**NHÓM 3 – BÀI TẬP ÔN TẬP**

# A. PHẦN TRẮC NGHIỆM

*(Đánh dấu X vào ô)*

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Câu**  **Đáp án** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** | **13** | **14** | **15** | **16** | **17** | **18** | **19** | **20** | **21** | **22** | **23** | **24** | **25** | **26** | **27** | **28** | **29** | **30** |
| **a** |  |  |  |  | **X** |  |  |  |  |  |  | **X** |  | **X** |  |  |  |  | **X** |  | **X** |  |  |  |  |  |  |  | **X** |  |
| **b** |  |  |  | **X** |  |  |  |  |  |  |  |  |  |  | **X** |  | **X** |  | **X** |  |  |  |  |  | **X** | **X** |  |  |  |  |
| **c** |  | **X** |  |  |  |  |  |  |  |  |  |  |  | **X** |  |  |  | **X** |  | **X** | **X** |  | **X** |  | **X** | **X** |  |  |  |  |
| **d** |  |  | **X** |  | **X** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | **X** | **X** |  | **X** |  |  |  | **X** |  | **X** |
| **e** | **X** |  | **X** |  |  | **X** | **X** | **X** |  | **X** | **X** | **X** |  |  | **X** |  |  | **X** |  |  |  |  | **X** |  |  |  |  |  |  |  |
| **f** | **X** |  |  |  |  |  |  |  | **X** | **X** | **X** |  | **X** |  |  | **X** |  |  |  |  |  |  |  |  |  |  | **X** |  |  | **X** |
| **g** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | **X** |  |  |  |  |  |

**Câu 19:** Rủi ro tiểm ẩn là: Tạo điểm lỗi đơn nhất (Single Point of Failure) cho toàn bộ hệ thống liên kết; nếu kẻ tấn công xâm nhập IdP hoặc đánh cắp token SSO, chúng có thể truy cập mọi dịch vụ mà không cần xác thực lại, cùng với nguy cơ session hijacking và lỗ hổng giao thức SAML/OAuth

**Câu 30:** Câu a, c, d đều đúng.

# B. PHẦN TỰ LUẬN

## Câu 31 (Phương)

|  |  |  |
| --- | --- | --- |
| **Loại tấn công mạng** | **Chiến lược QLRR áp dụng là…** | **Chiến lược QLRR của bạn là ….** |
| ***(1)*** | ***(2)*** | ***(3)*** |
| Malware | Risk Avoidance | *Risk Mitigation* |
| Phishing | Risk Transfer | *Risk Mitigation* |
| DDoS | Risk Mitigation | *Đồng ý* |
| MitM | Risk Acceptance | *Risk Mitigation* |
| Zero-day | Risk Mitigation | *Đồng ý* |

## Câu 32 (Huy)

|  |  |  |
| --- | --- | --- |
| **Stt** | **Biện pháp kỹ thuật** | **Yêu cầu ATTT liên quan** |
| (1) | (2) | (3) |
| **1** | Sử dụng các giao thức mã hóa mạnh như WPA2, WPA3 hoặc AES để bảo mật dữ liệu. | |  | | --- | | *Nhóm A.10 – Yêu cầu A.10.1 – Điều A.10.1.1* | |
| **2** | Triển khai IDS (Hệ thống phát hiện xâm nhập) có thể phát hiện tín hiệu gây nhiễu và có khả năng tự động chuyển sang các tần số và kênh thay thế. | *Nhóm A.12 Yêu cầu A.12.4 Điều A.12.4.1* |
| **3** | Luôn thiết kế mạng của bạn với tính dự phòng: Sử dụng công nghệ ‘Frequency Hopping’ để đổi tần số hoặc truyền tín hiệu trên một băng thông rộng để tránh bị gián đoạn mạng do bị gây nhiễu. | *Nhóm A.17 – Yêu cầu A.17.2 – Điều A.17.2.1* |
| **4** | Thường xuyên kiểm tra hệ thống, thiết bị để cập nhật chương trình và vá lỗi phần mềm. | *Nhóm A.12 – Yêu cầu A.12.6 – Điều A.12.6.1* |
| **5** | Phân đoạn mạng: Cô lập các hệ thống quan trọng. | *Nhóm A.13 – Yêu cầu A.13.1 – Điều A.13.1.3* |
| **6** | Bảo vệ các điểm truy cập không bị giả mạo vật lý - giữ chúng an toàn | *Nhóm A.11 – Yêu cầu A.11.1 – Điều A.11.1.2* |
| **7** | Giáo dục/Đào tạo: Đào tạo người dùng về nhận thức về mối đe dọa | *Nhóm A.7 – Yêu cầu A.7.2 – Điều A.7.2.2* |

