Trustwave®
Smart security on demand

HOSPITALITY TIP SHEET:

5 ESSENTIAL DATA SECURITY ACTIONS TO TAKE NOW

Hotels, restaurants, bars and cafés account for almost 33% of the data breach investigations carried out by Trustwave in 2013. Due to the complexity of such IT systems and high level of integration, the issue is around hundreds, and sometimes thousands of customer records easily compromised. And with customers sharing experiences on social media in real-time, one data breach can potentially turn away a whole segment of your audience in a blink of an eye.

In reality, attacks are increasing in volume and becoming more complex year on year. Hackers are targeting cardholder data and personally identifiable information (PII) that also has monetary value. Understandable that the high volume of payment cards used daily makes hospitality businesses an obvious target. Organised crime also targets your own business accounts, which can be drained overnight, if not secured properly.

With your business in mind, here is an easy 5-step tip sheet to help you assess the situation and setup a more secure environment starting today.

1. Start with PCI compliance, but keep the big picture in mind

To protect your customers and your brand image, a good place to start is the Payment Card Industry Data Security Standard (PCI DSS). The standard was established to help you protect cardholder data, but it is clear that maintaining compliance can be a challenge for a business as diverse as your organisation.

Start with reviewing your current PCI DSS scope and network segmentation diagrams and practices. Understand the new rules and how they will affect your approach to scope and segmentation

Penetration testing of your environment is another critical step in security and compliance to make sure no stone is unturned. The PCI council has expanded pen testing requirements to include any network segment that is near the cardholder data environment, and it expects expert testing. These and other actions improve the overall security of your business, so don't rely on just one or two measurements against risk. Rather, view them as part of a bigger plan for protecting your bottom line.

Learn more about latest requirements here.

2. Get better at passwords, and change them regularly

Cracking passwords is one of the easiest ways to get into your system. To reduce the risk you need to educate users of your systems to systematically select longer "passphrases".

Passwords that contain at least 8 characters, include letters and numbers are proven to be less predictable and far more difficult to crack. Also, make sure you use different passwords for all of your systems.

Strong password

"G00dLuckGuessingTh1sP@ssword"

instead of weak

"Password1!"

In addition, organisations should consider two-factor authentication for employees who access the network. This forces users to verify their identity with information other than simply their username and password, like a unique code sent to their mobile. IT administrators can do their part to mitigate cracking success by using unique, random salts when hashing stored passwords.

3. Avoid malware risk by educating your staff

The biggest challenge for many organisations is to trust but validate when it comes to their own staff. Following all the rules all the time is unrealistic, so you might want to consider a layered approach, which combines having protecting technologies installed with giving your employees the know-how to protect your data and network from malware.

59% of malicious spam comes from attachments and 41% from links
(Trustwave's SpiderLabs research)

Hospitality organisations servicing customers need to perform regular education training as well as protect users from themselves with technologies that guard against zero-day exploits, targeted malware and blended threats.

Even such simple rules like avoiding clicking on suspicious links on social media or opening suspicious attachments help. Also ensure you are running updated anti-virus on all computers, and doing regular scans and intrusion prevention.

Golden rule: If you weren't expecting an email that contains a link or an attachment, don't click on or open it.

4. Validate third-party applications before implementing

According to our 2014 Trustwave Global Security Report, 85% of the exploits detected were of third-party plug-ins, including Oracle Java and Adobe Acrobat, Reader and Flash.

In addition to having complex, flat networks that are easily exposed to potential compromise, franchise models and outsourcing are also common weaknesses in the hospitality industry. How to approach this?

First, define criteria for acceptably safe third-party apps that meet your standards and also satisfy compliance requirements. Then, work with partners and vendors to test their apps. Don't forget to ask numerous questions and follow-through to create a mature policy that requires providers to agree to follow these policies and guidelines. In addition, formalise and unify your patching efforts to reduce risk of damage for your brand and customer experience you offer.

Find out more tips for securely using third-party applications.

5. Secure your network through collaboration

It always takes a team effort to secure a large, complex network like yours. There are three groups of people that must be involved and items they need to keep in mind: IT managers and CISOs, application and database managers and senior management. Although they have different interests within organisations, a joint effort will help all of them reach their goals.

I we look at IT managers, they are often dealing with a variety of day-to-day tasks, and as they fall short on time and resource, this department would benefit greatly from outsourcing some of the security tasks with a trusted vendor. And this can be a much easier cost to absorb for the business, if the senior management is in line and understands how outsourcing can contribute to reducing risks and keeping revenue and brand protected from the growing IT threats.

On top of that, application and database managers need to work closely with all the stakeholders mentioned above, because there is a need to understand the bigger picture behind security, and how it influences overall business performance.

Needless to say that many business fall short on resource when it comes to facing organised crime. This is when it makes sense to partner with an external MSS provider, who will help you manage your security at all angles from day one. And this without you hiring and training additional staff.

Bonus Tip: monitoring as a core protecting action

To increase your ability to self-detect it is important to monitor access to critical assets and critical file changes to ensure you can identify a breach. Many companies don't monitor file changes using file integrity monitoring and therefore don't spot unusual development activity in order to assess whether it is routine application maintenance or a hacker planting malware.

The longer it takes to contain a breach, the more a business is at risk of being accused of failing to fulfil its security responsibilities and exposes itself to greater financial risk and liability. In the UK, the Information Commissioner's Office can issue fines of up to £500,000 for a data breach.

That is why we hope that with this tip sheet you take action today for assessing your organisation's state of security and start tapping into the latest risk prevention trends.