Security Alert for Businesses in the Hotel, Motel and Lodging Industries

Introduction

Many merchants in the hospitality industry operate multiple properties. Insecure network connections between these properties, in conjunction with poor security controls, can allow a single-site compromise to easily spread to additional properties.

This security alert addresses recent threats to the hotel, motel and lodging industries as observed by Trustwave over the past six months.

Today's Critical Data Security Issues in the Hospitality Industry

The results of Trustwave's investigations indicate common deficiencies within the hospitality industry that contributed significantly to the compromise of payment card data. The combination of default/weak system passwords, insecure remote-access applications and improper firewalling allowed attackers access to multiple systems within the hospitality network.

Trustwave also found that many of the systems analyzed in these investigations stored magnetic stripe data due to the use of non-compliant processing systems. Many of the breaches involved the use of malware that allowed attackers to steal cardholder data even when that data was not written to disk (i.e., stored or saved). This is concerning because it allows for the theft of cardholder data even from organizations that use payment applications that comply with Visa's Payment Application Best Practices (PABP) or the Payment Application Data Security Standard (PA-DSS). Though in the cases seen by Trustwave, those PA-DSS compliant payment systems were not configured in accordance with the PCI DSS.

However, it's important to note that the organizations that fell victim to this technique lacked certain controls needed to comply with the PCI DSS. Below are eight actions that Trustwave recommends businesses in the hospitality industry take immediately to protect their networks from this technique.

1. **Establish a firewall configuration that properly filters ingress and egress traffic between the processing environment and untrusted networks:** An untrusted network is not limited to just the Internet. As stated in the PCI DSS version 1.2, "An 'untrusted network' is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage."

2. **Upgrade to a PA-DSS validated payment application and ensure that it is configured in accordance with the PCI DSS:** While a PA-DSS validated application does not ensure full PCI compliance, a properly configured PA-DSS approved payment application does provide the foundation for compliance.

3. **Periodically re-boot payment systems to clear volatile memory:** Many malicious programs today are memory-resident (i.e., evidence of the program's presence does not exist on disk). A simple reboot will potentially deactivate malicious memory-resident programs from the system. Also, consider implementing a secure-wiping application to routinely clear the contents of the page file (also referred to as the swap file).

4. **Enforce a strong username/password policy for system access:** Review all processing systems to ensure default vendor-supplied credentials are not in use. Trustwave also recommends that usernames and passwords be unique to each local site to prevent the potential spread of a breach to multiple locations.

Trustwave®
Information Security & Compliance

5. **Properly secure remote access applications:** Remote access applications should be disabled when not in use or secured using two-factor authentication. Remote access permissions should only be granted to specific accounts as required.

6. **Ensure system activity logs are reviewed daily:** The proper review of system activity logs is instrumental in the detection of malicious events. Breaches often go undetected because system activity logs were not reviewed on a consistent basis.

7. **Disable Windows file sharing if not required. If required, grant access to shared folders only to specific user accounts with strong passwords:** Malicious software often spreads via insecure system shares. The disabling of insecure system shares can help with containment.

8. **Ensure anti-virus/anti-malware software is installed and updated consistently:** In order to properly protect the processing environment, anti-virus/anti-malware software must be installed and maintained on all systems within the processing environment.

Trustwave believes the theft of cardholder data by unauthorized third parties is a growing threat to businesses that leverage a distributed/franchise business model such as those seen in the hospitality industry. However, despite the sophistication of these attack techniques, full awareness and implementation of the PCI DSS along with continuous monitoring can mitigate much of the risk associated with these latest attack methods.

If you want to take immediate action to resolve these issues, please contact a Trustwave customer representative at 888-878-7817 to find out how Trustwave solutions can help you.

If you believe your systems may have already been compromised, please contact Trustwave at 866-659-9097 and select option 5 for our forensics and incident response team.