CHƯƠNG 3: CHIẾN LƯỢC ỨNG PHÓ SỰ CỐ AN TOÀN

Môn học: Giám sát & ứng phó sự cố ATM

Mục tiêu module

- Hiểu được khái niệm ứng dụng web
- Hiểu các mối đe dọa từ ứng dụng web
- Hiểu phương pháp lấy cắp dữ liệu ứng dụng web
- Tổng quan về các công cụ hack ứng dụng web
- Hiểu các biện pháp ứng phó với các cuộc tấn công ứng dụng web
- Tổng quan về các công cụ kiểm tra bảo mật ứng dụng web
- Tổng quan về kiểm thử thâm nhập ứng dụng web

1. Các sự kiện và sự cố an toàn thông tin
2. Tính cần thiết của ứng phó sự cố
3. Chính sách, kế hoạch, thủ tục ứng phó sự cố
4. Tổ chức của nhóm chuyên gia ứng phó sự cố

1. Các sự kiện và sự cố an toàn thông tin
2. Tính cần thiết của ứng phó sự cố
3. Chính sách, kế hoạch, thủ tục ứng phó sự cố
4. Tổ chức của nhóm chuyên gia ứng phó sự cố

Các sự kiện và sự cố an toàn thông tin

- **Sự kiện an toàn thông tin** (information security event): Sự kiện xác định của một hệ thống, dịch vụ hoặc trạng thái mạng cho thấy có khả năng vi phạm chính sách an toàn thông tin hay sự thất bại của các biện pháp kiểm soát hoặc một tình huống chưa biết có thể liên quan đến an toàn thông tin. [TCVN 11238:2015].
- **Sự cố an toàn thông tin** (information security incident): Một hoặc một loạt các sự kiện an toàn thông tin không mong muốn hoặc không dự tính có khả năng ảnh hưởng đáng kể các đến hoạt động nghiệp vụ và đe dọa an toàn thông tin. [TCVN 11238:2015].

