January 2015
Volume 10, Issue 1

2015 Cyber Security Outlook

Cuyahoga County
Department of Information Technology
Security and Research

From the Desk of the Department of Information Technology – Security & Research Team

For this year's outlook newsletter edition, we've asked experts at the Center for Internet Security (CIS) to share their thoughts on what issues we'll be talking about and dealing with in 2015. Below are some highlights of those topics. To read more from CIS experts about this year's trends and threats, visit the CIS blog.

Distributed Denial of Service (DDoS) Attacks

A Denial of Service (DoS) attack is an attempt to make a system (such as a website) unavailable to its users. Whenever multiple sources are coordinating in the DoS attack, it becomes known as a Distributed Denial of Service (DDoS) attack. DDoS attacks are not new, however, they remain pervasive and will continue to pose a threat to organizations in 2015. The main purpose behind a DDoS is the malicious consumption of resources, which can result in significant disruption and loss of productivity and/or revenue. To help minimize the risks and impacts, have an effective strategy in place. Establish and maintain partnerships with your upstream network provider, who can assist during an attack by implementing traffic blocks and other mitigation strategies. Minimize the likelihood that your organization becomes part of a DDoS attack in the first place by properly configuring firewalls and IDS/IPS devices to accept only traffic related to your organization's business needs, and to alert on anomalous traffic. Check out the CIS Guide to DDoS Attacks for additional mitigation steps.

Lee Myers, GCIA, GCIH - Security Operations Center Analyst

New Variants of Tech Support Call Scams

In a tech support call scam, malicious actors call victims and claim to work for well-known companies, informing the victim that their computer is either infected or attacking another computer and that only they can remediate the problem. The hacker will prompt the victim to take certain actions in order to successfully carry out the attack. In most cases, the main motive for these types of scams is monetary gain, which could be achieved by requesting payment for services or products, such as an antivirus, or by installing malware on your system without your knowledge in order to collect sensitive information. In 2014, CIS observed several new variations of the tech support call scam, which will likely become more popular throughout 2015, as cyber criminals continue to seek different ways to dupe end users. If you receive an unsolicited tech support call, you should hang up and report the incident to either your local police department, IT department, and/or the Internet Crime Complaint Center (IC3; www.ic3.gov). For more tips on recognizing and avoiding tech support calls scams, check out the CIS Primer.

Increased Use of Near Field Communications for Everyday Transactions

Near Field Communications (NFC)--which enables two devices to communicate with each other over a very short distance of just a few inches--will be increasingly used for everyday transactions and tasks as more devices become interconnected through the Internet of Things (IoT). NFC technology is built into some smartphones (via apps such as Google Wallet and Apple Pay) and credit cards, and many retailers are accepting this technology for payment. Other uses of NFC include file transfer, climate control management, and keyless/wireless home and car door locks. It is important to note that there is no security included in the NFC specification, and therefore it is critical that the application being accessed through NFC has proper security controls (e.g., password/PIN, encrypted communications).

Ted Fischer – Security Operations Center Analyst

The Evolution of Ransomware

Ransomware is malware that locks a computer and demands a ransom in exchange for the password. Typically, ransomware leaves the victim with one of two options: restore from backup or pay the ransom. However, in the coming year, victims might only have one choice—pay the ransom— as ransomware authors will likely look for ways to prevent file restoration from backup. Another likelihood in 2015 is the spread of self-replicating ransomware. Currently, ransomware encrypts drives connected to a single system and does not run again unless a user interacts with it. What would happen if the ransomware could spread from machine to machine? With the discovery of VirRansom, the first observed self-replicating ransomware in the wild, this threat will likely continue to evolve. Having proper security controls in place and using best practices, such as not clicking on suspicious links or opening unknown attachments, can help minimize the likelihood of becoming a victim of ransomware. For additional resources, check out the CIS technical paper Private and Public Key Cryptography and Ransomware.

Sarah Kelly, GCFA-Senior Computer Emergency Response Team (CERT) Analyst
David Kreuzburg, GCIA, GPEN, GCFA-CERT Analyst
Bradley Mcalister, GCFA, GXPN-CERT Analyst
Mike Richie, GCIH, GCFA, GREM-Senior CERT Analyst

Windows Server 2003 End of Life

On July 14, 2015, Microsoft will no longer provide support for Windows Server 2003/R2, meaning organizations will no longer receive patches or security updates for this software. Expect these outdated servers to become prime targets for hackers unless they are upgraded or isolated. If your organization hasn't already implemented a risk-based mitigation plan, do so immediately. Identify all Windows Server 2003/R2 instances; inventory the software and functions of each server; prioritize each system based on risk and criticality; map out a migration strategy; and execute the strategy.

Laura Iwan, CISSP, CISM - Senior Vice President, Programs

intended to help improve the organization's overall cyber security posture. This is especially critical if employees access their work network from their home computer. Organizations have permission and are encouraged to brand and redistribute this newsletter in whole for educational, non-commercial purposes.
Disclaimer: These links are provided because they have information that may be useful. The Center for Internet Security (CIS) does not warrant the accuracy of any information contained in the links and neither endorses nor intends to promote the advertising of the resources listed herein. The opinions and statements contained in such resources are those of the author(s) and do not necessarily represent the opinions of CIS.