SUMMER 2014 E-NEWSLETTER

At Digital Mountain we assist our clients with their computer forensics, e-discovery and cyber security needs. With data security breaches continuing to make headlines and an organization's intellectual property at risk, we chose to theme our Spring 2014 E-Newsletter on intellectual property protection.

SECURING YOUR ORGANIZATION'S DATA

Work evenings and weekends from home? While on the road? While on vacation? So too do about 99% of our clients and readers. But have you ever considered how safe it is to access company files when working remotely? Or even how safe it is when you're working from the office and using such popular programs as LogMeIn or GoToMyPC? Well you should, and so should your management teams. Your data is only as secure as the users and devices that have access to it.

Believe it or not, this includes your trusted, honest family members. If you have ever thought about allowing access to one of your devices, from which you work remotely, to another user - family or not - you should think again. There was a case in California that involved a travel agency employee doing work from home, who accessed her company's network via a VPN connection (which will be explained in further detail below). The employee's daughter was allowed personal use of the same computer and from it cyber-chatted with a "boy" she met online. This "boy" turned out to be a hacker and sent a bogus picture file that the daughter attempted to open. Unbeknownst to her and her mom, a Trojan program was loaded onto the computer that allowed for remote access. Later, while the mom logged into her work network, the hacker downloaded thousands of files containing the travel agency's customers' credit card information, which were then sold and used. Forensic examination of the computer located enough information to recreate how the incident occurred and helped law enforcement in their investigation. Unfortunately, that did little to resolve the issues created for the travel agency's clients who became victims.

Whether you are an intellectual property attorney, data security professional or in another role, your duty is to protect your client or organization. You may have already taken measures regarding wireless connectivity security, removable storage devices and threats posed by employees who access peer-to-peer sharing and questionable websites. You must be prepared to deal with the threat posed by remote desktop computing.

Remote desktop computing can effectively allow a user full control of a remote computer and all programs, devices and storage locations that it has privileges to access. A form of the software must be installed on both computers to allow the computers to communicate through a network connection. Once connected, a

user must be able to log into a user account with privileges on the remote computer to have access to the programs, devices and storage locations.

Remote desktop computing has long been used as a way for IT departments to remotely service systems and provide support to employees on a corporate network. Done from inside the corporate network, with properly configured and secure computers, the remote access to an employee workstation to install software, diagnose issues, or provide support to employees with questions can be very productive and the network and data remain secure.

The examples given above, LogMeIn and GoToMyPC, are two programs that provide remote desktop computing access from anywhere a host computer is connected to the Internet. This connection is a virtual tunnel through the corporate firewall allowing the remote user to access a networked computer with full access privileges of a user account on the computer.

Many people will argue that the increased productivity by employees having access to work files from home outweighs the risk to an organization's network and data security. Remote desktop software programs tout their Secure Socket Layer (SSL) or Virtual Private Network (VPN) connection and encrypted communications between host and remote computers.

All it takes is administrator level privileges on an organization's workstation for an employee to install one of the many software programs that will allow a remote desktop connection. Once installed, the software can be configured to allow the computer to be turned on remotely, logged into by the user, and allow the user full access to the devices, data storage locations, programs and services allowed by the permissions allowed in their user account. To the user, it's as though they were sitting at the remote computer. They will see the computer's desktop and have access to programs, devices and files. A user could perform a bulk transfer or deletion of files from the remote computer or locations on the network to their computer. They could essentially copy off and/or delete everything they have permissions to access.

On the network, it will appear as though the user is sitting at the computer. It will depend on the organization's internet server logs whether information regarding the remote connection is captured. Transaction logs can capture information on network file activities if the organization has configured such tracking. On the remote computer, it will depend on the remote desktop software and configuration whether any logging of the connection and file activity will be captured. It can take extensive forensic analysis of the server logs and the remote computer to determine what activity occurred. The connecting computer may also contain artifacts such as activity logs, but the computer may not be available for examination. Without an alert set up for network administrators for this type of remote connection, all investigation will have to occur after the fact, which may be difficult to de-construct. An employee or malicious hacker could pilfer important intellectual property from the organization.

The computer which a user may remote connect to an organization's computer from may not be sufficiently protected with firewall and anti-virus software installed. It could be the family computer used for downloading videos and music via peer to peer networks. A Trojan program or Virus on the computer could put your organization's network and data at risk as soon as the connection is made, as in the example of the travel agency employee.

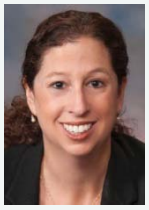
While remote desktop computing programs may offer opportunity for increased productivity, due diligence must be taken to ensure that the firewalls, servers and computers are properly configured to protect the organization's network and data. Windows 7 and 8 computers have many options built into the operating system that allow for logging of remote desktop activities and alerts to network administrators. There are enterprise remote desktop software programs that have logging, permissions, and session authorization built right into the software. Those programs offer a good platform if the decision is made to allow for remote desktop computing by employees. Restricting the use and tightly controlling the setup and configuration of the software can minimize opportunity for employee theft of intellectual property and threats to corporate network and data security.

UPCOMING INDUSTRY EVENTS

July 2014

Today's General Counsel Event: July 16-17
Masters Conference, Half Day EDiscovery and Social Media Conference: July 22
The 6th Annual Sedona Conference International Programme: July 23-24
The 15th Annual Sedona Conference On Antitrust Law & Litigation: July 24-25

Click here to see more upcoming events and links



Digital Mountain, Inc. Founder and CEO, Julie Lewis, will be presenting at some upcoming industry events. Please send requests for speaker or panel participation for her to marketing@digitalmountain.com.

Know someone looking for work in the e-discovery, computer forensics and cyber security industries, with entrepreneurial characteristics? If so, please share this great job opportunity with them: Seeking a Business Development Representative to join our energetic team. ***Read more...***

DIGITAL MOUNTAIN, INC.
5050 El Camino Real, Suite 205
Los Altos, CA 94022
866.DIG.DOCS

www.digitalmountain.com

Contact us today!