**INSTITUTE OF ACCOUNTANCY ARUSHA**


**INDIVIDUAL ASSIGNIMENT**

REGISTRATION NUMBER : BCS/0024/2021

NAME OF STUDENT : NEHEMIA JOHAVENES

PROGRAMME : BCS III

SEMESTER : VI

MODULE : COMPUTER SECURITY

CODE : ITU O8213

FACILITATOR : Ms. Wankyo

**ACADEMIC YEAR : 2023/2024**

1. Cyberattacks are attacks that target computer systems and networks by exploiting vulnerabilities in these information systems.Such weaknesses are usually leveraged by threats which can originate either internally or externally to an organization.The aim of such attacks is to steal data, disrupt operations, damage or destroy information, or even gain unauthorized access. Here are some examples of cyber attacks conducted against various organizations worldwide.

The 2013 JP Morgan chase attack whose origin was traced back to the People's Liberation Army (PLA) of China impacted the bank through compromise personal details about 76 million customers.

Another one is the Citigroup hack of 2011; it was allegedly Russian-based and resulted into thefts involving lots of client records causing around $2,7000000 loss for the firm. The attack was said to come from Russia and led to the theft of lots of customer info, causing a company loss of about $2.7 million.

In 2016, another attack targeted a financial group, The Saudi Arabian Monetary Agency. It was thought to be from an Iranian Cyber group called Izz Addin al-Qassam. Their goal was to mess with the country's financial activities, but what happened after wasn't shared with the public.

**Some typical attacks on financial places include:**

1. Social Engineering attacks. These tricks play on how people think, making them share secret info about the financial place.
2. Next, we have Malware attacks. This is when bad software like a Trojan is used to steal money info or mess up financial services.
3. Also, Ransomware attacks are a common threat to financial groups. These lock up the institution’s data and ask for money to unlock it. These attacks mess up a firm's money details, like customer info, and threaten to wipe the data if the firm doesn't pay up.
4. Zero-day attacks too hit financial groups through outside software. These attacks take advantage of holes that even the software makers don't know about yet.

**Some experts have come up with ways to fight these kinds of attacks.**

1. One way is to train staff. This means giving them regular lessons on what to do before and after an attack. This method can help stop attacks that play on staff mistakes, like tricking them into giving away secrets. The lessons can cover good habits like strong passwords, how to handle info safely, and how to spot fake emails.
2. Another way banks fight these attacks is by teaming up with the police. This helps by making clear laws that let police act to stop attacks or catch attackers after an attack happens.
3. Banks use plans called incident response plans to react when they are under attack or after it's happened. These plans can include using backup data sources after an attack, and making sure messages are safe during one. These plans help cut down on the time services are down, stop the attack from spreading, and lessen the damage caused by the attack.
4. Improving security measures. This is often another setup which points at regularly checking on and improving the originally set security measures to see if they are in match up with the current security arrangements. It moreover points at expelling any shortcomings which will be misused within the already set security measures, such as watchword lifetime, and information encryption procedures utilized.

2. Electronic Restorative Records (EMR) Cyber assaults are assaults particularly pointed at the therapeutic data in healing centers basically due to their touchy nature. These assaults point at weakening medical frameworks as a sign of countering, for ransom or as a frame of a fighting. A few illustrations of Cyber assaults on EMR systems done over the a long time incorporate the taking after.

The Florida Division of wellbeing assault in 2020. This was a phishing assault against the Florida Office of Wellbeing that compromised the emails of different of workers, inevitably driving to uncovering the clinic patients' information.

The Mageean Wellbeing assault of 2019, which drove to uncovering the personal data of more 3.6 million patients inside the healing center.

One of the common Hollywood Presbyterian Therapeutic Center assaults in 2016. This was a ransomware attack targeted at the therapeutic center which scrambled the hospital's EMR information, that compelled them to re-route ambulances and postpone several surgeries.

A few attacks common in EMR frameworks may include the following.

1. Phishing assaults. These are attacks that target to influence the healing center representatives to click on toxic links or open email attachment that can infect the hospital's EMR systems.
2. Information robbery. This includes purposely leaking or taking quiet information from the hospitals EMR frameworks. The stolen information is the sold within the dark advertise to encourage crimes such as character burglary, pantomime, and open blackmailing.
3. Ransomware is another common shape of assault in EMR frameworks. This basically includes holding the hospitals EMR frameworks prisoner by scrambling quiet information until a deliver is paid and in the event that the attackers' condition is not met a danger to devastate the information is made.

