

Boston Business Journal

HOW TO: SECURE YOUR COMPANY NETWORK

Protecting your network takes a moat-like mentality

BY KEITH REGAN
JOURNAL STAFF

No matter how much technology evolves, the basic rules of security really haven't changed much in a thousand years. Even in medieval times, those in charge of security knew the best approach was to have more than one level of defense.

"You didn't just build a castle, you put a moat around it and you had guys with buckets of tar on top of the walls," said **Danny Allan**, director of security research at Waltham-based Web application security firm **Watchfire Inc.** "You never want to rely on one defense."

Recent database breaches, such as the one that resulted in millions of customer records being stolen from **TJX Corp.** in Framingham, serve as stark reminders of the dangers facing businesses that have data they want to protect — which today is just about every business.

Indeed, just as keeping marauding armies out of castles took a layered approach, securing networks is rarely a one-step solution. Network perimeters can generally be secured and monitored with a host of outsourced and software solutions. Applications themselves, especially those facing the Web, can and should be secured,

since they are becoming increasingly popular avenues for hackers to spread malware, said Allan.

"Most networks have been secured, but the one place that needs to be kept open is that Web-facing port," he said.

Watchfire offers both outsourced vulnerability scanning services and software suites for automated scanning in organizations with IT and security staff.

Allan, who in the past tested network security as a so-called white-hat hacker, said the network security industry is maturing and getting better at helping to address the causes rather than the symptoms.

"For the past 15 years, the industry has been about chasing vulnerabilities," he said. "We're trying to put a heavy focus on the root causes and helping to determine why vulnerabilities happen, which would make it a lot easier to root out new problems in the future."

Bruce Harrington, information technology director for Boston-based design firm **Margulies & Associates**, said that while most solutions require



Allan: Need more than one defense

BEST DEFENSE

- A layered approach to securing a company network is considered the most effective for protecting expensive data.
- Some of the biggest threats to a network come from the inside. Know who is accessing your data.
- Think of your data as an asset. This will provide incentive to spend what's necessary to protect it.

investment, an ounce of prevention truly is worth a pound of cure in the case of data security.

"Protecting your IT infrastructure can save you thousands of dollars in time, productivity loss and lost financial assets," he said.

A good integrated solution includes fire walls or a virtual private network and protected entry points such as mail and Web servers and the Web browsers on desktop PCs. A good security regiment also includes two other elements, Harrington said: a reliable backup and recovery system and strong and constantly reinforced security procedures, such as tough and regularly changed passwords and informed end-users who can recognize

such threats as phishing attacks and e-mail and Web spoofing.

A growing number of businesses are also realizing that even the strongest perimeter security systems can't protect against threats that originate inside a company, said **Prat Moghe**, founder and CTO of **Tizor Systems** in Maynard.

"The reality is that most of the bigger incidents involving stolen data come from deep inside the enterprise," Moghe said.

Until recently, many companies didn't even have a good handle on where sensitive data was stored or who was accessing it. Tizor offers auditing and protection systems that can set the terms under which users can access data and provides alerts when someone accesses data in a way that's unusual.

While much of the data on corporate networks is encrypted, authorized users can get around that control as well, he said. "People are not used to thinking of data as an asset. They're comfortable thinking of a machine as an asset, but data is harder to quantify. Businesses now understand that data is a key asset. Once they come to that realization, they are motivated to provide protection specifically for that data."