Journal of educational equipment: Applied research, Volume 1, Issue 324 (November 2024)
ISSN 1859 - 0810

Một số công nghệ bảo mật thông tin hiện đại

Hoàng Minh Ngọc*, Đinh Thị Phượng*

**ThS Khoa Ngoại ngữ - Tin học, Học Viện Hành chính Quốc Gia*
Received: 03/10/2024; Accepted: 14/10/2024; Published: 30/10/2024

Abstract: *Information is a valuable asset that affects every aspect of life. Managing, protecting and using information effectively not only helps individuals and organizations achieve success but also contributes to the sustainable development of society. This article discusses the importance of information security and some modern technologies for information security.*

Keywords: *Safety, security, information, data*

1. Đặt vấn đề

Thông tin là một tài sản quý giá, ảnh hưởng đến mọi khía cạnh của cuộc sống. Sự phát triển mạnh mẽ của mạng Internet và các dịch vụ mạng trên nền Internet đã xuất hiện các sự cố mất an toàn thông tin liên tục xảy ra và đặc biệt các dạng tấn công, xâm nhập các hệ thống máy tính và mạng xuất hiện ngày càng phổ biến và mức độ phá hoại ngày càng nghiêm trọng. Vì vậy, vấn đề đảm bảo an toàn cho thông tin, các hệ thống và mạng trở nên cấp thiết và là mối quan tâm của mỗi quốc gia, cơ quan, tổ chức và mỗi người dùng. Vấn đề bảo mật thông tin đã được đưa vào giảng dạy trong các trường đại học. Môn học An toàn bảo mật hệ thống thông tin là môn học cơ sở chuyên ngành trong chương trình đào tạo đại học ngành Công nghệ thông tin. Sự phát triển nhanh chóng của khoa học, đặc biệt là trong lĩnh vực công nghệ thông tin, việc cập nhật một số công nghệ bảo mật thông tin hiện đại là việc làm cần thiết để nâng cao chất lượng và hiệu quả môn học.

2. Nội dung nghiên cứu

2.1. Khái niệm bảo mật thông tin:

Bảo mật thông tin, thường được viết tắt là InfoSec, là tập hợp các quy trình và công cụ bảo mật để bảo vệ trên diện rộng thông tin nhạy cảm của doanh nghiệp, tránh để thông tin đó bị lạm dụng, truy nhập trái phép, gián đoạn hoặc phá hủy. InfoSec bao gồm bảo mật vật lý và môi trường, kiểm soát truy nhập và an ninh mạng

Bảo mật thông tin là duy trì tính bảo mật, tính toàn vẹn toàn diện và tính sẵn sàng cho toàn bộ thông tin. Ba yếu tố không thể tách rời trong việc bảo mật từ A đến Z thông tin là:

– Tính bảo mật: Đảm bảo thông tin đó là duy nhất, những người muốn tiếp cận phải được phân quyền truy cập.

– Tính toàn vẹn. Bảo vệ sự hoàn chỉnh toàn diện cho hệ thống thông tin.

– Tính chính xác. Thông tin đưa ra phải chính xác, đầy đủ, không được sai lệch hay không được vi phạm bản quyền nội dung.

– Tính sẵn sàng. Việc bảo mật thông tin luôn phải sẵn sàng, có thể thực hiện bất cứ đâu, bất cứ khi nào.

Bảo mật thông tin (Information Security) và an ninh mạng (IT Security) có những điểm khác biệt nhất định: Bảo mật thông tin là khái niệm bao hàm rất rộng, nó là quá trình sử dụng các công cụ để bảo vệ thông tin khỏi các tác nhân vật lý, kỹ thuật độc hại, còn an ninh mạng thì hướng về bảo mật thông tin phần mềm, chủ yếu là bảo mật dữ liệu số thông qua bảo mật mạng máy tính. Đây là một khía cạnh nhỏ trong bảo mật thông tin nói chung.