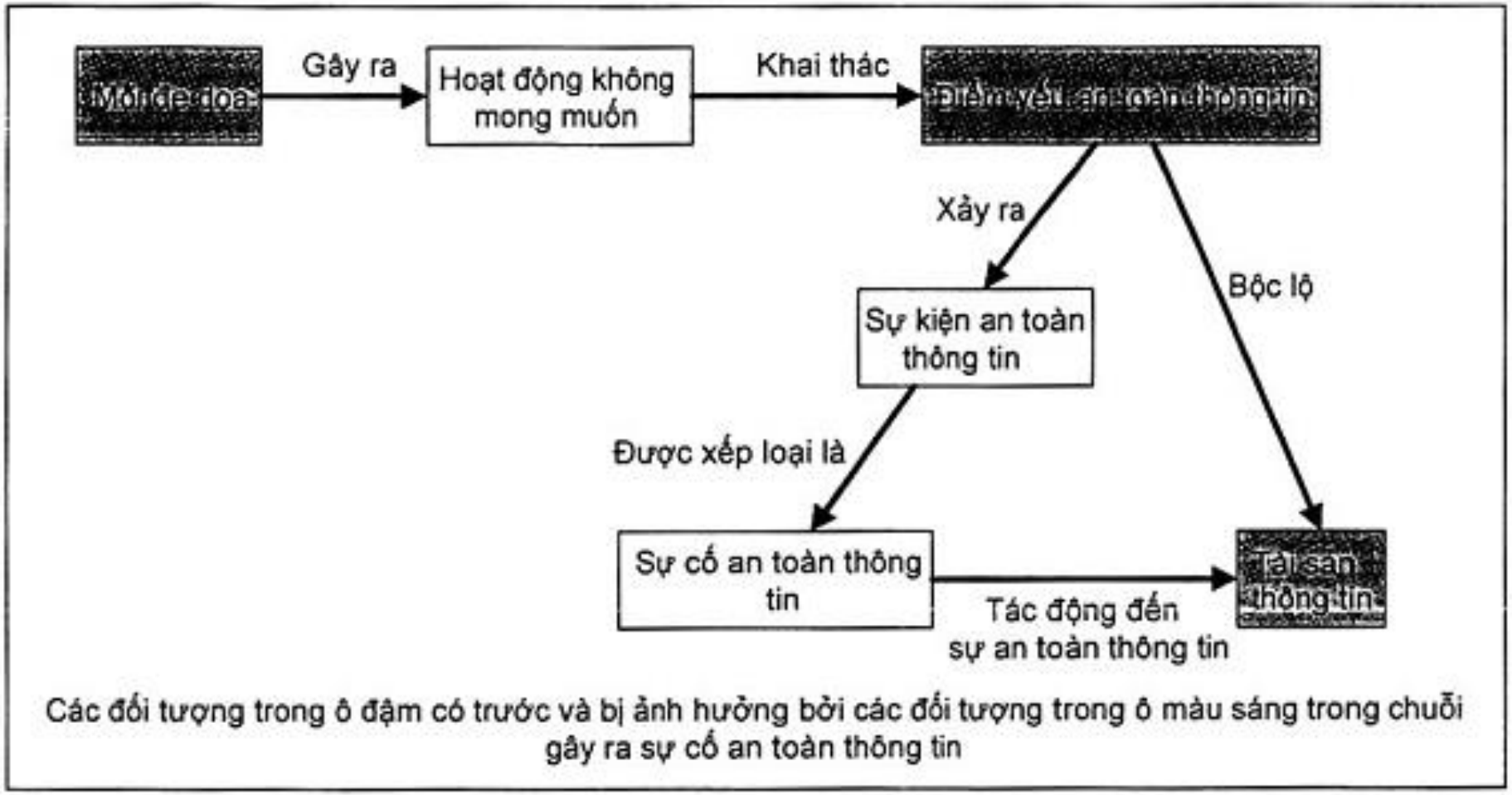
Các sự kiện và sự cố an toàn thông tin

- Việc xảy ra một sự kiện an toàn thông tin không phải lúc nào cũng có nghĩa là một cố gắng đã thành công hoặc có hệ quả nào đó đến tính bí mật, tính vẹn toàn và/hoặc tính sẵn sàng, tức là không phải mọi sự kiện an toàn thông tin đều được xếp loại là sự cố an toàn thông tin.

- Mối đe dọa khai thác các điểm yếu (nhược điểm) của các hệ thống, dịch vụ và mạng thông tin theo các cách không mong muốn, đó chính là sự xảy ra các sự kiện an toàn thông tin và tiềm ẩn gây ra các sự cố không mong muốn đối với các tài sản thông tin có điểm yếu.

Các sự kiện và sự cố an toàn thông tin

- Mối quan hệ giữa các đối tượng trong chuỗi gây ra sự cố an toàn thông tin.



Các đối tượng trong ô đậm có trước và bị ảnh hưởng bởi các đối tượng trong ô màu sáng trong chuỗi gây ra sự cố an toàn thông tin

Sự cố

Có 3 loại sự cố:

- Low level
- Middle level
- High level

Sự cố mức độ thấp

Sự cố mức độ thấp là loại sự cố ít nghiêm trọng nhất

Chúng phải được xử lý trong vòng một ngày sau khi sự kiện xảy ra

Sự cố mức độ thấp bao gồm:

- Mất mật khẩu cá nhân
- Quét và thăm dò không thành công
- Yêu cầu xem lại nhật ký bảo mật
- Tồn tại sự hiện diện của bất kỳ virus hoặc worms
- Không thể tải xuống chữ ký chống vi-rút
- Nghi ngờ hoạt động chia sẻ tài khoản của tổ chức
- Chính sách vi phạm nhỏ được tổ chức chấp nhận sử dụng

Sự cố mức độ trung bình

Các sự cố ở mức độ này tương đối nghiêm trọng hơn

Sự cố mức độ trung bình bao gồm:

- Truy cập trái phép từ ngoài/trong tới hệ thống
- Vi phạm quyền truy cập đặc biệt vào máy tính hoặc thiết bị máy tính
- Lưu trữ và xử lý dữ liệu trái phép
- Gây hủy hoại tài sản Sự bùng phát worm/ virus cục bộ
- Đánh cắp dữ liệu cá nhân
- Virus hoặc worms máy tính có mức độ ảnh hưởng tương đối lớn
- Truy cập bất hợp pháp
- Chính sách vi phạm được tổ chức chấp nhận sử dụng

Sự cố mức độ cao

Các sự cố ở mức độ cao cần được xử lý ngay sau khi xảy ra sự cố

Nó gây ra mối đe dọa ngay lập tức cho các hệ thống khác nhau dẫn đến các đe cáo buộc hình sự, tiền phạt theo quy định hoặc ảnh hưởng xấu cho tổ chức

Bao gồm các:

- Tấn công từ chối dịch vụ
- Nghi ngờ đột nhập máy tính
- Virus hoặc worms máy tính có mức độ hoạt động cao nhất; ví dụ.

  Trojan, back door
- Các thay đổi đối với phần cứng, chương trình cơ sở hoặc phần mềm hệ thống mà không cần xác thực
- Phá hủy tài sản vượt quá 100.000 đô la
- Trộm cắp cá nhân vượt quá 100.000 đô la và chuyển tiền điện tử bất hợp pháp
- Bất kỳ loại nội dung khiêu dâm, cờ bạc hoặc vi phạm bất kỳ luật nào

Ví dụ về sự cố bảo mật máy tính

Hacker breaches state network

DENNIS THOMPSON Statesman Journal
April 11, 2009

State computer security experts are investigating a hacker intrusion into a computer network operated by the Oregon Department of Human Services, officials said Friday

The security breach was detected about 3 p.m. Wednesday, said Lonn Hoklin, spokesman for the Oregon Department of Administrative Services.

Experts moved quickly to shut it down.

Web Sites Disrupted By Attack on Register.com

Web site host and domain name registrar **Register.com** has been the target of a sustained attack this week, disrupting service for thousands of customers.

The attacks began on Wednesday, causing a three-hour outage for many Web sites that rely on the company for hosting and/or use the company's domain name system (DNS) servers, said **Roni Jacobson**, executive vice president at Register.com.

The outage was the result of what's known as a distributed denial of service (DDoS) attack, in which attackers cause hundreds or thousands of compromised PCs to flood a target with so much junk traffic that the Web site can no longer accommodate legitimate visitors. Typically, DDoS attacks are waged as a way for criminals to extort money from the targets, who are told the attack will cease when a ransom demand is paid.

