WIND RIVER FINANCIAL

INDUSTRY TIPS

NETWORK SCANNING

Scan Your System Before a Hacker Does

While recent news articles report cardholder data being stolen by thieves hacking into the systems of large national merchants, most data compromises actually occur at smaller local merchants. And although these occurrences go unreported in the press, a considerable number of merchants are facing substantial fines and business reputation loss which is threatening their livelihood.

One of the best tools available for merchants to protect against data thieves is a network security scan. Generally security scans should be performed against all externally facing IP addresses including web servers and email servers. The scans are non-disruptive and actually use hacker techniques to probe for weaknesses or vulnerabilities in computer and server networks. Proactive scans allow any identified issues to be corrected before being exploited.

Unfortunately, many merchants fail to scan their networks before a hacker does, leaving their business exposed to considerable business and financial risk. Below are some of the common misconceptions that lead to this complacency.

Common Misconceptions

1. **In the national or global economy, our business is below the hackers' radar.**
   Reality: Because of the millions of computers on the web, many people assume their organization or system is nothing of consequence and would not be targeted by hackers. This might be true if it wasn't so easy to automate an attack on millions of computers through programming. Hackers write programs which can indiscriminately test millions of different computers for weaknesses. Many of the system attacks are attempted by foreign criminals who know nothing of the company they are compromising, but do know the value of unprotected cardholder data.

2. **Our data base (or web) server is behind a firewall and thus protected from viruses.**
   Reality: If employees have access to the internet or email, there is exposure to all servers on the network. Every computer that communicates on the internet uses an Internet Protocol (IP) address, and any computer with a public IP address means that it is accessible from any other computer on the internet. Upon discovery of any computer weakness, a direct virus or email worm will copy itself to the target computer and begin probing all computers on the network for confidential data. From this vantage point within the network, normal firewall protections may not apply.

3. **Our web site shopping cart uses industry standard encryption.**
   Reality: If the entire web site is not secure, hackers may insert fake pages into the purchase process to trick customers into providing card data prior to the actual encrypted purchase page.

4. **Our IT department/consultant has assured us that the system is secure.**
   Reality: A good vulnerability assessment system will point out holes you could never have found yourself; and will identify password problems, programming errors, and basic architecture issues. Over 80% of commercial websites failed an initial scan performed by one of the leading security assessment firms.

5. **It's hard to justify the expense of a security assessment.**
   Reality: Most companies can have their systems and networks scanned for $100 to $200 - with the scans providing protection from the potential negative consequences of compromised security. This expense can be considered similar to other insurance costs incurred to protect business, property, or financial risk.