UBND TỈNH ĐIỆN BIÊN
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập – Tự do – Hạnh phúc

Điện Biên, ngày……. tháng 10 năm 2023

KỊCH BẢN
Diễn tập thực chiến bảo đảm an toàn thông tin tỉnh Điện Biên năm 2023

I. Mục tiêu diễn tập

- Chủ đề: "Mạng LAN của một đơn vị bị tấn công, điều hướng người dùng tải về các phần mềm gián điệp, độc hại. Rà soát và xử lý phần mềm gián điệp, độc hại trên máy tính".

- Thời gian diễn tập: 02 ngày 10-11/10/2023.

- Hình thức diễn tập: Trực tiếp.

- Địa điểm: Hội trường tầng 3, Sở Thông tin và Truyền thông - Tổ 04, phường Nam Thanh, thành phố Điện Biên Phủ, tỉnh Điện Biên.

- Đơn vị tổ chức diễn tập: Sở Thông tin và Truyền thông tỉnh Điện Biên.

- Mục tiêu diễn tập thực chiến:

+ Giúp vận hành các hệ thống hạ tầng Công nghệ thông tin của các cơ quan, tổ chức, doanh nghiệp được tập dượt trước với các tình huống tấn công mạng có thể xảy ra nhằm kiểm soát các nguy cơ, ứng phó với các sự cố để đảm bảo hệ thống thông tin được hoạt động ổn định, được khôi phục nhanh nhất có thể khi xảy ra sự cố.

+ Nâng cao năng lực bảo vệ an toàn thông tin, sẵn sàng ngăn chặn, xử lý và ứng cứu sự cố tấn công trên không gian mạng cho cán bộ chuyên trách CNTT của các quan, đơn vị trên địa bàn tỉnh.

+ Trang bị những kỹ năng cần thiết để kịp thời phối hợp ứng phó, giải quyết các vấn đề thông qua tình huống tấn công vào hệ thống thực khi khai thác các hệ thống thông tin trên môi trường mạng cho đội ngũ cán bộ tại các Sở, ban, ngành, UBND các huyện, Thành phố, Đoàn thể và các Tổ chức chính trị xã hội trên địa bàn tỉnh Điện Biên.

+ Thực hiện đúng văn bản quy định, hướng dẫn của cấp trên về hoạt động diễn tập an toàn thông tin (Quy định tại Điều 1, mục II, khoản 4 của Quyết định số 1622/QĐ-TTg ngày 25 tháng 10 năm 2017: "Hàng năm mỗi bộ, tỉnh, thành phố tổ chức ít nhất 01 cuộc diễn tập chuyên đề an toàn thông tin, ứng cứu sự cố mạng trong phạm vi của bộ, ngành, địa phương mình; phối hợp, tham gia các cuộc diễn tập quốc gia và quốc tế do Cơ quan điều phối quốc gia, Bộ Thông tin và Truyền thông tổ chức).

II. Kịch bản chung

1. Kịch bản chung

Kịch bản mô phỏng tình huống: Một nhóm tin tặc (Hacker) sử dụng các công cụ rò quét, dự đoán mật khẩu truy cập được vào mạng nội bộ của Sở A thông qua hệ thống mạng không dây (Wi-Fi). Khi đã tiếp cận mạng nội bộ, Hacker thực hiện hành vi nghe trộm và đánh cắp các gói tin không được mã hóa trong mạng; phát hiện một gói tin chứa thông tin tài khoản và mật khẩu một người dùng sử dụng dịch vụ thư điện tử (email - do dịch vụ này sử dụng giao thức HTTP, không mã hóa thông tin trong quá trình truyền tải nội dung).

Hacker sử dụng thông tin tài khoản bị đánh cắp, gửi thư có đính kèm tập tin chứa mã độc đến danh sách địa chỉ thư điện tử của cán bộ, công chức, viên chức Sở A. Khi người dùng tải, mở tệp tin đính kèm bị cài cắm mã độc, mã độc được kích hoạt hoạt động và kết nối tới máy chủ điều khiển của Hacker. Từ đây, Hacker có quyền kiểm soát hoàn toàn máy tính, thực hiện các hành động đánh cắp và mã hóa dữ liệu quan trọng của người dùng.

Các Đội phòng thủ tham gia diễn tập đóng vai trò là Đội ứng cứu sự cố khẩn cấp của Sở A. Sau khi nhận được cảnh báo từ Trung tâm giám sát, điều hành an toàn thông tin mạng của tỉnh, Đội ứng cứu cần thực hiện các bước theo quy trình ứng cứu sự cố mất an toàn thông tin: Tiếp cận thông tin, phân tích, thông báo, xử lý, điều tra, đánh giá nguồn gốc cuộc tấn công, thực hiện khôi phục hệ thống và đưa ra các biện pháp phòng, chống trong tương lai.

