**TRƯỜNG ĐẠI HỌC CÔNG NGHỆ SÀI GÒN**

**KHOA CÔNG NGHỆ THÔNG TIN**

**\_\_\_oOo\_\_\_**



**AN NINH MẠNG**

(tái bản lần 1)

Sinh viên thực hiện

**Lê Hoàng Thân**

**MSSV: DH52201426**

THÀNH PHỐ HỒ CHÍ MINH – 2024

**Bài 1: Chào mừng đến với thế giới an ninh mạng**

**1. Giới thiệu về an ninh mạng**

An ninh mạng hay bảo mật là hoạt động đảm bảo tính bảo mật, tính toàn vẹn và tính sẵn có của thông tin bằng cách bảo vệ mạng, thiết bị, con người và dữ liệu khỏi bị truy cập trái phép hoặc khai thác trái phép.

Ví dụ: yêu cầu mật khẩu phức tạp để truy cập các trang web và dịch vụ sẽ cải thiện tính bảo mật bằng cách khiến tác nhân đe dọa khó xâm nhập hơn. Tác nhân đe dọa là bất kỳ cá nhân, nhóm hoặc tổ chức nào có nguy cơ gây ra rủi ro bảo mật.

Bảo mật an ninh chống lại các mối đe dọa bên ngoài và bên trong.

Mối đe dọa bên ngoài là ai đó bên ngoài tổ chức đang cố gắng truy cập vào thông tin, mạng hoặc thiết bị riêng tư.

Mối đe dọa bên trong đến từ nhân viên hiện tại hoặc nhân viên cũ, nhà cung cấp bên ngoài hoặc đối tác đáng tin cậy. Thông thường, những mối đe dọa nội bộ này là vô tình, chẳng hạn như nhân viên nhấp vào liên kết bị xâm phạm trong email. Trong những trường hợp khác, tác nhân nội bộ cố tình tham gia vào các hoạt động như truy cập dữ liệu trái phép hoặc lạm dụng hệ thống để sử dụng cho mục đích cá nhân.

Các nhóm bảo mật cũng đảm bảo tổ chức đáp ứng việc tuân thủ quy định, pháp luật và hướng dẫn yêu cầu triển khai các tiêu chuẩn bảo mật cụ thể.

Việc đảm bảo rằng các tổ chức tuân thủ đúng có thể cho phép họ tránh bị phạt tiền và kiểm tra, đồng thời duy trì nghĩa vụ đạo đức của mình để bảo vệ người dùng.

Đội ngũ an ninh cũng duy trì và nâng cao năng suất kinh doanh. Bằng cách thiết lập kế hoạch đảm bảo tính liên tục trong kinh doanh, nhóm bảo mật cho phép mọi người thực hiện công việc của mình, ngay cả trong trường hợp xảy ra sự cố như vi phạm dữ liệu.

Ý thức về bảo mật cũng có thể giảm chi phí liên quan đến rủi ro, chẳng hạn như khôi phục sau khi mất dữ liệu hoặc thời gian ngừng hoạt động và có khả năng tránh bị phạt.

Lợi ích cuối cùng của bảo mật là duy trì niềm tin vào thương hiệu. Nếu dịch vụ hoặc dữ liệu khách hàng bị xâm phạm, điều này có thể làm giảm niềm tin vào tổ chức, làm tổn hại đến thương hiệu và gây tổn hại cho doanh nghiệp về lâu dài. Mất niềm tin của khách hàng cũng có thể dẫn đến doanh thu ít hơn cho doanh nghiệp.

Một số công việc thuộc bảo mật: Security analyst or specialist (Nhà phân tích hoặc chuyên gia bảo mật), Cybersecurity analyst or specialist (nhà phân tích hoặc chuyên gia An ninh mạng), Security operation center or SOC analyst (Trung tâm điều hành bảo mật hoặc nhà phân tích SOC), Information security analyst (nhà phân tích bảo mật thông tin).

**2. Trách nhiệm của một nhà phân tích an ninh mạng cấp đầu vào**

Công nghệ đang thay đổi nhanh chóng và các chiến thuật cũng như kỹ thuật mà kẻ tấn công sử dụng cũng thay đổi. Khi cơ sở hạ tầng kỹ thuật số phát triển, các chuyên gia bảo mật ​​sẽ phải liên tục phát triển kỹ năng để bảo vệ và bảo mật thông tin nhạy cảm.

Các nhà phân tích bảo mật chịu trách nhiệm giám sát và bảo vệ thông tin và hệ thống.

Một nhà phân tích bảo mật có 3 trách nhiệm chính:

1. Bảo vệ hệ thống máy tính và mạng đòi hỏi nhà phân tích phải giám sát mạng nội bộ của tổ chức. Nếu một mối đe dọa được phát hiện thì nhà phân tích thường là người đầu tiên phản ứng. Các nhà phân tích cũng thường tham gia vào các hoạt động tìm kiếm điểm yếu trong hệ thống của tổ chức. Ví dụ: một nhà phân tích bảo mật có thể đóng góp vào việc kiểm tra thâm nhập hoặc hack có đạo đức. Mục tiêu là xâm nhập hoặc hack mạng nội bộ của tổ chức họ để xác định các lỗ hổng và đề xuất cách tăng cường các biện pháp bảo mật của họ.

