Logo Logo not found or type unknown

# Giải pháp ứng cứu và phục hồi hệ thống sau thảm họa tấn công mạng

13:29 13/11/2024

Tác giả: Đang cập nhật

**Với phương châm "cách phòng thủ hay nhất là chủ động tấn công", năm 2024, Liên minh An toàn Thông tin CYSEEX đã thực hiện diễn tập an ninh mạng trên 18 hệ thống, phát hiện 497 lỗ hổng, trong đó có 93 lỗ hổng nghiêm trọng. Chiến dịch phòng chống phishing cho hơn 14.000 nhân viên đã góp phần giảm 40% lỗ hổng nguy hiểm, nâng cao năng lực ứng phó và nhận thức bảo mật trong các tổ chức thành viên.**

Đây là thông tin được cung cấp tại hội thảo "Ứng cứu và phục hồi hệ thống sau thảm họa" do Liên minh An toàn Thông tin CYSEEX tổ chức tại Hà Nội, sáng 13/11 với sự tham dự của gần 300 khách mời là đại diện cơ quan quản lý, lãnh đạo doanh nghiệp và chuyên gia trong lĩnh vực công nghệ, an ninh thông tin.

**Chủ động ứng phó trước các cuộc tấn công mạng ngày càng tinh vi**

Hội thảo "Ứng cứu và phục hồi hệ thống sau thảm họa" nhằm chia sẻ kiến thức và kinh nghiệm, giúp các doanh nghiệp nâng cao nhận thức và chủ động ứng phó trước các cuộc tấn công mạng ngày càng tinh vi.


*Ông Nguyễn Xuân Hoàng, Chủ tịch Liên minh CYSEEX, Phó Chủ tịch HĐQT Công ty Cổ phần MISA phát biểu tại hội thảo.*

Phát biểu khai mạc, ông Nguyễn Xuân Hoàng, Chủ tịch Liên minh CYSEEX, Phó Chủ tịch HĐQT Công ty Cổ phần MISA cho biết, ứng cứu và phục hồi hệ thống sau thảm họa tấn công mạng là nhiệm vụ cấp thiết với các doanh nghiệp. Để bảo vệ an toàn và duy trì tính liên tục cho hệ thống, các doanh nghiệp công nghệ cần chuẩn bị kỹ lưỡng và nâng cao năng lực ứng phó trước mọi tình huống.

Đây là một khâu không thể thiếu để bảo đảm sự ổn định và an toàn của hệ thống thông tin trước những cuộc tấn công ngày càng tinh vi và nguy hiểm. Các bài học và kỹ năng thực tế không chỉ giúp giảm thiểu thiệt hại mà còn giúp tăng cường khả năng chống chịu, phục hồi hệ thống một cách hiệu quả và nhanh chóng nhất.

Khẳng định sự đồng hành cùng Liên minh CYSEEX, ông Trần Quang Hưng, Quyền Cục trưởng Cục An toàn thông tin, Bộ Thông tin và Truyền thông, ông Triệu Mạnh Tùng, Phó Cục trưởng Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Bộ Công an đồng chia sẻ: “Quyết tâm đồng hành cùng Liên minh CYSEEX để nâng cao hệ thống bảo mật, bảo vệ tối đa quyền lợi của người dùng cuối trong kỷ nguyên số”.

Với phần trình bày thuyết phục tại hội thảo, ông Lê Công Phú, Phó Giám đốc VNCERT nhấn mạnh về tầm quan trọng của Threat Hunting trong việc phát hiện mối đe dọa bảo mật tiềm ẩn. Đây là phương pháp chủ động tìm kiếm dấu hiệu độc hại mà không cần phụ thuộc vào cảnh báo trước, vượt qua những hạn chế của công nghệ phòng thủ truyền thống. Threat Hunting giúp giảm thời gian mà mối đe dọa có thể tồn tại trong hệ thống, đồng thời nâng cao khả năng phản ứng nhanh chóng trước các cuộc tấn công mạng ngày càng phức tạp.

**Nhận định các chiến lược phòng thủ và phục hồi hệ thống**

Báo cáo kết quả thực tiễn từ các cuộc diễn tập chống phishing và bảo mật hệ thống, ông Nguyễn Quang Hoàng, Trưởng Ban tổ chức tập trận CYSEEX kiêm Giám đốc An ninh Thông tin MISA đã có những thông tin: Năm 2024, Liên minh CYSEEX đã thực hiện diễn tập an ninh mạng trên 18 hệ thống, phát hiện 497 lỗ hổng, trong đó có 93 lỗ hổng nghiêm trọng. Chiến dịch phòng chống phishing cho hơn 14.000 nhân viên đã góp phần giảm 40% lỗ hổng nguy hiểm, nâng cao năng lực ứng phó và nhận thức bảo mật trong các tổ chức thành viên.

