InformationWeek :: reports

Reports.InformationWeek.com November 2011

Next

An Insider Threat Reality Check

Heightened concern that users could inadvertently expose or leak—or purposely steal—an organization's sensitive data has spurred debate over the proper technology and training to protect the crown jewels.

In this special retrospective of recent news coverage, *Dark Reading* takes a look at how organizations are handling the threat—and what users are really up to.

Presented with SECURITY dark READING Protect The Business Enable Access

TABLE OF CONTENTS

October 5, 2011

Are Users Too Dumb for Security Awareness Training?

By Ericka Chickowski

As the industry entered Cybersecurity Awareness Month (in October), many security practitioners likely gave a little snort of derision when they thought about the state of security awareness training. Even as vendors and enterprises spend millions on security education, trained users keep doing dumb things and data breach numbers keep going up. Most security pros would openly tell you that security training just doesn't work. But it doesn't have to be that way.

"Security awareness has a bad reputation, and to be honest, it deserves it," says Alan Paller, director of research at the SANS Institute. "Most programs have been poorly planned or executed."

According to Paller and a growing contingent of training advocates, it is time that the security industry takes a hard look in the mirror to understand why awareness programs are so ineffective today.

"The problem is not the users. The problem is us," says Mike Murray, managing partner for consultancy MAD Security, which recently landed a $1.2 million contract to provide security training and support to the U.S. Coast Guard for the next four years. "The thesis that we as an industry operate on is, 'Oh well, there's no point in training the users because they're too stupid to get it anyway and it's never going to work.' That's just not true. The problem is we do it wrong."

According to Murray, the big issue is that security people think that simply making users aware of security issues will make them want to change their behavior. But awareness doesn't equal action.

"If that were true, there's not one person in America who would ever smoke a cigarette," he says. "You can't just sit users down, give them 30 minutes of information about why security is important and expect that will change how they behave on a daily basis. That can't work because that's not how people work."

In order to really resonate with users, Murray says that the security world needs to take a page from the playbook of those who have for decades worked on the art and science of changing people's behavior: marketers.

"Everybody needs to stop talking about how to make users more aware and start talking about how to modify users' behavior," he explains. "So how do marketers do it? Well, first of all, they focus on small pieces of information that can infiltrate the human mind easily. whereas with awareness training we give someone 55 different topics in 15 minutes of training and expect them to remember it and change something."

Paller concurs with Murray; organizations need to improve how they communicate and do a better job deciding what to communicate.

"Unfortunately most awareness programs are communicated by security professionals, people who by nature tend to be bad communicators," he says. "Most awareness pro-

grams overwhelm people with long monolithic training, with no thought or research into *what* should be taught. As a result organizations are wasting time teaching people topics they do not need to know."

Additionally, Paller believes that organizations have to constantly reinforce concepts. Right now too many programs are rolled out on an ineffective annual basis.

"Just like computers, people must be patched at least every month. Awareness programs (should be on) a continuous life-cycle where employees must constantly be updated, trained and reinforced," he says. "Yet, most awareness programs are nothing more than a one-time event—and then people wonder why nothing happens."

"Most awareness programs are nothing more than a one-time event—and then people wonder why nothing happens."

What's more, even with fireworks and a halftime show, security training programs are still likely to fail if no consequences await users who choose not to change their behavior once they've been taught.

"If people make the same mistakes over and over, then at some point or another there needs to be some sort of disciplinary action," says Hord Tipton, executive officer for (ISC)2, "particularly if there has been good due diligence and the company has made good effort to teach people the right way to do things."

Making a Serious Point Lightheartedly

The consequences don't even necessarily have to be serious. Sometimes a little public embarrassment with a dash of good humor can do the trick, says Jeff Nigriny, CEO of CertiPath, an identity and compliance vendor. In his time as a CSO at an aerospace contractor, one of the policies he trained users on was that they needed to keep their PCs locked anytime they stepped away from them. He had a prankster's way of dealing with offenders.

