HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

BÀI GIẢNG MÔN HỌC
AN TOÀN MẠNG

CHƯƠNG 4. CÁC GIẢI PHÁP PHÒNG NGỪA VÀ NGĂN CHẶN TẤN CÔNG

Giảng viên: PGS.TS. Hoàng Xuân Dậu

E-mail: dauhx@ptit.edu.vn

Khoa: An toàn thông tin

NỘI DUNG CHƯƠNG 4

1. Xây dựng kế hoạch an toàn
2. Các giải pháp phòng ngừa, ngăn chặn tấn công
3. Ứng phó sự cố
4. Phục hồi sau sự cố và tiếp tục hoạt động.

4.1 Xây dựng kế hoạch an toàn

- Kế hoạch an toàn là gì?
- Tại sao kế hoạch an toàn lại quan trọng?
- Mục tiêu của lập kế hoạch an toàn
- Lợi ích của kế hoạch an toàn
- Các thành phần của một kế hoạch an toàn hiệu quả
- Các bước xây dựng kế hoạch an toàn hiệu quả
- Các điều cần tránh khi thực hiện kế hoạch an toàn.

Kế hoạch an toàn là gì?

- Kế hoạch an toàn là một tài liệu bằng văn bản bao gồm thông tin về các chính sách, thủ tục và kế hoạch khắc phục liên quan đến các biện pháp đối phó.
- Kế hoạch này nhằm đảm bảo tính toàn vẹn của hoạt động và tính bảo mật của các tài sản quan trọng của tổ chức.
- Đây là một công cụ quan trọng để bảo vệ khách hàng, nhân viên và thông tin bí mật của công ty.

Tại sao kế hoạch an toàn lại quan trọng?

- Các lý do về tầm quan trọng của kế hoạch an toàn:
  - Các cuộc tấn công mạng xảy ra thường xuyên không chỉ với các tổ chức, doanh nghiệp lớn mà cả với các doanh nghiệp vừa và nhỏ. Khi có tấn công, sự cố xảy ra, thiệt hại sẽ rất lớn nếu không được xử lý phù hợp. Nếu có kế hoạch ứng phó sự cố đầy đủ, hiệu quả, thiệt hại có thể giảm đáng kể. Do đó, phát hiện càng sớm thì việc xử lý và bảo mật dữ liệu càng dễ dàng.
  - Kế hoạch an toàn giúp phản ứng nhanh trước các mối đe dọa trên mạng cho phép bảo vệ thông tin quan trọng của nhân viên, khách hàng và các bên liên quan.
  - Kế hoạch an toàn bao gồm các biện pháp bảo mật có thể giúp ngăn chặn các cuộc tấn công mạng. Đảm bảo an toàn không bắt đầu sau khi một cuộc tấn công xảy ra. Đó là một quá trình liên tục đòi hỏi phải bảo trì và giám sát một cách nhất quán.

Mục tiêu của lập kế hoạch an toàn

- Mục tiêu của lập và thực hiện kế hoạch an toàn là đảm bảo một môi trường an toàn và không có rủi ro để giữ an toàn cho dữ liệu, mạng và thiết bị trước các mối đe dọa trên mạng;
  - Mối đe dọa có thể ở bất kỳ đâu, từ một lỗi nhỏ trong mã cho đến trách nhiệm chiếm quyền điều khiển hệ thống phức tạp thông qua nhiều hoạt động xâm nhập mạng và hệ thống khác nhau.
  - Việc lập kế hoạch an toàn, trong đó có khâu đánh giá rủi ro và ước tính chi phí tái thiết giúp tổ chức, doanh nghiệp luôn sẵn sàng và lường trước những tổn thất có thể xảy ra.

Lợi ích của kế hoạch an toàn

- Kế hoạch an toàn đầy đủ sẽ giúp các cơ quan, tổ chức có khả năng ứng phó hiệu quả với các sự cố an ninh mạng, giảm thiểu thiệt hại. Các lợi ích của kế hoạch an toàn gồm:
  - Hiểu rõ hơn về rủi ro
  - Kích hoạt tính năng bảo vệ chủ động
  - Phản ứng kịp thời
  - Tuân thủ các yêu cầu cần thiết
  - Ngăn chặn các mối đe dọa nội bộ.

