State of West Virginia

Monthly Cyber Security Tips

NEWSLETTER

January 2011 Volume 6, Issue 1

Cyber Security Emerging Trends and Threats for 2011

From the Desk of the West Virginia Office of Information Security and Controls – Jim Richards, Director
(Jim.A.Richards@wv.gov)

The year 2010 was another busy year for cyber security professionals and end users, as we faced a number of cyber security incidents and events. Twenty million new strains of malware were created (including new threats and variants of existing families) in 2010, the same amount as in the whole of 2009.[i][1] The number of malicious websites identified in 2010 increased more than 100% from 2009.[ii][2] More than 11 million records were involved in data breaches in 2010.[iii][3]

What are some of the challenges we'll face in 2011? Below are highlights of the cyber security threat landscape as we look ahead to the new year.

Mobile Devices
The growth in the use of mobile devices—and the applications being deployed on them--will continue, making these devices increasing targets for cyber criminals. Experts predict that threats for the mobile operating systems will increase significantly this year.

Botnets and Malware
As the automation and sophistication of botnets increase, they will continue to proliferate. Estimates are that 95% of the world's spam is generated by botnets, infecting approximately 100 million computers[iv][4]. Researchers are uncovering close to 100,000 new malware samples a day, making it increasingly difficult to protect against the high volume. [v][5]

Hactivism
Attacks carried out as cyber protests for a politically or socially motivated purpose are expected to increase. Some suggest that the recent WikiLeaks is a precursor of similar types of activities to come. Attack campaigns, such as those initiated by Anonymous group and Operation Payback, spam campaigns, and Distributed Denial of services will continue to gain popularity, despite attempts to criminalize these acts.

Exploits of Social Media
Social media sites will continue to be attractive targets for cyber criminals. The volume of users, along with the amount of personal information they are posting, is increasing exponentially. This combination provides a "petri dish" for social engineering and other scams. Sites that use URL-shortening devices will be of particular concern this year, as these shortened URLs make it easier for cyber criminals to direct unsuspecting users to malicious sites. McAfee estimates more than 3,000 shortened URLs per minute are being generated. [vi][6]

Application Vulnerabilities
Too many applications are deployed without adequate security controls. As more applications are developed and deployed across multiple platforms, cyber criminals will increasingly target these applications to gain access to data, due to vulnerabilities attendant in the applications.

Cloud Computing
The move to cloud computing will continue as organizations strive to save money and add flexibility to their operations. Due to the aggregate volume of data that is resident in the cloud computing environments, we anticipate that it will be a target that will attract cyber criminals. They will identify new methods to infiltrate these environments and gain access to data.

Increasing use of Apple Macintosh Computers
As the use of Apple Macintosh Computers increase, they may become larger targets for cyber criminals looking to take advantage of a growing pool of users and exploit potential vulnerabilities in the operating system.

What Can You Do?
By using sound cyber security practices, users and organizations can strengthen readiness and response to help defend against the myriad challenges, and mitigate potential impacts of incidents:

- Make sure that you have encryption and password features enabled on your smart phones and other mobile devices. Use strong passwords, ones that combine upper and lower case letters, numbers, and special characters, and do not share them with anyone.
- Properly configure and patch operating systems, browsers, and other software programs.
- Use and regularly update firewalls, anti-virus, and anti-spyware programs.
- Be cautious about all communications; think before you click. Use common sense when communicating with users you DO and DO NOT know; Do not open email or related attachments from un-trusted sources.
- Don't reveal too much information about yourself on social media websites. Depending on the information you reveal, you could become the target of identity or property theft. Be wary of scams, such as fake profiles designed to exploit your trust.
- Organizations considering a move to a cloud-based environment should fully research the risks and benefits of cloud computing before moving to that environment. It is critical that your security requirements are addressed in contractual agreements in advance.
- Allow access to systems and data only by those who need it, and protect those access credentials.
- Follow your organization's cyber security policies, and report violations and issues immediately.

For More Information:
Georgia Tech InfoSec Center
http://www.gtisc.gatech.edu/pdf/cyberThreatReport2011.pdf

McAfee List of Targets for Emerging Threats 2011
http://newsroom.mcafee.com/article_display.cfm?article_id=3711

Panda Labs Security Trends for 2011
http://press.pandasecurity.com/usa/news/pandalabs-predicts-security-trends-for-2011/

Websense 2010 Threat Report
http://www.websense.com/content/threat-report-2010-introduction.aspx

Follow your organization's cyber security policies, and report violations and issues without delay.
For more monthly cyber security newsletter tips visit:
http://www.technology.wv.gov/security/Pages/monthlynewsletter.aspx

Brought to you by: ***and***

www.msisac.org *www.wvisac.org*

---

[i] http://press.pandasecurity.com/wp-content/uploads/2010/05/PandaLabs-Annual-Report-2010.pdf

[ii] http://www.websense.com/content/threat-report-2010-web-security.aspx

[iii] http://www.privacyrights.org/

[iv] http://www.informationweek.com/news/security/reviews/showArticle.jhtml?articleID=227701135

[v] http://www.gtisc.gatech.edu/pdf/cyberThreatReport2011.pdf

[vi] http://newsroom.mcafee.com/article_display.cfm?article_id=3711