"Now, I wouldn't say this would necessarily work at a larger company, but at a smaller company where the HR policies weren't as stringent, I would walk around as a security officer and if I saw someone's PC was unlocked I would sit down and send emails under their name," he says. "I tried to make them funny." If organizations do a good job with engagement, behavior change and constant reinforcement, they should experience good results in the long run. That's why security pros need to complement a good training program with a solid set of metrics to make sure it's working. One of the biggest problems with awareness training programs these days is that organizations do nothing to measure before and after user performance.

"Step one is to get good measurements of user behavior before training and then the same measurements of the post-straining state to find out if you're actually getting a return on that time you spent," Murray says. He says that frequently he sees companies that tell him they don't know how many phishing attacks are succeeding before or after training. When asked if the training worked, "their answer is that 'Well, 100% of the people took the training. That's like measuring your kids performance in school by whether they showed up."

Air Force Says Malware Discovered 'a Nuisance,' Not a Keylogger

October 14, 2011

By Kelly Jackson Higgins

The U.S. Air Force recently said in a press statement that malware discovered on systems at its Creech Air Force Base was not a keylogger and did not impact its Remotely Piloted Aircraft, or drone, operations.

The statements came in response to a *Wired* report that said malware had infected computers at Creech Air Force Base in Nevada—home to the Predator and Reaper unmanned drone aircraft systems—and that it was logging the keystrokes of the pilots. Sources who spoke to *Wired* said the virus had been detected two weeks before, but it had neither disrupted any flight missions nor had any classified information been exposed. They said it was likely "benign," but difficult to kill.

The Air Force said that its 24th division detected the malware on Sept. 15, and alerted Creech Air Force Base "regarding the malware on their portable hard drives approved for transferring information between systems."

It identified the infection as a credential-stealing malware program that was discovered on a standalone Windows system used in its mission-support network. The malware was "more of a nuisance than an operational threat. It is not designed to transmit data or video, nor is it designed to corrupt data, files or programs on the infected computer. Our tools and processes detect this type of malware as soon as it appears on the system, preventing further reach," the Air Force said in its statement.

The infected machines were part of a separate ground control system that supports the drone operations, according to the Air Force, not the same systems that Air Force pilots use to remotely operate the drone aircraft. The malware had no impact on the drone flights, according to the statement.

An Air Force official told the Associated Press that the malware was the type used to steal usernames and passwords for users of online gambling and gaming sites.

Meanwhile, an Air Force Space Command spokesperson said in a statement that the Air Force's policy is not to discuss "the operational status of our forces."

"However, we felt it important to declassify portions of the information associated with this event to ensure the public understands that the detected and quarantined virus posed no threat to our operational mission and that control of our remotely piloted aircraft was never in question," said Colonel Kathleen Cook, spokesperson for Air Force Space Command. "We continue to strengthen our cyber defenses, using the latest antivirus software and other methods to protect Air Force resources and assure our ability to execute Air Force missions. Continued education and training of all users will also help reduce the threat of malware to Department of Defense systems."

Study: IT Execs Worried About Insider Threat

October 12, 2011

By Tim Wilson

The study of IT managers and network administrators, which has been conducted annually by Amplitude Research on behalf of VanDyke Software, shows a growing concern about insider threats, particularly unauthorized access by current and former employees.

Of the many reasons cited for network intrusions, more than half could be attributed to internal issues: lack of adequate security policies (17%); employee negligence (12%); unauthorized access by current or future employees (11%); employee Web usage (6%); and lack of software updates (6%). Concerns about unauthorized access nearly doubled from last year's study.

Small and midsize businesses (SMBs) are becoming more frequent targets of attacks, according to the study.

Hacker/network attacks accounted for only 14% of intrusions; viruses, malware and spyware were 10%.

SMBs at Risk

Small and midsize businesses (SMBs) also are becoming more frequent targets of attacks, according to the study. Half of the SMBs in the 2011 survey said they have experienced an intrusion of their user machines, office network and/or servers vs. 36% in 2005. There was a significant decline among large companies reporting a successful intrusion—from 67% in 2010 to 49% in 2011. In the previous year's study, a significant increase of intrusions among large companies was reported, jumping from 41% in 2009 to 67% in 2010.

