CÔNG TY TNHH AN NINH AN TOÀN THÔNG TIN CMC

CMC CYBER SECURITY CO. LTD.

Tầng 15 tòa nhà CMC, phố Duy Tân, Dịch Vọng Hậu, Cầu Giấy, Hà Nội | Tel: 84.4.3795 8282 | Fax: 84.4.3984 5053 | www.cmccybersecurity.com

15th Floor, CMC Tower, Duy Tan Street, Dich Vong Hau, Cau Giay, Hanoi | Tel: 84.4.3795 8282 | Fax: 84.4.3984 5053 | www.cmccybersecurity.com

DỊCH VỤ XỬ LÝ SỰ CỐ AN NINH AN TOÀN THÔNG TIN

BY CMC SOC

Thành viên chính thức của AVAR và ICSA

CMC CYBER SECURITY CO., LTD.

Version	2.0
Date	
Document Type	Service Description

1. Mô tả dịch vụ

Dịch vụ xử lý sự cố là hoạt động nhằm xử lý, khắc phục sự cố gây mất an ninh an toàn thông tin, bao gồm: theo dõi, thu thập, phân tích, phát hiện, cảnh báo, điều tra, xác minh sự cố, ngăn chặn sự cố, và khôi phục hoạt động bình thường của hệ thống thông tin.

Sự cố an ninh an toàn thông tin là việc thông tin, hệ thống thông tin bị tấn công hoặc gây nguy hại, ảnh hưởng tới tính nguyên vẹn, tính bảo mật hoặc tính khả dụng.

Một số nhóm sự cố AN ATTT như sau (theo tiêu chuẩn quốc gia TCVN 11239:2015 ISO/IEC 27035:2011):

- ***Truy cập trái phép:*** bao gồm các hành động cố gắng để truy cập hoặc lợi dụng trái phép hệ thống, dịch vụ hoặc mạng để truy cập. Dưới đây là một số ví dụ về sự cố truy cập trái phép:
  - Các cố gắng lấy các dữ liệu nhạy cảm,
  - Các tấn công làm tràn bộ đệm để cố dành quyền
  - Sự khai thác các điểm yếu của giao thức để chiếm quyền hoặc làm sai hướng các kết nối hợp lệ,
  - Các cố gắng nâng cao đặc quyền hoặc thông tin vượt quá quyền của người dùng hoặc quản trị viên

- ***Tấn công từ chối dịch vụ:*** là sự cố làm cho hệ thống, dịch vụ hoặc mạng không thể tiếp tục hoạt động với năng lực dự kiến, dẫn đến từ chối hoàn toàn các truy cập hợp lệ của người dùng. Dưới đây là một số ví dụ điển hình về các sự cố DoS/DDoS:
  - Ping các địa chỉ mạng quảng bá nhằm làm tràn băng thông mạng,
  - Gửi dữ liệu theo các định dạng không mong muốn đến một hệ thống, dịch vụ, hoặc mạng nhằm đánh sập hoặc làm gián đoạn hoạt động,
  - Mở nhiều phiên hợp lệ với một hệ thống, dịch vụ hoặc mạng nhất định

  Các cuộc tấn công như vậy thường được thực hiện thông qua các Botnet, đây là tập hợp của các robot phần mềm (mã độc) chạy độc lập, tự động. Các Botnet có thể bao gồm hàng trăm đến hàng triệu máy tính. Trong phạm vi xử lý sự cố an ninh an toàn thông tin, CMC Cyber Security sẽ không cung cấp việc xử lý liên quan đến loại tấn công từ chối dịch vụ này.

- ***Mã độc, phần mềm độc hại:*** Mã độc là một chương trình hoặc một phần của chương trình được đưa vào một chương trình khác với mục đích làm thay đổi tính năng ban đầu của chương trình đó nhằm thực hiện các hoạt động nguy hiểm như trộm cắp thông tin, phá hủy thông tin, từ chối dịch vụ, phát tán thư rác....