2.2. Một số công nghệ bảo mật thông tin hiện đại

2.2.1. Mã Hóa Dữ Liệu

Mã hóa là một trong những kỹ thuật bảo mật cơ bản nhưng vô cùng hiệu quả. Các thuật toán mã hóa như AES (Advanced Encryption Standard) giúp bảo vệ thông tin bằng cách biến đổi nó thành một dạng không thể đọc được mà chỉ những người có khóa mã mới có thể giải mã.

2.2.2. Tường Lửa Thế Hệ Mới

Tường lửa thế hệ mới (Next-Generation Firewall - NGFW) là một loại tường lửa hiện đại, không chỉ thực hiện chức năng cơ bản của tường lửa truyền thống mà còn tích hợp nhiều tính năng bảo mật tiên tiến để bảo vệ mạng khỏi các mối đe dọa phức tạp.

a) Các Tính Năng Chính của NGFW:

- *Kiểm soát ứng dụng*: NGFW có khả năng xác định và kiểm soát lưu lượng mạng dựa trên ứng

dụng, không chỉ theo địa chỉ IP hoặc cổng. Điều này cho phép quản trị viên quản lý và giám sát các ứng dụng cụ thể.

- *Phát hiện và ngăn chặn xâm nhập (IPS)*: NGFW thường tích hợp chức năng IPS để phát hiện và ngăn chặn các cuộc tấn công, giúp bảo vệ mạng khỏi các mối đe dọa.

- *Bảo vệ chống malware*: NGFW có khả năng quét lưu lượng mạng để phát hiện và ngăn chặn mã độc và virus, bảo vệ hệ thống khỏi các phần mềm độc hại.

- *Xác thực người dùng*: Hỗ trợ xác thực người dùng để đảm bảo rằng chỉ những người dùng hợp lệ mới có quyền truy cập vào mạng.

- *Quản lý và phân tích lưu lượng*: NGFW cung cấp các công cụ phân tích sâu về lưu lượng mạng, giúp nhận diện các hành vi bất thường và đưa ra báo cáo chi tiết.

- *Tích hợp với các công nghệ bảo mật khác*: NGFW có thể tích hợp với các giải pháp bảo mật khác như hệ thống phát hiện xâm nhập (IDS), công nghệ chống virus, và quản lý sự kiện và thông tin bảo mật (SIEM).

b) Lợi Ích của NGFW:

- *Bảo mật toàn diện*: Với nhiều lớp bảo vệ, NGFW giúp bảo vệ tổ chức khỏi các mối đe dọa từ nhiều nguồn khác nhau.

- *Quản lý linh hoạt*: Cung cấp khả năng kiểm soát chi tiết về lưu lượng mạng và ứng dụng, giúp tổ chức dễ dàng điều chỉnh chính sách bảo mật theo nhu cầu.

- *Giảm thiểu rủi ro*: Tính năng phát hiện và ngăn chặn xâm nhập giúp giảm thiểu nguy cơ bị tấn công thành công.

c) Thách Thức Khi Triển Khai NGFW:

- *Chi phí*: NGFW thường có chi phí cao hơn so với tường lửa truyền thống, cả về phần cứng và phần mềm.

- *Yêu cầu về tài nguyên*: Việc xử lý và phân tích lưu lượng mạng phức tạp có thể yêu cầu tài nguyên phần cứng lớn hơn.

- *Cần có chuyên môn*: Để triển khai và quản lý NGFW hiệu quả, tổ chức cần có đội ngũ nhân sự có kỹ năng chuyên môn trong lĩnh vực bảo mật.

Tường lửa thế hệ mới (NGFW) là một phần không thể thiếu trong hệ thống bảo mật mạng hiện đại. Với khả năng phát hiện, phân tích và kiểm soát lưu lượng một cách sâu sắc, NGFW giúp bảo vệ tổ chức khỏi các mối đe dọa ngày càng tinh vi trong thế giới số.