## Câu 33 (Thiên)

|  |  |  |  |
| --- | --- | --- | --- |
| **Stt** | **Thành phần** | **“Shielding” là …** | **Yêu cầu ATTT liên quan là ….** |
| **(1)** | **(2)** | **(3)** | **(4)** |
| **1** | Network (Mạng) | Tường lửa (‘firewall’), hệ thống phát hiện/ngăn chặn xâm nhập (‘IDS/IPS’) | **13.1.1 Các biện pháp kiểm soát mạng** (Kiểm soát an toàn mạng) |
| **2** | Data (Dữ liệu) | Mã hóa (‘encryption’) | **10.1.1 Chính sách về sử dụng kiểm soát mật mã**  (Chính sách kiểm soát mật mã) |
| **2** | sers (Người dùng) | Đào tạo người dùng (‘user training’) | **7.2.2 Nhận thức, giáo dục và đào tạo về an toàn thông tin** (An toàn nhân sự) |

## Câu 34 (Chiến)

### Câu 34.1

|  |  |  |
| --- | --- | --- |
| **Stt** | **Các mối đe dọa cho MySQL** | **Biện pháp kiểm soát (“control”) theo ISO 27001:2013 (Phụ lục A)** |
| (1) | **(2)** | **(3)** |
| **1** | ‘**Mismanagement of Account Access**’:  Quản lý quyền truy cập tài khoản không tốt hay chỉ định sai loại quyền truy cập tài khoản cho người dùng. | *Nhóm A.9 – Yêu cầu A.9.2 – Điều A.9.2.2, A.9.2.3, A.9.2.5, A.9.2.6* |
| **2** | **‘Weak Passwords’**: mật khẩu yếu | *Nhóm A.9 – Yêu cầu A.9.4 – Điều A.9.4.3*  *Nhóm A.9 - Yêu cầu A.9.2 - Điều A.9.2.4* |
| **3** | **‘DDoS Attacks’**: tấn công DDoS  Kẻ tấn công sử dụng nhiều tài khoản truy vấn giả mạo liên tiếp vào CSDL để làm chậm và cuối cùng là làm sập cơ sở dữ liệu. | *Nhóm A.9 Yêu cầu A.9.1 Điều A.9.1.1;*  *Nhóm A.9 Yêu cầu A.9.4 Điều A.9.4.2* |
| **4** | **‘SQL Injection Attacks’**: tấn công tiêm SQL  Kẻ tấn công tiêm lệnh vào chuỗi truy vấn gây hư hỏng CSDL hoặc đánh cắp dữ liệu. | *Nhóm A.14 Yêu cầu A.14.2 Điều A.14.2.5, A.14.2.8* |
| **5** | **‘Remote Preauth User Enumeration’**: Liệt kê người dùng xác thực trước từ xa - tấn công này được sử dụng để xác thực xem một người dùng nào đó đã có trong CSDL hay không để kẻ tấn công có thể xác định tài khoản dùng làm điểm nhập. | *Nhóm A.14 Yêu cầu A.14.2 Điều A.14.2.5, A.14.2.8* |

### Câu 34.2.

- **Stt 3 (DDoS Attacks)**: Không đồng ý, vì DDoS chủ yếu là tấn công làm gián đoạn dịch vụ (availability) nên các biện pháp kiểm soát phù hợp hơn nằm ở **Nhóm A.12 (Operations security)** hoặc **Nhóm A.17 (**I**nformation Security Aspects of Business Continuity Management)** hoặc **Nhóm A.13 (Communications security )** chứ không phải A.9.1.1 và A.9.4.2