- ***Khai thác và thu thập thông tin trái phép (Hacking):*** bao gồm các hoạt động liên quan đến việc xác định các mục tiêu và tìm các dịch vụ hoạt động trên các mục tiêu đó. Đây là loại sự cố liên quan đến do thám, mục đích để xác định:

- Sự tồn tại của một mục tiêu, các cấu trúc mạng quanh mục tiêu, và đối tượng mà mục tiêu thường xuyên liên lạc,
- Các điểm yếu tiềm ẩn có thể khai thác được của mục tiêu hoặc quanh môi trường mạng của mục tiêu

Dưới đây là các ví dụ về tấn công thu thập thông tin:

- Việc ping tới các địa chỉ mạng để tìm những những hệ thống còn "sống",
- Việc thăm dò hệ thống nhằm xác định hệ điều hành,máy chủ…,
- Việc quét các cổng mạng trên hệ thống nhằm xác định các dịch vụ liên quan và xác định phiên bản phần mềm của các dịch vụ này,

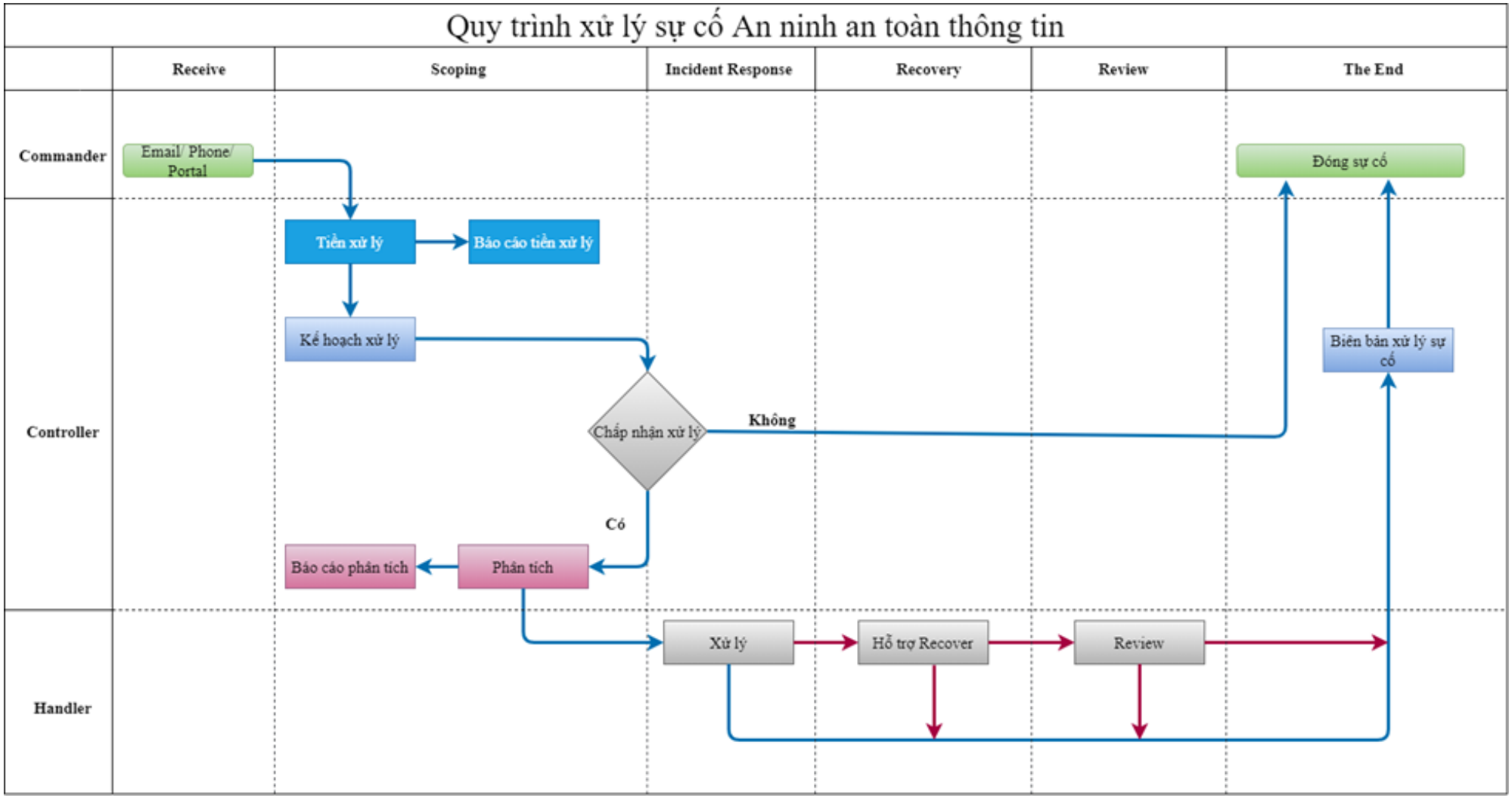
– ***Rò rỉ dữ liệu:*** Sự cố loại này xảy ra khi người dùng vi phạm các chính sách an toàn hệ thống thông tin của một tổ chức, dẫn đến các thông tin nội bộ bị lộ lọt ra bên ngoài.

