EXPRESS Hospitality
FORTNIGHTLY INSIGHT FOR THE HOSPITALITY TRADE

Printer Friendly Version

'The hospitality sector is a favourite target for cyber criminals'

The hotel industry that possesses sensitive data like customer credit card details and other financial transactions, is one of the most vulnerable sectors facing threats ranging from data breaches to Trojan attacks, states ***Govind Rammurthy****, CEO & MD, eScan.*
By Sudipta Dev

What are the data security threats that the hospitality sector is vulnerable to?

Hospitality businesses have a database of their staff and customers that includes their addresses, contact telephone numbers, email addresses, and credit or debit card details. Hence, just like any other sector, hospitality sector too remains as one of the popular targets accounting for 15 per cent of data breaches.

There are a number of frauds that hospitality sector may be vulnerable to. Majorly these scams are committed via internet or email. Credit card fraud is one of the most common scam faced by the industry, wherein financial details of customers are targeted. To steal the confidential information stored by the hotel of its customers, Man-in-the-Middle based attacks are carried out, intercepting the data traffic between the client system and the server.

To gain unauthorised access to confidential data, cyber criminals also use the phishing technique, that is an e-mail spoofing fraud attempt targeting a specific organisation in an effort to unwitting employees disclosing confidential information or lace their computer system with Trojans, so as, to further increase the attack footprint.

Other frequently used attack methods include SQL injection, wherein a database of the organisation is targeted through its corporate website. Through this technique, a security vulnerability in a website's software is exploited by injecting from the web form into the database of an application (like queries) to change the database content or dump the database information like credit card or passwords to the attacker.

Which are the most common attack techniques?

The most commonly used technique is remote-access application attacks that exploit the web

Govind Rammurthy

channels created by internal or external IT staffs/specialists. Such systems are lightly defended from external attacks and come with either- no password or feature common/easy to guess passwords.

In addition, hackers use Botnet technique to infect the computers that can be then controlled remotely for the commission of further criminal activities. With this, hackers can also initiate DoS attacks by sending a flood of traffic. This will make websites inaccessible to legitimate users. Moreover, hotel web servers may be compromised and malicious content hosted, effectively targeting the customers who frequently visit the website for online reservation and other tasks. This can result in the loss of reputation of the hotel.

According to Forrester Research, approximately 85 per cent of the security breaches involve internal employees. This happens due to an employee’s carelessness or unauthorised access to confidential information, laptop theft, password mismanagement, etc., resulting in a drastic revenue loss, legal liabilities, as well as affects the brand image.

Are these instances common in India?

Cyber crimes are not limited to any particular geographical location.

What are the most effective solutions for a hotel company to prevent such attacks?

A security solution that suffices all the security needs of the customer is the right solution. It must provide multilayered real-time protection to their network against the known, as well as zero-day threats.

The product should have an efficient scanner that even detects the zero-day vulnerabilities in the applications, network as well as operating system. It should include a firewall that efficiently filters the traffic that enters and exits the network. Network Access Control is also the necessary feature that prevents any unauthorised devices connecting to the network. Moreover, the solution should be capable of monitoring the network in real-time and identify as well as notify any malicious activity and even prevent it spreading in the network.

Are most hotel companies in the country, across all categories, aware of IT security?

Hospitality business involves customer credit card numbers, financial transactions, credit information and other sensitive data, due to which, it is one of the top most targeted sectors. Hence, majorly the entire sector is very much aware about the IT security. Moreover, with the increasing cyber crime, the awareness is increasing and the sector has started taking IT security as a serious issue.

How vulnerable are restaurant businesses (both standalone and chains)?

Standalone restaurants have a very small footprint with respect to intrusion, handful of people are allowed access to the PC and most

Indian Express Business Publications Division

of the time it is limited to access the Hotel Management Software, in their small group of interconnected computers. Their risk factor increases when external devices are attached or malicious sites are browsed, without their systems being protected.

However, the network takes the shape of a corporate network in case of chain restaurants/hotels, where every rule, which governs IT security, is picked from the handbook of hackers. These networks are susceptible to insider threats, data breaches, Trojans et al.

What according to you would be the most foolproof way on how the hospitality sector can deal with such risks in the future?

As mentioned earlier, the hospitality sector is the favourite target amongst cyber criminals. Hence, there is no single foolproof method, but a series of steps/basic precautions must be taken in order to protect financial loss, alongwith the reputation of the company.

- **Closed network:** no access to internet except for the intranet site and internal mails, with a special attention should be given to the Wi-Fi network services provided by the hotel to their customers.
- External devices viz. pen-drives, USB modems, etc., should have restricted usage on the systems being used the employees of the hotel.
- Adhering to the norms laid down for securing data/ databases e.g. PCI –DSS for storing CC information.
- Centralised management of the IT infrastructure vis-à-vis IT security, adherence to IT policies like patch updates, regular AV updates, access restriction and application control.

Information about your products for the hospitality industry.

In order to fulfil the security needs for standalone systems we have eScan Internet Security Suite that is easy-to-use and proactively secures the computer against security threats.

For medium sized networks, we have eScan Internet Security Suite for SMBs that has been especially designed focusing on the growing security needs of the small and medium businesses. It provides corporate level next generation protection to small and medium businesses from viruses, spyware, spam, phishing, hacking, data theft and Zero day threats with a very low cost of ownership and ensures business continuity. In case of large networks, we have eScan Corporate Edition/ eScan Enterprise Edition that effectively secures the large networks and provides Zero-Day Protection to both, servers and endpoints. It also includes eScan Management Console (EMC) with a secure web interface that facilitates dynamic security management of the server and endpoints in the large network.

FEEDBACK: We would love to hear from you -- what you like about our content, what you dont, and even how you think we can improve. Please send your feedback to: *editorial.eh@expressindia.com*