APOLLO

A4 Machine learning

HL

Computer Science
First assessment 2027
1 questions | questions

APOLLO

Shared case study

Read this source alongside the questions that refer to it.

Diploma Programme
Programme du diplôme
Programa del Diploma

Computer science
Case study: Preventing network security attacks

Specimen paper

Instructions for candidates

- Case study booklet required for higher level and standard level paper 1 computer science examinations.

4 pages

© International Baccalaureate Organization 2025

Introduction

The integration of technology in healthcare has transformed how medical services are delivered. However, with this increased use of technology, healthcare institutions like private hospitals have become attractive targets for cybercriminals and therefore face significant security challenges that could have devastating impacts. This case study highlights the interventions used to prevent security incidents by one private hospital, TaylorMade Healthcare, and explores some network security practices.

Background

TaylorMade Healthcare uses high-speed internet to operate its network infrastructure, which includes computers, servers, switches, routers, wireless access points, and *firewalls*. These devices and systems are connected internally and to the internet, enabling staff to access medical records, communicate with other users and patients, exchange information, and transfer data. The devices and systems work cohesively and are vital for the hospital's smooth operation, including patient care, data management, and resource handling.

TaylorMade Healthcare stores vast amounts of sensitive data, such as patient health records, financial information, and confidential documents, which it must safeguard to maintain trust and confidence among its patients, staff, and stakeholders.

The hospital's director acknowledges the importance of securing the network and data against risks like *malware* infections, *phishing* attacks, and unauthorized access. The director also knows that it is critical to implement effective security measures to protect the hospital's network infrastructure and data.

Bring-your-own-device (BYOD) policy

TaylorMade Healthcare has adopted a bring-your-own-device (BYOD) policy that permits staff to use personal electronic devices for work tasks. Although a BYOD policy can provide many benefits, such as increased flexibility and convenience, it also has several weaknesses.

Ransomware and *rootkit* attacks

TaylorMade Healthcare recently suffered a ransomware attack that targeted its network infrastructure. The attack was launched through a phishing email that appeared to be from a trusted source. When an unsuspecting staff member clicked on the link in the email, the ransomware gained access to the hospital's network and quickly spread, encrypting sensitive data and rendering it inaccessible.

The consequences of the attack were severe, leading to significant data loss and system downtime. The ransomware attack encrypted patients' data and prevented staff from accessing patient records for several days. This led to substantial disruptions.

TaylorMade Healthcare's reputation has suffered due to the attack, with patients expressing concern about the security of their data. There was also a significant financial impact, with TaylorMade Healthcare paying the attackers a ransom to regain access to its encrypted data.

Another notable concern is a rootkit attack, which uses malicious software to hide itself within an operating system to gain administrative-level access to the network. Rootkits are notoriously difficult to remove.

Interventions

“Dealing with the ransomware attack was a wake-up call for our entire team,” said Jane Wang, Head of Cybersecurity. “We realized the importance of being proactive and creating a culture of security awareness,” she added, “and we also realized that a comprehensive security strategy is essential for protecting sensitive data and networks.”

Since the attack, TaylorMade Healthcare has identified several measures to prevent future attacks:

- Data backup and *disaster recovery plans*
- *Email filtering*
- *Failover systems*
- Firewall implementation
- Network segmentation and *access control*
- Regular software and security updates
- *Third-party services*
- *User awareness training*

Implementing network segmentation and access control reduced the risk of cyber-attacks and improved the security of TaylorMade Healthcare’s network. These and the other interventions have contributed to reducing the effects of security breaches, ensuring the confidentiality and integrity of sensitive information. These safeguards have also minimized system downtime and strengthened data protection, which is vital for the hospital’s uninterrupted functioning.

Challenges faced

TaylorMade Healthcare’s goal is to build resilience to address the following challenges.

Standard level and higher level:

- Develop strategies to create an awareness of cybersecurity, especially ransomware and rootkit attacks.
- Consider the benefits of a bring-your-own-device (BYOD) policy while preparing for its security weaknesses.

Higher level only:

- Explore the viability of network segmentation and access control.
- Develop procedures to restore operations in case of a breach.

Additional terminology

Access control
Bring your own device (BYOD)
Cybercriminal
Disaster recovery plan
Email filtering
Failover system
Firewall
Malware
Phishing
Ransomware
Rootkit attack
Third-party services
User awareness training

Some companies, products, or individuals named in this case study are fictitious and any similarities with actual entities are purely coincidental.

Section A

Answer **all** questions from this section. Answers must be written within the answer boxes provided.

4. A hospital uses a deep learning convolutional neural network (CNN) to analyse chest X-rays and predict the likelihood of a patient developing pneumonia.

(a) State **one** of the layers in a convolutional neural network (CNN). [1]

. . . . . .

. . . . . .

(b) Identify **one** reason data cleaning is carried out before training a convolutional neural network (CNN). [1]

. . . . . .

. . . . . .

(c) Outline **one** reason a graphics processing unit (GPU) is recommended when training a deep learning convolutional neural network (CNN) model using a large dataset. [2]

. . . . . .

. . . . . .

. . . . . .

. . . . . .

(d) Describe how the deep learning convolutional neural network (CNN) model could be evaluated using an F1 score. [3]

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

(This question continues on the following page)

(Question 4 continued)

The hospital purchased a self-learning robotic cleaner that uses reinforcement learning (RL).

(e) Justify why a robotic cleaner would use reinforcement learning (RL) instead of supervised learning (SL). [3]

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

A deep learning algorithm was implemented to automatically monitor the hospital's social media sites. The model uses natural language processing to classify comments into categories like "compliments" and "complaints".

Members of the public are asked to remove any comments that are not supported by evidence. However, the hospital's CEO is concerned about the ethical issues of doing this, as it may be considered online harassment.

(f) Discuss whether the hospital should ask members of the public to retract their comments. [5]

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .