By Cait O'Dell

Protecting Guest Data

A Proactive Approach to Security

Recent successful hacker attacks may leave you wondering whether data security is reasonable at all. If huge corporations like Citi® and Sony® fall victim to attacks, can a hotel have the safeguards in place to protect guest data?

Vulnerability scanning is one of the most important preventive measures you can take to ensure top security, and it is a requirement of PCI DSS (Payment Card Industry Data Security Standard). If you have replaced or upgraded your property management system, back office accounting system or sales and catering system, you should perform a vulnerability scan. Most people recommend that you perform a second scan a month after the changes are in place. There are many types of vulnerability scanners on the market, and they all help you secure your guests' data and any other types of confidential data you need to protect.

Vulnerability scanners are tools that scan computers or networks for weak spots that are exploitable. For example, a scanner might find that you haven't installed the latest Microsoft update. If the update contains a security patch, you have vulnerability.

These scans address programs within your computer or network and systems you use on the Internet. It is particularly important to address vulnerabilities on the Internet, such as centralized accounting systems or online reservations. If an attacker cannot gain direct access to your database through a malicious email, he can gain access using a Web-based attack. Since so much business is conducted online, it is even more crucial to ensure your Web services are secure.

In a Web-based attack, the thief may create an advertisement that requires a website visitor's computer to access information via Flash or another reader. Once that website visitor's computer accepts the information exchange with the advertisement, it opens a channel through which the attacker can install a malicious program or steal information. If a rogue ad appears on your company website, a hacker could obtain any information being entered or transacted.

A vulnerability scanner that scans Web-based applications will point out potential holes in your firewall or other Internet security devices you may use. If properly addressed, information gained from a vulnerability scanner can patch a hole before a hacker finds it.

Penetration tests are similar to vulnerability tests in that both look for vulnerabilities. The difference lies in what is done with those vulnerabilities. A penetration test is generally performed by a hacker who will exploit your vulnerabilities any way possible. He may attack your network remotely, or he may use social engineering to gain access to restricted areas. In a vulnerability test, a technician addresses vulnerabilities found by the automated testing system. In short, a vulnerability scan can be done by your own employees, while a penetration test requires hiring an outside vendor.

When considering using a vulnerability scanner, be sure to use one that is designed for your operating system. Some scanners are built specifically for Windows, while others are specific to Linux. Some scanners are free and open source (meaning they are updated by other users), while others are expensive.

One of the downsides to vulnerability scanners is that they can slow down programs or devices being scanned. Sometimes they may even make the program or device inoperable for the duration of the scan. To avoid this potential problem, conduct scans at night or at times when there are not many guests checking in and out.

Another potential downside is that the reports from scans conducted merely tell you where vulnerabilities are, but do not tell you how to fix them or how important a vulnerability is. Unless you have someone who understands how to deal with technology and security, it is a good idea to consider hiring an outside vendor to manage your vulnerabilities. There are many reputable firms who can do that for you.

Vulnerability scans ought to be conducted on a regular basis. Regularly scanning helps your security team learn what is normal, so they can be prepared to notice something amiss.

If huge corporations like Citi® and Sony® fall victim to attacks, can a hotel have the safeguards in place to protect guest data?

If you decide to hire an outside vendor, you should find someone with experience in technology security. It is critical to find an honest, reliable vendor, as your entire security program relies on his findings within your infrastructure. Vulnerability scanning is important, but having a good vendor can make a huge difference in how protected you are.

Security risk management firms can also do the vulnerability scan for you, with your discretion as to what is scanned and when it is scanned. After the scan is over, the security risk manager delivers a report, detailing which vulnerabilities are most important and why, leaving it your choice which ones are addressed immediately.

Whether you hire an outside professional or not, a vulnerability scanner is one of the easiest and most cost-effective ways to ensure your guests' private data stays private. Knowledge is power, and a good vulnerability scan gives you knowledge about how to protect valuable information.

Even though hotels are not large banks, they are still attractive targets. Security should never be downplayed. Not only is it potentially damaging to your guests' experiences and bank accounts, it can damage your brand reputation. Just as guests expect hotels to have fire safety measures in place, they are trusting hotels to have the appropriate safeguards for their personal and private data.

CAIT O'DELL is a marketing analyst for VerSprite.