- **Stt 4 (SQL Injection Attacks)**: Đồng ý, việc ngăn chặn tiêm SQL đòi hỏi **A.14.2.5 (Secure system engineering principles)** và **A.14.2.8 (System security testing)** để mã hóa tham số và kiểm thử bảo mật

- Stt 5 (Remote Preauth User Enumeration): Không đồng ý, vì ngoài các điều trên ra thì cần bổ sung các điều thuộc Nhóm A.9 như A.9.4.2 và A.9.2.4

## Câu 35 (Quân)

|  |  |  |
| --- | --- | --- |
| **Stt** | **Biện pháp kiểm soát** | **Yêu cầu ATTT liên quan** |
| **(1)** | **(2)** | **(3)** |
| 1 | Sử dụng các giải pháp bảo mật phù hợp, cung cấp khả năng bảo vệ theo thời gian thực, hiển thị mối đe dọa. | *Nhóm A.12 - Yêu cầu A.12.2 – Điều A.12.2.1* |
| 2 | Đào tạo về an ninh mạng cho nhân viên. | *Nhóm A.7 – Yêu cầu A.7.2 – Điều A.7.2.2* |
| 3 | Thiết lập chính sách truy cập vào tài sản của công ty, bao gồm hộp thư điện tử, thư mục dùng chung và tài liệu trực tuyến. | *Nhóm A.9 – Yêu cầu A.9.1 – Điều A.9.1.1* |
| 4 | Cập nhật liên tục và xóa quyền truy cập khi nhân viên không còn nhu cầu sử dụng hoặc nghỉ việc. | *Nhóm A.9 – Yêu cầu A.9.2 – Điều A.9.2.6* |
| 5 | Đảm bảo thông tin của doanh nghiệp (công ty) được an toàn trong trường hợp khẩn cấp bằng cách thường xuyên sao lưu các dữ liệu cần thiết. | *Nhóm A.12 – Yêu cầu A.12.3 – Điều A.12.3.1* |

## Câu 36 (Như)

|  |  |  |
| --- | --- | --- |
| **Stt** | **Biện pháp kiểm soát** | **Yêu cầu ATTT liên quan** |
| **(1)** | **(2)** | **(3)** |
| **1** | Keep employees security-wise | *Nhóm A.7 Yêu cầu A.7.2 Điều A.7.2.2;* |
| **2** | Apply the Principle of Least Privilege (PLP) | *Nhóm A.9 Yêu cầu A.9.2 Điều A.9.2.3;*  *Nhóm A.9 Yêu cầu A.9.4 Điều A.9.4.4;* |
| **3** | Enforce USB port access policy | *Nhóm A.5 Yêu cầu A.5.1 Điều A.5.1.1;* |
| **4** | Go with the Zero Trust security model | *Nhóm A.5 Yêu cầu A.5.1 Điều A.5.1.1;* |
| **5** | Enforce a safe BYOD policy | *Nhóm A.5 Yêu cầu A.5.1 Điều A.5.1.1;* |
| **6** | Encrypt endpoints | |  | | --- | | *Nhóm A.10 Yêu cầu A.10.1 Điều A.10.1.1* | |
| **7** | Strengthen passwords | *Nhóm A.9 Yêu cầu A.9.2 Điều A.9.2.1* |
| **8** | White/blacklisting apps | |  | | --- | | *Nhóm A.12 Yêu cầu A.12.6 Điều A.12.6.2* | |
| **9** | Only use VPN access for remote endpoints | |  | | --- | | *Nhóm A.13 Yêu cầu A.13.1 Điều A.13.1.1* | |
| **10** | Leave no door open: patch & secure all devices | *Nhóm A.12 Yêu cầu A.12.6 Điều A.12.6.1* |

