|  |  |
| --- | --- |
| UBND TỈNH ……………………**SỞ THÔN G TIN VÀ TRUYỀN THÔNG**  | **CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM****Độc lập - Tự do - Hạnh phúc** |
| Số: /BC-STTTT | *…… , ngày …… tháng …… năm 202…* |

**BÁO CÁO
Kết quả phòng thủ của Đội phòng thủ số …**

**trong diễn tập thực chiến bảo đảm an toàn thông tin mạng**

**I. THÔNG TIN VỀ TỔ CHỨC/CÁ NHÂN BÁO CÁO**

- Tên tổ chức/cá nhân báo cáo:

- Địa chỉ:

- Điện thoại: Email:

**II. NGƯỜI LIÊN HỆ**

- Họ và tên: Chức vụ:

- Điện thoại: Email:

**III. THỜI GIAN DIỄN TẬP**

|  |
| --- |
| Thời gian thực hiện diễn tập |
| Thời gian bắt đầu: … giờ ... phút, ngày …… tháng …… năm …… | Thời gian kết thúc: … giờ … phút, ngày …… tháng …… năm …… |

**IV. KẾT QUẢ PHÒNG THỦ**

*Kết quả phòng thủ cần được thể hiện rõ ràng, chi tiết gồm: chú thích, hình hảnh, bằng chứng, làm rõ được tình trạng an toàn thông tin của hệ thống sau đợt diễn tập thực chiến. Phân tích được các cuộc tấn công, ứng phó và ngăn chặn tấn công.*

**Thực hiện báo cáo tổng hợp cuối cùng**

Báo cáo tổng hợp cuối cùng là một báo cáo quan trọng, nó thể hiện thấy toàn bộ quá trình giám sát, phòng thủ, ngăn chặn và xử lý, ứng cứu, khôi phục của đội phòng thủ trong suốt thời gian diễn tập thực chiến diễn ra. Thể hiện được sự đối kháng, tấn công và phòng thủ qua lại giữa các đội redteam và đội blueteam.

Báo cáo tổng hợp cuối cùng cần đạt được các tiêu chí tương ứng với các tiêu chí chấm điểm đã được quy định trong nội quy của diễn tập và gửi về BTC theo đúng quy định.

**Các phần mục của báo cáo tổng hợp cuối cùng**

**Phần giới thiệu hệ thống mục tiêu diễn tập**

Giới thiệu tổng quan, ngắn gọn về hệ thống:

1. Mục đích của hệ thống
2. Các thành phần quan trọng của hệ thống cần bảo vệ
3. Dữ liệu quan trọng của hệ thống

Lưu ý: Ở diễn tập thực chiến, chúng tôi quy định các mục tiêu thực sự của hệ thống mục tiêu là:

* Tài nguyên của hệ thống: Bao gồm bản thân các máy chủ, năng lực tính toán, lưu trữ, mạng, tên miền,... của hệ thống mục tiêu
* Dữ liệu (thông tin): Bao gồm dữ liệu được sinh ra bởi hệ thống, dữ liệu được sử dụng bởi hệ thống (có thể là dữ liệu được query ở nơi khác và được hệ thống xử lý, hiển thị hoặc lưu trữ)
* Người dùng: Ảnh hưởng tới người dùng của hệ thống, như chiếm đoạt tài khoản người dùng hệ thống, tiết lộ tính riêng tư của thông tin người dùng, lừa đảo người dùng, người dân,...

**Phần quy trình, công nghệ, con người**

Phần này, đội phòng thủ sử dụng các thông tin đã chuẩn bị trước diễn tập về Con người, Công nghệ, Quy trình để làm rõ việc hệ thống được quan tâm, bảo vệ về an toàn thông tin.

**Phần nhận định chung**

Đội phòng thủ nhận định về hệ thống sau toàn bộ thời gian diễn ra diễn tập thực chiến. Cần khẳng định được hệ thống đã bị xâm nhập hay chưa, mất an toàn thông tin hay rò rỉ dữ liệu không, người dùng hệ thống, người dân sử dụng hệ thống có an toàn không.

Phần nhận định chung sẽ cho người đọc báo cáo (BGK) có cái nhìn tổng quan về tình hình an toàn thông tin của hệ thống, đánh giá được mức độ an toàn và đánh giá được hoạt động phòng thủ, bảo đảm an toàn thông tin của toàn bộ Hệ thống công nghệ, quy trình, con người.

**Phần chi tiết quá trình phòng thủ**

Đội phòng thủ diễn giải quá trình phòng thủ trong thời gian diễn tập diễn ra. Các diễn giải có thể được thực hiện theo dòng thời gian và mỗi dòng thời gian được phân cách với nhau bởi 01 ngày.

