

### Tuvieron a un hotel de rehén: hackearon las cerraduras inteligentes de las habitaciones

Cibercriminales ingresaron por Internet y obtuvieron acceso al sistema centralizado



Hotel Romantik Seehotel Jaegerwirt

Era la apertura de la temporada de invierno para el Romantik Seehotel Jaegerwirt, un hotel 4 estrellas en los Alpes austríacos. Fue construido hace más de un siglo, pero el hotel incorporó en los últimos años tecnología de todo tipo, incluyendo un sistema centralizado para gestionar las llaves electrónicas de las puertas de las habitaciones.

Pero durante la inauguración de la temporada los 180 huéspedes encontraron, de un momento para el otro, que no podían abrir las puertas para entrar a sus habitaciones (aunque sí podían salir). Los empleados del hotel tampoco. Ninguna funcionaba.

Nadie supo qué sucedía, hasta que llegó un mensaje. Un grupo de criminales había tomado el control en forma remota de todo el sistema de gestión del hotel, y pedía una recompensa para rehabilitarlo, una forma más sofisticada del ransomware clásico. El monto era menor (1500 euros en bitcoins) así que la administración decidió pagarlo. Era la tercera vez que sufrían un ciberataque, según le admitió Christoph Brandstaetter, gerente del hotel, al sitio austríaco Thelocal.at.

Poner el sistema en marcha las veces anteriores les había costado mucho más dinero, así que aquí aceptaron pagarlo y en un instante recuperaron el funcionamiento de las llaves electrónicas para abrir las puertas.

### A todos nos puede pasar

El factor humano en la Seguridad de la Información, siempre presente.



No hace falta abundar en la información, que recientemente, tomó estado público: hackearon la cuenta de Twitter y de mail de la Ministra de Seguridad de la Nación.

Nos parece importante reflexionar sobre lo siguiente: Nadie cuestionó la herramienta, nadie adujo fallas en Twitter ni sospechó de la inse-

No hace falta abundar en la información que hace algunas semanas tomó estado público: hackearon la cuenta de Twitter y de mail de la ministra de Seguridad de la Nación.

Nos parece importante reflexionar sobre lo siguiente: nadie cuestionó la herramienta, nadie adujo fallas en Twitter ni sospechó de la inseguridad del medio. Por el contrario, rápidamente se expuso la fragilidad de los sistemas cuando se descuida el uso, ya sea por exposición del soporte (PC, celular, etc) o el uso de claves de

