Survey finds internal security a concern

June 15 2006

While outside attacks are still a primary concern for security officers, internal network security is becoming more of a concern, according to a study by Deloitte Touche Tohmatsu.

Nearly half of financial institutions reported having experienced an internal breach of security, according to Deloitte's 2006 Global Security Survey released this week.

Though external security breaches still outnumber internal breaches, at 78 percent, the rise of internal breaches shows that security officers may have been putting too much emphasis on keeping outsiders at bay, according to Paul Kurtz, executive director of the Cyber Security Industry Alliance.

"It's been an oversight more than anything," he said. "The idea was always perimeter security."

Many of the most often-reported attacks, such as phishing and pharming, are types of attacks intended to extort monetary gain, a fact that cements the changing prototype of a computer hacker away from the college student in his basement, Kurtz said.

"This survey confirms yet again that the folks behind these attacks are getting even more sophisticated," he said, calling the old stereotype "a thing of the past."

"There's real money to be made here. The attackers are getting more

stealthy as they go forward."

Ted DeZabala, a principle in Deloitte & Touche's enterprise risk services group, said that security officers now have to be prepared for attacks that are well organized and multi-pronged.

"We're seeing more sophisticated and more coordinated plans of attack," he said.

DeZabala said companies will have to respond with multiple layers of protection, mixing system resiliency, various forms of encryption and monitoring.

"We're going to see more aggressive monitoring activities to watch traffic and look for anomalies," he said. "That's not new, but it's becoming more sophisticated."

Similarly, he said that encryption for data at rest is a technology that's been around for a while but should see wider implementation soon.

"Only just now we've seen big institutions take these steps and utilize stronger authentication techniques," he said.

Kurtz agreed that encryption is, along with identity management technology, the key points to take from this year's Deloitte study.

"The difference between last year's study and this year's is that the key findings are getting more granular," he said.

Kurtz said that data encryption is becoming an essential security measure.

"There's no reason to put data at risk," he said. "The technology is

evolving as well to make it easier and more seamless."

Multi-factor authentication is going to be the key to improving identity management, Kurtz said.

"The evolution from a place where we use password authentication to a place where we use multi-factor authentication is on its way," he said.

He noted that multi-factor authentication provides security not only externally but within an organization as well.

DeZabala said that multi-factor authentication is beneficial but is not a security cure-all.

"Regulatory bodies are pushing multi-factor authentication," he said. "It probably will not prevent that many of these kinds of phishing and pharming attacks. It will get rid of some of the more mundane types of attacks, though."

DeZabala said that user entitlement and employee access systems are a key aspect of identity management, especially for the financial sector.

"They appear to be getting attention in financial services because of the advent of access controls," he said. "The banking industry is interested in them because they have a lot of activity in dealing with user control."

Elsewhere, almost half of respondents called disaster recovery and business continuity a top security initiative, with 88 percent of respondents claiming to have an enterprise-wide business continuity management program in place.

Kurtz said that Hurricane Katrina last year called attention to the need for business recovery and the lack of plans to deal with disaster

possibilities.

"I don't think it's nearly as sophisticated as it should be," he said, "but at least security officers are starting to ask the right questions. I bet business continuity will expand for a variety of reasons."

DeZabala said that seeing the damage many companies suffered from Katrina induced many companies to examine the continuity policies they have in place.

"They're rethinking how much risk they're willing to live with," he said.

DeZabala said that the damage from Katrina caught the attention of industry regulators.

"Regulators are pushing for addressing proximity risk, which is the risk that a particular region might be affected by a wide-scale disaster," he said. "Many organizations would probably not put programs in place to deal with a nuclear disaster, for example."