*Diễn giả trình bày việc phát hiện, xử lý, ứng cứu và hỗ trợ phục hồi hệ thống khi bị tấn công mạng.*

Ông Nguyễn Quang Hoàng cũng chia sẻ kinh nghiệm tăng cường phòng thủ mạng, nhấn mạnh vai trò của mô hình SecDevOps trong giảm thiểu lỗ hổng, nâng cao nhận thức an toàn và triển khai hiệu quả các chiến dịch phishing. Định hướng cho năm 2025, CYSEEX sẽ mở rộng thành viên, tổ chức diễn tập thực chiến hàng tháng và đẩy mạnh triển khai kỹ thuật Threat Hunting để tăng cường khả năng bảo mật cho các thành viên trong Liên minh.

Chia sẻ về kinh nghiệm thực chiến ứng cứu và phục hồi hệ thống sau khi bị tấn công, ông Nguyễn Công Cường, Giám đốc Trung tâm SOC,Công ty An ninh mạng Viettel đã nêu rõ cách thức của các nhóm như APT41 và Lazarus từ khai thác lỗ hổng đến triển khai ransomware. Báo cáo cũng chỉ ra các điểm yếu bảo mật phổ biến và đề xuất giải pháp giám sát liên tục, đánh giá định kỳ và lập kế hoạch ứng phó sự cố để tăng cường "sức khỏe" hệ thống.

Đại diện Dell, ông Cao Giang Nam, phụ trách nhóm giải pháp bảo vệ dữ liệu, thị trường Việt Namvà khu vực Đông Dương giới thiệu Power Protect với nền tảng Zero Trust, giúp doanh nghiệp bảovệ và phục hồi dữ liệu trước các mối đe dọa ransomware. Giải pháp sử dụng phân tách vật lý, khóabảo mật và AI thông minh, đảm bảo tính toàn vẹn và phục hồi dữ liệu nhanh chóng trong môitrường đa đám mây, tăng cường an ninh và tính liên tục cho hoạt động doanh nghiệp.

Tại hội thảo, ông Nguyễn Thành Đạt, Product Manager SONIC đã có những nhận định các chiến lược phòng thủ và phục hồi hệ thống cho doanh nghiệp trước mối đe dọa ransomware. Nội dung bao gồm các phương thức tấn công phổ biến như email lừa đảo, đánh cắp tài khoản và giải pháp bảo mật như Zero Trust, phân đoạn mạng, nâng cao nhận thức nhân viên và sao lưu dữ liệu 3-2-1 để đảm bảo khôi phục nhanh chóng.


*Thành viên Liên minh CYSEEX.*

Bên canh đó, các chuyên gia cũng chia sẻ về giải pháp bảo vệ dữ liệu doanh nghiệp với Pure Storage, giúp tăng cường khả năng phục hồi trước tấn công mạng. Công nghệ SafeMode Snapshot cho phép sao lưu an toàn, phát hiện bất thường sớm và khôi phục nhanh chóng, giúp đảm bảo toàn vẹn dữ liệu và giảm thiểu tổn thất khi gặp sự cố an ninh.

Theo ông Hoàng Hiếu, Trưởng nhóm Giải pháp AWS Việt Nam đã có chia sẻ cách AWS bảo vệ và phục hồi dữ liệu trước ransomware qua cập nhật hệ thống, quản lý quyền hạn, phân đoạn mạng và sao lưu an toàn với AWS Backup, AWS DRS, giúp khôi phục nhanh, đảm bảo an toàn và liên tục cho doanh nghiệp.

Theo đại diện Liên minh CYSEEX, với chiến lược năm 2025, Liên minh CYSEEX khẳng định cam kết

mạnh mẽ trong việc bảo vệ không gian mạng trước các mối đe dọa lừa đảo ngày càng phức tạp, tập trung phòng chống phishing. Liên minh không chỉ hướng tới việc giảm thiểu nguy cơ đánh cắp dữ liệu và các tổn thất tài chính, mà còn giúp duy trì sự ổn định và tin cậy của môi trường kinh doanh số. Đây sẽ là nền tảng vững chắc giúp cá nhân và doanh nghiệp an tâm phát triển trong một môi trường số an toàn hơn.

Liên minh An toàn Thông tin CYSEEX (viết tắt của Cyber Security Exercise) là liên minh do MISA khởi xướng thành lập cùng Sapo, Viettel Solutions, Bảo Việt, Mobifone, Bravo với mục đích: Chia sẻ kiến thức và kinh nghiệm giúp nâng cao năng lực trong việc phòng ngừa và ứng phó các sự cố về an ninh thông tin trên không gian mạng.

Hội thảo thường niên CYSEEX được tổ chức thường niên từ năm 2022 là dịp để chia sẻ kiến thức và kinh nghiệm, giúp các thành viên nâng cao năng lực phòng ngừa và ứng phó sự cố an ninh mạng.

**PV**

**Link bài viết:** https://nguoilambao.vn/giai-phap-ung-cuu-va-phuc-hoi-he-thong-sau-tham-hoa