Hospitality Sector: New Target for Cyber Crime?
The Problem

Last year the hospitality industry experienced the most data security breaches of all market sectors. Hospitality businesses accounted for 38% of all data security breaches reported in 2010. When compared to 19% for financial services and 14% for retail businesses, this statistic is both alarming and revealing. What factors account for the dramatic increases in this sector? Why is this industry suddenly so vulnerable to attack? What can we do about it?

One of the primary reasons that the industry is fast becoming a favourite target for hackers is the vast amount of credit card data it processes, transmits and stores across their networks. Hotels specifically with their need to conduct charge backs or maintain customer data in their systems amass a huge amount of sensitive credit card data across their networks.

While other industries subscribe to the “less is more” approach continually cleanse their networks of card data – this approach is not operationally achievable in the hospitality sector. This and the fact that the hospitality industry is not known for stringent network security due to its penchant for outsourcing their ICT infrastructures has resulted in the hacking community’s recent recognition of the easy target they are.

When businesses outsource their ICT requirements, simple basic security defences such as well configured firewalls, logging and intrusion detection or prevention systems are often overlooked leaving these managed networks wide open to unauthorised and unrecorded access.

If security is considered and deployed, it’s usually after the fact or as the result of regulatory (Payment Card Industry Data Security Standard) or legislative (Data Protection Act) requirements. This “bolt on” network security approach is not as effective as “security by design” and does not result in the strongest defences against hackers.

If for example you wanted to build a fence to surround your property and keep trespassers out, you would build the strongest fence possible within your budget ensuring a design conducive to turning away intruders. But if your city or council came to you and told you to build a fence, you would only build it where told and design it to meet their requirements. This second fence surely wouldn’t be as effective as the first in preventing intruders. This quite simply illustrates the problem in the hospitality industry: if they have a fence at all – it is only there because they were told to build it by someone else. Hackers like intruders can spot a good fence or a bad one quite easily. This industry is fast getting a reputation for bad fencing.
In addition to credit card data, hackers target customer personal data for purposes of identity theft. Once again large volumes of personal information is processed, stored and transmitted in the hospitality industry with little or no understanding of its worth to hackers.

Personal data is extremely valuable to the hacker community. Why? To commit identity theft you need identity data. A person's name, date of birth, address and national identity number for example can be currently sold on the Internet for £1.00 per record. A customer data base then of some 5000 records can be sold for £5,000.00. Database theft is big business to hackers today with rewards reaped through both credit card and identity fraud pay outs.

While the hospitality industry recognises the value of detailed customer information in their efforts to provide world-class service (smoking/non-smoking, dietary habits or existing medical conditions), they do not understand that this same information may be valuable to hackers. Quite simply, they do not understand that data = cash to a hacker. Consequently, they do little to protect it.

The Solution

If you've read any information security white papers before you would have heard that there are no security silver bullets. Computer security is an oxymoron. There is no such thing as a secure network. No matter what you do, you cannot guarantee that your business will not experience breach. The most effective approach therefore is risk management.

The best you can do to prevent data breaches is to implement cost-effective processes to identify, minimise and manage the security threats to your business.

The Payment Card Industry (PCI) Data Security Standard (DSS) for instance should be implemented as a risk management framework. All the stated controls should be aligned to your business processes and objectives to be effective. It must not be implemented as a checklist. If you do, it will have little effect on preventing a breach.

The only real solution then is to implement a security program based on risk management principles instilling a clear understanding in your stakeholders of the value of the data. Data = cash
Practical Tips

Orthus has compiled a range of guidelines for the hospitality sector including advice on emerging technologies like data encryption and tokenisation, which would help secure card data when it is being moved or stored and make it simpler to achieve both security and compliance.

Retention of credit card data is a real and growing concern for the industry. On many occasions, card data in both physical format (till receipts etc.) and logical format (scanned copy of cards, electronic receipts in emails etc.) may have to be retained securely for future reference in case of charge back issues. Encrypting this sensitive data is a cost-effective solution and is mandated in international regulation and legislation.

Only store authentication data if you have a legitimate business need to do so. Decryption keys must not be stored on the local system unless access to the keys is controlled in a manner that is independent of operating system access control mechanisms (simple windows login for instance), and a separate encryption method must be implemented for removable media (Such as USB memory sticks and CD/DVDs).

When providing WiFi hotspots to guests, remember that a hotspot is an “open” network. Technically any device on the network can be accessed by any other device on the network. Whenever deploying a wireless hotspot try to:

- Limit user activity to web surfing only.
- Disable peer-to-peer networking, file sharing, and remote access protocols.
- Advise users to use a good personal firewall.
- Advise users not to use hotspots for online banking, bill paying, or for making purchases that require confidential information such as a credit card number.
- Ensure all your wireless infrastructure is up to date and patched.

Consider deploying wireless intrusion detection systems (IDS) which form a small but critical piece of the data security jigsaw puzzle alerting you to intrusions and attacks aimed at computers or networks. Also the usage of intrusion prevention systems (IPS) which both monitor and block malicious activity based on signatures. IDS/IPS can be highly effective as a defensive tool but both technologies need to be configured with great care and attention.

Vendor-supplied defaults for passwords or other security information must be changed for Property Management Systems (PMS) or Hotel Management Systems (HMS) and all point of sale (POS) payment systems. This is the central and core component in which cardholder data is stored, processed and transmitted to perform authorisation and settlement across other payment terminals in the network.
Each person with access to sensitive (card holder) data should be assigned a unique login ID. Also, a dual-factor authentication method for remote system access via the Internet should be implemented which would mitigate unauthorised access into PMS/HMS and POS payment systems. All access to network resources and cardholder data must be monitored at all times in order to track any anomalies and suspicious attack activity.

**Conclusion**

The Hospitality industry will continue to experience a rise in the number of data breaches until they begin to understand the value of the personal and financial data they process and implement an effective risk management framework to identify, minimise and manage the threats to their businesses.

Hackers have clearly set their sites on Level 4 Merchants in the Hospitality industry as “low hanging fruit” and the industry has done little to respond and change this perception. Until they do these breaches will increase. While the implementation of such things as PCI DSS is a good start – it must be used as a risk management framework and be customised to the business to be effective. Otherwise you are just ticking boxes and doing little to stop the breaches.

The statistics also show that the industry has overlooked the threat from within: authorised users who remove data account for a significant portion of the breaches. The insider is most likely to be from the Accounts or Customer Services Department, uses a mobile PC rather than a desktop computer and more often than not will copy the sensitive data to a memory stick and walk straight out of the front door with it. The data theft may take place at any time during the extended working day.

Until the industry accepts that almost half of all data losses are associated with authorised users and implement the necessary controls where they are most effective - between the user and the information - these losses will also continue.

Time to wake up. Information security must be implemented into your day-to-day business processes or your business will be the next statistic.

**About the Authors**

Orthus are a leading provider of a portfolio of innovative and independent “security as a service” (SaaS) solutions. A seasoned Qualified Security Assessor Company (QSAC) Orthus possess extensive expertise in solving compliance problems in the hospitality industry.

For more information on our services – including PCI DSS compliance programs - please visit http://www.orthus.com, call +44 (0) 203 170 8955, or email us at: info@orthus.com.