

INTERNET SECURITY IN COMPANIES

Nowadays, many companies have suffered from cyber attacks, that's why it is important for them to properly secure their data and protect their employees and customers information.



Useful Words

Introduction & general overview

Internet safety nowadays has become a serious and sometimes dangerous issue for the users and the companies. Internet security is all about trust at a distance. That is because you are dealing with everyone remotely and not able to confirm identity or authenticity in the traditional sense. Even with secure connections, encryption, and the various other authentication schemes there is always a way to spoof identity, provide forged documents or credentials, hold computers and servers hostage to “ransomware” or allow cyber-criminals to be whoever they want to be. No organization is immune to the loss or compromise of confidential and sensitive data.

Malicious Code: Program which causes internal damage to a computer network.

Spear Phishing: Spear phishing is an email that appears to be from an individual or business that you know but it isn't.

WPA: The name for a number of standards to use encryption on a Wireless LAN.

Cyber Attack: Cyber-attack is any type of offensive maneuver employed by individuals or whole organizations that targets computer information systems, infrastructures, computer networks, and/or

Introduction & general overview

Consumer information, employee records, proprietary and trade secret information, and intellectual property are all available for the taking if infrastructures are not properly protected and contingency plans developed should a breach occur. While many businesses may understand the potential threat they are often not prepared to deal with an incident, or they naively believe it will never happen to them. It is not simply a technical issue and can impact customers, employees business associates and the public perception of

PROBLEM: Malicious Code is the term used to describe any code in any part of a software system or script that is intended to cause undesired effects, security breaches or **damage** to a system.

SOLUTION: Install and use **anti-virus programs**, anti-spyware programs, and firewalls on all computers in your business. Moreover, ensure that all computer software is up-to-date and contains the most recent patches (i.e., operating system, anti-virus, anti-spyware, anti-adware, firewall and office automation software).

PROBLEM: Spear Phishing is an **email** that appears to be from an individual or business that you know. But it isn't. It's from the same criminal hackers who want your credit card and bank account numbers, passwords, and the financial information on your PC.

SOLUTION: It's important to make your employees aware of what a spear phishing attack is and to be on the look out for anything in their in-box that looks **suspicious**. Employees should never respond to spam or pop-up messages claiming to be from a business or organization that you might deal with

PROBLEM: Unsecured Wireless Internet Networks According to news reports, hackers pulled off the "biggest data breach ever" through a **wireless network**.

SOLUTION: When setting up a wireless network, make sure the default password is changed. Most network devices, including wireless access points, are pre-configured with default administrator passwords to simplify setup. Changing default passwords makes it harder for attackers to take control of the device. Moreover, make sure you **encrypt** your wireless network with WPA encryption.



Useful Links

<http://smallbiztrends.com/2007/06/top-five-small-business-internet-security-threats.html>

<http://us.norton.com/spear-phishing-scam-not-sport/article>

<http://www.referenceforbusiness.com/small/Inc-Mail/Internet-Security.html>

http://www.webopedia.com/TERM/M/malicious_code.html

Sony Entertainment Hack

The Sony Pictures Entertainment hack was a release of confidential data belonging to Sony Pictures Entertainment on November 24, 2014. The data included personal information about Sony Pictures employees and their families, e-mails between employees, information about executive salaries at the company, copies of (previously) unreleased Sony films, and other information. The hackers involved claim to have taken over 100 terabytes of data the hackers implanted Wiper on Sony's computer infrastructure, a malware software program designed to erase data from the servers. Sony Pictures set aside \$15 million to deal with damages from the hack.

Anthem Medical Data Breach

On February 4, 2015, Anthem, Inc. disclosed that criminal hackers had broken into its servers and potentially stolen over 37.5 million records that contain personally identifiable information from its servers. According to *The New York Times* about 80 million company records were hacked, and there is fear that the stolen data will be used for identity theft. The compromised information contained names, birthdays, medical IDs, social security numbers, street addresses, e-mail addresses and employment information, including income data.

Staples cyber attack

Staples has revealed that a cyberattack that hacked into two of its stores in July and continued at 111 or more stores through September stole personal information from an estimated 1.16 million payment cards. The malware responsible for the attack penetrated the cash registers and terminals that dealt with credit and debit cards. The malware seized information that was on the cards, including the name on the card and the card number, as well as the expiration date and the card verification code on the back of the card.

SUMMARY

In today's world Internet Security is vital for both private people but even more for companies. Without proper security important data might be stolen and everyone is in danger of being hacked. To protect the companies it's good to install proper software like anti-virus programs and inform the employees. Additionally it is advisable to only use secured wireless networks by encrypting it with a WPA encryption.

Group members

Pavlos Nikolaou
Sandra Mayer
Sara Luks
Leon Axwalter
Atle Espenes



