** and under no circumstances ask you for your bank details by electronic means. If you receive a call or message requesting this type of data, NEVER share it.

2. In case of receiving PRINSOTEL advertising by email, SMS, or social media, **always verify the identity** of the sender and, if in doubt, never click on any link that you do not trust.

3. **Beware of calls on our behalf** or from any of our hotels. Verify that it is a call from a known operator and again, never provide private data.

Additionally, we would like, through this document, to warn you of all possible fraud attempts that may be resulted from the incident, such as Phishing, Spear Phishing, Vishing, Smishing, Pharming, Whaling, etc. so that you can be aware of any of these malicious actions.

These types of attacks or frauds are detailed below so that you can identify any anomalous behaviour and prevent any of these actions:

- ***Phishing:*** Phishing is a social engineering technique that consists in sending emails that impersonate companies or public bodies and request personal and banking information from the user. Through a link included in the email, they try to redirect you to a fraudulent website to enter your credit card number, National Identity Document, password to access online banking, etc.

  These fraudulent emails usually include the logo or brand image of the entity, might contain grammatical errors, and sometimes try to convey urgency and fear so that the user will perform the actions they request.

  A phishing email can also include an attached file infected with malicious software. The goal of this malware is to infect the user's computer and steal their confidential information.

- ***Spear Phishing:*** Attackers create fake emails, web pages, and even short messages that look authentic and ask for users' login information. This is how scammers get hold of login details for online stores, social media, or cloud storage spaces. In the worst cases, they even obtain bank information or credit card details. Scammers know that there are many users who do not take password security seriously and who use the same password for different services. This way, with a simple phishing website, they can obtain sensitive data, that is, information that has a high economic value in the digital black market.

- ***Vishing:*** The term 'vishing' is a combination of the words 'voice' and 'phishing', which is why it is also sometimes called 'voice phishing'. With this technique, attackers use VoIP (voice over IP) technology to make numerous fraudulent calls, affordably or free of charge, and thus obtain codes, passwords, or bank details from the victim, who is usually unsuspicious.

- ***Smishing:*** The term 'smishing' comes from combining the elements of SMS and phishing. Similar to phishing, the cybercriminals who send these messages pose as representatives of a trusted company or organisation, only instead of emails, they use SMS (Short Message Service). These mobile messages are used either to urge the victim to reveal their account data, or to install malware and Trojans on their device without them noticing.

- ***Pharming:*** Pharming, a combination of the words 'phishing' and 'farming', is an online scam similar to phishing, in which a website's traffic is manipulated and sensitive information is stolen. This is a type of social engineering cyberattack in which criminals redirect users who try to access a specific website to a different, fake site. These fake sites intend to capture the victim's personal identification information and login credentials, such as passwords, social security numbers, account numbers, etc., or attempt to install pharming malware on their computer.

- ***Whaling:*** A whaling attack is a method used by cybercriminals to simulate holding senior positions in an organisation and thus directly attack senior executives or other important people within it, with the aim of stealing money, obtaining confidential information, or gaining access to their computer systems for criminal purposes. Whaling, also known as CEO fraud, is similar to phishing in that it uses methods, such as website and email spoofing, to trick the victim into revealing sensitive information or making money transfers, among other actions.

We are very sorry for this situation that has befallen us, but please, bear in mind that, for us, your peace of mind comes first and we have tackled and contained this situation quickly and effectively.

Prinsotel is already working on the action plan generated after the incident and, specifically, on the implementation of reinforced security measures to avoid similar situations in the future.