Quá trình diễn tập ứng cứu sự cố gồm các nội dung: Sau khi nhận được thông tin cảnh báo, Đội ứng cứu sự cố bắt đầu tiếp cận hiện trường, phân tích sơ bộ, xác nhận sự cố; báo cáo Ban Lãnh đạo cơ quan quản lý; đánh giá mức độ ảnh hưởng ban đầu, xử lý tạm thời; thu thập, phân tích truy tìm nguyên nhân; xử lý các thành phần độc hại; vá lỗ hổng, khôi phục hệ thống, đề xuất các giải pháp phòng chống và tổng hợp báo cáo.

2. Các bước xử lý

Các bước ứng cứu, xử lý sự cố ATTT bao gồm các Phase (Giai đoạn) dưới đây, Ban Tổ chức (BTC) sẽ lần lượt gửi các thông tin và yêu cầu Diễn tập qua kênh diễn tập được cung cấp, các đội nhận yêu cầu và phản hồi trực tiếp trên hệ thống.

TT	Nội dung	Số điểm	Thời gian
1	Giai đoạn Chuẩn bị - làm quen hệ thống	0	10’
2	Giai đoạn 1 - Tiếp cận hiện trường, ghi nhận và xác nhận sự cố	200	20’
3	Giai đoạn 2 - Thông báo	100	10’
4	Giai đoạn 3 - Ngăn chặn tạm thời	200	10’
5	Giai đoạn 4 - Thu thập bằng chứng và truy tìm thủ	500	30’

	phạm		
6	Giai đoạn 5 - Xử lý nguyên nhân gây ra tấn công	400	20’
7	Giai đoạn 6 - Khôi phục hệ thống	500	20’
8	Giai đoạn 7 - Hoạt động sau sự cố và gửi báo cáo	100	20’
Tổng		**2.000**	140’

3. Hướng dẫn

- Quy trình tham gia diễn tập.

- Nhận các yêu cầu của BTC và phản hồi qua kênh trao đổi được cung cấp.

4. Thông tin liên hệ và hỗ trợ

- Kênh diễn tập: Hệ thống CTF Diễn tập ATTT tỉnh Điện Biên.

- Website: https://drill.whitehat.vn/

- Kênh hotline: 0215.3824.568

- Email: ict@dienbien.gov.vn

III. Hạ tầng, thành phần, công cụ phục vụ diễn tập

1. Cơ sở hạ tầng

- Hạ tầng kỹ thuật: Hệ thống hạ tầng mạng mô phỏng Sở A.

- Đơn vị vận hành hệ thống: Trung tâm Công nghệ thông tin và Truyền thông

- Chủ quản hệ thống: UBND tỉnh Điện Biên

- Hệ thống đưa vào diễn tập: Hệ thống hạ tầng kỹ thuật mô phỏng diễn tập thực chiến, hệ thống giám sát SOC và các thiết bị CNTT phục vụ diễn tập.

- Phân loại cấp độ của hệ thống thông tin: Cấp độ 2 và 3.

2. Thông tin chi tiết về hệ thống được đưa vào diễn tập

- Hệ điều hành sử dụng: Linux, Windows.

- Các dịch vụ có trên hệ thống: DNS, DHCP, Web server.

- Các biện pháp an toàn thông tin đã triển khai: Antivirus, Firewall, hệ thống phát hiện xâm nhập; hệ thống giám sát, điều hành an toàn thông tin (SOC); nền tảng điều phối xử lý sự cố an toàn thông tin mạng.

- Tên miền của hệ thống: dientap.dienbien.gov.vn

- Mục đích chính sử dụng hệ thống: Diễn tập ứng cứu, xử lý sự cố mạng LAN của một cơ quan đơn vị bị tấn công điều hướng người dùng tải về các phần mềm gián điệp, độc hại. Rà soát và xử lý phần mềm gián điệp, độc hại trên máy tính người sử dụng.

3. Thành phần, nhân sự tham gia diễn tập

- **Ban Tổ chức:** Sở Thông tin và Truyền thông tỉnh Điện Biên.

- **Ban giám khảo gồm:** Lãnh đạo Sở Thông tin và Truyền thông, đại diện Cục An toàn thông tin, đại diện Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam - VNCERT, chuyên gia ATTT Công ty cổ phần BKAV.

- **Đội tấn công gồm:** Các Chuyên gia An toàn thông tin, Sở Thông tin và Truyền thông.

