TẠP CHÍ PHÒNG CHÁY VÀ CHỮA CHÁY ĐIỆN TỬ
JOURNAL OF FIRE ONLINE
e-ISSN: 3093-3595

Ngày nhận bài: 05/3/2025; Ngày thẩm định: 27/3/2025; Ngày nhận đăng: 08/4/2025.

ĐỀ XUẤT MÔ HÌNH BẢO ĐẢM AN TOÀN MẠNG NỘI BỘ TẠI CÁC TRƯỜNG CÔNG AN NHÂN DÂN TRONG KỶ NGUYÊN SỐ

Trung tá, TS NGUYỄN TÀI NĂNG LƯỢNG
Khoa Khoa học cơ bản và Ngoại ngữ, Trường Đại học PCCC
*Tác giả liên hệ: Nguyễn Tài Năng Lượng (Email: tailuong2003@gmail.com)

***Tóm tắt**: Trong bối cảnh chuyển đổi số, an toàn mạng nội bộ đóng vai trò then chốt trong hoạt động giáo dục, đào tạo và quản lý tại các trường Công an nhân dân. Tuy nhiên, hệ thống mạng này đang đối mặt với nhiều thách thức như các cuộc tấn công mạng, rò rỉ dữ liệu và hạn chế trong nhận thức bảo mật. Bài viết đề xuất mô hình bảo đảm an toàn mạng nội bộ dựa trên các công nghệ hiện đại như trí tuệ nhân tạo (AI), Blockchain, mô hình Zero Trust và hệ thống giám sát an ninh SIEM.*

***Từ khoá**: mạng nội bộ, Zero Trust, SIEM, Blockchain, trí tuệ nhân tạo, hệ thống giám sát.*

***Abstract**: In the context of ongoing digital transformation, internal network security is of paramount importance to educational, training, and managerial functions of people's police higher education institutions. However, this network reveals several challenges such as cyber attacks, data leaks, and deficiencies in maintaining confidentiality. Therefore, this article proposes a model that leverages modern technologies, including the integration of Artificial Intelligence (AI), Blockchain, the Zero Trust model, and SIEM security monitoring system.*

***Keywords**: Internal network, Zero Trust, SIEM, Blockchain, Artificial Intelligence, Security Monitoring System.*

1. Trong bối cảnh chuyển đổi số mạnh mẽ, hệ thống mạng nội bộ tại các trường Công an nhân dân đóng vai trò quan trọng trong công tác giảng dạy, nghiên cứu và lưu trữ dữ liệu. Tuy nhiên, hệ thống này đang phải đối mặt với nhiều nguy cơ tấn công mạng như tấn công có chủ đích, mã độc tống tiền hay sự xâm nhập trái phép và rủi ro từ chính người dùng nội bộ.

Thực tế cho thấy, mặc dù đã triển khai một số biện pháp bảo mật như tường lửa, phần mềm diệt Virus và kiểm soát truy cập, nhưng những giải pháp này còn rời rạc, thiếu tính đồng bộ và chưa tận dụng hiệu quả các công nghệ hiện đại. Điều này đặt ra yêu cầu cấp thiết về một mô hình bảo đảm an toàn mạng nội bộ toàn diện hơn.

Bài viết đề xuất một mô hình bảo mật tích hợp các công nghệ tiên tiến như AI trong giám sát và phát hiện tấn công, Blockchain trong bảo mật dữ liệu, mô hình Zero Trust trong kiểm soát truy cập và hệ thống giám sát an ninh tập trung SIEM (Security Information and Event Management). Mô hình này giúp tăng cường khả năng bảo vệ hệ thống, đảm bảo an toàn thông tin và nâng cao hiệu quả quản lý mạng nội bộ tại các trường Công an nhân dân.

2. Một trong những vấn đề lớn là nhiều trường Công an nhân dân vẫn đang sử dụng hệ thống mạng được triển khai từ nhiều năm trước, với các thiết bị cũ kỹ, chưa được nâng cấp kịp thời. Hệ thống bảo mật truyền thống như: tường lửa, phần mềm diệt Virus và phương thức kiểm soát truy cập cũ không còn đủ khả năng đối phó với các mối đe dọa hiện đại như tấn công

