The 12 Entry Points

For Security Breaches That Every MSP Should Know

Malicious hackers are becoming more sophisticated, often involving organized crime and even foreign governments. As mobile devices and applications continue to permeate businesses and society as a whole, the magnitude of the security threats grows exponentially. As a result, IT experts are predicting that 2015 will be the worst year on record as it pertains to IT security breaches.

The good news is that managed services providers will play a critical role in protecting their clients. But as smart SPs know, security solutions are only as strong as their weakest link. Here are the top areas (in no particular order) where SPs need ensure they have air tight security solutions to keep their clients protected from potential business-crippling IT attacks.

1. **Phishing:** Phishing is a method of online identity theft to steal someone's personal and financial data. Most phishing schemes involve e-mails messages the mimic banks, credit card companies or other legitimate businesses. These messages look authentic and attempt to get victims to reveal their personal information. Endpoint security needs the ability to detect and block phishing attacks.
2. **Malicious Emails:** These threats can come in the form of ransomware, where all it takes is one wrong click or the opening of the wrong e-mail attachment and a company's critical files can be quickly encrypted. Some companies don't have good backup management policies so when they get hit, they are hit hard. Antimalware with advanced heuristics, that can monitor all active processes, is required to stop these Advanced Persistent Threats (APTs).
3. **Open Remote Access:** Many organizations allow their employees to have open remote access to their office systems from their personal systems or mobile devices. However, the risk develops when the personal (or remote) device does not have the same level of security as the office system being accessed, creating a security vulnerability. Many IT breaches occur through unsecured remote access sessions.
4. **Password Reuse:** Often employees use the same passwords for all their digital accounts—personal and professional—and across multiple machines and devices. If just one of those accounts is hacked, every other account is put at risk. Employers need to emphasize that their employees utilize different passwords with automatic timeouts to ensure that they're changed periodically.

5. **Misconfigured Equipment:** This can run the gamut from not having the right IP addresses, internally and externally, to weak passwords, subpar security policies and unsecured user accounts. These all create weak links in the IT security chain and open the doors for potential attacks.

6. **Vishing:** While many security breaches and viruses spread through email campaigns, other communication methods are being exploited as well. Vishing is the telephone equivalent of phishing, utilizing the telephone to scam the victim into surrendering private information that will be used for identity theft or system breach.

7. **Failure to do employee lock-outs:** In many cases when an employee quits or is terminated, the company fails to disable that employee's Active Directory account. In some cases employees are still logging in, reading e-mails, stealing information, gaining access to conference calls, etc.

8. **Failure to patch:** Many businesses ignore software updates and the associated patching. It can be argued that good patching is more important than a firewall for protection. There are far too many breaches as a result of failure to follow good patching policy.

9. **Physical loss or theft of a mobile device, laptop or PC:** With 2 million laptops lost or stolen in the US each year (not to mention mobile devices) physical security and protection policies are paramount. Any MSP whose customers work in highly regulated industries, such as the healthcare or financial sectors, must pay special attention. A simple solution for safe harbor is to encrypt storage.

10. **Unauthorized software on machines:** Employees are constantly downloading games and other personal applications on their mobile devices, PCs and laptops without approval from internal IT or you the MSP. This opens the gateway to security breaches that can impact not only the individual device, but the entire network.

11. **Device Control:** Mobile storage has made it simple to move files between systems with remote drives and USB sticks. Unfortunately these USB attachable devices also make it simple to share malware from one machine to another. Endpoint security should include device control policies and the ability to manage the use of external devices.

12. **Dangerous URLs:** While malware and ransomware can be spread through email attacks, one of the largest threats today come from authentic looking but bogus websites or genuine websites that have been hacked. Employees enter these sites and unwittingly infect themselves and their networks. SPs need to ensure their endpoint security solutions have a URL analysis component that stops the employee from reaching malicious websites.