Bằng kinh nghiệm và nhân lực của CMC Cyber Security, khách hàng sẽ rút ngắn tối đa thời gian bị ảnh hưởng do các sự cố AN ATTT gây ra. Khách hàng sẽ nhanh chóng xác định được nguyên nhân mức độ ảnh hưởng của sự cố.

2. Service Level Agreement

Service Level Agreement sẽ được cung cấp tuỳ theo từng khách hàng và dự án

3. Quy trình


Quy trình xử lý sự cố An ninh an toàn thông tin
Receive
Scoping
Incident Response
Recovery
Review
The End
Commander
Controller
Handler
Email/ Phone/ Portal
Tiền xử lý
Báo cáo tiền xử lý
Kế hoạch xử lý
Chấp nhận xử lý
Không
Có
Báo cáo phân tích
Phân tích
Xử lý
Hỗ trợ Recover
Review
Đóng sự cố
Biên bản xử lý sự cố

- **Định nghĩa các pha công việc:**
  - ***Receive**:* Ở pha này, CMC SOC sẽ tiếp nhận các yêu cầu về xử lý sự cố an ninh an toàn thông tin qua email, điện thoại hoặc thông tin trên SOC Portal.
  - ***Scoping:*** Sau khi tiếp nhận yêu cầu từ khách hàng qua email/điện thoại, tại pha scoping bộ phận/nhóm Commander có trách nhiệm tiếp nhận các yêu cầu từ khách hàng dựa theo các kịch bản và khả năng chuyên môn, Commander sẽ thực hiện phân tích tiền xử lý trên những thông tin khách hàng cung cấp. Sau khi thực hiện tiền xử lý xong, bộ phận commander sẽ có trách nhiệm viết báo cáo tiền xử lý và chuyển cho Controller. Từ báo cáo tiền xử lý, bộ phận/nhóm Controller có trách nhiệm phân tích chuyên sâu vấn đề khách hàng gặp phải. Trong trường hợp các thông tin chưa đầy đủ, Controller có thể sẽ yêu cầu Commander trao đổi thêm với khách hàng xác minh thêm thông tin. Sau khi thông tin đầy đủ, Controller sẽ phân tích, đưa ra kế hoạch xử lý để gửi tới khách hàng. Ở giai đoạn này, Controller sẽ trực tiếp trao đổi với khách hàng về kế hoạch xử lý.
    - Trong trường hợp khách hàng không đồng ý với kế hoạch xử lý, quy trình xử lý sẽ được đóng và sẽ gửi lại báo cáo phân tích sự cố.
    - Trong trường hợp khách hàng đồng ý với kế hoạch xử lý, thì nhóm Handler sẽ tiếp tục thực hiện xử lý theo kế hoạch bao gồm việc phân tích chuyên sâu về sự cố và sau khi hoàn thành công việc sẽ thực hiện gửi báo cáo xử lý sự cố.
  - ***Incident Response:***
    - Bộ phận Handler thực hiện công việc theo kế hoạch xử lý mà bộ phận Controller đã thống nhất với khách hàng.
    - Trong quá trình xử lý, mọi vấn đề phát sinh nhóm Handler có trách nhiệm ghi nhận và báo cáo cho Controller trước khi có hành động phản ứng tiếp theo. Kết thúc quá trình xử lý, nhóm Handler sẽ có trách nhiệm viết biên bản xử lý và gửi lại khách hàng.
  - ***Recovery:*** Ở pha này, ngoài việc xử lý sự cố, nhóm Handler sẽ hỗ trợ khách hàng trong việc khôi phục hoạt động bình thường của hệ thống. Khách hàng sẽ trực tiếp khôi phục hệ thống, nhóm Handler chỉ đóng vai trò hỗ trợ và đưa khuyến nghị.
  - ***Review:*** sau khi hệ thống đã xử lý sự cố và khôi phục hoạt động bình thường, nhóm Handler sẽ có trách nhiệm kiểm tra, xác nhận lại toàn bộ các công việc trong Kế hoạch xử lý trước khi bàn giao lại cho khách hàng. Trong pha này, CMC Cyber Security sẽ đưa ra các khuyến nghị/hành động nhằm tối ưu hệ thống (nếu có). Sau quá trình xử lý, khách hàng sẽ nhận được biên bản kết quả xử lý tương ứng với gói dịch vụ lựa chọn.

