TOP SECURITY THREATS FOR 2013

As cyberthreats intensify and workers bring more devices to work, IT shops need to sharpen their security tools.

It's the stuff that makes IT leaders queasy. In September, major U.S. bank websites were hit with the largest denial of service (DoS) attacks in history.

At the same time, a surge of smaller cyberattacks was reported. South Carolina taxpayer servers were hacked in October compromising 3.6 million Social Security numbers. Just this year, hackers broke into The New York Times computer systems and stole passwords of high-profile reporters and staff.

Even Microsoft and Apple weren't immune. In February, both reported that small numbers of computers had been infected with malicious software. Is anyone safe?

State-sponsored groups, hacktivists, organized crime and run-of-the-mill hackers are growing more organizationally and technically sophisticated. What's more, the number and complexity of systems, networks, devices and applications continues to grow. Both require IT shops to step up their game with new vigilance and approaches to security.

Network Convolution

In 2013, users are embracing a wider variety of platforms, each with its own user interface, operating system (OS) and security model. At the same time, organizations are working to protect intellectual property and business information as they tackle cloud platforms, consumerization and bring-your-own-device (BYOD) initiatives, mobility and virtualization.

This plethora of computing challenges makes opportunities for cybercriminals greater, with more potential vulnerabilities for threat actors to gain profit, steal information and sabotage their targets' operations. The current risk landscape requires a shift to a transformed security approach based on a defense-in-depth security management model.

Here security professionals outline the top security threats to the organization in 2013, along with the defensive moves they recommend to stay out of harm's way.

Advanced Persistent Threats

APTs — attacks on a specific organization's people, systems, vulnerabilities and data — are growing rapidly and are no longer just blasted-out threats to see who takes the bait. They're much more targeted.

Today's APT hackers are more operationally sophisticated. "These guys are doing their own security research. They're finding their own vulnerabilities and are able to exploit them," says Tom Cross, director of security research at Lancope Inc., an Atlanta-based security software firm. "The exploits of their malware will not be detected by commercial off-the-shelf security solutions. That's what makes them very difficult to defend against."

Patching system vulnerabilities remains important, but internal networks should be examined as well. "A lot of solutions build the high castle walls," Cross says. "But if we acknowledge that they're breaching these castle walls, we then have to take a look inside and see if we can find them."

Lancope software examines network flow and allows security teams to see the network transactions happening inside the network. "It profiles behaviors and looks for anomalous behaviors," he adds.

Security solutions provider Trend Micro recommends that IT departments develop external and local threat intelligence as part of a defense strategy against targeted attacks. Install security solutions that can provide network-wide visibility, insight and control needed to combat APTs and targeted attacks.

They should also consider solutions that can detect and identify evasive threats in real time and provide in-depth analysis and

relevant actionable intelligence that can help assess, remediate and defend against targeted attacks.

Trend Micro's Deep Discovery advanced threat protection product and McAfee's Deep Defender solution are just a couple of the products offering specific protection against APTs.

Spear-phishing Attacks

These email attacks are a subset of APTs. However, they warrant their own caution because they affect more entities more often.

According to the SANS Institute, 95 percent of all attacks on enterprise networks are the result of successful spear phishing. Somebody received an email and either clicked on a link or opened a file that they weren't supposed to. For example, Chinese hackers successfully broke into computers at The New York Times through spear phishing.

Traditionally, these attacks came in the form of offers for money, coupons or incredible discounts or bargains. Or they falsely come from your bank or email account provider announcing frozen accounts and the request to reenter credentials or personal information.

Today's spear-phishing is much more targeted at specific companies to gather specific information. "Some email security solutions can't handle it well because they haven't seen it before," says Aaron Colwell, inside solution architect for security at CDW. "It's a uniquely created email that somebody only sent 20 of, so they're not out in the databases."

So what are the steps that IT managers can take to protect enterprise networks from spear phishing? Companies need a more intelligent email security solution than in the past, Colwell says.

Solutions such as IronPort web and email security appliances by Cisco Systems and Websense email and web security products are able to tie those two databases together, he says. They can detect whether an email link "is trying to take you out on the web to a bad place."

BYOD and the Consumerization of IT

The trend toward allowing workers to bring their own devices to work has skyrocketed in the past year. More than half of 610 professionals surveyed by CDW in four industries say they use a tablet at work, for instance, and a third of those tablets are the employees' own. Personal smartphones are even more prevalent.

Each mobile platform requires a different approach to security. Similarly, as online activities move away from browsers and toward apps, it is harder to give accurate advice on security and privacy issues, according to Trend Micro.

Ransomware is one of several threats for mobile devices that, if not detected, could spread to business systems. The new scam involves hijacking a user's smartphone, tablet or computer and holding it hostage.

The ransomware pops up disguised as a note from law enforcement claiming that a computer user is doing something illegal, such as downloading illegal content. The device is then locked, and the message suggests that the owner must pay a couple hundred dollars for a code to "unlock" it.

But therein lies the scam. Users are not getting that decryption code or that password in return. The malware then unleashes a virus that monitors and steals personal information.

As workers now use their mobile devices for business and have access to office systems through portable browsers, the number of ransomware for mobile devices will likely grow, according to McAfee's 2013 Threat Predictions report.

IT shops must require BYOD users to engage the smartphone's built-in security features. Device users must also avoid using free but unsecured Wi-Fi access, scrutinize every app they download and understand the permissions or capabilities they are allowing an app to have on their smartphone.

Web and Cloud Commoditization

As workers continue to use cloud services to develop their own apps or store company information, IT departments begin to lose visibility of their data.

Many workers "are trying to create new apps, and they'll create those apps in the cloud and sidestep their own IT department," Cross explains. "So IT is struggling to maintain awareness of the apps and the data that their user base is putting out there."

He recently spoke with one company that resorted to using employees' expense reports to identify when people were expensing cloud services on their corporate card. "That is how they identified that applications and data were moving out there."

Most entities don't have to go to those extremes, Cross says. Start with a governance plan that outlines acceptable cloud uses within the company. From a solutions standpoint, companies need a solution "allowing the enterprise to see what activity is going back and forth — even if they don't necessarily control it."

"You've got to think how your information assets could be valuable to a bad guy," Cross says. "It's important to understand who's likely to target you and what are they likely to desire — and then focus on that specific risk." ■

CONSIDER CDW'S SECURITY ASSESSMENTS AS A SERVICE, IDENTIFYING POINTS OF RISK ALONG WITH REMEDIATION GUIDANCE.