2.2.3. Hệ thống phát hiện xâm nhập (IDS)

Hệ thống Phát hiện Xâm nhập (Intrusion Detection System - IDS) là một công nghệ bảo mật mạng dùng để phát hiện và phản ứng với các hành vi xâm nhập hoặc các hoạt động đáng ngờ trong hệ thống máy tính hoặc mạng.

a) Chức Năng Chính của IDS:

- *Giám sát và Phân tích*: IDS liên tục theo dõi lưu lượng mạng và hoạt động hệ thống để phát hiện các dấu hiệu của xâm nhập hoặc hành vi bất thường.

- *Cảnh báo*: Khi phát hiện một hành vi khả nghi, IDS sẽ gửi cảnh báo tới quản trị viên hoặc hệ thống quản lý bảo mật để tiến hành kiểm tra và phản ứng.

- *Ghi lại sự kiện*: IDS ghi lại các sự kiện để phục vụ cho việc phân tích và điều tra sau này, giúp hiểu rõ hơn về các mối đe dọa.

b) Các Loại IDS:

- *IDS Dựa trên Mạng (NIDS)*: Giám sát toàn bộ lưu lượng mạng để phát hiện các mối đe dọa. Thường được triển khai tại các điểm nút của mạng để theo dõi lưu lượng vào và ra.

- *IDS Dựa trên Hệ thống (HIDS)*: Giám sát và phân tích các hoạt động trong hệ thống máy tính hoặc máy chủ. HIDS thường kiểm tra các tệp log, sự thay đổi tệp hệ thống và các thông tin khác để phát hiện xâm nhập.

c) Các kỹ thuật phát hiện:

- *Phát hiện dựa trên chữ ký (Signature-based)*: So sánh lưu lượng hoặc hành động với một cơ sở dữ liệu các mẫu xâm nhập đã biết. Cách này hiệu quả với các cuộc tấn công đã được xác định, nhưng có thể bỏ lỡ các cuộc tấn công mới hoặc chưa được biết đến.

- *Phát hiện dựa trên hành vi (Anomaly-based)*: Xây dựng một mô hình hành vi bình thường của hệ thống hoặc mạng, từ đó phát hiện các hành vi bất thường. Phương pháp này có khả năng phát hiện các cuộc tấn công mới, nhưng cũng có thể dẫn đến cảnh báo giả (false positives).

c) Lợi Ích của IDS:

- *Bảo vệ trước các mối đe dọa*: Giúp phát hiện và ngăn chặn các cuộc tấn công trước khi chúng gây ra thiệt hại lớn.

- *Tăng cường khả năng phản ứng*: Cung cấp

thông tin kịp thời để quản trị viên có thể thực hiện các biện pháp cần thiết.

- *Cải thiện việc tuân thủ quy định*: Giúp tổ chức duy trì các tiêu chuẩn bảo mật và tuân thủ các quy định pháp lý.

d) Thách thức:

- *Cảnh báo giả*:

IDS có thể tạo ra nhiều cảnh báo giả, làm cho quản trị viên khó khăn trong việc xác định mối đe dọa thực sự.

- *Chi phí và tài nguyên*:

Triển khai và duy trì IDS có thể tốn kém và yêu cầu nguồn lực đáng kể.

Hệ thống Phát hiện Xâm nhập (IDS) là một phần quan trọng trong chiến lược bảo mật của bất kỳ tổ chức nào. Việc triển khai IDS giúp bảo vệ tài nguyên và dữ liệu khỏi các mối đe dọa, đồng thời cung cấp thông tin cần thiết cho việc quản lý an ninh mạng

2.2.4. Công Nghệ Zero Trust

Công nghệ Zero Trust là một mô hình bảo mật mạng mới, được thiết kế để ngăn chặn các cuộc tấn công từ bên ngoài và bên trong bằng cách không tin tưởng mặc định vào bất kỳ người dùng hoặc thiết bị nào, ngay cả khi chúng nằm trong mạng nội bộ.

a) Các nguyên tắc chính của Zero Trust:

- *Không tin tưởng ai:* Tất cả người dùng và thiết bị đều phải được xác thực, xác minh và phân quyền trước khi truy cập vào bất kỳ tài nguyên nào.