## Câu 37 (Phúc)

|  |  |  |
| --- | --- | --- |
| **Stt** | **Đặc điểm của mô hình** | **Yêu cầu ATTT liên quan** |
| **(1)** | **(2)** | **(3)** |
| **1** | Ongoing monitoring and verification | *Nhóm A.12 Yêu cầu A.12.4 Điều A.12.4.1;*  *Nhóm A.12 Yêu cầu A.12.4 Điều A.12.4.3;*  *Nhóm A.9 Yêu cầu A.9.2 Điều A.9.2.5* |
| **2** | Apply the Principle of Least Privilege (PLP) | *Nhóm A.9 Yêu cầu A.9.1 Điều A.9.1.1;*  *Nhóm A.9 Yêu cầu A.9.2 Điều A.9.2.3;*  *Nhóm A.9 Yêu cầu A.9.4 Điều A.9.4.1* |
| **3** | Network micro-segmentation | *Nhóm A.13 Yêu cầu A.13.1 Điều A.13.1.3;*  *Nhóm A.9 Yêu cầu A.9.1 Điều A.9.1.1* |
| **4** | Multi-factor authentication. | *Nhóm A.9 Yêu cầu A.9.4 Điều A.9.4.2;*  *Nhóm A.9 Yêu cầu A.9.2 Điều A.9.2.1* |
| **5** | Workloads security (Bảo mật ‘workloads’)  *(A workload is a computational task, process or data transaction. Workloads encompass the computing power, memory, storage and network resources required for the execution and management of applications and data. Within the cloud framework, a workload is a service, function or application that uses computing power hosted on cloud servers.)* | *Nhóm A.9 Yêu cầu A.9.4 Điều A.9.4.2;*  *Nhóm A.11 Yêu cầu A.11.1 Điều A.11.1.2;*  *Nhóm A.11 Yêu cầu A.11.2 Điều A.11.2.1, A.11.2.2, A.11.2.3, A.11.2.4;*  *Nhóm A.10 Yêu cầu A.10.1 Điều A.10.1.1;*  *Nhóm A.13 Yêu cầu A.13.1 Điều A.13.1.3* |
| **6** | Data usage controls  (Kiểm soát sử dụng dữ liệu) | *Nhóm A.5 Yêu cầu A.5.1 Điều A.5.1.1;*  *Nhóm A.6 Yêu cầu A.6.2 Điều A.6.2.1;*  *Nhóm A.8 Yêu cầu A.8.2 Điều A.8.2.3;*  *Nhóm A.8 Yêu cầu A.8.3 Điều A.8.3.1;*  *Nhóm A.14 Yêu cầu A.14.3 Điều A.14.3.1;*  *Nhóm A.18 Yêu cầu A.18.1 Điều A.18.1.3* |
| **7** | Threat and risk analysis  (Phân tích mối đe dọa và rủi ro); | *Điều 6 khoản 6.1 điểm 6.1.1 và 6.1.2*  *thuộc nội dung “6 Planning” của tài liệu ISO 27001:2013;* |

## Câu 38 (Huy)

|  |  |  |
| --- | --- | --- |
| **Stt** | **Tám (8) thực hành lập trình tốt nhất *(the top eight secure programming best practices)* khi thực hành “Secure Coding”** | **Yêu cầu ATTT liên quan** |
| **(1)** | **(2)** | **(3)** |
| 1 | Security by Design (Bảo mật theo thiết kế) | *Nhóm A.14 – Yêu cầu A.14.1 – Điều A.14.1.1* |
| 2 | Password Management (Quản lý mật khẩu) | *Nhóm A.9 – Yêu cầu A.9.4 – Điều A.9.4.3* |
| 3 | Access Control (Kiểm soát truy cập) | *Nhóm A.9 – Yêu cầu A.9.1 – Điều A.9.1.1* |
| 4 | Error Handling and Logging (Xử lý lỗi và ghi nhật ký) | *Nhóm A.12 – Yêu cầu A.12.4 – Điều A.12.4.1* |
| 5 | Cryptographic Practices (Thực hành mật mã) | *Nhóm A.10 Yêu cầu A.10.1 Điều A.10.1.1* |
| 6 | Threat Modeling (Mô hình hóa mối đe dọa) | *Nhóm A.14 Yêu cầu A.14.1 Điều A.14.1.1* |
| 7 | System Configuration (Cấu hình hệ thống) | *Nhóm A.12 Yêu cầu A.12.2 Điều A.12.2.1;*  *Nhóm A.12 Yêu cầu A.12.5 Điều A.12.5.1;*  *Nhóm A.12 Yêu cầu A.12.6 Điều A.12.6.1;*  *Nhóm A.12 Yêu cầu A.12.6 Điều A.12.6.2,*  *Nhóm A.14 Yêu cầu A.14.2 Điều A.14.2.2;*  *Nhóm A.14 Yêu cầu A.14.2 Điều A.14.2.4* |
| 8 | Input Validation and Output Encoding  (Xác thực đầu vào và mã hóa đầu ra) | *Nhóm A.14 Yêu cầu A.14.2 Điều A.14.2.8;*  *Nhóm A.14 Yêu cầu A.14.2 Điều A.14.2.9* |

