CERT'S PODCASTS: SECURITY FOR BUSINESS LEADERS: SHOW NOTES

More Targeted, Sophisticated Attacks: Where to Pay Attention

Key Message:Business leaders need to take action to better mitigate sophisticated social engineering attacks.

Executive Summary

As a security community, we continue to struggle with mitigating the impacts of attacks that exploit poorly written and vulnerable software. Implementing a range of security controls is still the best mitigation strategy. Social engineering has become the attack weapon of choice in the last 12 to 18 months because it capitalizes on the weakest link – people. Business leaders and users need to become much more educated about how to protect themselves and their organizations from sophisticated, targeted social engineering attacks.

In this podcast, Marty Lindner, a CERT principal engineer focused on threat and incident analysis, discusses how the cyber-threat has evolved since Marty's last podcast in 2006 and what actions to take.

PART 1: THE EVOLVING THREAT AND WHAT'S DRIVING IT

A Perspective on Today's Threats

Today's threats can be categorized as follows:

1. Those caused by social engineering
2. Those caused by software flaws and poorly written software

The threat landscape has not changed in any appreciable way with respect to exploiting software flaws in the last year or so. Adversaries continue to use every means at their disposal to take advantage of these.

A layered defense (also known as defense in depth) works reasonably well but there will always be exploitable holes.

Social Engineering

The sophistication of social engineering attacks has increased considerably in the last 12 to 18 months. We've moved from broad-based, untargeted spam to targeted, personalized messages.

Motivation

It's all about money – obtaining any information that can be turned into cash such as Social Security numbers (SSNs), bank account numbers, and intellectual property.

There is a very active underground economy where, for example, credit card numbers are traded for telephone calling card numbers. This bartering process may include SSNs and eBay account numbers.

Those interested in conducting business – trading information for personal gain and as part of committing crimes – find one another easily on the Internet.

PART 2: CHALLENGES FOR LAW ENFORCEMENT; DEALING WITH EXTERNAL SUPPLIERS

Cybercrimes Are Complex

More cybercrime cases are being brought to trial as investigators and prosecutors better understand the unique challenges and complexities of Internet-based crime.

That said, the prosecution of drug cases continues to greatly outweigh cybercrime cases even though, by some reports, cybercrime now exceeds illegal drug sales in terms of annual proceeds. Compared to cybercrime, drug cases are just easier to prosecute.

Geography and Jurisdiction

Historically, law enforcement agencies cover a well-defined geographical area. For example, the FBI has local field offices to deal with bank robberies in their immediate vicinity.

The Internet has no such geographical boundaries and many jurisdictions. This is a new challenge for law enforcement that calls for effective cooperation and collaboration across agencies and locations.

Even if you know who the bad guy is and where he is, you may not be able to do anything about it if there is no jurisdictional reciprocity between law enforcement agencies.

External Providers and Partners

Most organizations outsource to save money and improve service. But you need to compare the provider's security posture and practices with yours.

Be sure to confirm that your information will be protected and managed in the same fashion as within your organization. Recent security breaches resulted from lower security thresholds in provider processes.

When dealing with a global supply chain partner, having the right terms and conditions and service level agreements are essential. Make sure to audit partner practices to ensure they are doing what they claim.

PART 3: MITIGATING YOUR EXPOSURE; TRENDS TO PAY ATTENTION TO NOW

Social Engineering – Actions to Take

Training and education help mitigate the risks caused by social engineering. Make sure users understand the threat and the risk they take every time they click on a link.

Implementing digitally signed and encrypted email provides strong protection. Many social engineering phishing attacks can be eliminated by blocking unsigned email at your network gateways.

In these days of increased transparency, consider the risks of publicly posting organizational policies, procedures, forms, and templates. Adversaries can download these, modify them, and use them to launch social engineering attacks that appear legitimate.

As a case in point, adversaries obtained a publicly available application form for a new account that required a signature. They downloaded another document that contained a signature, put the two together, submitted the application, and created an accessible account in the person's name which the adversaries controlled.

Exercise Your Response Process Regularly

When something bad happens, you don't want to go into fire drill mode. Make sure all key roles and people that need to be involved are identified in advance and prepared to respond.

The U.S. National Transportation Safety Board is a good example. When a plane crashes, response team members mobilize immediately at the crash site. People responsible for forensics, public relations, and law enforcement know what actions to take.

Advance preparation includes conducting regular team exercises so members are prepared to deal with realistic attack situations when they occur.

Emerging Threats – Mobile Devices

New technology is available every day. Mobile devices such as iPhones, Blackberries, and iPods serve as yet another place to store sensitive information, including your user names and passwords.

Software on mobile devices has vulnerabilities too – just like the applications on your desktop or laptop. Organizations need to pay attention and secure device software as they would desktop software.

Emerging Threats – Social Networking Sites

When it comes to sites like Facebook, MySpace, Twitter, YouTube, and LinkedIn, keep in mind that everything you watch and download may contain malicious code.

Given all of the personal information they make available, social networking sites have often served as a primary source for social engineering attacks. Users need to carefully consider how much they divulge.

Proceed with caution when conducting business in virtual communities such as Second Life. Adversaries commit crimes here just as they would in the real world.

Many employees, particularly those in the net generation, expect their organizations to provide access to social networking sites during normal business hours.

Some organizations are investing in creating a second, separate network for this type of access. They can then enforce more secure access and restrictions on their “for business” networks while satisfying employee needs and behaviors.

Resources

CERT podcast: Proactive Remedies for Rising Threats

CERT podcast: Getting in Front of Social Engineering

CERT podcast: Virtual Communities: Risks and Opportunities

Lynch, C. G. “Can Social Networking Be Secure at Work?” CIO.com, May 5, 2009.

Prince, Brian. “RSA: The Elusive Structure of the Cyber-Criminal Economy.” eWeek.com, April 23, 2009.

Harris, Shane. “The Cybercrime Wave: Grifters, Fraudsters, and Thieves Go Virtual.” National Journal Magazine, February 7, 2009.