

White Paper

Types of IT Security Threats and their Consequences

Introduction

Businesses face huge hazards and liabilities in the event of a security breach through their web applications, network or office environment.

Due to the shadowy relationship of hackers to organized crime, the ability of cyber criminals to launch multiple attacks simultaneously and the limited ability of businesses to detect when a breach has occurred, measuring the size of the overall threat is a challenge. But industry analysts tend to agree that threats have increased exponentially just in the past few years. This has occurred even as the ability of law enforcement, regulators and targeted organizations struggle to adapt.

Regular network vulnerability and web application vulnerability assessments are recommended as part of a series of security procedures for organizations to gain compliance. Security is a process of steady assessments and improvements, not a one-time fix.

This white paper is an introduction for CEOs, department heads and managers who want a better understanding of the threats that organizations face today.

The Security Threat

There are a wide range of security threats that can penetrate web applications and networks. Managers should note that while the vast majority of attacks come from the outside, security breaches from the inside (from disgruntled former employees, industrial spies, etc.) can be even more damaging. Organizations need to ensure technology, procedures and systems are in place to protect against threats to their network assets and online applications from either direction.

Below is a discussion of some threats organizations may face, although it is not an exhaustive list (For a comprehensive list of the most recent security threats, it is recommended to read the SANS Institute Top-20 Security Threats list available online).

Browsing for trouble

The most basic online activities of your staff, including browsing the web, can create serious vulnerabilities. All browsers, including the most popular ones today, such as Internet Explorer and Firefox, contain vulnerabilities. They require constant patching and upgrading to keep up with the latest hacker threats. Un-patched browsers represent a significant threat, as computer systems can become compromised simply from staff browsing infected sites.

Even if an organization has instituted the most effective security to protect its own web applications, browsing of infected websites by employees can lead to a security breach. Regular updating of browsers and avoidance of known insecure sites is recommended as minimum precautions to protect organizations from a security breach.

In order to mitigate the risk, it is recommended for organizations to demand a high level of web security compliance from partners and suppliers. Businesses can at least try to ensure a level of security in the organizational networks that they routinely contact. As more informal business networks enforce this minimal level of security, the risk of security breaches across entire industries may be reduced.

Security vulnerabilities in your network

Network assets such as applications and hardware that have become integral to modern businesses are also potential vectors for infections to computer systems.

For instance, common office applications such as word processing and spreadsheet applications, presentation software and other applications have a number of vulnerabilities. Media players for audio, video or images can also be exploited to install malware and hijack operating systems. Even physical hardware like keyboards and printers have been involved in attempts to hack into systems.

Email is another critical problem area, where phishing attacks, attempting to persuade victims to hand over private information, have become frustratingly prevalent.

Threats to websites and web applications

Hackers can penetrate web applications and install malicious code through a range of vulnerabilities, including forms, comment areas, third-party widgets and many other points.

Hackers can deface sites with obscene or hateful messages. But more sophisticated hackers attempt to hide their presence, so they can use the infected site as a vector to hack all of the website visitors' computer systems. Other hackers may attempt to access databases or gain access to other organization systems. A web application firewall and regular web security assessments are recommended to deal with this threat.

Consequences of a Security Breach

The direct costs associated with a security breach depend on a number of factors including (but not limited to) the method of the breach, scope, duration before the breach is discovered, effectiveness in containing the threat, and speed and effectiveness of damage control to back-end systems as well as reassuring partners and customers to counteract damage to brand reputation.

With so many factors, it is difficult to generalize consequences for businesses across different industries, each using a unique network and sets of online applications. Nonetheless, some facts may help provide something approximating a benchmark of consequences.

- A widely-cited Forrester Research study from 2007 surveying 28 companies showed the average cost of a security breach cost between \$90 and \$305 per compromised record (Sharon Gaudin, "Security Breaches").
- A recent Ponemon Institute study said the average number of compromised records from a security breach was about 99,000. (Darwin Professional Underwriters, "Tech//404")
- The 2007 CSI Computer Crime and Security Survey also provides a "hard-numbers" analysis of the costs of a web security breach. The average annual loss reported in the survey shot up to \$350,424 from \$168,000 the previous year. Not since 2004 have average losses been this high.
- According to marketing networking group CMO Council, a data breach could cost an average of \$14 million on recovery costs, including damage control to restore a firm's reputation. Data breaches typically caused losses of an average of 2.6% of a breached company's total customer base. (Marketing Institute, "Why IT Security Can Still Instill Confidence").

Clearly, the immediate consequences to an organization's reputation and ability to sustain continued operations can be put at risk by even a single security breach.

This is before even considering the costs of violating legal and regulatory regimes that typically call on organizations to demonstrate reasonable steps have been taken to ensure security and privacy. For instance, regulations such as PCI DSS call for stiff fines levied on behalf of credit card companies in the event that customers' private information is compromised due to insufficient network and web application security measures.

Conclusion

Organizations are facing a relentless overall security and privacy threat to their external-facing and internal IT assets and online presence. These threats can strike a company's web application or network assets, and even hardened computer systems can be compromised by unsecure behavior such as using a web browser to search on compromised sites.

The consequences of a security breach, including financial costs and injury to reputation, can be enough to seriously damage an organization or even put it out of business.

Given the scope of the threat and the seriousness of its consequences, it is incumbent on organizations to ensure reasonable steps are taken to protect computer systems and customers privacy.

Works Cited

Wikipedia. "OWASP Top 10 2007". http://www.owasp.org/index.php/Top_10_2007

Sharon Gaudin. "Security Breaches Cost \$90 to \$305 Per Lost Record". Information Week. 11 April 2007.

http://www.informationweek.com/news/security/showArticle.jhtml?articleID=199000222&cid=tab_art_sec

Darwin Professional Underwriters. "Tech//404: Data Loss Cost Calculator". <http://www.tech-404.com/calculator.html>

Computer Security Institute. "2007 CSI Computer Crime and Security Survey Shows Average Cyber-Losses Jumping After Five-Year Decline". 14 September, 2007.

<http://www.gocsi.com/press/20070913.jhtml>

Marketing Institute. "Why IT Security Can Still Instill Confidence in a Company's Reputation and Brand". 12 September, 2007. <http://knowledge.emory.edu/article.cfm?articleid=1075>

About

Pacific Coast Information Systems Ltd.

Pacific Coast Information Systems (PCIS) Ltd. is a full-service technology and consulting firm based in Vancouver. Founded in 1995, PCIS offers packaged infrastructure and network solutions that enable organizations to address security and compliance issues within today's complex IT environment.

PCIS combines the specific tools, expertise and proven processes to accelerate the problem identification and resolution of security compliance thereby lowering costs for customers.

More information about PCIS can be found at www.pcis.com

Boonbox

Boonbox, a division of PCIS, was created in 2007. Boonbox provides solutions for identity management, data backup and recovery, and managed network services.

More information about Boonbox can be found at www.boonbox.net