SECURITY darkREADING
Protect The Business Enable Access

Attack Of The Mini-Botnets

All eyes may be on the big spamming botnets, but it's the small, silent ones that are most dangerous

By Kelly Jackson Higgins, DarkReading
March 31, 2009
URL:http://www.darkreading.com/story/showArticle.jhtml?articleID=216402026

Big-name botnets like Kraken/Bobax, Srizbi, Rustock, the former Storm -- and even the possible botnet-in-waiting, Conficker -- have gained plenty of notoriety, but it's the smaller and less conspicuous ones you can't see that are doing the most damage in the enterprise.

Salt Lake Tribune
Updated:04/10/2009 05:54:34 PM MDT

The Salt Lake Tribune http://www.sltrib.com

A computer virus is causing headaches and heartburn at the University of Utah.
The Conficker virus, which can slow computers and steal personal information, hit the U.'s network late this week. So far, the virus has mainly affected health sciences, including the university's three hospitals, medical school, College of Nursing, College of Pharmacy and College of Health, said Chris Nelson, spokesman for health sciences at the U.

Dấu hiệu của sự cố

Phát hiện và đánh giá chính xác các sự cố là phần quan trọng và khó khăn nhất của quá trình ứng phó sự cố

Các dấu hiệu điển hình về bảo mật sự cố bao gồm:

- Một hệ thống cảnh báo hoặc chỉ báo tương tự từ một phát hiện xâm nhập
- Cố gắng đăng nhập vào tài khoản người dùng mới
- Tấn công DoS hoặc người dùng không thể đăng nhập vào tài khoản
- Hệ thống bị treo hoặc hiệu suất hệ thống kém
- Hoạt động trái phép của một chương trình hoặc thiết bị thám thính để
- nắm bắt lưu lượng mạng
- Các mục nhập đáng ngờ trong hệ thống hoặc kế toán mạng hoặc
- các mâu thuẫn kế toán khác

Dấu hiệu của sự cố (tiếp)

Các dấu hiệu của sự cố thuộc một trong hai loại sau:

- Điềm báo là dấu hiệu của sự cố có thể xảy ra trong tương lai
- Chỉ định là dấu hiệu của sự cố đã xảy ra hoặc có thể đang diễn ra

Các ví dụ về điềm báo là:

- Các mục nhật ký máy chủ web hiển thị việc sử dụng trình quét lỗ hổng bảo mật web
- Thông báo về cách khai thác mới nhắm vào lỗ hổng trên máy chủ thư của tổ chức
- Một mối đe dọa từ một nhóm hacktivist nói rằng nhóm sẽ tấn công tổ chức

Các ví dụ về chỉ định là:

- Phần mềm chống vi-rút cảnh báo khi phát hiện máy chủ bị nhiễm worm
- Người dùng gọi cho bộ phận trợ giúp để báo cáo một email đe dọa
- Nhật ký hệ thống IDS và IPS chỉ ra độ lệch bất thường so với các luồng lưu lượng mạng điển hình

1. Các sự kiện và sự cố an toàn thông tin
2. Tính cần thiết của ứng phó sự cố
3. Chính sách, kế hoạch, thủ tục ứng phó sự cố
4. Tổ chức của nhóm chuyên gia ứng phó sự cố

Ứng phó sự cố

Ứng phó sự cố là một quá trình ứng phó với các sự cố có thể đã xảy ra do vi phạm bảo mật trong hệ thống hoặc mạng

Mục tiêu của ứng phó sự cố là xử lý các sự cố theo cách giảm thiểu thiệt hại, giảm thời gian và chi phí khắc phục

Nó đóng một vai trò quan trọng khi bảo mật của hệ thống bị xâm phạm

Nó bao gồm:

- Ứng phó với các sự cố một cách có hệ thống để các bước thích hợp được thực hiện
- Giúp nhân viên phục hồi nhanh chóng và hiệu quả sau các sự cố an ninh, giảm thiểu mất mát hoặc đánh cắp thông tin và gián đoạn dịch vụ
- Sử dụng thông tin thu thập được trong quá trình xử lý sự cố để chuẩn bị cho việc xử lý các sự cố trong tương lai theo cách tốt hơn và cung cấp khả năng bảo vệ mạnh mẽ hơn cho hệ thống và dữ liệu
- Xử lý đúng các vấn đề pháp lý có thể phát sinh khi xảy ra sự cố

Xử lý sự cố

Xử lý sự cố bao gồm tất cả các quy trình, hậu cần, thông tin liên lạc, điều phối và lập kế hoạch để ứng phó và khắc phục sự cố một cách hiệu quả

Xử lý sự cố giúp tìm ra xu hướng và mô hình hoạt động của kẻ xâm nhập

Các quy trình xử lý sự cố giúp quản trị viên mạng khôi phục, ngăn chặn và phòng ngừa sự cố

Các chính sách xử lý sự cố giúp các nhân viên tương tác hiểu được quy trình ứng phó và giải quyết các mối đe dọa không mong đợi và vi phạm bảo mật