Các thành phần của một kế hoạch an toàn hiệu quả

- Làm việc trong một Framework
- Nhận thức về thông tin mối đe dọa (Threat Intelligence)
- Các thành phần cơ bản của an ninh mạng (Tường lửa, IDS/IPS, SIEM, lọc thư rác, chống phishing, mật khẩu mạnh, xác thực đa nhân tố, mã hóa dữ liệu)
- Hợp tác với các bên liên quan nội bộ
- Đánh giá rủi ro toàn diện
- Lập kế hoạch ứng phó sự cố
- Hỗ trợ và vận hành dữ liệu
- Vai trò và Trách nhiệm.

Các bước xây dựng kế hoạch an toàn hiệu quả

- Bước 1: Tiến hành đánh giá rủi ro bảo mật
- Bước 2: Đặt mục tiêu an toàn
- Bước 3: Đánh giá công nghệ
- Bước 4: Chọn Khung bảo mật (tiêu chuẩn/framework)
- Bước 5: Đánh giá chính sách bảo mật
- Bước 6: Xây dựng kế hoạch quản lý rủi ro
- Bước 7: Thực hiện kế hoạch an toàn
- Bước 8: Đánh giá kế hoạch an toàn.

Các bước xây dựng kế hoạch an toàn hiệu quả

- Bước 1: Tiến hành đánh giá rủi ro bảo mật
  - Nhận dạng các tài sản ATTT
  - Nhận dạng các mối đe dọa
  - Phân loại dữ liệu
  - Nhận dạng và xếp hạng các rủi ro.
- Bước 2: Đặt mục tiêu an toàn
  - Đảm bảo tính bí mật, toàn vẹn và sẵn dùng của thông tin, hệ thống
- Bước 3: Đánh giá công nghệ
  - Cần hiểu và đánh giá các công nghệ, hệ thống sử dụng để chủ động giảm thiểu rủi ro.
  - Gồm: Nhận dạng hệ điều hành sử dụng, phân loại thiết bị, triển khai nhân sự bảo trì các tài sản quan trọng, loại bỏ các dịch vụ trùng lặp...

Các bước xây dựng kế hoạch an toàn hiệu quả

- Bước 4: Chọn Khung bảo mật (tiêu chuẩn/framework)
  - Các framework cung cấp các mô hình chuẩn được đánh giá toàn diện làm định hướng cho triển khai thực tế.
  - Một số framework/chuẩn: ISO 27001, PCI DSSm NIST CSF...
- Bước 5: Đánh giá chính sách bảo mật
  - Theo dõi các chính sách ở một vị trí tập trung
  - Xem xét các chính sách hàng năm và/hoặc khi doanh nghiệp cần thay đổi phù hợp và có lý do chính đáng
  - Truyền đạt những thay đổi chính sách phù hợp trong tổ chức
  - Các chính sách đều chứa bảng thông tin phiên bản và sửa đổi.

Các bước xây dựng kế hoạch an toàn hiệu quả

- Bước 6: Xây dựng kế hoạch quản lý rủi ro
  - Xác định tài sản có giá trị nhất
  - Kiểm toán dữ liệu và sở hữu trí tuệ
  - Thực hiện đánh giá rủi ro mạng
  - Phân tích mức độ an toàn và mối đe dọa
  - Tạo kế hoạch ứng phó sự cố.
- Bước 7: Thực hiện kế hoạch bảo mật
  - Triển khai kế hoạch an toàn mạng là nhiệm vụ quan trọng nhất trong toàn bộ chiến lược và điều này đi kèm với một cách tiếp cận theo nhiều lớp.
  - Các nhóm nội bộ thảo luận chi tiết về kế hoạch và phân công nhiệm vụ khắc phục một cách phù hợp.

