

Best Western Statement Regarding Sunday Herald Data Theft Story

2008-08-26

This statement is intended to provide further detail on the largely erroneous story originated by The Sunday Herald newspaper in Scotland, concerning the breach of Best Western's Central Reservations System.

We can confirm that on August 21, 2008, three separate attempts were made via a single log-on ID to access the same data from a single hotel. The hotel in question is the 107-room Best Western Hotel am Schloss Kopenick in Berlin, Germany, where a Trojan horse virus was detected by the hotel's anti-virus software. The compromised log-in ID permitted access to reservations data for that property only. The log-in ID was immediately terminated, and the computer in question has been removed from use.

We can also confirm that we have been able to narrow down the number of customers affected by this breach to ten. We are currently contacting those customers and offering assistance as needed.

We are working with the FBI and international authorities to investigate further.

Points of note:

The compromised user ID permitted access only to the reservations at a single hotel, and there is no evidence of unauthorized access to data for any other Best Western hotel.

Best Western purges reservations data within seven days of guest departure, thereby limiting potential data exposure to (1) guests who departed up to one week prior to the exposure, (2) current guests, and (3) future guests of that particular hotel.

There is no evidence of any unauthorized access to any other customer data.

In the day-to-day conduct of our business, we comply with the Payment Card Industry (PCI) Data Security Standards (DSS). To maintain that compliance, Best Western maintains a secure network protected by firewalls and governed by a strong information security policy. We regularly test our systems and processes in an effort to protect customer information, and employ the services of industry-leading third-party firms to evaluate our safeguards. We also delete credit card information and all other personal information upon guest departure.

Given the nature of IT security, absent evidence of actual attempts to enter our system without authorization, Best Western's highest level of response must consist of the following: (1) to continue to monitor for such activity, (2) to assist law enforcement authorities and our credit card partners with their investigation, (3) to amplify our already stringent data security regime, which is of course compliant with PCI standards, (4) to reinforce best data protection practices at our 4000 worldwide hotels. We are actively engaged in all four of these areas, on behalf of our valued customers and member hotels.

We will release other critical information as it becomes available. Customers with concerns are encouraged to call Best Western Customer Care at US 800-528-1238.

This article comes from Hotel News Resource

<http://www.hotelnewsresource.com>

The URL for this story is:

<http://www.hotelnewsresource.com/article34266.html>

© 1998 - 2008 Nevistas and the author.

Brought to you by Hotel News Resource

Distribute your news on our Network

See what all the buzz is about at:

http://www.hotelnewsresource.com/Info-news_account_info.html