Outsourcing continues to be a major strategy for many corporations, but IT pros are split as to whether outsourcing creates security issues. Thirty-six percent said outsourcing has had a positive impact on their organizations' network security; another 36% said it has had a negative impact. Twenty-eight percent felt there was no impact.

"Many of those who felt there was a negative impact described a feeling of uncertainty or concern about the potential network security risk involved in outsourcing technology jobs offshore," said Steve Birnkrant, CEO of Amplitude Research. "In contrast, many of those who felt there was a positive impact explained that outsourcing technology jobs offshore has worked well for their organization and/or there were cost savings."

ISP Backlash Over Feds' Bot Notification Initiative

October 5, 2011

By Kelly Jackson Higgins

A new Department of Homeland Security (DHS) and National Institute for Standards and Technology (NIST) effort to establish voluntary best practices for how ISPs should notify their customers whose machines are part of a botnet has met with some resistance from the service provider community.

The Messaging Anti-Abuse Working Group (MAAWG), which is made up of ISPs, email providers and security vendors including AT&T, Cisco, McAfee, Facebook and Verizon, sees the federal effort as unnecessary and redundant, and is balking at the idea of the government legislating how ISPs handle bot-infected customers. MAAWG issued its own set of best practices (PDF) two years ago for mitigating bots, and several ISPs today already have their own bot notification mechanisms in place, according to MAAWG.

"There is no need for mandated action in this area, since the market is already moving forward. Many ISPs are already doing a great deal to combat the menace of bots and malware. All over the U.S., ISPs currently have notification systems in place to tell their users they are infected and—whether they deliver these warnings via email, phone, walled gardens or inline warnings—the warnings are being delivered," says Michael O'Reirdan, chairman of the MAAWG. "Other ISPs currently have pilot programs or technology development efforts in place, and there will be more deployments in the near future."

O'Reirdan says ISPs handled the spam battle on their own, and can also do so for battling bots. It has become a business issue for them, he says. "No one had to mandate anti-spam platforms: ISPs put them in place to deal with the menace of spam because, if they had not, they would have lost customers if customers' mailboxes were overrun with spam. The same is happening with anti-bot platforms. It is becoming a 'table stakes' issue for ISPs, and legislating in this arena will merely lock the response of ISPs in stone to conform with the legislation rather than allow innovation and development to meet the rapidly varying nature of the bot challenge posed by the bad guys," he says.

The Department of Commerce and DHS recently issued a request for information in the Federal Register, looking for input for a voluntary "industry code of conduct" for detecting and notifying infected bot machine owners and mitigating botnets. Comments are due by Nov. 4.

"To promote voluntary best practices in botnet detection, notification and mitigation, one suggestion has been to provide companies that take action with certain types of lia-

bility protection in order to foster greater marketplace certainty. Another suggestion is to encourage ISPs to send consumer support queries to a centralized consumer resource center that could be supported by a wide number of players. Such a resource center could reduce the burden on corporate customer support centers by pooling resources," the Federal Register entry entitled "Models to Advance Voluntary Corporate Notification to Consumers Regarding the Illicit Use of Computer Equipment by Botnets and Related Malware" says.

ISPs traditionally have been uneasy about being too hands-on or invasive with bot-infected customers. They've been hesitant to suspend infected accounts for fear of repercussions with unhappy customers or lost business.

But ISPs such as Comcast, which two years ago was one of the first to employ a bot-notification service, notify customers whose machines they spot as bot-infected. Comcast's free Constant Guard Security program directs the infected user to the antivirus center, where he follows directions to remove the bot malware.

"From the perspective of MAAWG, the industry is already voluntarily moving very decisively in this direction without legislation. A lot is happening with the big ISPs, and the smaller ISPs may need help, but they don't need compulsion," MAAWG's O'Reirdan says.