2. Chủ động làm việc để ngăn chặn các mối đe dọa xảy ra ngay từ đầu, làm việc với các nhóm công nghệ thông tin để cài đặt phần mềm phòng ngừa nhằm mục đích xác định rủi ro và lỗ hổng. Có thể tham gia phát triển phần mềm và phần cứng. Làm việc với các nhóm phát triển để hỗ trợ bảo mật sản phẩm bằng cách thiết lập các quy trình và hệ thống phù hợp nhằm đáp ứng nhu cầu bảo vệ dữ liệu của tổ chức.

3. Kiểm toán an ninh định kỳ. Kiểm toán an ninh là việc xem xét hồ sơ, hoạt động bảo mật và các tài liệu liên quan khác của tổ chức. Ví dụ: một nhà phân tích có thể kiểm tra các vấn đề bảo mật nội bộ, chẳng hạn như đảm bảo rằng thông tin riêng tư, như mật khẩu máy tính cá nhân, không được cung cấp cho tất cả nhân viên.

Các nhà phân tích bảo mật là một phần quan trọng của bất kỳ tổ chức nào. Nhiệm vụ hàng ngày là bảo vệ các doanh nghiệp nhỏ, công ty lớn, tổ chức phi lợi nhuận và cơ quan chính phủ.

**3. Thuật ngữ an ninh mạng phổ biến**

Có nhiều thuật ngữ và khái niệm quan trọng mà các chuyên gia bảo mật cần biết. Làm quen với thuật ngữ giúp xác định rõ hơn các mối đe dọa có thể gây hại cho tổ chức cũng như mọi người.

Một nhà phân tích bảo mật hoặc nhà phân tích an ninh mạng tập trung vào việc giám sát các mạng để phát hiện các vi phạm. Ngoài ra, còn giúp phát triển các chiến lược để bảo mật tổ chức và nghiên cứu các xu hướng bảo mật công nghệ thông tin (IT) để luôn cảnh giác và được thông báo về các mối đe dọa tiềm ẩn.

**Compliance** **–** **Tuân thủ l**à quá trình tuân thủ các tiêu chuẩn nội bộ và quy định bên ngoài, đồng thời cho phép các tổ chức tránh bị phạt và vi phạm an ninh.

**Security frameworks –Khung bảo mật** là các nguyên tắc được sử dụng để xây dựng kế hoạch nhằm giúp giảm thiểu rủi ro và mối đe dọa đối với dữ liệu và quyền riêng tư.

**Security controls** **– Kiểm soát bảo mật** là các biện pháp bảo vệ được thiết kế để giảm thiểu rủi ro bảo mật cụ thể. Chúng được sử dụng cùng với **Security frameworks** để thiết lập một thế trận bảo mật mạnh mẽ.

**Security posture** **– Tình trạng bảo mật** là khả năng của tổ chức trong việc quản lý việc bảo vệ các tài sản và dữ liệu quan trọng cũng như phản ứng với những thay đổi. Một trạng thái bảo mật mạnh mẽ dẫn đến rủi ro thấp hơn cho tổ chức.

**Threat actor – Tác nhân đe dọa** hoặc malicious attacker – kẻ tấn công độc hại là bất kỳ cá nhân hoặc nhóm nào gây ra rủi ro bảo mật. Rủi ro này có thể liên quan đến máy tính, ứng dụng, mạng và dữ liệu.

**internal threat** **– Mối đe dọa nội bộ** có thể là nhân viên hiện tại hoặc nhân viên cũ, nhà cung cấp bên ngoài hoặc đối tác đáng tin cậy gây ra rủi ro bảo mật. Đôi khi, một mối đe dọa nội bộ là vô tình. Ví dụ: một nhân viên vô tình nhấp vào liên kết email độc hại sẽ bị coi là mối đe dọa vô tình. Đôi khi, tác nhân đe dọa nội bộ cố tình tham gia vào các hoạt động rủi ro, chẳng hạn như truy cập dữ liệu trái phép.

**Network security** **– An ninh mạng** là hoạt động giữ an toàn cho cơ sở hạ tầng mạng của một tổ chức khỏi bị truy cập trái phép. Điều này bao gồm dữ liệu, dịch vụ, hệ thống và thiết bị được lưu trữ trong mạng của tổ chức.

**Cloud security** **–** **Bảo mật đám mây** là quá trình đảm bảo rằng các tài sản được lưu trữ trên đám mây được định hình đúng cách hoặc được thiết lập chính xác và quyền truy cập vào các tài sản đó được giới hạn ở những người dùng được ủy quyền. Đám mây là một mạng được tạo thành từ một tập hợp các máy chủ hoặc máy tính lưu trữ tài nguyên và dữ liệu ở các vị trí vật lý từ xa được gọi là trung tâm dữ liệu có thể được truy cập qua internet. Bảo mật đám mây là một lĩnh vực an ninh mạng đang phát triển, đặc biệt tập trung vào việc bảo vệ dữ liệu, ứng dụng và cơ sở hạ tầng trên đám mây.

**Programming –** **Lập trình** là một quá trình có thể được sử dụng để tạo ra một bộ hướng dẫn cụ thể để máy tính thực hiện các tác vụ. Những nhiệm vụ này có thể bao gồm:

* Tự động hóa các tác vụ lặp đi lặp lại (ví dụ: tìm kiếm danh sách các miền độc hại)
* Xem xét lưu lượng truy cập web
* Cảnh báo hoạt động đáng ngờ