Cybersecurity Practices for Preventing Computer Hacking

Posted on August 10, 2018

Key Concepts in Hacking and Cybersecurity

Hacking: Getting unauthorized access to data that is not public for ill use or personal benefits. (National Institute of Standards and Technology, 2024)

Hackers: the people who hack into the computers.

Cyber: “of, relating to, or involving computers or computer networks (such as the Internet) the cyber marketplace” (Webster’s Dictionary)

Warfare: Is a conflict using or targeting computer

Computer Hacking and Cyberwarfare

Hacking is a term used to access data through skills. It is illegal but has socioeconomic benefits for hackers. Hackers access classified data of the state, company, or individual and steal personal, company, or the state’s important data.

Hackers: competent computer hackers are people with expert computer skills who remain far away and access information on the computers of individuals or agencies.

Cyber: It is related to computers and the internet

Cyberwarfare is the conflict or war targeting computers within the country or organizations in other countries to damage the computers and networks, delete the data, steal it, or sell it to earn money or defeat competing companies.

Common Cyberattack Techniques

Ransomware: malware that restricts access to the file or computer and demands payment

Malware: Malicious software that infects the computer

Phishing: Fake emails, messages, and websites that look like authentic

Spyware: Software to collect personal information

The man in the middle: The hacker alters the communication between two people

Keylogging: Records keystrokes

Botnets: malware that infects the computer without the computer owner's knowledge

Hacking Methods and Business Risks

These are the various techniques hackers use to attack computers and data on them. With the advancements in technology, many new techniques are introduced to hack and steal information from people. In ransomware, a message pops up when a user opens theipopupster to deny their access to the computer and demand payment to get access. The malware infects computers and damages data saved in computers. It also steals information and sends emails on the company's or person's behalf. Phishing or spoofing is the fake emails that appear authentic and steal information from people. Spyware collects personal data without consent or being visible to the owner of the computer. It is software that gets installed on the computer with free installation programs that are downloaded. The man in the middle is a technique through which the hacker goes in the middle of two parties to hack the information. They can lead and alter the conversation to get information. In key Logging, every keystroke is recorded, and the activities of the users are recorded with each stroke using software that records the strokes and the information. Bonnets are a network of private computers infected with malicious software and controlled as a group without the owners' knowledge, e.g., to send spam. There are other types of hacking techniques that are not mentioned here, and the number of techniques is increasing as people get remedies for the old hacking techniques.

- For Fun
- For experimenting with their skills
- To damage the reputation
- For monetary gains

Some people do it for fun, and others are interested in testing their computer skills. They want to know what real hacking is and what threats it is related to. However, some malicious people do it for monetary gain. To impersonate others and access their credit cards or tax returns. Big companies do it to damage their competitors or create problems for them. In some instances, they use their data and plans to get projects.

- To create problems for the competitors
- To get information
- To Steal

Some countries use hacking to get information about other countries and companies so that they

know what other companies are up to and whether they are a threat to their security or not. Therefore, the purposes can vary from person to person and company to company. However, the heinous ones are those where people use hacking to stain the reputation of other companies or individuals. They do not seek money; they only want to damage the reputation of the person in the society. It is a problem because:

- It can affect anyone.
- The threat to privacy
- Damages the reputation of companies or individuals
- Identity theft
- Financial fraud

Hacking is a problem because the target can be anyone. People cannot be at peace because it is someone else. It makes everyone vulnerable. Hackers can target anyone. It is a threat to the privacy of computer users. Unknown people trolling and getting information about you is discomforting and creates problems. It enhances insecurity and anxiety among people. It decreases privacy, making people vulnerable to hackers who stay behind computers. Hackers can also use the information they obtain to damage the reputation of the company or individuals. They can change the facts and bring forth the secrets of a company and individuals. Moreover, some of the hackers can use their identity to attack others or gain monetary benefits by applying for tax returns or health insurance. They can use the personal information for fraudulent activities that hamper the person and might indulge in criminal activities. Many companies lose important information to hackers, which can create problems for the employees or company. For instance, Sony paid around $14 million to former employees because the hackers distributed emails and other personal information to the employees in 2014. Targeting personal information such as credit card and tax returns is a way to avail financial opportunities.