Tính cần thiết của ứng phó sự cố

- Là một phần chính trong chiến lược an toàn thông tin tổng thể.
- Ứng phó sự cố giúp giảm thiểu mất mát hoặc đánh cắp thông tin và gián đoạn dịch vụ do sự cố gây ra.
- Hỗ trợ ứng phó với các sự cố một cách có hệ thống (tuân theo một phương pháp xử lý sự cố nhất quán) để thực hiện các hành động thích hợp.
- Sử dụng thông tin thu được trong quá trình xử lý sự cố để chuẩn bị tốt hơn cho việc xử lý các sự cố trong tương lai và tăng cường khả năng bảo vệ cho hệ thống và dữ liệu

Tính cần thiết của ứng phó sự cố

- Mục đích của ứng phó sự cố là hỗ trợ nhân viên khắc phục nhanh chóng và hiệu quả sau sự cố.
- Phản ứng sự cố được yêu cầu để xác định các cuộc tấn công đã xâm phạm thông tin hoặc dữ liệu cá nhân và doanh nghiệp.
- Phản ứng sự cố được yêu cầu nhằm mục đích
  - Bảo vệ hệ thống
  - Bảo vệ nhân viên
  - Sử dụng hiệu quả các nguồn lực
  - Giải quyết các vấn đề pháp lý

Mục tiêu của ứng phó sự cố

- Kiểm tra sự cố
- Giảm thiểu tác động của sự cố lên các cá nhân, tổ chức
- Ngăn chặn các cuộc tấn công, sự cố trong tương lai
- Tăng cường bảo mật hệ thống máy tính
- Đảm bảo các quyền riêng tư được thiết lập bởi luật pháp và chính sách
- Cung cấp các báo cáo chính xác và các khuyến nghị hữu ích
- Hỗ trợ cơ quan thực thi pháp luật trong việc truy tố tội phạm kỹ thuật số
- Bảo vệ danh tiếng và tài sản của tổ chức

1. Các sự kiện và sự cố an toàn thông tin
2. Tính cần thiết của ứng phó sự cố
3. Chính sách, kế hoạch, thủ tục ứng phó sự cố
4. Tổ chức của nhóm chuyên gia ứng phó sự cố

Chính sách ứng phó sự cố

- Mỗi tổ chức có chính sách ứng phó sự cố khác nhau.
- Một chính sách ứng phó sự cố thường bao gồm:
  - Mục đích và mục tiêu của chính sách,
  - Phạm vi của chính sách (áp dụng cho ai, những gì và trong những trường hợp nào),
  - Cơ cấu tổ chức và định nghĩa về vai trò, trách nhiệm và cấp độ quyền hạn; thẩm quyền của nhóm ứng phó sự cố,
  - Định nghĩa các sự cố bảo mật máy tính và các thuật ngữ liên quan,
  - Xếp hạng mức độ ưu tiên hoặc mức độ nghiêm trọng của các sự cố,
  - Các bước thực hiện ứng phó sự cố,
  - Các biểu mẫu báo cáo và liên hệ.

Kế hoạch ứng phó sự cố

- Là lộ trình thực hiện các biện pháp ứng phó sự cố.
- Một kế hoạch ứng phó sự cố thường bao gồm:
  - Chiến lược và mục tiêu,
  - Cách tiếp cận để ứng phó sự cố,
  - Cách thức liên lạc giữa nhóm ứng phó sự cố với tổ chức và với các tổ chức khác,
  - Lộ trình hoàn thiện khả năng ứng phó sự cố,
  - Phê duyệt của lãnh đạo.

