CYBER SECURITY 101

MAINTAINING A SAFE VIRTUAL ENVIRONMENT BY: JACI FINNEY

Introduction:

The use of virtual environments has without a doubt increased the capabilities of businesses throughout the world by increasing efficiency and communication. Along with the benefits of virtual environments come a variety of security risks and heightened risk of identity theft and theft of sensitive data. To combat threats, it is paramount that companies focus on a comprehensive information security policy and controls which help prevent access to or the manipulation of systems and/or data. The objective of this paper is to provide readers with information about common threats and tools and techniques that can be used to protect and maintain a safe virtual environment.

Defining Security Terms:

Cybersecurity: Cyber Security consists of principles and practices that are designed to protect a company's critical infrastructure with special focus on computing assets and online information

Security Threats: Security threats comes in a variety of different forms including: intrusions, viruses, worms, trojan horses, phishing, spyware or spam (defined below).

Threat	Definition
Intrusion	Unauthorized individuals trying to gain access to computer systems in order to steal information.
Virus, Worm, Trojan Horse (Malware)	Programs that infect your machine and carry malicious codes to destroy the data on your machine or allow an intruder to take control of your machine.
Phishing	The practice of using email or websites to lure the recipient into providing personal information.
Spyware	Software that enables a user to obtain information about another's computer

	activities by transmitting data covertly from their hard drive.
Spam	Programs designed to send a message to multiple users, mailing lists or email groups.

Identity Theft: Identity Theft is a crime where an imposter steals key pieces of personally identifiable information (PII) such as social security numbers, driver's license numbers, bank account information, credit card information and other valuable information for personal gain that comes at the expense of someone else. Examples of how PII can be used are as follows: opening a line of credit, purchasing goods or services, or renting or buying a house.

Sensitive Data: Sensitive data comes in a variety of forms including trade secrets, source code, customer information, employee records or PII that a company does not want to disclose without authorization. The theft of this information can have major implications, including the loss of business, public-image damage and financial loss.

Combating Cyber Security Threats:

There are several steps that companies and individuals can take to mitigate cyber security risks. Five key activities appear below.

1. Create and maintain passwords and passphrases.

- Create and maintain strong passwords (i.e., use a combination of alphanumeric characters, upper and lower case letters, symbols, etc.)
- Consider using a passphrase
- Avoid sharing passwords
- Avoid reusing the same password for multiple accounts
- Avoid storing your password where others can see it, or storing it electronically in an unencrypted format
- Do not use automatic logon functionality
- Change passwords at least every 90 days

2. Secure your computer.

- Log off or shutdown when going home

- Disconnect your computer from the wireless network when using a wired network
- Patch and update your operating system regularly
- Install and update your anti-virus and anti-malware with the latest security definitions
- Create a unique user ID when sharing a computer with others
- Enable pop-up blocker on your browser
- Make an informed and rational decision prior to installing or downloading software on your computer
- Lock your computer when not attended
- Lock your office when you leave

3. Protect the data you are handling.

- Understand the type of data stored on your machine
- Avoid storing PII on local storage devices, e.g. laptop, USB, hand-held computers
  - Keep any PII data that you need for work on a centrally managed, secure file system.
- Consider the following when you have to email sensitive data:
  - Encrypt the data
  - Set password controls
  - Send the document password in a separate email
  - Ensure that the recipient has a need for the sensitive data
- Back up your data regularly
- Segregate your personal files by project or work type
- Securely delete data from systems before disposal when replacing or upgrading your computer

4. Assess risky behavior online.

- Be wary of phishing scams
- Be cautious when handling attachments and links

5. Be aware of internal security guidelines, policies and procedures.

Combating Identify Theft:

Cyber criminals use multiple methods to trick users into giving up personal information. Some of these methods include:

- Computer viruses
- Phishing and Social Engineering
  - Links to fraudulent web sites
  - Email
  - Phone Call

    - Mail
- Social Networking accounts

Knowledge is power in fighting against identity theft. With knowledge comes insight into the methods that cybercriminals use as well as simple steps to protect one's personal information. Most people keep important information on work and personal computers, cell phones or tablets. To protect the data stored on these devices, it is important to always lock devices using password protection while in public places to keep them safe. Passwords should be easy to remember for the user but hard to guess and configured to include at least eight characters, including letters, numbers and symbols.