- **Đội phòng thủ gồm:** Đội ứng cứu sự cố an toàn thông tin mạng tỉnh Điện Biên; Cán bộ, công chức, viên chức, chuyên trách, phụ trách công nghệ thông tin các Sở, ban, ngành, UBND các huyện, thị xã, thành phố, Công an tỉnh, Bộ Chỉ huy Quân sự tỉnh, Bộ Chỉ huy Bộ đội biên phòng tỉnh, Tòa án Nhân dân tỉnh, Viện Kiểm soát Nhân dân tỉnh; các doanh nghiệp viễn thông.

4. Công cụ diễn tập

Mã độc được ban tổ chức thiết kế phục vụ diễn tập, mô phỏng lại các hành vi giống như các dòng mã độc trong thực tế, bao gồm các hành vi chính như sau:

- **Hành vi mạng:** Mã độc liên tục giữ kết nối với máy chủ điều khiển, mà không gửi bất cứ thông tin gì ra bên ngoài.

- **Hành vi gián điệp:** Mục tiêu của cảnh báo giả là cố gắng lôi kéo người dùng gửi cảnh báo càng nhiều càng tốt qua email.

- **Hành vi thay đổi registry hệ thống:** Nhằm mục đích kích hoạt lại mã độc khi máy tính được khởi động lại.

IV. Nội dung diễn tập

1. Tình huống mô phỏng

Đầu tháng 10/2023, Hacker phát hiện hệ thống mạng không dây (Wifi) của Sở A sử dụng mật khẩu yếu, dễ đoán và thực hiện kết nối vào hệ thống mạng LAN thông qua mạng Wifi đó.

Sử dụng các công cụ rò quét, phân tích, Hacker đánh giá: Hệ thống mạng LAN của sở A được thiết kế theo mô hình mạng ngang hàng, không phân quyền sử dụng, bất kỳ ai tham gia vào hệ thống mạng cũng có thể sử dụng dữ liệu được chia sẻ giữa các máy tính người dùng; thông tin quản trị của các thiết bị mạng sử dụng thiết lập mặc định của nhà sản xuất.

Hacker thực hiện các hành vi sau:

+ Nghe trộm, đánh cắp thông tin tài khoản và mật khẩu một người dùng sử dụng dịch vụ thư điện tử (email - do dịch vụ này sử dụng giao thức HTTP, không mã hóa thông tin trong quá trình truyền tải nội dung).

+ Thực hiện cuộc tấn công với hành vi giả mạo đối với người dùng trong Sở A: gửi email chứa mã độc đến toàn thể cán bộ, công chức, viên chức sở thông qua hệ thống thư điện tử. Khi người dùng tải xuống, mở tệp tin đính kèm bị cài cắm mã độc, Hacker kiểm soát hoàn toàn máy tính, đánh cắp và mã hóa dữ liệu quan trọng của người dùng.

2. Các bước ứng cứu, xử lý sự cố

2.1. Giai đoạn 1: Tiếp cận hiện trường, ghi nhận và xác nhận sự cố

Tiếp nhận thông tin từ Trung tâm giám sát, điều hành an toàn thông tin – SOC, Đội ứng cứu sự cố tiếp cận hiện trường, phân công nhiệm vụ cho các thành viên theo quy định.

Ngay sau khi tiếp nhận thông tin, Đội ứng cứu sự cố tiến hành thu thập thông tin, phân tích sơ bộ, đánh giá mức độ của sự cố.

- Mục đích:

+ Biết cách tiếp nhận thông tin sự cố; Nắm vững quy trình tiếp nhận thông tin ứng cứu và phân công nhiệm vụ.

+ Biết cách thu thập thông tin để xác thực sự cố và nhận định các hệ thống bị ảnh hưởng.

+ Phân loại sự cố tùy theo tài nguyên bị ảnh hưởng; Đánh giá sự cố nào có mức độ ảnh hưởng cao cần được ưu tiên xử lý.

- Thời gian thực hiện: 20 phút.

- Yêu cầu:

+ Chỉ ra hiện trạng;

+ Xác nhận sự cố, khoanh vùng phạm vi ảnh hưởng.

2.2. Giai đoạn 2. Thông báo

Đội ứng cứu sự cố sau khi phân tích xong và đánh giá đây là sự cố mất an toàn thông tin ở mức độ nghiêm trọng, cần phải thực hiện theo quy trình thông báo đã quy định.

- Mục đích: Biết cách báo cáo lãnh đạo quản lý hệ thống thông tin và đưa ra thông báo, cảnh báo đến các bên liên quan.

- Thời gian thực hiện: 10 phút.