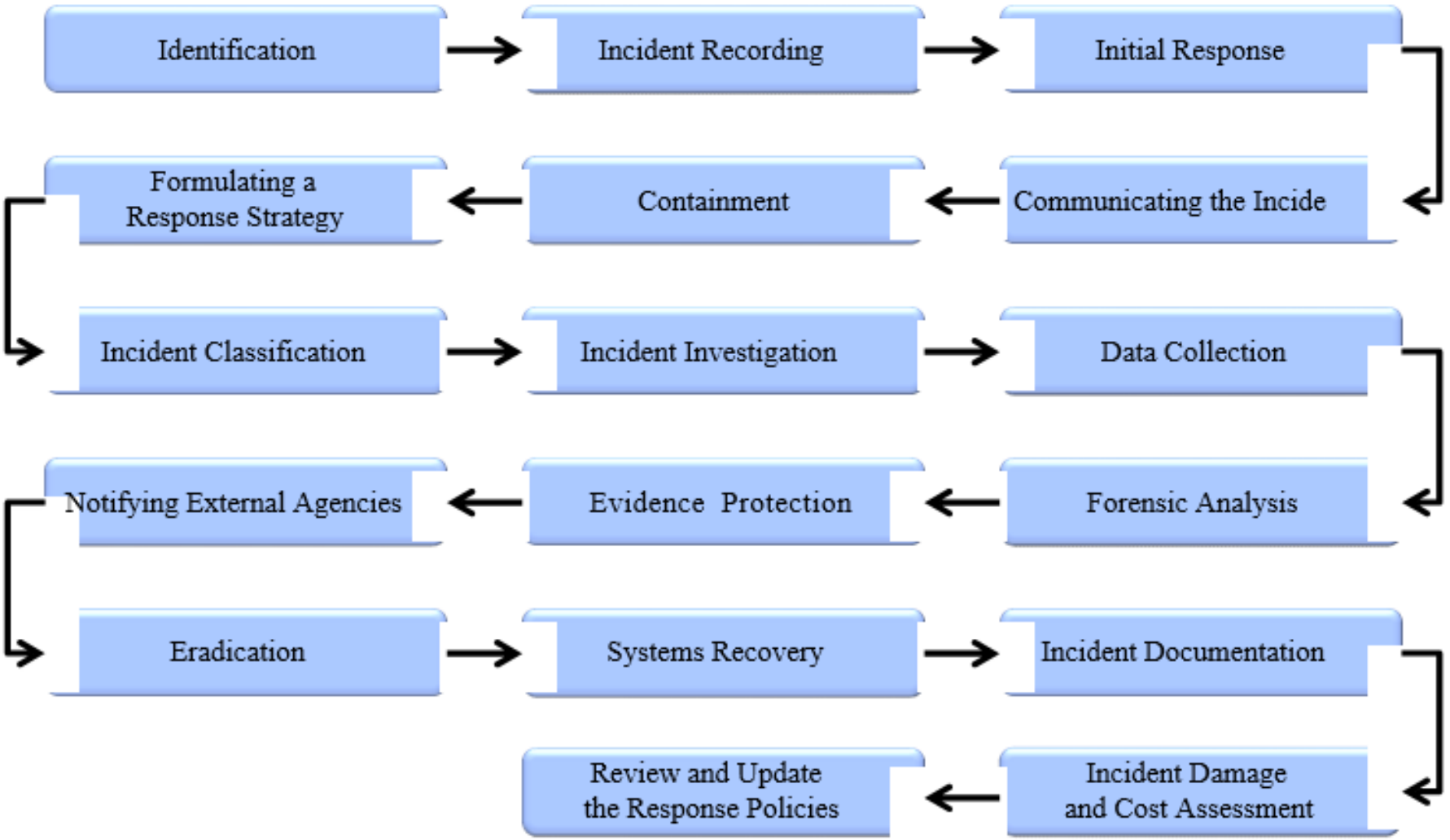
Kế hoạch ứng phó sự cố

- Mỗi tổ chức cần có một kế hoạch đáp ứng các yêu cầu riêng biệt, liên quan đến sứ mệnh, quy mô, cấu trúc và chức năng của tổ chức.
- Cần xem xét lại kế hoạch ít nhất hàng năm để đảm bảo tổ chức đang tuân theo lộ trình hoàn thiện năng lực và hoàn thành các mục tiêu về ứng phó sự cố.

Thủ tục ứng phó sự cố

- Các thủ tục ứng phó sự cố phải dựa trên chính sách và kế hoạch ứng phó sự cố.
- Quy trình vận hành tiêu chuẩn (SOP): bản mô tả các quy trình kỹ thuật, kỹ thuật, danh sách kiểm tra và biểu mẫu cụ thể được sử dụng bởi nhóm ứng phó sự cố.

Các bước xử lý và ứng phó sự cố



Bước 1: Nhận dạng

Giai đoạn xác định bao gồm xác nhận, xác định và báo cáo sự cố

Giai đoạn này là cần thiết để phân loại và ứng phó với các sự cố

Xác định các sự cố với sự trợ giúp của các phần mềm như phần mềm chống vi-rút và trong các công cụ phát hiện thích hợp nhất

Nhật ký kiểm tra hệ thống và mạng cũng có thể cung cấp đầy đủ thông tin để quyết định xem hoạt động trái phép có xảy ra hay không

Bước 1: Nhận dạng

Các hành động được thực hiện trong giai đoạn xác định bao gồm:

- Thu thập, kiểm tra và phân tích nhật ký kiểm toán
- Báo cáo và đánh giá sự cố
- Thu thập và bảo vệ thông tin hệ thống
- Xác định danh tính sự kiện và mức độ nghiêm trọng
- Phân tích hệ thống khác
- Chỉ định các thành viên lực lượng đặc nhiệm sự cố

Bước 2: Ghi lại sự cố

Ghi sự cố là một quá trình lưu trữ chính xác các thông tin chi tiết về sự cố xảy ra

Thông tin thu thập nên bao gồm:

- Ngày và giờ sự việc xảy ra
- Ngày và giờ mà sự cố được bắt đầu
- Ai đã báo cáo sự việc
- Thông tin chi tiết về vụ việc gồm:
    - Mô tả sự cố
    - Hệ thống liên quan
    - Sao lưu thông tin như thông báo lỗi, nhật ký bay, v.v.

