PRINSOTEL

Information sur la cyberattaque à Prinsotel du 16 mai dernier

1. Description générale et chronologie de l'incident

Le 16-05-24 à 8h 15 au siège de Prinz Hoteles SA, sise c/Ter 27 Palma (Espagne), société qui gère les établissements PRINSOTEL (La Dorada, La Pineda, Alba, Mal Pas et La Caleta), a été décelé une attaque de *malware* (*ramsomware*) qui a bloqué l'ensemble des serveurs du groupe, les attaquants annonçant qu'ils avaient crypté nos données.

Nous avons donc fait appel à un service d'experts en cybersécurité a été engagé pour gérer les processus de contention, de remédiation et d'analyse criminalistique. Après analyse des ordinateurs touchés par l'attaque, nous avons pu constater que certaines des données prises en otage avaient en fait été exfiltrées et que certaines d'entre-elles avaient à son tour été publiées par divers groupes cybercriminels.

2. Description des données et de informations personnelles concernées

Nous tenons à vous informer que la société technologique qui nous a accompagnés après l'incident a pu vérifier que parmi les données volées se trouvaient des coordonnées personnelles des clients et des utilisateurs de PRINSOTEL, à savoir : noms, prénoms, adresses, pièces d'identité, passeports, téléphones et adresses électroniques. D'autre part, l'attaque a également affecté les informations de la société PRINSOTEL. **Dans aucun cas, il n'a été prouvé que des données financières ou des mots de passe ont été volés.**

3. Récapitulatif des mesures mises en œuvre jusqu'à présent pour contrôle les éventuels dommages

Du moment où PRINSOTEL a eu connaissance de l'incident, nous avons mis en œuvre un plan de réponse engageant l'intervention d'une équipe technique experte dans le but d'identifier l'origine de la brèche et contenir l'attaque, qui a été communiquée d'immédiat aux autorités (Guardia Civil) (pour renvoi à la Brigade centrale d'investigation technologique de la police nationale), ainsi qu'à l'Agence espagnole de protection des données.

PRINSOTEL a mis en place un comité de crise composé d'experts professionnels dans le but de contenir l'incident et de gérer l'ensemble les communications avec les personnes concernées afin de les tenir informées à tout moment de l'incident. À l'heure actuelle l'incident a été résolu et Prinsotel dispose déjà d'un plan d'action détaillé afin d'éviter que des situations similaires ne se reproduisent.

Du moment où PRINSOTEL a eu connaissance de l'exfiltration, c'est à dire, le 26 juin, nous avons pris le soin d'adresser aux clients et utilisateurs concernés un courriel avec des informations détaillées sur l'incident ainsi qu'avec des instructions précises sur les mesures à prendre pour éviter qu'ils ne soient directement affectés par le comportement frauduleux.

À l'heure actuelle l'incident a été résolu et Prinsotel dispose déjà d'un plan d'action détaillé afin d'éviter que des situations similaires ne se reproduisent. Parmi les autres mesures de ce plan d'action se trouve la mise en place d'un service de surveillance et de gestion des incidents de sécurité par l'intermédiaire d'un SOC (*Security Operation Center*) qui intègre les principaux systèmes de sécurité de l'organisation avec le SIEM défini. Ce service comprendra : (i) surveillance des systèmes périmétriques, AD, IDS/IPS, serveurs critiques et EDR, entre autres. Ce service sera également en mesure de gérer le système EDR de l'organisation, (ii) il fournira à Prinsotel un service de gestion des vulnérabilités pour ses systèmes numériques (serveurs, endpoints, etc.) et d'alerte précoce en cas de menaces, dans le but de renforcer la sécurité

continue de l'organisation, et (iii) il inclura les lignes directrices en matière de durcissement sécurisé pour les systèmes existants.

4. **Contacter le délégué à la protection des données de PRINSOTEL**

Pour toute question ou précision complémentaire, veuillez contacter le délégué à la protection des données à l'adresse suivante dataprotection@prinsotel.es.

5. **Exercer ses droits en matière de protection des données**

Vous pouvez toujours exercer vos droits en matière de protection des données : droit d'accès, de rectification, d'effacement ou de portabilité de vos données personnelles ou droit d'opposition ou de limitation de certains traitements de vos données en écrivant à l'adresse électronique indiquée.

Pour des plus amples renseignements concernant le traitement de vos données (finalités du traitement, catégories de données, origine et destinataires des données, durée de conservation, etc.) consultez notre politique de confidentialité en vous rendant à l'adresse https://www.prinsotel.com/es/politica-privacidad/.

6. **Recommandations des actions à prendre après l'incident**

Suite à cette attaque, c'est notre obligation de vous fournir quelques instructions afin d'assurer la sécurité de vos données personnelles :

1. Nous **ne** vous demanderons, jamais et en **aucun** cas, vos coordonnées bancaires par voie électronique. Si vous recevez un appel ou un message vous demandant ce type de données, ne les partagez JAMAIS.

2. Si vous recevez de la publicité de PRINSOTEL par e-mail, SMS ou sur les réseaux sociaux, **vérifiez toujours l'identité** de l'expéditeur et, en cas de doute, ne cliquez jamais sur un lien qui vous semble douteux.