The next step to protecting data is to focus on the network payer and use of firewalls, virus and spyware protection software that is updated automatically or regularly. Virus and spyware protection should never be downloaded by a source unless it is known such as McAfee or Norton Antivirus which can be downloaded straight from the vendor websites. Finally, always remain skeptical of web pop-up windows and unsolicited messages. These often contain viruses or other forms of malware that can harm or be setup to steal information from your computer.

Another common method employed by cyber criminals is known as phishing, which involves email, mail or phone calls designed to trick users into thinking they are legitimate representatives from a bank, store, government agency or some other official organization. A good rule of thumb is to never give out personal information unless you made the initial contact. And NEVER respond to a request for your account number or password information as a legitimate company would generally not ask for this information.

If there is suspicion of a security breach it is important to take the following steps:

1. Disconnect from the Network

2. Do NOT turn off the computer

3. Do NOT use or modify the computer

4. Contact the company Information Security Officer (ISO)

5. Preserve external backup or log

Combating Theft of Sensitive Data:

The theft of sensitive data can originate internally or externally. The complexity of computing environments in addition to multipart network perimeters and decentralized storage of sensitive data creates opportunities to steal information. Because of this, it is important for management to monitor their systems for intruders.

To protect against intruders, there are products to monitor e-mail, websites and other system usage to keep malware from entering the network as well as block or flag inappropriate use. These tools identify breaches and suspicious usage based on pre-selected and customizable network protocols, traffic patterns and file types in communication streams. Some tools analyze words and groupings of words for suspicious activity, while others can determine the context of what's being done with files. Many look for binary signatures of sensitive information and files rather than relying on filenames and extensions, which can easily be removed, renamed, or otherwise obscured. Some even analyze network traffic patterns and build a big-picture vision of suspicious behavior, alerting security administrators to top talkers--computers, applications or users generating the most network traffic--and protocols in use.[1]

In addition to monitoring sensitive data, it is also important to know how to handle sensitive data.

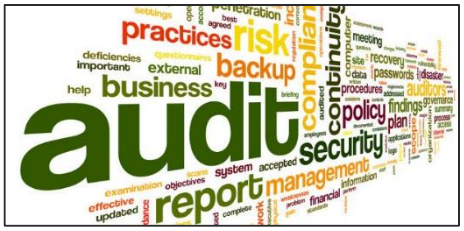
These steps include:

1. Know what data is stored on your computer

2. Delete what is not needed or move information that is not in a correct location

3. NEVER store sensitive data on a personal computer

4. ALWAYS encrypt sensitive data that is at rest and or in motion



General Remediation Strategies

Security Audits and Controls

A survey by a computer security institute ranked internal cybersecurity audits as the strongest fraud deterrent in the prevention and detection of cybersecurity vulnerabilities. Cybersecurity audits are most successful when a company has a risk assessment program in place to identify risks and assess the severity of each risk to develop mitigation strategies.

Once an audit or risk assessment has taken place and vulnerabilities have been identified, preventive controls should be put into place. A few examples include:

- Timely and proactively scanning and patching of vulnerabilities
- Comprehensive logical access controls such as role based access privileges, firewalls, Intrusion Prevention Systems (IPS) and Intrusion Detection Systems (IDS)

[1] http://searchsecurity.techtarget.com/magazineContent/Preventing-Data-Theft-Combating-Internal-Threats

- Monitoring systems using tools and techniques such as an IT infrastructure monitoring tool, penetration testing, and a heartbeat monitoring tool

Conclusion

The anonymity of cybercriminals and technical nature of their crimes makes them extremely different from traditional criminals. But the fact is that, many times, their crimes are just as destructive to the person or company being targeted. And unfortunately, the fact that they are remote, helps them successfully commit crimes and evade law enforcement. Over the past few years there has been a significant increase in the number of cybercrimes taking place. In fact, organized crimes rings have expanded their operations to include computer hackers to further exploit and increase damage to their victims. In short, the face of crime is rapidly evolving and we need to take proactive steps to keep up. Having the knowledge and resources to prevent and detect cybercrimes is the key to successful information and data security.

Resources:

1. https://www.dhs.gov/cybersecurity-overview

2.http://www.aicpa.org/INTERESTAREAS/INFORMATIONTECHNOLOGY/RESOURCES/PRIVACY/CYBERSECURITY/Pages/InformationSM.aspx

3. http://searchsecurity.techtarget.com/magazineContent/Preventing-Data-Theft-Combating-Internal-Threats