ISP Has Botnet Combat Potential

But others say that the federal effort for ISP best practices could go a long way in stemming the bot explosion. Maxim Weinstein, president and executive director for StopBadware, says the ISP's role in combating botnets is critical. "The ISP is the only player in the ecosystem that has the knowledge of what the customer is that is attached to a particular IP address, and that has a relationship with that person. That is really important in the case of bots," Weinstein says.

"ISPs are divided on where they are on this. Some are already doing things…others aren't sure if or what they are able to do," he says.

Weinstein, along with O'Reirdan, White House cybersecurity coordinator Howard Schmidt, and high-ranking federal officials from Commerce, DHS, NIST and the FCC, participated in a recent panel discussion hosted by the CSIS Technology and Public Policy Program on the possible ISP role in fighting bots. He says one takeaway from the day was that ISPs and MAAWG's O'Reirdan note while ISPs do have a role to play in this, it should not just all fall on their shoulders.

"They made it clear that ISPs do have a role to play here, but it's not appropriate to put the entire onus on ISPs. It's much broader than that, and you shouldn't single out ISPs," Weinstein says of the ISP reaction.

ISPs worry whether they are equipped to handle bot notification and remediation, for instance, and whether it's a revenue opportunity, he says.

There is at least one part of the effort that should reach consensus, he says: a centralized mechanism for reporting bots to ISPs. "A

bunch of third parties have information about bots. Why not make it as easy as possible to get that to ISPs?" Weinstein says.

But the toughest sell will be the potential hot button of a centralized resource for helping infected bot customers, he says. DHS and NIST laid out three scenarios for a resource center that would "inform and educate" users whose machines had been infected: a private sector-run center, a government-run center or a public/private partnership-run center.

"It will be much more difficult deciding to what extent and what form a centralized resource for helping customers for remediation [should be]," he says. An ISP that already offers its own services and products for remediation might see it as competition, while a smaller ISP might welcome it as a handy resource.

"From our perspective—representing individual users—it would be great to have a central resource," Weinstein says.

Meanwhile, the FCC's Communications Security, Reliability and Interoperability Council (CSRIC) Working Group (WG) has a set of best practices for botnet protection for consumers, and the Internet Engineering Task Force is drafting the "Recommendation for the Remediation of Bots in ISP Networks."

FAST FACT

44%

of mobile users who don't lock down their devices say passwords are "too cumbersome."

September 29, 2011

No Passwords, PINs for Most Smartphone and Tablet Users

By Kelly Jackson Higgins

Fat-fingering a password or PIN is an all-too-frequent frustration to mobile users today, and more than half of smartphone and tablet users say they don't bother with authentication on those devices.

In a new survey published recently by Confident Technologies, which sells image-based authentication, some 44% of those mobile users who don't lock down their devices say passwords are "too cumbersome" on those hand-held devices. And close to 90% of those surveyed say their mobile devices are their own and aren't company-issued equipment, while 65% of them say they use them for accessing work email or the company network.

"Internet-enabled smartphones and tablets are quickly becoming the device of choice for everything from accessing work email, to social networking to even banking and shopping," said Curtis Staker, CEO of Confident Technologies. "However, people's lax security habits have made the mobile platform the new frontier for hackers, malware and fraud. The onerous process of typing complicated passwords on a smartphone for every app or online account means that people instead choose to sacrifice security for convenience,

leaving themselves and, in many cases, their businesses at risk of data theft and fraud."

Lack of Concern

Confident's survey also found that many users are basically lax or unaware of the security risks of having these unprotected devices at work. Approximately 30% of those who don't password-protect their smartphone or tablet aren't concerned about the security risk, and 97% have email running on their smartphones or tablets; 50% of them operate banking, financial or stock trading apps on them; 77% have social networking apps like Facebook or LinkedIn; and 35% have online shopping or auction accounts.

