Types of software attacks

Bastiaan Vermeulen

Business Information System COM-327-CA02

Abstract

Available evidence suggests that cyber threats are a growing problem that has big consequences for companies digitally and financially, not the least of which is billions of dollars in financial damage. There is a growing need for cybersecurity to protect businesses' intellectual properties. The scenario for this paper is that as a newly hired assistant manager you get asked by your manager to conduct a good review of different types of software attacks. This paper is about what types of software attacks there are, how devices get infected by them, how the malicious software operates, and what actions the manager should take in order to prepare and defend the organization against these types of attacks. The hypothesis is knowing the possible threats and using countermeasures such as anti-virus and anti-malware software efficiently to ensure sensitive data is safe.

Types of software attacks

Cybercrime is on the rise, worldwide 600 billion dollars is lost to cybercrime each year, nearly one percent of global GDP, according to the Center for Strategic and International Studies (Lewis 2018). School districts, hospitals, local and state governments, law enforcement agencies, small businesses, large businesses, basically everyone is subject to this phenomenon. A total of 978 million people in 20 countries were affected by cybercrime in 2017, according to Norton Cyber Security Insights Report Global Results. These numbers clearly support the opinion that cybercrime is one of the biggest challenges any type of organization will face in this digital era.

So it's reasonable for companies to assess their technological security vulnerabilities and to prepare for possible attacks. There are many ways in which a hacker attacks a secured network or an organization. Before the hacker attacks, it will decide on its target such as an application, network, password, a cryptographic algorithm and so on. If one of the systems in a network is compromised, then the hacker can get all the information going through the network. It's critical for a business to make sure their network as a whole is waterproof against software attacks. This paper is about what types of software attacks there are, how they can infect devices, how it operates, and what actions the manager should take in order to prepare and defend the organization against these types of software attacks. The hypothesis is knowing the possible threats and using countermeasures such as anti-virus and anti-malware software efficiently to ensure sensitive data is safe.

The different types of software attacks are spyware and adware, phishing and baiting, keystroke loggers, sniffing and spoofing, computer crime and fraud (Bidgoli 2019). These software attacks can be used to invade the user's privacy and commit computer crimes. Many of these attacks can be prevented by minimizing the risks by installing system updates regularly, using good antivirus software, and using e-mail security features.

Spyware and adware are one of the most common threats on the internet. It can easily infect a device and it can be hard to identify whether it is already running on your computing device. Spyware is a threat to everyone since it can steal sensitive information and harm your network and computing device. Spyware is classified as a type of malware: "malicious software designed to gain access to or damage your computer, often without your knowledge. Spyware gathers your personal information and relays it to advertisers, data firms, or external users" (What is spyware? And how to remove it 2019). Spyware can infect a company's computer by using trojans, viruses, cookies, private networks, unsecured and unencrypted websites. Spyware infects your device and gathers information about you, including the websites you use, the things you download, your usernames and passwords, payment information, and the emails you send and receive. Adware can collect that information about the user and provide misleading marketing in your browser by offering (fraudulent) software bundles, sensitive information that is found can be used against you or can be forwarded to other entities without the consumer's consent. Spyware can cause two main problems, it can steal personal information that can be used for identity theft or intellectual property theft and it can damage your hardware and software by taking up an enormous amount of storage, making it run slow, causing the system to crash, freeze and even overheat causing permanent damage. Besides that, spyware can manipulate search engine results and deliver unwanted websites in your browser, which can lead to potentially harmful websites or fraudulent ones, It can also alter some of your computer's settings in order to disturb the computer.

Phishing is defined as "sending fraudulent e-mails that seem to come from legitimate sources, such as a bank or university. The e-mails usually direct recipients to false web sites that look like the real thing for the purpose of capturing personal information, such as social security numbers, passwords, bank account numbers" (Bidgoli 2019). Phishing is similar to baiting which differs from phishing by a promise that the baiter gives to the recipient, for

example, a website could ask to fill in a form and as a reward, you get a gift card or an iPad, by doing this it tries to steal personal information. This phenomenon is really based on the social engineering principle which “is the act of tricking someone into divulging information or taking action, usually through technology. The idea behind social engineering is to take advantage of a potential victim’s natural tendencies and emotional reactions” (What is social engineering? Tips to help avoid becoming a victim). This means that phishing and baiting try to deceive a user by having the user put in personal information for a “specified”, illegitimate reason or reward.