- Loss of information (200,000 people Equifax)
- The threat to intellectual property
- Security Threat
- Damage to property
- Financial losses

Loss of information is a serious threat to people using hacking techniques. In 2017, 200,000 employees and former employees lost their social security numbers, passport numbers, credit card numbers, email addresses, names, birthdates, tax ID numbers, home addresses, phone numbers, driver's license numbers, and other personal information to hackers. It leads to crimes using the personal information of these people. Moreover, the hackers are a threat to the intellectual property. (Joint Task Force, 2020)

The hackers can access the private unfinished work of creative innovators and hack their products and damage the property to publish the work online or sell it to the competitors. Like Sony, many

other companies, such as Equifax, have lost a huge amount of money in settling cases related to internet security.

Major Cyberattacks and Data Breaches

Here are some famous cases of Hacking in the US:

- Morris worm 1988 (affected 6000 computers costing $10-100m)
- Mafiaboy 2000 (attacked commercial websites cost 1.2 b)
- Stole millions of credit card details (2009)
- In the 2013 attack on Yahoo

Tappan Morris created the first virus that cost 10-100 million dollars. He was then a student at Cornel University. His virus replicated and damaged computers. Mafiaboy was a DDoS attack by a 15-year-old that affected websites such as eBay, Yahoo, Amazon, CNN, and others. In 2009, Albert Gonzalez stole more than 130 million credit card details, and he was formerly working with the US government. He staged one of the biggest identity thefts in 2009 from banks and payment systems. Similarly, in 2013, one billion user accounts were stolen from Yahoo. It includes personal information, phone numbers, credit card information, and other information. These were the only glimpses of the threats of cyber attacks. Many companies lost billions of dollars in 2016 and 2017.

- WannaCry: Attack health service providers
- Petya?Notpetya: infected networks in Multiple countries
- Wikileaks: stole 8761 documents from the CIA
- Attack on global banks 2015 (£650 M)

WannaCry ransomware debilitated the health system in the UK for almost a month. Most of the machines and computers could not work, and it pushed back the health services to the time of manual data entries and services. Petya/Not Petya was better than wanna cry and affected US pharmaceutical companies along with many other companies in various countries. The attack affected Ukraine the most. Wikileaks created a lot of controversies because it disclosed classified information from the CIA regarding spying and operations. (Cybersecurity and Infrastructure Security Agency, n.d.)

In 2015, Russian hackers used malware to infiltrate banks and stole £650 million from 100 institutions around the world. These cases are a few examples of the famous attacks that caused billions of financial losses to companies. As you can infer from the cases, all kinds of institutions can be the target, whether it is a financial institute or a health care system. Hackers only focus on the benefits, and they do it to damage and gain money in most cases. Therefore, it becomes an ethical concern for people.

- Stealing

- Threatening
- Destroying

It is a serious problem because it poses a threat to the property of individuals and companies. Individuals work hard to save money, but hackers steal their money using credit card information. Similarly, they damage a company's property and data for personal gain. It is ethically wrong to steal or damage other people's property. It is unethical to troll people's emails and messages; it is unethical to access emails and other data without consent. It is also unethical to threaten and damage the reputation of the people to take revenge or stain the reputation of the company.

