intelligent enterprise

November 2006
http://www.intelligententerprise.com/showArticle.jhtml?articleID=193200355

Dashboard: Take Four Steps Toward Data Security

Where should a company start when tackling data security? Experts brought together by Xerox for a security summit suggest a number of first steps.

By Penny Crosman

Data privacy continues to make headlines, from AOL's leak of member search data to the European Union's refusal to share airline passenger data with the United States due to privacy concerns. Vendors are responding with more robust security technologies, from Microsoft's Vista security features to Oracle's encryption, access control and identity management tools.

The trouble is, the number of points at which data can be hacked, inappropriately accessed, and inadvertently or deliberately compromised is almost limitless--text messages, e-mail and attachments; a camera-phone photo of a computer screen displaying customer data or product designs; USB drives and laptops loaded with sensitive information leaving the premises; documents printed to an insecure location. No one product can secure all company data.

Important security questions include: Which data must be protected? Can you trust your employees not to reveal the corporate secrets or personally identifiable information to which they have access? If someone is really determined to break into a database or share proprietary information, is there a foolproof way to stop them? What's the best way to deter data theft--monitoring, encryption, training, severe punishment for offenders, rewards for not breaking the rules?

Perhaps the most fundamental question is: Where should a company start when tackling data security? Experts brought together by Xerox for a September security summit suggest a number of first steps:

• Start an internal debate about which types of information are public, private or secret, then segment those data types, advises information security consultant Andrew Colarik. "My identity was stolen from a database at Kent State, where I got my MBA 10 years ago," he notes. "Why was that database still connected to a network? It should be on a machine that's kept disconnected from other computers and the Internet."

• Re-evaluate access and trust extended to employees, whether in HR, IT, accounting or any other department. "You're [probably] giving people access to things they have no business accessing," Colarik says. "That means you trust them, but you need to distinguish between giving free trust and limited trust in increments that make sense." This might be enforced

through stricter access control policies within computer systems, tougher personnel policies, or both.

• Focus on trade secret security, says attorney R. Mark Halligan. "Most U.S. corporations don't have systems in place for the identification and classification of trade secrets" including copyrights and trademarks, he says. The danger with this type of information is that a company may never know certain files containing product design details were compromised until a competitor shows up at a trade show introducing the same new product. Halligan says trade secrets should only be shared on a need-to-know basis, and he suggests setting up a holding company devoted to protecting intellectual property.

• Monitor policy compliance and punish violations. "Security policies are meaningless without some way to enforce them," says Dan Verton, executive editor of Homeland Defense Journal. "Employees should know that if they steal secrets, the company will find out and they will go to jail." Suppliers can be threatened with loss of business unless they comply with security standards or best practices. --*Penny Crosman*

[KEY PERFORMANCE INDICATORS]

Blocked E-mail Messages

What percent of the e-mail messages your company sends out get bounced, rather than arriving at their destination? More than 20 percent of legitimate, business-critical e-mail is blocked, according to a study of ISP data by StrongMail. The company estimates that related efforts to track down and fix problems result in annual losses of up to $5 billion among Fortune 500 companies.

Privacy Lapses and Stock Prices

A study by Enterprise Management Associates found the stock prices of six companies that had disclosed information security breaches between February 2005 and June 2006 fell by an average of 5.0 percent within a month and remained 2.4 percent to 8.5 percent below the predisclosure prices for another eight months. Prices didn't recover for nearly a year.

Security at the VA

After its close brush with data-breach disaster this summer, the U.S. Department of Veterans Affairs is installing $3.7 million worth of GuardianEdge and Trust Digital encryption software on 300,000 laptops, computers, servers and PDAs--every end-user computing device. Background checks will be conducted on employees who have access to sensitive data.