- *Xác thực liên tục:* Thay vì chỉ kiểm tra một lần khi người dùng đăng nhập, Zero Trust yêu cầu xác thực liên tục dựa trên hành vi và bối cảnh của người dùng.

- *Phân quyền tối thiểu*: Người dùng chỉ được cấp quyền truy cập tối thiểu cần thiết để thực hiện nhiệm vụ của họ, giúp hạn chế khả năng truy cập của những người không có quyền.

- *Kiểm soát truy cập dựa trên danh tính*: Việc kiểm soát truy cập không chỉ dựa vào địa chỉ IP hoặc vị trí mà còn dựa trên danh tính người dùng và thiết bị.

- *Theo dõi và ghi lại hoạt động:* Mọi hoạt động trong hệ thống đều được theo dõi và ghi lại để phát hiện và phản ứng nhanh chóng với các hành vi bất thường.

b) Lợi ích của mô Hình Zero Trust:

- *Bảo vệ trước các mối đe dọa nội bộ và bên ngoài:* Giúp ngăn chặn các cuộc tấn công từ cả bên ngoài và những người có quyền truy cập trong nội bộ.

- *Giảm thiểu rủi ro:* Việc phân quyền tối thiểu và kiểm soát truy cập chặt chẽ giúp giảm thiểu nguy cơ mất mát dữ liệu.

- *Tăng cường khả năng phản ứng với sự cố:* Với việc theo dõi và ghi lại hoạt động, tổ chức có thể phát hiện và ứng phó nhanh chóng với các mối đe dọa.

c) Thực hiện Zero Trust:

- *Xác thực đa yếu tố (MFA):* Sử dụng nhiều hình thức xác thực để đảm bảo rằng chỉ những người dùng hợp lệ mới có thể truy cập.

- *Phân tích hành vi người dùng:* Sử dụng công nghệ học máy để phát hiện các hành vi bất thường của người dùng.

- *Chia nhỏ mạng:* Tạo ra các khu vực bảo mật khác nhau trong mạng để giới hạn quyền truy cập và giảm thiểu thiệt hại nếu có sự cố xảy ra.

Zero Trust là một phương pháp bảo mật hiệu quả trong môi trường hiện đại, nơi mà các mối đe dọa ngày càng tinh vi. Bằng cách không tin tưởng mặc định, tổ chức có thể bảo vệ tài nguyên và dữ liệu của mình tốt hơn trước các mối đe dọa từ mọi phía.

3. Kết Luận

Học viện Hành chính Quốc gia chủ trương xây dựng Học viện số đáp ứng chiến lược phát triển của Học viện. Xây dựng Học viện số bảo đảm gắn kết chặt chẽ với bảo đảm an toàn thông tin, an toàn mạng, an ninh quốc gia, bảo vệ thông tin cá nhân. Trong bối cảnh công nghệ ngày càng phát triển, việc áp dụng các công nghệ và kỹ thuật bảo mật thông tin là vô cùng cần thiết để bảo vệ tổ chức khỏi các mối đe dọa tiềm tàng. Bên cạnh đó, chúng ta cần tiếp tục nâng cao nhận thức và kỹ năng bảo mật trong toàn bộ tổ chức, từ lãnh đạo đến nhân viên.

Tài liệu tham khảo

1. Trần Văn Đạt (2016), *Giáo trình phương pháp mghiên cứu khoa học giáo dục,* NXB Đại học Quốc gia.

2. Vũ Nguyễn Đức, *Giáo trình Phương pháp nghiên cứu khoa học*, NXB Đại học Huế.

3. Nguyễn Thị Thanh Vân (2023, chủ biên), *Giáo trình an ninh mạng,* NXB Đại học Quốc gia.

4. Trần Đức Sự (chủ biên), *Giáo trình an toàn và bảo mật dữ liệu*, NXB Đại học Thái Nguyên