2.3. Giai đoạn 3: Ngăn chặn tạm thời

Sau khi thông báo cho Lãnh đạo quản lý, Đội ứng cứu nhận được phản hồi từ Trung tâm điều phối, nhận định đây là một sự cố mất an toàn thông cần phải tập trung ngăn chặn phạm vi lây lan, khoanh vùng ảnh hưởng của cuộc tấn công để bảo vệ các tài nguyên khác, cũng như giảm thiểu mức độ tổn thất, thiệt hại dữ liệu người dùng ở mức thấp nhất.

- Mục đích: Đội ứng cứu cần phải đưa ra được phương án xử lý, ngăn chặn tạm thời.

- Thời gian thực hiện: 10 phút.

2.4. Giai đoạn 4: Thu thập bằng chứng và truy tìm thủ phạm

Đây là thời điểm quan trọng trong quy trình xử lý sự cố, đội ứng cứu phải thu thập bằng chứng liên quan đến sự cố từ các tài nguyên bị ảnh hưởng; từ đó sử dụng các công cụ, kỹ thuật khác nhau để phân tích.

- Mục đích:

+ Biết cách xác định được nguồn gốc tấn công; cách phân tích log, đánh giá tương quan sự kiện và thông tin lưu lượng mạng;

+ Bảo vệ hiện trường và đảm bảo an toàn bằng chứng trong quá lưu trữ và vận chuyển;

+ Tạo báo cáo điều tra, gửi cho các bên liên quan;

+ Tùy vào từng trường hợp có thể xem xét xử lý nội bộ hoặc đưa ra pháp luật.

- Thời gian thực hiện: 30 phút.

2.5. Giai đoạn 5: Xử lý nguyên nhân gây ra tấn công

Sau khi đã thu thập bằng chứng và phân tích, đội ứng cứu sẽ có được thông tin cụ thể về sự cố, từ đó loại bỏ được tận gốc vấn đề.

- Mục đích:

+ Biết cách tìm ra nguyên nhân của sự cố;

+ Cảnh báo cho đơn vị cung cấp và phát triển ứng dụng, dịch vụ của cơ quan, đơn vị bị ảnh hưởng;

+ Đưa ra phương án để giảm thiểu thiệt hại;

+ Kiểm tra các hệ thống tương tự có bị tấn công hay không;

+ Kiểm thử hệ thống trước khi bắt đầu quá trình khôi phục.

- Thời gian thực hiện: 20 phút.

2.6. Giai đoạn 6: Khôi phục hệ thống.

Sau khi loại bỏ được tận gốc vấn đề, đội ứng cứu phải xác định xem dữ liệu có bị thất thoát hay không, phục hồi lại dữ liệu từ bản Backup nếu dữ liệu bị mất. Khởi động lại hệ thống, ứng dụng và dịch vụ để duy trì hoạt động liên tục cho đơn vị.

- Mục đích:

+ Biết cách khôi phục lại các ứng dụng, dịch vụ bị ảnh hưởng và phục hồi lại dữ liệu;

+ Đảm bảo Backup không còn tồn tại mã độc;

+ Sau khi khôi phục tất cả dữ liệu bị mất, đội ứng cứu cần phải khởi động lại tất cả tiến trình, ứng dụng, dịch vụ đã bị gián đoạn; Thực hiện kiểm thử sau khi khôi phục.

- Thời gian thực hiện: 20 phút.

2.7. Giai đoạn 7: Hoạt động sau sự cố và gửi báo cáo

Để kết thúc một quy trình xử lý sự cố, Đội ứng cứu cần thực hiện các công việc cụ thể để cải thiện năng lực ứng cứu sự cố của đơn vị, chuẩn hóa quy trình, đưa ra các biện pháp phòng chống tấn công trong tương lai. Đồng thời, đội ứng cứu cần liên hệ, chia sẻ thông tin với các đơn vị hoạt động trong cùng lĩnh vực để cảnh báo kịp thời.

- Mục đích:

+ Phải tạo báo cáo rõ ràng, theo văn bản mẫu và có thể chỉnh sửa, chia sẻ thông tin đến đơn vị liên quan, lưu trữ để tham khảo;

+ Đánh giá thiệt hại sự cố gồm: Chi phí liên quan đến thất thoát thông tin bí mật, luật pháp, nhân công, thời gian gián đoạn dịch vụ, cài đặt;

+ Phân tích mục đích, động cơ của Hacker;

+ Sửa đổi quy trình, chính sách, quy định nếu cần;

+ Đào tạo nhận thức toàn đơn vị;

+ Đóng quá trình ứng cứu sự cố;

+ Công bố thông tin sự cố (nếu cần).

- Thời gian thực hiện: 20 phút./.