Hazards of Web-Surfing on “Company Time”

Trevor Reschke, Turiss, Managing Director, Mid-West

Computer security is a state of mind, not an end goal. Cyber threats continue to find ways to present themselves, regardless of the size of your organization, or how stringent the border protection is on your computer network to protect the network from external threats.

Undoubtedly, the most difficult challenge to securing a corporate network is the end user. The latest and most popular means of targeting computer networks is through the weakest link, the user’s web sessions.

There are currently over three pages of documented vulnerabilities listed for Internet Explorer 6.0 with service pack two. This is the most commonly used and up to date version of the application. In addition to vulnerabilities, there are various tools available on the internet that allow a person to setup a website with embedded malicious logic designed specifically for malicious purposes. The combination of inherent vulnerabilities and malicious web sites is unauthorized access to the contents of the visiting computers data.

Like all technology, misguided people spend their days trying to make a name for themselves by finding flaws in system design or poor software coding. Due to the inherent desire to offer the greatest “browsing experience” for a user, internet browsers offer a good deal of “plug ins” and third party applications that interface with the browser. For example, the latest remote access vulnerability in the Microsoft Internet Explorer is based on an “Improper Memory Access Vulnerability” in Macromedia Flash Player.

Obviously, the sites employing this type of malicious logic on their website are not going to be reputable web sites affiliated, or directly owned and operated by public companies. These malicious websites will be commonly found on the underbelly of the internet to include hacker sites, pornography (legal and not), gambling, Warez (stolen software/movies/music) and the random mix of "garbage" sites.

Visiting malicious websites commonly results in sensitive or personal data on the user’s computer to be accessed by persons unauthorized to do so. Once remote access has been established, the traditional escalation techniques are employed to gain total access to the computer. In many situations, the remote user then expands their footprint within the organization by targeting additional soft targets from the inside out. In extreme cases, the remote user will target computers behind the perimeter defenses using tools exploiting the other computers.

There are other hazards associated with “surfing” unauthorized Websites that could possibly damage the professional reputation of an organization. Certain information about an organization is commonly “projected” to the public when they are online. Web logs from companies who operate websites provide a great deal of information about a visiting person. This can include their IP address, which can then be resolved using a DNS reverse lookup to identify who, or what organization, is registered to the IP address.
Example:
IP address: 192.168.25.100
DNS: ip192-168-25-100.company-name.com
Registered to: Company name, names, addresses, contact information, etc.

Organizations must develop sound security policy and train employees in proper security precautions. The security policy serves as a pivotal defensive cornerstone that is enforced through rigorous training of individuals so that they know how to protect both themselves and the organization. This is simultaneously backed up through both hardware and software solutions to provide prevention, detection, monitoring, non-repudiation of information, contingency and recovery solutions. Only by providing a balanced approach to the security problem through both training and security mechanisms can an organization maximize their security posture to guard against cyber threats.

About Turiss

Turiss is a Computer Security and Information Protection consulting firm specializing in computer forensics, incident response, network security assessments, and business continuity planning.

Turiss has delivered invaluable findings, supported numerous highly sensitive projects, and proven to be the top choice when discretion is paramount.

Turiss staff leverage years of experience in conducting computer crime and intrusion investigations, computer emergency response, and corporate IT security, to assist your organization in the prevention or mitigation of complex technology incidents.

Turiss
1930 Isaac Newton Square, Suite #250
Reston, VA 20190

www.turiss.com
info@turiss.com