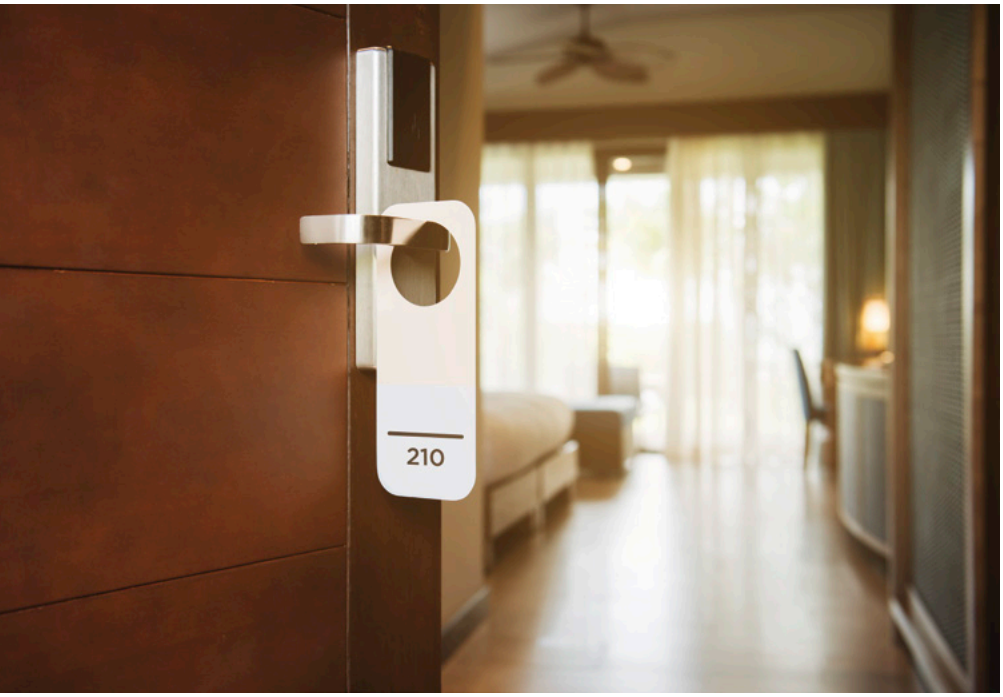
¿Por dónde pasa el futuro de los sistemas de autenticación y apertura segura?

Mario Mendiguren / Director de Marketing de Alai Secure

Hace apenas unos meses leíamos en la prensa digital el caso de un hotel de lujo en los Alpes, concretamente en la zona austriaca de Turrach, que fue atacado en plena temporada alta por un *ramsonware* que bloqueó las puertas de todas las habitaciones del hotel impidiendo a sus huéspedes poder entrar a sus alojamientos. Los secuestradores exigieron el pago del rescate en *bitcoins* como condición previa para enviarles la clave con la que desbloquear los archivos de sus sistemas. Al principio los dueños del hotel se cuestionaron el pago, algo completamente comprensible, pero al cabo de unos minutos, ante la avalancha de reclamaciones en la recepción del hotel, cambiaron rápidamente de opinión y procedieron al pago del rescate, sin más garantías que las que nos da el anonimato en Internet en estado puro. Al cabo de unas semanas, los intentos de nuevos secuestros se volvieron a suceder, si bien es verdad que ninguno culminó con éxito.

Esta anécdota no deja de ser, por desgracia, otro ejemplo más de hasta dónde pueden llegar los tentáculos de esta nueva ciberdelincuencia con la que cada vez estamos más familiarizados: secuestrar nada menos que un hotel completo, un ascensor en un edificio de oficinas, un autobús público lleno de gente en plena calle… El "qué" muchas veces es lo de menos. La nueva ciberdelincuencia no tiene límites. En muchos casos, lo único que quieren los ataques es demostrar qué se puede hacer, pero ¿qué pasaría si realmente se quisiera hacer daño?



Analicemos qué pudo fallar. El hotel, según su dirección general, dispone de un sistema centralizado de autenticación y apertura remota conectado con todas las habitaciones que se gestiona de forma remota y centralizada desde la recepción. A su vez, está integrado con el resto de los sistemas del hotel: medios de pago, reservas, etc. Cuenta con todas las medidas de seguridad básicas: antivirus, firewall... El personal que atiende la recepción asigna las habitaciones, habilita los accesos y gestiona los permisos de forma centralizada. Las cerraduras de las habitaciones no son de última generación, sino que llevan instaladas unos años, y hasta ahora eran más que suficientes para garantizar la seguridad física de los alojamientos frente a intentos de robo por parte de algún extraño. Lo que a primera vista parece un sistema bien diseñado y más o menos completo y seguro, adolece de algunas lagunas de seguridad que, si bien hasta hace unos meses/años eran más que suficientes, parecen completamente insuficientes frente a la llegada de esta nueva ciberdelincuencia.