Bước 3: Phản hồi ban đầu

Bước đầu tiên trong quá trình điều tra là thu thập đầy đủ thông tin cần thiết để xác định cách ứng phó sự cố thích hợp

Bao gồm:

- Điều tra ban đầu
- Thông tin chi tiết về vụ việc
- Tạo nhóm ứng phó sự cố
- Thông báo cho các cá nhân về sự cố

Mục đích của giai đoạn ứng phó ban đầu là ghi lại các bước cần tuân theo để ứng phó một sự cố

Bước 3: Phản hồi ban đầu(tiếp)

Trong phản hồi ban đầu bạn nên:

- kiểm tra xem bạn có đang đối mặt với một sự cố thực sự hay không
- thu thập đầy đủ thông tin về mức độ nghiêm trọng và loại sự cố hoặc cuộc tấn công
- ghi lại các hành động của bạn và sự cố

Bước 15: Tài liệu hóa sự cố

- Nhóm ứng phó sự cố nên ghi lại các quy trình khác nhau trong khi xử lý và ứng phó với một sự cố
- Ghi lại các bước và câu kết luận ngay sau hoàn thành quy trình pháp y
- Tài liệu cần được tổ chức, kiểm tra, xem xét và được kiểm tra từ ban quản lý và người đại diện theo pháp luật
- Tài liệu cần cung cấp:
  - Mô tả về vi phạm bảo mật
  - Chi tiết của hành động diễn ra như:
  - Ai đã xử lý sự cố
  - Khi sự cố đã được xử lý
  - Lý do đằng sau sự cố xảy ra

Bước 15: Tài liệu hóa sự cố (tiếp)

- Cách tốt nhất để truy tố (những) người vi phạm là thông qua tài liệu thích hợp

- Tài liệu được chuẩn bị phải là:
  - Ngắn gọn và rõ rang: Chuẩn bị các báo cáo theo cách rõ rang được mọi người hiểu
  - Định dạng tiêu chuẩn: Duy trì một định dạng chuẩn để viết báo cáo có thể mở rộng, tiết kiệm thời gian và nâng cao độ chính xác
  - Người biên tập: Đảm bảo rằng các báo cáo pháp y được chỉnh sửa đúng cách

Bước 16: Thiệt hại do sự cố và ĐGCP

- Hai bằng chứng quan trọng cần thiết cho pháp lý truy tố là thiệt hại do sự cố và chi phí

- Chi phí bao gồm:
  - Chi phí do mất thông tin bí mật
  - Chi phí pháp lý
  - Chi phí nhân công
  - Chi phí thời gian ngừng hoạt động của hệ thống
  - Chi phí lắp đặt

Bước 17: Xem lại và cập nhật CSƯP

- Xem lại quy trình sau khi hoàn thành cả hai tài liệu và các bước khôi phục

- Thảo luận với các thành viên trong nhóm của bạn về các bước được triển khai thành công và những sai lầm đã phạm

- Xem xét phản hồi và cập nhật chính sách sẽ làm giảm tác động của sự cố và giúp bạn xử lý các sự cố trong tương lai

Các khuyến nghị

- Các khuyến nghị chính trong quá trình tổ chức ứng phó sự cố an toàn thông tin:
  - Cần thiết lập khả năng ứng phó sự cố một cách nhanh chóng và hiệu quả khi sảy ra sự cố ATTT.
  - Xây dựng chính sách ứng phó sự cố.
  - Xây dựng kế hoạch ứng phó sự cố dựa trên chính sách ứng phó sự cố.
  - Xây dựng quy trình ứng phó sự cố.
  - Thiết lập các chính sách và thủ tục liên quan đến việc chia sẻ thông tin liên quan đến sự cố.

Các khuyến nghị (tiếp)

- Các khuyến nghị chính trong quá trình tổ chức ứng phó sự cố an toàn thông tin:
  - Cung cấp thông tin thích hợp về các sự cố cho tổ chức thích hợp.
  - Xem xét các yếu tố liên quan khi lựa chọn mô hình đội ứng phó sự cố.
  - Lựa chọn những người có kỹ năng thích hợp cho đội ứng phó sự cố.
  - Xác định các nhóm khác trong tổ chức có thể cần tham gia vào việc xử lý sự cố.

1. Các sự kiện và sự cố an toàn thông tin
2. Tính cần thiết của ứng phó sự cố
3. Chính sách, kế hoạch, thủ tục ứng phó sự cố
4. Tổ chức của nhóm chuyên gia ứng phó sự cố

Tổ chức của nhóm chuyên gia ứng phó sự cố

Đội ứng phó sự cố cần xử lý sự cố bất cứ khi nào sự cố được xác định bởi bất kỳ người nào trong tổ chức

Họ cần nhanh chóng:

- Phân tích dữ liệu sự cố
- Kiểm tra tác động của sự cố
- Giảm thiểu thiệt hại và khôi phục hệ thống hoạt động bình thường

Nhóm ứng phó sự cố bao gồm:

- Đội ứng phó sự cố trung tâm
- Các nhóm ứng phó sự cố phân tán
- Nhóm điều phối

Tổ chức của nhóm chuyên gia ứng phó sự cố

- Cấu trúc của nhóm chuyên gia ứng phó sự cố:
  - **Đội Ứng phó Sự cố Trung tâm**: Một nhóm ứng phó sự cố duy nhất xử lý các sự cố trong toàn bộ tổ chức. Mô hình này hiệu quả cho các tổ chức nhỏ và cho các tổ chức có sự đa dạng địa lý tối thiểu về tài nguyên máy tính.
  - **Đội ứng phó sự cố phân tán**. Tổ chức có nhiều nhóm ứng phó sự cố, mỗi nhóm chịu trách nhiệm về một phân đoạn hệ thống cụ thể của tổ chức. Mô hình này hiệu quả cho các tổ chức lớn và cho các tổ chức có tài nguyên máy tính lớn ở các vị trí xa.
  - **Nhóm điều phối**. Nhóm ứng phó sự cố cung cấp khuyến nghị cho các nhóm khác mà không có thẩm quyền đối với các nhóm đó.