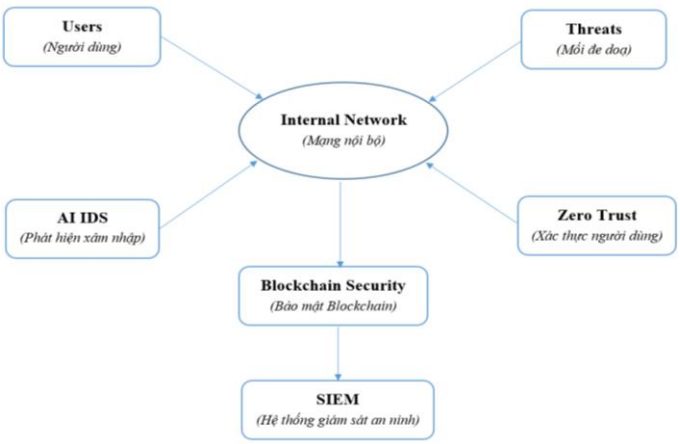
có chủ đích, mã độc tống tiền, hay các cuộc tấn công từ chối dịch vụ phân tán DDoS [1]. Sự hạn chế về mặt công nghệ khiến các trường dễ bị tổn thương trước các cuộc tấn công mạng ngày càng tinh vi.

Ngoài các yếu tố kỹ thuật, an toàn mạng nội bộ còn chịu tác động từ yếu tố con người. Nhận thức về bảo mật thông tin của cán bộ, giảng viên và học viên trong môi trường đào tạo vẫn còn hạn chế. Nhiều người sử dụng mạng nội bộ mà không tuân thủ các quy tắc an toàn thông tin, vô tình hoặc cố ý tạo ra các lỗ hổng bảo mật. Việc sử dụng thiết bị cá nhân như USB, điện thoại thông minh để kết nối với mạng nội bộ mà không có biện pháp bảo vệ thích hợp có thể tạo điều kiện cho tin tặc xâm nhập hệ thống.

Hơn nữa, khi sự cố an ninh mạng xảy ra, quy trình xử lý tại nhiều trường vẫn chưa đồng bộ và thiếu sự chủ động. Nhiều cơ sở chưa triển khai hệ thống giám sát an ninh tập trung SIEM hoặc chưa có các chính sách bảo mật toàn diện để kiểm soát các mối đe dọa một cách hiệu quả. Điều này dẫn đến tình trạng khi bị tấn công làm cho hệ thống không thể phản ứng kịp thời, gây ra hậu quả nghiêm trọng.

Trước thực trạng này, việc ứng dụng các công nghệ tiên tiến để nâng cao an toàn mạng nội bộ tại các trường Công an nhân dân là yêu cầu cấp thiết.

3. Để triển khai một hệ thống bảo đảm an toàn mạng nội bộ hiệu quả, cần có sự đầu tư đồng bộ về hạ tầng kỹ thuật, nhân lực và quy trình vận hành. Mô hình bảo đảm an toàn mạng nội bộ tại các trường Công an nhân dân nên bao gồm các thành phần chính như hình 1.



Hình 1: Mô hình an toàn mạng nội bộ.

Người dùng (Users): Bao gồm cán bộ, giảng viên, học viên sử dụng hệ thống mạng nội bộ để truy cập thông tin, tài nguyên giảng dạy và nghiên cứu. Người dùng có thể vô tình hoặc cố ý tạo ra rủi ro bảo mật nếu không tuân thủ các quy tắc an toàn thông tin. Do đó, việc đào tạo, nâng cao nhận thức về an ninh mạng cho người dùng là một yếu tố quan trọng.

Mối đe dọa (Threats): Hệ thống mạng nội bộ có thể bị ảnh hưởng bởi các cuộc tấn công mạng, mã độc tống tiền, tấn công có chủ đích, và các nguy cơ an ninh khác. Việc xác định và đánh giá các mối đe dọa tiềm ẩn là nền tảng để xây dựng một chiến lược bảo mật hiệu quả.

Hệ thống mạng nội bộ (Internal Network): Là trung tâm của mô hình, nơi diễn ra tất cả các hoạt động kết nối giữa người dùng và các tài nguyên trong trường. Hệ thống này cần được bảo vệ khỏi các mối đe dọa thông qua các công nghệ bảo mật tiên tiến.

Hệ thống phát hiện xâm nhập AI (*AI IDS - Intrusion Detection System)*: Thông qua học máy và công nghệ máy trắc viễn CPU, AI có thể nhận diện các mối đe dọa tiềm ẩn, ngay cả những cuộc tấn công tinh vi khó phát hiện, đồng thời cung cấp cảnh báo theo thời gian thực. Ngoài ra, AI hỗ trợ săn tìm mối đe dọa bằng cách giám sát hệ thống để phát hiện các dấu hiệu tấn công dựa trên các mô hình đã biết. Không chỉ dừng lại ở việc phát hiện, AI còn có khả năng tự động khắc phục sự cố bằng cách sử dụng các thuật toán học sâu để phản ứng với các mối đe dọa mới, dựa trên kinh nghiệm từ các tình huống tương tự trước đó.