Analysts have proposed a few configurations against these attacks which include following.

1. Network segmentation. This involves separating the healing facilities configuration into smaller portions which might be useful too when part of the hospital's configuration is compromised. The main advantages of this configuration is limiting lateral spread of development (meaning indeed when an employee's workstation is compromised e.g. a doctor's workstation it doesn't give a way to get to other imperative workstations), as well as reducing attack surface within the EMR's configuration for attackers.
2. Information backup and recovery. This solution allows healthcare providers to deliver administrations even in the case of a ransomware attack which primarily common in EMR frameworks. The backup and recovery plans must be well documented and routinely moved to expect compromising the whole system within the context of an attack.

3. Information encryption must be implemented for information that's stored inside the system's server (information at rest) and the information that's being effectively transmitted through the hospital's data frameworks (information on travel). This ensures privacy of all information that's inside the healing center indeed when the system happen to be breached.

4. Strong Access controls  must be implemented to ensure that as it were authorized work force have access to the EMR framework and not something else. Some of the common strategies that can be used in get to control is Role-based verification (RBAC) and multi-factor authentication. Also, the least required parts must be provided to the fitting faculty ensure that each worker has the right set of parts only.

3. Student Information Management Systems are configurations designed to manage students' data in educational education. These data frameworks have been targeted by attackers over the a long time due to the kind of information they have, especially understudy reports and individual data. The following are a few cases of assaults performed on different instructive teach over the a long time.

The attack on the College of California Berkeley (2020). This was a ransomware attack that compromised the data server hosting personal data of students and staff inside the college, the personal data included names, social security numbers and restorative data. The college afterward had to advise the compromised students and staff almost the assault and advertised remediation within the form of credit checking administrations.

Another attack was the Phishing assault on Emory College (2016). The assailants utilized phishing emails camouflaged as formal college emails to convince the university's staff to uncover their login accreditations to the university's data framework. The assault drove to the compromise of the understudy data framework through the stolen staff data.

The attack at Marist College (2018). This assault was done by a previous IT representative at the college. The ex-employee altered the grades and monetary data of numerous understudies inside the data framework, subsequently modifying the system's integrity which could be a violation to the standards of security.

**The following are the types of assaults common in student data frameworks.**

1. One of the common attacks is data leakage. Such sensitive information like the personal details of students and their grades can leak due to cyber attacks for malicious purposes such as making counterfeit IDs for identity theft.The data leakage can too point at the misguidedly revealing of student grades without the consent of the institutions administration board.

2. Denial-of-Service assault (DOS). This attacks the point at making the instructive institutions' data frameworks accessible to the staff and understudies. It may be done deliberately by aggressors as a frame of assault or inadvertently by the staff and understudies because of destitute scaling and activity taking care of strategies.

3. Insider dangers are another frame of assault, where an existing or former representative or understudy of the institution violates the data because of destitute access to control hones.

The following are a few arrangements recommended by experts against these types of attacks towards the student information frameworks.

1. Audit logging and monitoring. This involves tracing the activity of the information framework and the client get to to detect abnormal conduct or behavior within the system. This is due to the fact that, before most attacks certain designs within the system's activity can be seen subsequently monitoring and logging these designs can prove effective against attacks.

2. Information minimization is another solution in anticipating attacks in data systems. This includes collecting the least essential data from the students and staff to be used and neatly/securely arranging of the unnecessary information.

3. Patch management. The data framework ought to be continually updated and fixed in case any vulnerabilities show within the framework are found by assailants and are inevitably exploited.

4. Adherence with security principles standards presented by experts as well as actualizing them in our data frameworks in order to ensure that all of the data as well as parties included are guarded.

## References

National Institute of Standards and Technology (NIST). (2020, December). Special Publication 800-161 Revision 1: Cybersecurity Supply Chain Risk Management Practices (IR 800-161 Rev 1). National Institute of Standards and Technology (.gov). https://csrc.nist.gov/pubs/sp/800/161/r1/final

Healthcare Information and Management Systems Society (HIMSS). (2020, April). Cybersecurity Framework for Healthcare Organizations. HIMSS Cybersecurity Committee. https://www.himss.org/news/cybersecurity-framework-implementation-guide-helps-healthcare-organizations-manage-risks