## Câu 39 (Phúc)

|  |  |  |
| --- | --- | --- |
| **Stt** | **Năm thách thức và rủi ro hàng đầu trong bảo mật đám mây**  ***(5 Top Challenges & Risks of Cloud Security)*** | **Biện pháp kiểm soát (“control”) theo ISO 27001:2013 (Phụ lục A)** |
| **(1)** | **(2)** | **(3)** |
| 1 | Misconfiguration (Cấu hình sai) | *Nhóm A.12 Yêu cầu A.12.1 Điều A.12.1.2;*  *Nhóm A.12 Yêu cầu A.12.6 Điều A.12.6.1;*  *Nhóm A.14 Yêu cầu A.14.2 Điều A.14.2.2* |
| 2 | Unauthorized Access (Truy cập trái phép) | *Nhóm A.9 Yêu cầu A.9.1 Điều A.9.1.1;*  *Nhóm A.9 Yêu cầu A.9.2 Điều A.9.2.1;*  *Nhóm A.9 Yêu cầu A.9.4 Điều A.9.4.1* |
| 3 | Hijacking of Accounts (Chiếm đoạt tài khoản) | *Nhóm A.9 Yêu cầu A.9.4 Điều A.9.4.2;*  *Nhóm A.9 Yêu cầu A.9.2 Điều A.9.2.3;*  *Nhóm A.12 Yêu cầu A.12.4 Điều A.12.4.1* |
| 4 | External Sharing of Data (Chia sẻ dữ liệu bên ngoài) | *Nhóm A.13 Yêu cầu A.13.2 Điều A.13.2.1;*  *Nhóm A.8 Yêu cầu A.8.2 Điều A.8.2.1;*  *Nhóm A.15 Yêu cầu A.15.1 Điều A.15.1.1* |
| 5 | Unsecured Third-Party Resources (Tài nguyên của bên thứ ba không an toàn) | *Nhóm A.15 Yêu cầu A.15.1 Điều A.15.1.1;*  *Nhóm A.14 Yêu cầu A.14.2 Điều A.14.2.7;*  *Nhóm A.12 Yêu cầu A.12.6 Điều A.12.6.1* |

## Câu 40 (Thiên)

|  |  |  |
| --- | --- | --- |
| **Stt** | **Năm rủi ro tiềm ẩn hàng đầu trong bảo mật đám mây**  ***(Top 5 Hidden Cloud Risks)*** | **Biện pháp kiểm soát (“control”) theo ISO 27001:2013 (Phụ lục A)** |
| **(1)** | **(2)** | (3) |
| **1** | Lack of visibility (Thiếu khả năng hiển thị) | *Nhóm 12. An toàn hoạt động,*  *Yêu cầu 12.4. Giám sát,*  *Điều 12.4..1 Ghi nhật ký sự kiện* |
| **2** | Misconfiguration (Cấu hình sai), | *Nhóm 12. An toàn hoạt động,*  *Yêu cầu 12.6. Quản lý lỗ hổng kỹ thuật,*  *Điều 12.6.1. Quản lý các lỗ hổng kỹ thuật* |
| **3** | Lack of encryption (Thiếu mã hóa) | *Nhóm 10. Kiểm soát mật mã,*  *Yêu cầu 10.1. Các yêu cầu kiểm soát mật mã,*  *Điều 10.1.1. Chính sách về sử dụng kiểm soát mật mã* |
| **4** | Zero-day vulnerabilities (Lỗ hổng zero-day) | *Nhóm 12. An toàn hoạt động*  *Yêu cầu 12.6. Quản lý lỗ hổng kỹ thuật*  *Điều 12.6.1. Quản lý các lỗ hổng kỹ thuật* |
| **5** | Unsecured APIs (API không an toàn) | *<đề không yêu cầu>* |