Bên cạnh đó, AI còn giúp quản lý lỗ hổng bảo mật bằng cách phân tích hệ thống quản lý và ứng dụng để xác định những khu vực rủi ro cần khắc phục. Đặc biệt, với khả năng tích hợp ở cấp độ phần cứng, AI có thể bảo vệ điểm cuối của thiết bị, giúp phát hiện và ngăn chặn các phần mềm độc hại. Điều này giúp giảm độ trễ, cải thiện khả năng kiểm soát dữ liệu và tối ưu chi phí so với các giải pháp dựa trên đám mây [4].

Bảo mật dữ liệu bằng Blockchain: Blockchain là một công nghệ nổi bật với khả năng bảo mật cao nhờ cơ chế mã hóa mạnh mẽ và tính chất phi tập trung. Khi được ứng dụng trong bảo mật dữ liệu mạng

nội bộ, Blockchain giúp đảm bảo tính toàn vẹn của dữ liệu. Thông tin được ghi vào các khối và liên kết với nhau bằng cơ chế băm, ngăn chặn việc chỉnh sửa hoặc giả mạo. Nhờ đó, hệ thống có thể duy trì dữ liệu chính xác và không thể bị thay đổi một cách trái phép.

Bên cạnh đó, Blockchain giúp hạn chế truy cập trái phép nhờ cơ chế xác thực phi tập trung. Chỉ những thực thể được cấp quyền mới có thể tham gia vào mạng nội bộ và thực hiện các thao tác trên dữ liệu. Điều này giúp tăng cường bảo mật, giảm nguy cơ rò rỉ thông tin nhạy cảm và ngăn chặn sự can thiệp trái phép từ bên ngoài.

Một ưu điểm quan trọng khác của Blockchain là khả năng ghi nhận và kiểm tra lịch sử truy cập. Mọi thao tác trên dữ liệu đều được lưu trữ thành các giao dịch không thể thay đổi, giúp hệ thống trở nên minh bạch và dễ dàng kiểm tra khi cần. Việc truy vết các hoạt động trong mạng nội bộ trở nên chính xác, hỗ trợ công tác kiểm soát và giám sát an ninh hiệu quả.

Với cơ chế lưu trữ phân tán, Blockchain còn giúp chống lại các cuộc tấn công mạng. Không giống như các hệ thống tập trung dễ bị tấn công vào một điểm duy nhất, dữ liệu trong Blockchain được sao chép và lưu trữ trên nhiều nút khác nhau, giảm thiểu nguy cơ mất mát hoặc rò rỉ thông tin [2].

Cơ chế liên tục xác thực người dùng Zero Trust: Ứng dụng mô hình Zero Trust trong kiểm soát truy cập mạng nội bộ giúp nâng cao mức độ bảo mật bằng cách yêu cầu xác minh danh tính và quyền truy cập của mọi người dùng, ngay cả khi người dùng đang hoạt động trong mạng nội bộ. Thay vì mặc định tin cậy vào các thiết bị hoặc người dùng nội bộ, Zero Trust áp dụng nguyên tắc “không tin cậy mặc định”, buộc hệ thống phải liên tục xác thực và giám sát các phiên truy cập. Khi kết hợp với xác thực đa yếu tố, mô hình này giúp giảm thiểu nguy cơ truy cập trái phép, ngăn chặn các mối đe dọa từ bên trong và bên ngoài tổ chức. Nhờ đó, chỉ những người dùng được ủy quyền mới có thể tiếp cận các tài nguyên quan trọng, đảm bảo an toàn cho hệ thống mạng nội bộ trước các rủi ro bảo mật tiềm ẩn.

Bên cạnh kiểm soát danh tính, Zero Trust còn tích hợp các cơ chế giám sát liên tục và phân tích hành vi người dùng để phát hiện các dấu hiệu truy cập bất thường. Nếu một thiết bị hoặc tài khoản có hoạt động đáng ngờ, hệ thống có thể tự động yêu cầu xác thực bổ sung hoặc chặn quyền truy cập ngay lập tức. Ngoài ra, Zero Trust còn kết hợp với các chính sách phân quyền chặt chẽ, chỉ cấp quyền theo nguyên tắc "ít đặc quyền nhất", giới hạn phạm vi tiếp cận của người dùng đối với tài nguyên cần thiết nhằm giảm thiểu nguy cơ lây lan khi có sự cố bảo mật xảy ra [5].

