COLLEGE OF BUSINESS, PEACE, LEADERSHIP, AND GOVERNANCE

NCIS 207: FUNDAMENTALS OF INFORMATION SECURITY

END OF SECOND SEMESTER EXAMINATIONS

APRIL/MAY 2023

LECTURER: MRS L. TEMBANI-FUNDISI

DURATION: 3 HOURS

INSTRUCTIONS

Answer all questions from **Section A (compulsory) [25 marks**]

Answer **ANY 3** questions from **Section B** [**75 marks**]

Begin your answer to each question on a fresh page.

Question One: <u>Case Study</u>

Amazon suffers 'fraud attack' from cybercriminals

By CISOMAG - May 10, 2019

E-Commerce giant Amazon recently suffered a fraud attack in which hackers syphoned funds from its merchant accounts over six months last year. The Seattle-based e-tailer stated that unknown cybercriminals broke into around 100 seller accounts and syphoned money into their own accounts, the Bloomberg reported. Amazon said the hack took place between May 2018 and October 2018, and it's unclear how much money was stolen in the incident.

According to Amazon's legal team, the hackers managed to alter account details on the Seller Central platform to their own at Barclays Plc and Prepay Technologies Ltd. It's believed that the accounts were compromised by using phishing techniques that deceived sellers into giving up sensitive information.

Amazon stated that its investigation is still ongoing and asked the London judiciary for approval of searching the accounts of hackers.

In a similar incident, Amazon suffered a technical glitch on its India portal that affected its sellers and vendors. The e-tailer stated that a bug in its website caused a data breach on January 08, 2019, that exposed sensitive financial information, including sales, category-wise split and inventory data of its sellers and vendors. Having around 400,000 online vendors and sellers across the country, Amazon said the issue was resolved within a few hours, but, the exact figure of affected members is not yet discovered.

The issue came to light after some Amazon vendors reported that they received incorrect data while downloading their Merchant Tax Reports (MTR) from the portal. It has been said that data of some sellers were visible to other competing sellers. An MTR statement holds information of all the other transactions processed by a seller on the e-commerce platform, which is usually downloaded from the portal between 8th-10th of every month.

Recently, a group of researchers from the cybersecurity firm UpGuard revealed that Facebook user account information was exposed on Amazon cloud servers. The security team at UpGuard stated that they found two data breach incidents in different regions. UpGuard stated the data was stored in Amazon's cloud service without password protection and could easily be accessed by outsiders.

The first incident was originated from the Mexico-based media company Cultura Colectiva which exposed around 146 GB of data that contained over 540 million records detailing comments, likes, reactions, account names, FB IDs, and other sensitive information. The second was a separate database from a Facebook-integrated app named 'At the Pool' which exposed data via an Amazon S3 bucket. This database contained the backup information like fb_user_id, fb_user, fb_friends, fb_likes, fb_music, fb_movies, fb_books, fb_photos, fb_events, fb_groups, fb+checkins, fb_interests, and passwords, according to UpGuard.

Source: ***https://cisomag.eccouncil.org/amazon-suffers-fraud-attack-from-cybercriminals/***

[Disclaimer: The story might not be true]

Question 1

a. Name the mistakes /weaknesses found in Amazon Inc. that would have enabled an attacker to compromise the company's system (15 marks)
b. Considering the information mentioned in the case, elaborate on all the ways Amazon would be able to further enhance its Information Security posture. (10 marks)

SECTION B

Question 2

a. List the advantages and disadvantages of the bottom up approach (7 marks)
b. Information security performs four important functions for an organization. Outline them (8 marks)
c. Briefly explain the five major goals of information security governance (10 marks)

Question 3

Draft a brief Enterprise Information Security Policy for Africa University. Make sure you include all the vital ICT infrastructure components of the policy discussed in class (25marks)

Question 4

"Information security is viewed as the first line of defense in any organization"**.** Discuss. (25marks)

Question 5

Explain in detail the evolution of Information Security from World War 11 (25marks)

END OF EXAMINATION