Tổ chức của nhóm chuyên gia ứng phó sự cố

- Mô hình nhân sự cho nhóm ứng phó sự cố:
  - **Employees**. Tổ chức thực hiện tất cả các công việc ứng phó sự cố của mình.
  - **Partially Outsourced**. Tổ chức thuê ngoài các phần công việc ứng phó sự cố của mình.
  - **Fully Outsourced**. hoàn toàn thuê ngoài công việc ứng phó sự cố của mình.

Tổ chức của nhóm chuyên gia ứng phó sự cố

- Khi lựa chọn mô hình cấu trúc và nhân sự phù hợp cho đội ứng phó sự cố, cần xem xét các yếu tố sau:
  - Yêu cầu về đảm bảo ứng phó 24/7
  - Tỷ lệ nhân viên toàn thời gian/bán thời gian.
  - Chi phí cho ứng phó sự cố: đảm bảo ứng phó 24/7, kinh phí để đào tạo kỹ năng, chi phí bảo mật vật lý cho các khu vực làm việc của nhóm và cơ chế liên lạc ….
  - Chuyên môn của nhân viên.
  - Tinh thần nhân viên.

Nhóm ứng phó sự cố

- Nhóm ứng phó sự cố chịu trách nhiệm giải quyết các sự cố an toàn thông tin tiềm ẩn hoặc thời gian thực
- Nhóm phải bao gồm một số người có kiến thức và kỹ năng trong các lĩnh vực khác nhau
- Đại diện của đội ứng phó sự cố là:
  - Bảo mật CNTT
  - Hoạt động CNTT
  - Bảo mật vật lý
  - Nguồn nhân lực
  - Bộ phận pháp lý
  - Quan hệ công chúng
  - Chuyên môn bên ngoài

Tổ chức của nhóm chuyên gia ứng phó sự cố

- Yêu cầu với nhân viên ứng phó sự cố:
  - Có kỹ năng tốt về các vấn đề kỹ thuật liên quan như: quản trị hệ thống, quản trị mạng, lập trình, hỗ trợ kỹ thuật, phát hiện xâm nhập...
  - Có kỹ năng giải quyết vấn đề tốt và khả năng tư duy phản biện.

Thành viên Nhóm Ứng phó Sự cố

- Cán bộ An ninh Thông tin (ISO)
- Cán bộ Công nghệ Thông tin (ITOC)
- Cán bộ bảo mật thông tin (IPO)
- Quản trị mạng
- Quản trị hệ thống
- Ứng dụng Kinh doanh và Nhân viên Bán hàng Trực tuyến
- Kiểm toán viên nội bộ

Các vai trò và trách nhiệm

- Các vai trò và trách nhiệm của các thành viên trong nhóm ứng phó sự cố
- Cán bộ An ninh Thông tin (ISO):
  - Cung cấp đào tạo về xử lý sự cố cho các thành viên
  - Chuẩn bị tóm tắt về các hành động khắc phục được thực hiện để xử lý sự cố
- Cán bộ Công nghệ Thông tin (ITOC):
  - Đầu mối liên hệ cho các sự cố an ninh khác nhau
  - Thông báo cho ISO để cung cấp cho nhóm ứng phó sự cố
- Cán bộ bảo mật thông tin (IPO):
  - Tổ chức các hoạt động bảo mật với ISO
  - Phát triển giao tiếp với các tổ chức bị ảnh hưởng bởi sự cố bảo mật

Các vai trò và trách nhiệm (tiếp)

- Các vai trò và trách nhiệm của các thành viên trong nhóm ứng phó sự cố
- Quản trị mạng:
  - Phân tích lưu lượng mạng để tìm các dấu hiệu của sự cố
  - Thực hiện các hành động khắc phục chống lại kẻ xâm nhập bị nghi ngờ bằng cách chặn mạng
- Quản trị hệ thống:
  - Cập nhật các gói dịch vụ và bản vá
  - Kiểm tra nhật ký hệ thống để xác định các hoạt động độc hại

Các vai trò và trách nhiệm (tiếp)

- Các vai trò và trách nhiệm của các thành viên trong nhóm ứng phó sự cố
- Ứng dụng Kinh doanh và Nhân viên Bán hàng Trực tuyến:
  - Xem xét các ứng dụng và dịch vụ kinh doanh để tìm các dấu hiệu của sự cố
  - Kiểm tra nhật ký kiểm tra của các máy chủ quan trọng dễ bị tấn công
- Kiểm toán viên nội bộ:
  - Kiểm tra xem hệ thống thông tin có tuân thủ các chính sách và kiểm soát bảo mật hay không
  - Xác định và báo cáo bất kỳ lỗ hổng bảo mật nào cho ban quản lý

Phát triển kỹ năng cho nhân viên ứng phó sự cố

Duy trì đủ nhân viên trong tổ chức để các thành viên trong nhóm có thời gian làm việc không bị gián đoạn