3. **Méfiez-vous des appels passés en notre nom** ou faites depuis l'un de nos hôtels. Vérifiez qu'il s'agit bien d'un appel venant d'un opérateur connu et, encore une fois, ne partagez jamais des données privées.

En outre, par ce document, nous souhaitons vous avertir de toutes les tentatives de fraude possibles à la suite de l'incident, telles que le *phishing, spear phishing, vishing, smishing, pharming, whaling*, et autres, pour que vous puissiez être vigilant face à ces actions malveillantes.

Vous trouverez ci-dessous les descriptions de ces types d'attaques ou fraudes afin que vous puissiez identifier tout comportement anormal et les éviter :

- ***Phishing :*** Le *phishing* (ou hameçonnage) est une technique d'ingénierie sociale consistant à envoyer des courriels en supplantant l'identité d'entreprises ou des organismes publics et en demandant à l'utilisateur ses coordonnées personnelles et bancaires. Au moyen d'un lien inclus dans le courriel, on tente de rediriger l'utilisateur vers un site web frauduleux pour lui amener à saisir son numéro de carte de crédit, son numéro de pièce d'identité, son mot de passe pour accéder aux services bancaires en ligne, etc.

  Ces courriels frauduleux comportent souvent le logo ou l'image de marque de l'entreprise ou organisme en question, peuvent contenir des erreurs grammaticales et tentent parfois

de faire passer un message d'urgence et de peur afin de contraindre l'utilisateur à faire les actions demandées.
Un courriel de *phishing* peut également comporter une pièce jointe infectée par un logiciel malveillant (*malware*). L'objectif de ce logiciel malveillant est d'infecter l'ordinateur de l'utilisateur et de lui voler des informations confidentielles.

- ***Spear phishing :*** Dans ce cas, les attaquants créent de faux courriels, de pages web fausses et même des messages courts faux qui semblent authentiques pour demander aux utilisateurs ses informations de connexion. C'est ainsi que les escrocs s'emparent des données d'accès aux boutiques en ligne, aux réseaux sociaux ou aux espaces de stockage en nuage. Dans le pire des cas, ils s'emparent même des informations bancaires ou des données de cartes de crédit. Les escrocs savent bien que bon nombre d'utilisateurs ne prennent pas la sécurité des mots de passe au sérieux et utilisent le même mot de passe pour différents services. Ainsi, une simple page web d'hameçonnage peut être utilisée pour obtenir des données sensibles, des informations qui ont un valeur économique élevé sur le marché noir numérique.

- ***Vishing :*** Le terme *vishing* est une combinaison des mots « voice » (voix) et « phishing » (hameçonnage), c'est pourquoi on parle aussi parfois de *voice phishing* (hameçonnage vocal). En se servant de cette technique, les attaquants utilisent la technologie VoIP (*Voice over IP*) pour passer de nombreux appels frauduleux gratuits ou très économiques afin d'obtenir des codes, des mots de passe ou des données bancaires de la victime qui, souvent, ne se doute de rien.

- ***Smishing :*** Le terme *smishing* est une combinaison des éléments SMS et *phishing*. Comme dans le cas du *phishing*, les cybercriminels qui envoient ces messages se font passer pour des représentants d'une entreprise ou d'une organisation de confiance, mais au lieu d'envoyer des courriels, ils envoient des SMS (*Short Message Service*). Ces messages servent soit à inciter la victime à partager les détails de son compte, soit à installer des logiciels malveillants et des chevaux de Troie sur l'appareil de la victime à son insu.

- ***Pharming :*** Le *pharming*, combinaison des mots « phishing » et « farming », est une escroquerie en ligne similaire au *phishing*, dans laquelle le trafic d'un site web est manipulé afin de voler des données sensibles. C'est ainsi un type de cyberattaque d'ingénierie sociale dans laquelle les criminels redirigent les utilisateurs qui tentent d'accéder à un site web donné vers un autre site différent et faux. Ces « faux » sites tentent de s'emparer des données personnelles identifiables et des identifiants de connexion de la victime, tels que ses mots de passe, ses numéros de sécurité sociale, ses numéros de compte bancaire, etc. ou bien tentent d'installer des logiciels malveillants de *pharming* sur l'ordinateur de la victime.

- ***Whaling :*** Le *whaling* est une méthode utilisée par les cybercriminels pour prétendre occuper des postes à responsabilité au sein d'une organisation afin d'attaquer directement des cadres supérieurs ou d'autres personnes importantes au sein de l'organisation, dans le but de voler de l'argent, d'obtenir des informations confidentielles ou d'accéder à leurs systèmes informatiques à des fins criminelles. Le *whaling*, également connu sous le nom de fraude au PDG (*CEO fraud*), est similaire au *phishing* en ce sens qu'il utilise des méthodes telles que l'usurpation de sites web et d'adresses électroniques pour tromper la victime et l'amener à révéler des informations confidentielles ou à effectuer des virements d'argent, entre autres.

PRINSOTEL

Nous sommes sincèrement désolés de cette situation, mais nous tenons à vous assurer que votre tranquillité d'esprit est notre priorité, et que nous avons abordé et maîtrisé cette situation de manière rapide et efficace.

Prinsotel travaille d’ores et déjà sur le plan d'action élaboré après l'incident et, en particulier, sur la mise en place de mesures de sécurité renforcées afin d'éviter que des situations similaires ne se reproduisent à l'avenir.