"Many people fail to recognize that smartphones bring great risks for exposure of personal information," said Joanna Crane, executive advisor to the Identity Theft Resource Center. "Consumers can protect themselves and their personal information by following best security practices including locking the devices, installing security software, paying attention to what information is being captured by an application and thinking about whether that app really needs it, and using remote wiping technology if the phone is lost or stolen."

Convenience is the main driver, of course: two-thirds of them leave applications logged in if they can, and 30% complain that they "often forget or mistype" passwords on their smaller keyboards. Around 60% say they would like an easier way to authenticate to their mobile apps.

FAST FACT

30%

of those who don't password-protect their smartphone or tablet aren't concerned about security.

Most Users Respect, Follow Company Security Policies

By Kelly Jackson Higgins

September 20, 2011

For once, some relatively good news about enterprise security: Only one-fourth of employees bypass their organizations' security policies, and most agree it's important to follow their employers' security policies, according to a new survey.

Ninety-five percent of the 2,500 employees polled by Webroot in the U.S., U.K. and Australia said that complying with their organization's security policies is necessary, and 89% said security policies help prevent malware infections. More than 60% said the security policies at their companies never or "rarely" impede them in doing their jobs, and only 7% said they are extremely worried about their employers monitoring their online activities.

"We were surprised—quite pleasantly, I might add—by how few employees skirt around corporate computer security policies. Given the proliferation of new social tools, mobile devices, browsers and all other emerging tech form factors, we assumed it'd be tempting for employees to get

around policies prohibiting their use as IT departments grapple with how to incorporate them," says Jacques Erasmus, chief information security officer at Webroot.

Just because most employees play by the security rules doesn't mean your organization is in the clear for insider theats.

So why the apparent discrepancy of 25% still trying to break policies? "People are used to being connected—to their devices and to each other via social networks. Particularly for younger workers who've grown up with these technologies as a part of their daily lives, it can take some adjustment to do without them if their company says it must be so," Erasmus says. "We found that a greater proportion of employees between the ages of 18 to 29 disabled or modified restrictive settings on their computers and used mobile devices for restricted activities more than any other age group."

Around 15% say they used a mobile device to perform activities banned at work, as compared with 6% of users in all age brackets. Around 12% of the 18- to 29-year-olds visited prohibited websites on a mobile device, versus 6% of all users; 6% of that younger age bracket changed their browser settings, while 3% overall did.

But just because most employees play by the security rules doesn't mean your organization is in the clear for insider threats or social engineering.

"While we were generally encouraged by the number of employees who respect their companies' computer security policies, all it takes is one employee to fall victim to a social engineering tactic or targeted attack. Cybercriminals have realized it's easier to hit the soft targets—the employees—before they try to get past the infrastructure companies have invested a lot of money in," such as firewalls, anti-malware solutions, IDSes and other products, Erasmus says.

MORE LIKE THIS

Want More Like This?

Making the right technology choices is a challenge for IT teams everywhere. Whether it's sorting through vendor claims, justifying IT projects or implementing new systems, there's no substitute for experience. And that's what *InformationWeek* provides—analysis and advice from IT professionals. Our Reports site houses more than 900 reports and briefs, and more than 100 new reports are slated for release in 2012. Right now, you'll find:

Four Steps to Virtualization Security: While virtualization changes the way organizations use servers, provision applications and configure networks, it doesn't change bedrock security principles. This report outlines four steps, or processes, that organizations can take to manage the risks inherent in a virtualization environment.

Research: Mobile Device Management: As you develop mobility policies, your ultimate goal should be the certainty that any data contained within a device, or any connectivity profiles—VPN or Wi-Fi—that provide access to corporate networks, is completely secure, even if the smartphone or tablet is lost or stolen.

Strategy: Biometrics: Use of biometrics has long been touted as the best way to overcome the vulnerabilities associated with password- and token-based authentication. With nonbiometric authentication, as long as people enter the correct combination of user name and password, they are granted access, regardless of who they actually are.

PLUS: Find signature reports, such as the *InformationWeek* Salary Survey, *InformationWeek* 500 and the annual State of Security report; full issues; and much more.