NEWS & TECH

March/April 2014

Reprinted with permission from Newspapers & Technology, 2014

www.newsandtech.com

conley MAGAZINES

The premier resource for insight, analysis and technology integration in newspaper, magazine, digital and hybrid production.

Policies, staff involvement crucial to data security

▸BY KATHERINE MICHALETS CONTRIBUTING WRITER

Busseri

Whether you're operating a large corporation like Target or a local newspaper, security experts agree that everyone from the college intern to the CEO needs to be vigilant about how they store and access data.

George Rentz, co-founder and chief operating officer of idRadar and former vice-president of customer operations and vice-president of marketing for Time Warner's National Division, said companies' IT departments must be constantly aware of possible attacks, whether there are hundreds of employees on multiple campuses or a local newspaper with five employees.

At idRadar, which provides security solutions for individuals and corporations that protect and monitor identity data, credit information, Internet use and digital communications, they also employ espionage experts who can determine if someone's information has already been compromised.

The real threat, he said, is a targeted attack such as a phishing email, which could result in one employee affecting the whole company network. These phishing emails can be as something innocuous as a prize announcement saying the person won dinner for two at a restaurant they recognize. Once the item is clicked on, malware can infect the network, even if it has been fortified by the IT staff.

"Essentially, these are the criminals that are now inside your network and they are not detected," Rentz said. "They are traversing the servers you have and they are finding ways to enter more servers."

Data thieves are looking for specific data, such as personal information, medical information and intellectual property, and will then exfiltrate it at a slow rate so the IT staff does not detect it, he said.

Secure mobile access

Tony Busseri, CEO of Route1 Inc., a security and ID management company that provides solutions for secure, remote access to the U.S. Department of Defense and the U.S. Department of Homeland Security, said newspapers need to think about keeping mobile access to networks used by reporters and other staff secure.

Rentz

"When you have a mobile workforce, keep firewalls closed and protected," Busseri said. "Don't create an opening."

He said people's sense of entitlement for access is a security weakness and can

Policies continued on page 2

Data security tips

- Ensure your enterprise data always stays within your network's perimeter — do not use a technology that takes your data beyond your firewall, i.e. no portable drives, no VPN and no browser-based solutions.
- Close all your inbound ports. The only reason they are open is to support a mobility strategy that is using an inferior technology. Use the correct technology and you can close your inbound ports and consequently you shut down a number of vulnerabilities to your network.
- Authenticate users before they are allowed access or entitlements. Your technology choice should be multi-factor, device independent, smart card based and integrated with your mobility software.
- Don't let the big names fool you — deployment of security technology should save the enterprise money; saving more than the investment for a net cost reduction.
- Use a technology that was built with security as the first priority.
- Use a technology that integrates seamlessly into your existing IT infrastructure — no (a) capital investment, (b) network changes or reconfiguration, and (c) additional servers, needed or required.

Source: Tony Busseri, chief executive officer, Route1

Policies from page 1

extend from the reporter to the CEO.

It's often those at the top of a company, Rentz said, who are not as likely to take the necessary precautions.

"They are targeted not only to an organization or a company, they are targeting people at the top end of organizations because they likely have the keys to the castle," Rentz said.

Busseri stressed the importance of authenticating the user, keeping firewalls closed and using technology — especially in the case of the mobile worker — that doesn't create vulnerability. For a temporary employee like an intern or consultant, it's important to keep them from accessing and taking data that could be used in ways it isn't intended to be.

"We give access to people we want to give access," Busseri said.

While there are technologies out there that keep networks secure, he acknowledges they can get costly.

"Inherently, human beings, they make mistakes," he said. "If technology takes away the human risk element, why not deploy it?"

For starters, employees should be trained on how to keep data secure. A company should have a policy and procedures in place, Busseri said.

"If we expect everyone to understand the latest technology, it is a recipe for disaster," he said.

It's also important to keep in mind the bigger technology picture.

"There is only one network and it's all connected and it's the Internet," Rentz said.

For the past three to four years there have been advanced, persistent attacks, he said, and he only anticipates that to continue. ▲