As you can see, this is the record of major data breaches that have affected various companies globally. The data provided presents the major data breaches from 2007 to Oct 2017. Identity theft was the cause of 50 percent of these breaches, making it the most common way of hacking security threats. JP Morgan Chase affected 76 million households. The data for 76 million households were stolen. Similarly, Friends Finder Network Inc. lost data of 412 million people. However, Yahoo faced the highest data loss. The revelation of December 2016 showed around 3000 million families were affected by the data loss. The victims of the attacks can bear severe legal consequences for:

- Theft
- Fraud
- Forgery
- Intellectual Property

Hackers use the personal information of other people to commit theft, fraud, and other crimes. These crimes can cause legal consequences for the victims because the hackers use their information to commit crimes. They use the information for forgery. Moreover, it is a serious threat to the intellectual property of innovative or creative people.

Economic Costs and Affected Industries

The graph shows the worldwide average annual cost of cybercrimes in a million US dollars. For instance, cybercrimes have cost the hospitality industry an average of 5.04 million US dollars worldwide, and it is the industry with the least attacks by cybercriminals. Other industries, such as education and transportation, are affected hugely.

The most affected industries are financial services industries, with a loss of 18.28 million US dollars to hackers or cybercriminals, but it is an average annual cost. One industry suffers millions of dollars every year from cyber-attacks, which is a huge amount of money.

This graph shows the total cost that an organization incurs after a cyber-attack and data breach. It includes the cost of settling the lawsuits if the employees demand the company to publicly share their personal information and settling the problems in the business that the data breach caused. In 2017,

the average cost of data breaches was 7.35 US million dollars. With that amount of money, a new small setup could have been established, but the data breaches cost the companies an enormous amount of money.

The graph shows data breaches in the US by industry. It is obvious from the graph that in the US businesses and medical healthcare industry suffers most of the breaches. It is heinous because these people are already suffering due to their health problems but the hackers are targeting them makes them vulnerable socially and economically. Therefore, it is important to improve security measures.

Cybersecurity Prevention and Ethical Hacking

As you can see from the graph, the number of incidents is increasing rapidly with the advancement and accessibility of the internet and computers. Therefore, it is crucial to come up with techniques to be secure from the attacks. Otherwise, it can cause serious health problems in the form of stress and depression.

- Use HTTPS instead of HTTP
- Use Strong Password
- Never save your passwords on the device
- Use two-step verification

These are some of the techniques to avoid being attacked or, even if attacked, to be safe from damage. HTTPS is safer than HTTP, so always use HTTPS instead of HTTP because of its inscription. The online data is safe. The password must be strong. A weak password is easy to guess, and hackers would not be able to discern a strong password easily. Never save your passwords online because it makes it easier for the attackers to access the password. Using two-step verification makes it difficult for criminals because each time before logging in, the code is sent to a trusted device, and it is workable for 60 seconds. Due to this, it becomes difficult for the attacker to access Gmail or other accounts. Phishing emails usually have poor grammar and links that lead the user to malicious sites.

- Do not use public Wi-Fi.
- Beware of extensions and popups.
- InstallAntiviruss
- Updapopups security system of the companies

Also, using public Wi-Fi makes the user vulnerable to attacks because the attacker could also be using the same Wi-Fi, or it might be set up by the hackers to trap the users. Therefore, public Wi-Fi must be avoided. Similarly, popups and extensions are sometimes malicious, which can damage computers and data. Installing an antivirus program and scheduling regular cleaning would help users be secure. Thus, these steps are crucial to being safe and secure in a world surrounded by constant makeup.

Lastly, the student can learn ethical hacking that benefits society. The teaching can focus on

responsibility and honesty. It is essential for the educational institutes to produce students who are responsible and honest. Although it might be difficult, schools are meant to teach basic humanity along with technical expertise. Therefore, the teachers must focus on the ethical hacking.

References

National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0. https://doi.org/10.6028/NIST.CSWP.29

Cybersecurity and Infrastructure Security Agency. (n.d.). Cybersecurity best practices. https://www.cisa.gov/topics/cybersecurity-best-practices

Joint Task Force. (2020). Security and privacy controls for information systems and organizations (NIST SP 800-53 Rev. 5). https://doi.org/10.6028/NIST.SP.800-53r5