Xây dựng chương trình hỗ trợ do các nhân viên kỹ thuật cao cấp để giúp các nhân viên ít kinh nghiệm hơn biết về quy trình xử lý sự cố

Thuê các chuyên gia để đào tạo

Xây dựng các kịch bản khác nhau về nhóm ứng xử và xử lý sự cố, thảo luận về cách xử lý chúng

Tiến hành diễn tập xử lý sự cố

Sự phụ thuộc của nhóm ứng phó sự cố

- Ban quản lý
- Bảo mật thông tin
- Viễn thông
- Hỗ trợ IT
- Bộ phận pháp lý
- Quan hệ công chúng và truyền thông
- Nguồn nhân lực
- Kế hoạch kinh doanh liên tục
- Quản lý An ninh Vật lý và Cơ sở vật chất

Triển khai ứng phó sự cố thực tế

- Bình tĩnh
- Đánh giá tình huống
- Xác định nhân lực để xử lý sự cố
- Lập kế hoạch giải quyết: Xác định vấn đề, Không gây ra bất kỳ thiệt hại nào, Giải quyết vấn đề
- Ghi lại mọi thứ
- Phân tích bằng chứng để xác nhận rằng một sự cố đã xảy ra
- ...

Triển khai ứng phó sự cố thực tế

- Thông báo cho những người có liên quan
- Dừng sự cố nếu nó vẫn đang diễn ra
- Xác định vấn đề quan trọng nhất
- Bảo quản bằng chứng
- Xóa sạch mọi ảnh hưởng của sự cố
- Xác định và giảm thiểu tất cả các lỗ hổng bảo mật đã bị khai thác
- Ngăn sự cố tái diễn
- Xem xét nguyên nhân và cách giải quyết
- Xác nhận rằng các hoạt động đã được khôi phục lại bình thường
- Tạo báo cáo cuối cùng

Tổng kết

Mục đích của việc ứng phó sự cố là để hỗ trợ phục hồi nhanh chóng và hiệu quả sau khi 1 sự cố an ninh xảy ra

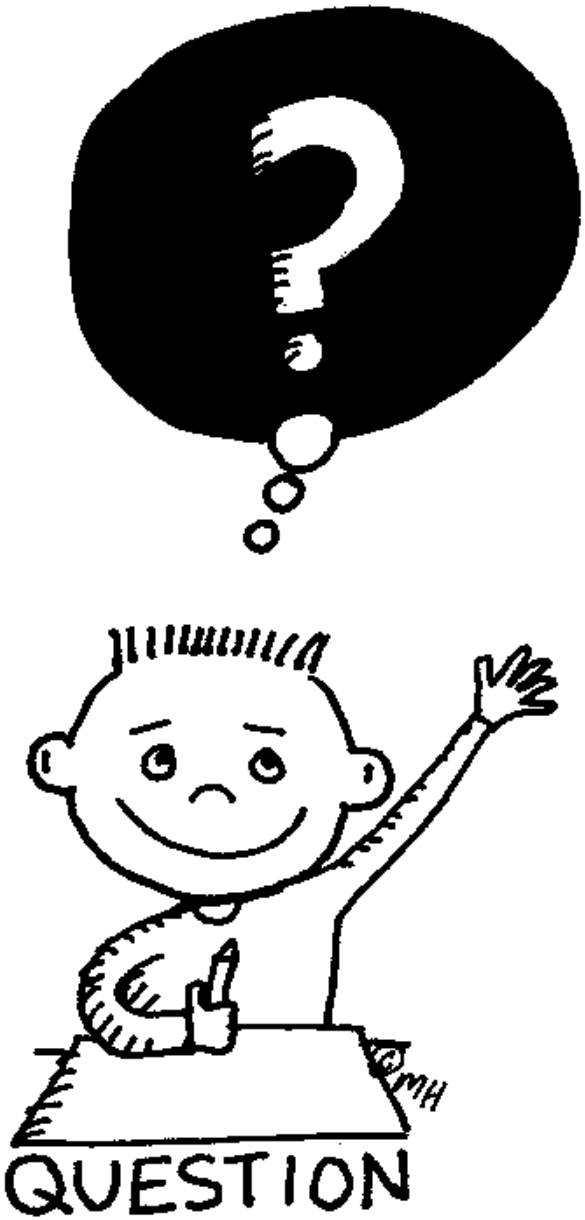
Kế hoạch ứng phó bao gồm 1 tập hướng dẫn để phát hiện và phản ứng lại 1 sự cố

Kế hoạch đó sẽ thu thập các tài nguyên liên quan theo 1 quy trình đã được chuẩn bi nhằm xác định các sự cố liên quan đến vấn đề an toàn của một hệ thống máy tính

Chuẩn bị là yếu tố quan trọng nhất để phản ứng lại trước các sự cố từ trước khi chúng xảy ra

Để thực hiện các chính sách về ứng phó sự cố cần có hiểu biết và nhận thức tốt về vấn đề này

Quản li sự cố không chỉ là phản ứng lại mà còn ngăn chặn các sự cố trong tương lai bằng tối thiểu các thiệt hại mà chúng có thể gây ra


QUESTION