Các bước xây dựng kế hoạch an toàn hiệu quả

- Bước 8: Đánh giá kế hoạch bảo mật
  - Kế hoạch bảo mật phải được theo dõi và kiểm tra thường xuyên để đảm bảo các mục tiêu phù hợp với bối cảnh mối đe dọa.
  - Các bước cần tuân theo để duy trì sự giám sát liên tục và toàn diện:
    - Thiết lập các bên liên quan nội bộ từ tất cả các bộ phận trong tổ chức để được hỗ trợ liên tục.
    - Thực hiện đánh giá rủi ro định kỳ
    - Nhận phản hồi thường xuyên từ các bên liên quan, gồm cả bên trong và bên ngoài tổ chức.

Các điều cần tránh khi thực hiện kế hoạch an toàn

- Bỏ qua các mối đe dọa mạng phổ biến
- Bỏ qua việc cập nhật phần mềm thường xuyên
- Sụp đổ trước các mối đe dọa mạng phổ biến
- Không đào tạo nhân viên
- Không sử dụng mật khẩu mạnh
- Không có chính sách an toàn mạng
- Không bảo vệ dữ liệu doanh nghiệp.

4.2 Các giải pháp phòng ngừa, ngăn chặn tấn công

- Đảm bảo an toàn môi trường vật lý
- Đảm bảo an toàn cho hệ điều hành, dịch vụ và ứng dụng
- Đảm bảo an toàn cho các thiết bị di động
- Quản lý bản vá
- Đảm bảo an toàn cho người dùng.

Đảm bảo an toàn môi trường vật lý

- Phân loại tài sản
- Đánh giá các lỗ hổng vật lý
- Lựa chọn các vị trí đảm bảo an toàn
- Bảo vệ tài sản: Khóa và kiểm soát ra vào
- Phát hiện xâm nhập vật lý
- Tuân thủ theo chuẩn.

Phân loại tài sản

- Phân loại tài sản nhận dạng các tài sản vật lý và gán mức độ quan trọng và giá trị cho chúng để phát triển các biện pháp kiểm soát và quy trình giản lược nhằm bảo vệ chúng một cách hiệu quả.
- Sau phân loại, các danh mục tài sản có những đặc điểm chung và cố hữu cho phép thiết lập các biện pháp bảo vệ cơ bản theo danh mục.
- Đối với tài sản quan trọng, tiêu chí tối thiểu sau phải được ghi chép đầy đủ: giá trị khấu hao, chi phí ban đầu, chi phí thay thế, chủ sở hữu tài sản, nhà cung cấp, phiên bản và số sê-ri (nếu có).

Phân loại tài sản

- Các tài sản vật chất của công ty thường sẽ gồm các loại:
  - Các thiết bị máy tính (máy chủ, NAS, SAN, máy trạm, máy xách tay...)
  - Các thiết bị truyền thông (Bộ định tuyến, switch, tường lửa...)
  - Các thiết bị kỹ thuật (Nguồn điện, UPS, điều hòa không khí...)
  - Các phương tiện lưu trữ (Mảng đĩa, SSD...)
  - Nội thất và đồ đạc
  - Tài sản có giá trị trực tiếp bằng tiền (tiền, đồ trang sức, trái phiếu...).

Đánh giá các lỗ hổng vật lý

- Các dạng lỗ hổng vật lý có thể tồn tại trong:
  - Tòa nhà: gồm các lỗ hổng trong quản lý, vận hành tòa nhà có thể tạo điều kiện cho xâm nhập từ bên ngoài.
  - Các thiết bị tính toán và ngoại vi: gồm các lỗ hổng trong quản lý, sử dụng thiết bị tính toán và ngoại vi cho phép truy cập trái phép vào các máy chủ, máy tính và các thiết bị khác.
  - Các tài liệu: gồm các lỗ hổng trong quản lý, sử dụng các tài liệu nhạy cảm.
  - Các hồ sơ và thiết bị: gồm các lỗ hổng trong quản lý, sử dụng các hồ sơ và thiết bị (nhất là các hồ sơ, thiết bị cá nhân, như điện thoại, máy tính không khóa, có thể bị xâm nhập trái phép).