Hệ thống giám sát an ninh SIEM: Hệ thống SIEM là công cụ quan trọng trong việc giám sát và phân tích các sự kiện an ninh mạng theo thời gian thực. SIEM giúp thu thập, tổng hợp và phân tích dữ liệu từ nhiều nguồn khác nhau trong hệ thống, bao gồm tường lửa, thiết bị đầu cuối, máy chủ và ứng dụng. Nhờ đó, hệ thống có thể phát hiện sớm các cuộc tấn công mạng, đưa ra cảnh báo kịp thời và cung cấp thông tin chi tiết để xử lý sự cố một cách nhanh chóng, chính xác.

Việc triển khai SIEM giúp các trường Công an nhân dân tăng cường khả năng giám sát an ninh mạng một cách chủ động và hiệu quả. Thay vì chỉ phản ứng sau khi xảy ra sự cố, hệ thống này hỗ trợ phát hiện sớm các mối đe dọa tiềm ẩn, từ đó ngăn chặn kịp thời các hành vi xâm nhập, tấn công hoặc rò rỉ dữ liệu. SIEM còn cho phép phân loại mức độ nghiêm trọng của các sự kiện bảo mật, giúp các chuyên gia an ninh ưu tiên xử lý những nguy cơ cấp bách nhất, tránh lãng phí tài nguyên vào các cảnh báo giả.

Bên cạnh đó, SIEM còn tích hợp khả năng tự động hóa trong quá trình xử lý sự cố, giảm thiểu sự can thiệp thủ công và tăng tốc độ phản ứng với các mối đe dọa. Khi phát hiện một hành vi bất thường, hệ thống có thể tự động kích hoạt các biện pháp phòng vệ, chẳng hạn như chặn địa chỉ IP đáng ngờ, cách ly thiết bị nhiễm mã độc hoặc gửi cảnh báo khẩn cấp đến bộ phận quản trị. Nhờ đó, các trường Công an nhân dân có thể duy trì một môi trường mạng an toàn, ổn định, hạn chế tối đa rủi ro an ninh.

Ngoài khả năng giám sát và cảnh báo, SIEM còn đóng vai trò quan trọng trong việc tuân thủ các quy định về an ninh thông tin. Đặc biệt, SIEM có thể tích hợp với các công nghệ bảo mật tiên tiến khác như trí tuệ nhân tạo và học máy để phát hiện các mẫu hành vi bất thường một cách thông minh, nâng cao khả năng phòng chống tấn công mạng hiện đại [3].

4. Việc đảm bảo an toàn cho hệ thống mạng nội bộ tại các trường Công an nhân dân là một yêu cầu cấp thiết nhằm bảo vệ thông tin quan trọng và duy trì hoạt động ổn định của hệ thống. Trước sự gia tăng của các mối đe dọa an ninh mạng, cần có những giải pháp đồng bộ, bao gồm nâng cấp công nghệ bảo mật, tăng cường giám sát, nâng cao nhận thức của người dùng và xây dựng quy trình phản ứng nhanh trước sự cố.

Nghiên cứu này không chỉ góp phần nhận diện những lỗ hổng còn tồn tại mà còn đề xuất hướng tiếp cận phù hợp để nâng cao khả năng phòng thủ của mạng nội bộ trong môi trường đặc thù của các trường Công an nhân dân. Việc triển khai các giải pháp an toàn mạng một cách hiệu quả sẽ giúp đảm bảo tính bảo mật, toàn vẹn và sẵn sàng của hệ thống, hỗ trợ tốt hơn cho công tác giảng dạy, nghiên cứu và quản lý trong nhà trường.■

TÀI LIỆU THAM KHẢO

1. L. Tan, Y. Pan, J. Wu, J. Zhou, H. Jiang, Y. Deng (2020), *A New Framework for DDoS Attack Detection and Defense in SDN Environment*, IEEE Access, vol.8, p.161908-161919.

2. Anna L. Buczak, Erhan Guven (2016), *A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection*, IEEE Communications Surveys & Tutorials, 18(2), p.1153-1176.

3. Sandeep Bhatt, Pratyusa K. Manadhata, Loai Zomlot (2014), *The Operational Role of Security Information and Event Management Systems*, IEEE Security & Privacy 12(5) , p.35-41.

4. K. Adhikary, S. Bhushan, S. Kumar, K. Dutta (2020), *Decision Tree and Neural Network Based Hybrid Algorithm for Detecting*, International Journal of Innovative Technology and Exploring Engineering, 9(5).

5. NIST (National Institute of Standards and Technology), *Zero Trust Architecture* (NIST SP 800-207).