AFRICA
UNIVERSITY
A United Methodist-Related Institution

COLLEGE OF BUSINESS, PEACE, LEADERSHIP AND GOVERNANCE

NCIS207-FUNDAMENTALS OF INFORMATION SECURITY

END OF SECOND SEMESTER EXAMINATIONS

MAY 2021

LECTURER: MRS L. TEMBANI-FUNDISI

TIME: 7 HOURS

INSTRUCTIONS

Answer all questions from **Section A (compulsory) [50 marks**]

Answer **ONE** question from **Section B** [50 marks]

Begin your answer to each question on a fresh page.

Question 1

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]

Questions

a. Identify major security breaches and attacks arising from the story? [10 marks]
b. If you were the Chief Information Officer of this organisation, discuss some of the technical interventions you would have done to keep the organization secure? [25 marks]
c. Other than internal security measures, discuss any external measures that the organisation could employ to enforce security. [15 marks]

SECTION B

Question 2

i. Using the components of risk assessment documentation, draft a tentative risk assessment of a laboratory, department, or office at your university. Outline and discuss the critical risks you might find. [25 marks]
ii. Outline some of the security measures that were implemented by your university and assess their effectiveness [25 marks]

Question 3

i. As an Information Security Officer of an organization , discuss some of the measures you can implement to ensure personnel adhere to the policies implemented by you to ensure security [10 marks]
ii. Analyse the physical security measures suitable for the banking sector. Justify your analysis. [15 marks]

iii. Go to a popular online e-commerce site like Amazon.com. Place several items in your shopping cart, and then go to ‘check out’. When you reach the screen that asks for your credit card number, click the **key sign** (locking key sign) on the web browser. What can you find out about the cryptosystems and protocols in use to protect this transaction? *(Copy the url of the website you browsed to do this attempt and paste it in your answer sheet)* [10marks] *iv.* Repeat exercise (iii) on a different website. Does this site use the same or different protocols? Describe them. *(Copy the url of the website you browsed to do this attempt and paste it in your answer sheet)* [15 marks]

END OF EXAMINATION