- **Mô tả vai trò các bộ phận:**
  - ***Commander:*** là bộ phận/nhóm tiếp nhận các thông tin sự cố từ phía khách hàng. Nhóm có trách nhiệm tiếp nhận thông tin, tiền xử lý các thông tin sự cố. Trong trường hợp các thông tin không đầy đủ để giải quyết sự cố hoặc cần hỗ trợ thêm để xử lý, nhóm này có trách nhiệm chuyển toàn bộ các thông tin tiếp nhận cho bộ phận xử lý cấp trên (controller)
  - ***Controller:*** là bộ phận/nhóm phân tích, định hướng và điều phối xử lý. Nhóm này có trách nhiệm phân tích chi tiết các thông tin sự cố tiếp nhận, xác định phương hướng xử lý và chịu trách nhiệm điều phối cho toàn bộ quá trình xử lý sự cố. Để việc xử lý hiệu quả, nhóm này có thể yêu cầu khách hàng bổ sung hoặc phối hợp bổ sung thông tin chi tiết về sự cố trong quá trình tiếp nhận và phân tích.
  - ***Handler:*** là bộ phân/nhóm trực tiếp phân tích và xử lý các sự cố. Thành viên nhóm này có thể bao gồm cả nhân viên kỹ thuật của CMC InfoSec và đội ngũ kỹ thuật của khách hàng. Nhóm này sẽ xử lý sự cố theo hướng dẫn và điều phối xử lý của Controller. Trong quá trình xử lý, mọi vấn đề phát sinh nhóm có trách nhiệm ghi nhận và báo cáo cho Controller trước khi có hành động phản ứng tiếp theo.

4. Phạm vi cung cấp dịch vụ

Dịch vụ này được cung cấp trên phạm vi:

- Các máy chủ:
  - Máy chủ ứng dụng
  - Máy chủ cơ sở dữ liệu
  - Máy chủ web server
  - Máy chủ chia sẻ file
  - Máy chủ Proxy
  - Máy chủ DNS
  - Máy chủ AD
  - Máy chủ email
  - Máy chủ vật lý
- Máy trạm:
  - Máy trạm Windows (tất cả các phiên bản win 7 trở lên)
  - Máy trạm Linux, Unix, Solaris, AIX
  - Máy trạm MAC (tất cả các phiên bản)
- Thiết bị mạng: Switch, Router, Firewall

Dịch vụ này không bao gồm việc khôi phục dữ liệu.