:

Comunicaciones seguras

¿Qué podríamos haber hecho para mejorar la seguridad de nuestro sistema y evitar un caso como este? Hablemos de comunicaciones seguras. La primera medida sería la de mantener aislados el sistema de gestión de autenticación y apertura remota, así como todos los servicios relacionados con la seguridad del hotel. El objetivo es independizarlos completamente del acceso a Internet, indistintamente de cómo decidamos operar el servicio, ya sea en local o en la nube.

En el caso de que optemos por operar el servicio en la nube, la siguiente medida que deberíamos adoptar sería la de establecer una conexión securizada entre el sistema de gestión –situado en la recepción– y el sistema central de autenticación y apertura remota utilizando cualquiera de las tecnologías de tunelización de red disponibles en el mercado: VPN securizada, ADSL dedicada, línea dedicada… Esto nos va a permitir acotar el servicio y definir una serie de funcionalidades –limitadas y filtradas–, lo que nos posibilitará, además, poder monitorizar el tráfico que pase por el túnel y poder desplegar un sistema de alarmas que nos avise cada vez que se detecte un uso malintencionado o simplemente un comportamiento anómalo del servicio. Esto nos permitiría poder reaccionar rápidamente y tomar las medidas oportunas. El factor tiempo es clave, ya que disponer de toda la información del servicio al momento es decisivo para poder reaccionar inmediatamente.

Una tercera medida, menos sencilla y menos barata, pero que nos proporcionaría minimizar al máximo los efectos de un hipotético ataque, sería la de cambiar las cerraduras de todas las habitaciones del hotel por otras nuevas inteligentes de última generación mucho más seguras y con nuevas funcionalidades y, lo más importante, que no estén conectadas. ¿Qué quiere decir esto? Es necesario para garantizar la seguridad del servicio que las cerraduras que escojamos no estén conectadas a Internet. Estas cerraduras no conectadas no utilizan el protocolo IP, sino que utilizan tecnologías de radio de proximidad como Bluetooth, NFC, etcétera, lo que nos admitiría impedir un hackeo masivo que se llevara a cabo de forma remota desde Internet.

De esta manera, en el caso extremo de que se viera comprometida la seguridad de una cerradura, no afectaría al resto de las otras 180 de las que dispone actualmente el hotel y daría tiempo suficiente al personal a reaccionar y a tomar las medidas oportunas.

El uso del teléfono móvil se convierte en la antesala de cualquier sistema de autenticación y apertura remota

La cuarta medida, la más ambiciosa y segura, implica un cambio de filosofía del servicio un poco más profundo que pasaría por la modificación del soporte de apertura, cambiando las tarjetas de proximidad por el teléfono móvil, y el despliegue de un protocolo de autenticación y apertura seguro, además, cómo no, de la implementación de las medidas anteriores.

'Smartphone'

Adicionalmente, el *smartphone* juega un papel crítico al desempeñar una doble función: por un lado, de soporte para autenticarse y poder abrir, y por otro, de *gateway* entre la cerradura y el sistema central. De esta manera, la cerradura –no conectada– siempre sabrá qué clientes tienen permiso en cada momento. Cambiar las tarjetas o las mismas llaves físicas por el teléfono móvil a día de hoy puede implicar un cambio cultural y generacional, pero es la antesala de un futuro cada vez más próximo en cualquier sistema de autenticación y apertura remota.

Además del soporte necesitamos desplegar un protocolo de comunicaciones que cuente con el mayor nivel de seguridad y encriptación posible. Un soporte en el que las claves de autenticación nunca viajen por el aire y en el que se pueda llevar a cabo una doble autenticación mediante la que el sistema autentifica al dispositivo y el dispositivo autentifica a la vez al sistema. No se puede dar nunca el uno sin el otro. De esta forma podemos evitar los ataques del tipo *man in the middle*. Nunca podremos evitar que haya alguien escuchando la información que viaja por el aire, lo que si podremos es impedir que el hacker descubra la clave y pueda replicar el modelo.

Si a esto último sumamos las medidas comentadas al principio estaríamos en condiciones de decir que, a día de hoy, contamos con un sistema de autenticación y apertura remota seguro. ¿Podrían las centrales receptoras de eventos aplicar sus activos y su *know how* en la monitorización y gestión de este tipo de alarmas? S