Cyber Attacks & Audit Controls to Prevent Them

CYBR615 Written Assignment 11

Daniel Carbajal

Bellevue University

February 24, 2023

A cyber attack is any attempt to gain unauthorized access to a computer, computing system or computer network with the intent to cause damage, or harm including financial gain. Cyber attacks aim to disable, disrupt, destroy, or control computer systems or to alter, block, delete, manipulate, or steal the data held within these systems.

Any individual or group can launch a cyber attack from anywhere by using one or more various attack strategies. People who carry out cyber attacks are generally regarded as cybercriminals. Often referred to as bad actors, threat actors and hackers, they include individuals who act alone, drawing on their computer skills to design and execute malicious attacks. They can also belong to a criminal syndicate, working with other threat actors to find weaknesses or problems in the computer systems -- called vulnerabilities -- that they can exploit for criminal gain.

Government-sponsored groups of computer experts also launch cyber attacks. They're identified as nation-state attackers, and they have been accused of attacking the information technology (IT) infrastructure of other governments, as well as nongovernment entities, such as businesses, nonprofits, and utilities.

**FlexBooker**

At the end of 2021 and the start of 2022, appointment management business FlexBooker was hit by a vast attack that affected around three million of its users. Confidential data including ID information, drivers’ licenses and passwords was stolen by the hackers and then offered for sale on popular hacking message boards, and many powerful users have left FlexBooker because of the breach. A hacking group called Uawrongteam was responsible for the hack, and it wasn’t a particularly sophisticated affair – the group cracked FlexBooker’s AWS servers and installed malware to control the firm’s systems.

A security policy and a few audit controls could have prevented this attack. For one a set of controls are required for the cloud computing AWS servers. Risk management and analysis needs to be assessed and implemented to ensure the AWS servers are secure. Will have to manage security protocols with AWS in order to ensure safe practices and policies are in place. Secure systems for data and client processing need to be in place. And testing and upgrading of security systems need to be in place to ensure that there are no weaknesses and something hackers can easily exploit in order to protect user data. A centralized user authentication method can be used to protect all data from their millions of users and make security policies and procedures that can be tested and implemented over a quick period of time in order to circumvent future attacks.

**Ronin**

Ronin is a blockchain gaming platform that relies on cryptocurrency, and it was attacked between November 2021 and March 2022. Ronin’s Axie Infinity game enables players to earn digital currency and NFTs, and its increasing popularity saw the firm dial back security protocols so its servers could handle a growing audience. That helped Axie Infinity deal with the number of people who wanted to play, but it also let criminals in, and they stole $600 million of cryptocurrencies. Ronin’s parent company is working with authorities to identify the culprits and recover funds, but it’s a lesson that any business can learn never compromise your security standards.

Ronin should have not relaxed its security standards. Ensuring the computer networks and crypto block changes are subjected to routine security reviews should be implemented. The implementation of procedures and policies should be created and assessed to prevent unauthorized users from accessing the computer systems at Ronin. Investigating potential flaws in the security of the computer systems and the crypto change need to be done routinely to ensure security of the funds and data information should be done immediately. Overall, audit security controls could have been used to ensure that these cyber attacks would not have happened in the first place.

**References**

Cyber Attack - Glossary | CSRChttps://csrc.nist.gov

Jennings, M.,"Top data breaches and cyber-attacks of 2022,"Techradar, Jan 11, 2023.

Otero, A. R., Information Technology Control and Audit, Fifth Edition, CRC Press, 2020.