Keyloggers can capture just about anything a user’s computer. The malicious program monitors all keystrokes on a computer. All emails, chats, websites visited, programs run, passwords put in are stored and can be viewed by a hacker. Computers often get infected by keyloggers through pieces of software that are disguised as legitimate software or as freeware, called trojans. This is possibly one of the worst attacks a user and a company could overcome because it can literally do anything to the computer and the network, stealing information, altering information, destroying information, encrypting the computer and making a fraudulent offer to the user to decrypt the system for money (Grebennikov 2007).

Sniffing means capturing and recording network traffic. These practices can be done for legitimate reasons such as monitoring and troubleshooting network traffic, but hackers use it to look through data packets that are sent over a network, trying to steal sensitive information. Spoofing is trying to gain access to a network by posing as an authorized user in order to find sensitive information related to the business. To prevent sniffing happening to the organization, employees should only connect to trusted networks with their devices (no public networks), the company should encrypt all the traffic that leaves the system (this makes sure that even if the traffic is being sniffed, the hacker will not be able to read the data packets), and networks must be scanned for any kind of intrusion or irregularities in the

network, network administrators must monitors networks to ensure the safety of the sensitive information. To prevent spoofing employees should be educated on this phenomenon, trying to find the signals that the person that actually tries to use social engineering to get in a system through a legitimate employee of the company (Passi 2018).

Computer fraud is the unauthorized use of computer data for personal gain. Examples of this could be transferring money from someone else's account to yours or charging purchases to someone else's account. Besides that computer crimes is a broad topic, it includes denial-of-service attacks, identity theft, intellectual property theft, distributing child pornography, e-mail spamming, spreading malicious programs, stealing information, changing information illegally.

Any malware installed on one of the company's devices can be removed by using good anti-virus software and firewall that will find and remove any malicious programs from the computers. Good anti-virus software vendors are Kaspersky, McAfee, Norton, and Bitdefender.

Ways to prevent software attacks from infecting the company's systems depend on the employee's online behavior. It is critical that any employee that works with the internet, e-mail, and information systems, is well-educated on possible software attacks and security vulnerabilities. Behavior like not clicking on links within pop-up windows, not downloading free downloadable software, not clicking on any weird email links claiming to offer any too good to be true offers, only use secure and encrypted networks. Besides this education, all systems need to be patched, need to have firewalls and anti-virus software, and need to be overseen by a network administrator with a good understanding of information security.

To conclude this research, there must be a good understanding of how important information security is in nowadays society. On every level in a company, there should be

enough knowledge about information security, there should be educational meetings where the most recent trends of software attacks and security vulnerabilities for the company are discussed. All systems have to be patched, protected, and the network should be overseen by a network administrator.

References

Bidgoli, H. (2019). *MIS9 Management Information Systems*. Boston, MA: Cengage.

Grebennikov, N. (2007, March 29). Keyloggers: How they work and how to detect them . Retrieved November 12, 2019, from https://securelist.com/keyloggers-how-they-work-and-how-to-detect-them-part-1/36138/.

Lewis, J. A. (2018, February 21). Economic Impact of Cybercrime. Retrieved November 12, 2019, from https://www.csis.org/analysis/economic-impact-cybercrime.

Passi, H. (2018, August 14). What is a Sniffing attack and How can you defend it? Retrieved from https://www.greycampus.com/blog/information-security/what-is-a-sniffing-attack-and-how-can-you-defend-it

What is social engineering? Tips to help avoid becoming a victim. (n.d.). Retrieved November 22, 2019, from https://us.norton.com/internetsecurity-emerging-threats-what-is-social-engineering.html.

.