Đội phòng thủ báo cáo chi tiết cần chú ý đến 3 mục sau:

**Mỗi hành động của kẻ tấn công**

Đội phòng thủ cần phát hiện được mỗi hành động của kẻ tấn công trên hệ thống mục tiêu. Sau khi phát hiện, cần đưa ra được biện pháp phòng thủ, chống lại việc tấn công đó, cần đánh giá được hiệu quả của việc phòng thủ. Một số ý đội phòng thủ cần thể hiện:

* Hình thức/loại hình tấn công
* Payload mà đội Redteam đã sử dụng để tấn công
* Endpoint/Chức năng mà đội Redteam nhắm tới
* Phân tích payload và đưa ra mức độ ảnh hưởng của cuộc tấn công tới hệ thống mục tiêu
* Đánh giá thiệt hại, dữ liệu bị rò rỉ
* Thể hiện được việc cập nhật lại hệ thống giám sát, tự động ngăn chặn dựa trên payload

Tất cả các chi tiết cần có hình ảnh bằng chứng cụ thể chứng minh.

**Mỗi kẻ tấn công (threat actor)**

Đội phòng thủ cần theo dấu kẻ tấn công trên hệ thống hoặc các cuộc tấn công từ cùng 1 kẻ tấn công. Nhận định được thời gian kẻ tấn công bắt đầu tấn công, kết thúc tấn công và các hành động của kẻ tấn công đã thực hiện trên hệ thống. Nhận định được việc kẻ tấn công đã xâm nhập hay chưa xâm nhập thành công vào hệ thống, các mốc thời gian cụ thể và hình ảnh bằng chứng chứng minh.

Ví dụ: Kẻ tấn công có IP 1.2.3.4 đã thực hiện rà quét trên hệ thống, sau đó kẻ tấn công thực hiện đăng ký tài khoản và thực hiện upload một tệp mã độc (shell) lên hệ thống qua chức năng upload avatar. Tuy nhiên việc upload đã không bị hệ thống ngăn chặn dẫn tới việc kẻ tấn công đã xâm nhập được thành công hệ thống.

**Mỗi ngày**

Đội phòng thủ nhận định tình hình hệ thống sau mỗi ngày diễn ra diễn tập thực chiến. Các nhận định sẽ trả lời được các câu hỏi:

1. Tình hình an toàn thông tin của hệ thống sau mỗi ngày?
2. Các sự kiện an toàn thông tin đáng chú ý sau mỗi ngày?
3. Hành động của đội phòng thủ mỗi ngày?

**Phần tổng kết, rút kinh nghiệm**

Đội phòng thủ tự nhận định, rà soát lại các lỗ hổng về Con người, quy trình và có kế hoạch bổ sung, khắc phục lỗ hổng kịp thời. Đội phòng thủ thảo luận, rút kinh nghiệm về việc phối hợp phòng thủ, phát hiện, ngăn chặn, ứng cứu và khôi phục hệ thống. Đội phòng thủ đề xuất các biện pháp tiếp theo, sắp tới để nâng cấp, bảo đảm an toàn thông tin cho hệ thống. Cuối cùng là đề xuất với BTC về phản hồi về Diễn tập thực chiến để cải thiện và hoàn thiện quy trình phối hợp giữa redteam, blueteam, BTC, BGK và Nội quy, quy định của diễn tập thực chiến.

**1. Giới thiệu về mục tiêu diễn tập**

**2. Nhận định chung về tình trạng an toàn thông tin của hệ thống**

**3. Báo cáo về quy trình, công nghệ, con người**

**4. Báo cáo chi tiết quá trình phòng thủ**

**4.1. Báo cáo về năng lực phát hiện, phân tích tấn công**

**4.2. Báo cáo về khả năng ngăn chặn, ứng cứu sự cố tấn công mạng**

**4.3. Báo cáo về diễn biến phòng thủ mỗi cuộc tấn công**

**4.4. Báo cáo về diễn biến phòng thủ mỗi ngày**

**4.5. Báo cáo về diễn biến phòng thủ mỗi kẻ tấn công (threat actor)**

**5. Tổng kết, rút kinh nghiệm**

**KIẾN NGHỊ, ĐỀ XUẤT**

|  |
| --- |
| Mô tả về đề xuất, kiến nghị |
| *Đề nghị cung cấp tóm lược về các kiến nghị và đề xuất hỗ trợ trong tổ chức thực hiện phòng thủ; cách thức phối hợp tổ chức, điều phối của BTC; kiến nghị giúp cải thiện chất lượng phòng thủ, cải thiện diễn tập thực chiến trong tương lai.* |

**THỜI GIAN THỰC HIỆN BÁO**: …/…/… (ngày/tháng/năm).

|  |  |
| --- | --- |
| ***Nơi nhận:***- Ban tổ chức (b/c);- Lưu: VT,...  | **ĐẠI DIỆN ĐỘI PHÒNG THỦ***(Ký tên, đóng dấu)* |