Local banks beef up security

InfoSec News
Thu Jan 10 00:19:28 CST 2008

By Tina Reed
The Ann Arbor News
January 09, 2008

University Bank's new computer security hardware is only the size of a typical DVD player.

But the bank announced last month that it's betting the Promia Raven 1100 security system will help improve its defense against potential hackers with technology previously used only by the U.S. Navy.

Within the system's first day of use, the bank was alerted that hackers were trying to enter the system from North Korea, China and Oman, said Stephen Ranzini, company president and chairman.

The bank and its parent company, University Bancorp Inc. (Nasdaq: UNIB), are housed at the renovated Hoover Mansion on Washtenaw Avenue in Ann Arbor. The company employs about 30 people and reported earnings for the first nine months of 2007 of $1 million.

"You hear about this stuff all the time, how people overseas are trying to break into networks, but where's the proof?" Ranzini said. "If they're going to come after us, they'll go after everyone."

Other local banks say they are constantly investing in new products as hacker threats continue to increase, with many of the banks upgrading their systems within the last year. And when it comes to network security, smaller banks are using more sophisticated technology - and sharing more information with other banks about combating threats - than ever before, said Larry Ponemon, founder of the Ponemon Institute, a
Traverse City-based data protection research group.

"Banks are seeing security not just as a cost of compliance, but also as a reputation issue," Ponemon said. "If they can have better security over data they are protecting, customers might actually flock to those institutions."

Some of the most common threats to bank security are phishing and pharming schemes, which involve the use of fake bank e-mails or Websites, and social engineering, which involves digging for information about the bank culture online to trick information out of bank employees, said Jay Patterson, vice president of information technology for United

Bancorp Inc., in an e-mail. Ann Arbor's United Bank and Trust is part of United Bancorp's organization of banks.

United Bank and Trust has many different layers of security that are regularly tested using simulated electronic and social engineering attacks. Last year, the bank upgraded its Web content filtering and phishing prevention service. In 2007, it made major investments in security to respond to direct attacks and was able to minimize the damage from those attacks, Patterson said.

"Bank security is a 24 x 7 x 365 initiative," Patterson said.

Chelsea State Bank also has invested in a new security system, which blacklists IP addresses that try to maliciously break in, said Scott Tanner, chief operations officer.

He declined to reveal what brands of systems are in place at the bank, but said it's a full-time job monitoring all the layers of security and keeping up with new threats.

One of the most reliable and credible ways to keep up is by remaining active in a national banking user group that Chelsea State Bank joined back in 1985, he said.

"We found out early on we had a lot in common that we had to work on," including security, Tanner said. "Because banks were from around the country, we weren't sitting down with competitors from across the street, so we could really lay our cards down."

For University Bank, investing in the Raven system seemed to be the best choice, Ranzini said, because it links the bank to other Raven users.
That creates a much broader malicious IP address blacklist that keeps those addresses from ever being able to guess any of the networks' passwords again. It also tracks attacker activity for possible prosecution and can alert network administrators to unauthorized internal use and computer malfunctions.

"Time is the issue for the bad guys," Ranzini said. "All cryptography is based on the amount of time it would take to break in. Why give them all that time?"

Despite all the efforts that banks are making, Tanner said, it's the customers' responsibility to monitor their own banking statements - especially since they are available to check almost immediately online.

"No technology in the world can alert us to a problem as effectively as the consumer actually looking for it themselves."