Lựa chọn các vị trí đảm bảo an toàn

- Vị trí/địa điểm phù hợp để đặt các thiết bị đóng vai trò rất quan trọng trong công tác đảm bảo an toàn.
- Một số vấn đề cần xem xét:
  - Khả năng tiếp cận (đi lại, sơ tán khi cần thiết)
  - Chiếu sáng (khả năng chiếu sáng 24x7)
  - Gần tòa nhà khác (khả năng sự cố an ninh vật lý xảy ra cao hơn khi quá gần các tòa nhà khác)
  - Gần cơ quan thực thi pháp luật và ứng phó khẩn cấp
  - Chặn bắt truyền dẫn không dây và sóng radio (liên quan đến rủi ro bị chặn lưu lượng, nghe lén)
  - Độ tin cậy của các tiện ích
  - Xây dựng, khai quật và phá dỡ (ảnh hưởng đến hệ thống truyền thông).

Bảo vệ tài sản: Khóa và kiểm soát ra vào

- Hệ thống khóa cho:
  - Cửa và tủ hồ sơ
  - Máy tính xách tay
  - Trung tâm dữ liệu, tủ cáp, phòng mạng
- Kiểm soát ra vào:
  - Hệ thống kiểm soát truy cập tòa nhà
  - Bẫy săn trộm
  - Thẻ truy cập cho nhân viên và khách vào tòa nhà
  - Sử dụng xác thực sinh trắc
  - Sử dụng nhân viên bảo vệ.

Phát hiện xâm nhập vật lý

- Các hệ thống, thiết bị có thể sử dụng cho phát hiện xâm nhập vật lý:
  - Sử dụng camera giám sát (Closed-Circuit Television - CCTV)
  - Sử dụng chuông, loa, còi cảnh báo.

Tuân thủ theo chuẩn

- Chuẩn ISO 27002
  - ISO/IEC 27002:2022 (Chương 4 Physical Controls)
  - ISO/IEC 27002:2013 (Chương 7 Physical and environmental security)
- COBIT
  - Là một Framework do tổ chức ISACA tạo ra để quản lý và quản trị CNTT;
  - Framework này tập trung vào hoạt động kinh doanh và xác định một tập hợp các quy trình chung để quản lý CNTT.
    - Nội dung liên quan đến đảm bảo an toàn môi trường vật lý.

Đảm bảo an toàn cho hệ điều hành, dịch vụ và ứng dụng

- An toàn cho hệ điều hành
- An toàn cho các dịch vụ
- An toàn cho các ứng dụng.

An toàn cho hệ điều hành

- Các mô hình, cơ chế đảm bảo an toàn thường được sử dụng cho HĐH:
  - DAC (ACM - Access Control Matrix và ACL- Access Control List)
  - MAC, RBAC, Rule-Based AC.
- Các mô hình đảm bảo an toàn cổ điển:
  - Bell-LaPadula, Biba, Clark-Wilson
  - TCSEC (Trusted Systems Security Evaluation Criteria)
- Một số cơ chế bảo mật khác:
  - Các bộ giám sát tham chiếu (Reference Monitor)
  - Các cơ chế an toàn sử dụng phần cứng (như TPM)
  - Bảo mật hệ thống file (phân quyền truy cập cho người dùng dựa trên DAC, MAC và RBAC)
  - Sử dụng tường lửa.

An toàn cho hệ điều hành

- Các vấn đề bảo mật và cơ chế an toàn trong MS Windows (đã học trong môn An toàn hệ điều hành)
- Các vấn đề bảo mật và cơ chế an toàn trong Linux (đã học trong môn An toàn hệ điều hành).

An toàn cho các dịch vụ

- An toàn cho dịch vụ email
- An toàn cho dịch vụ web
- An toàn cho dịch vụ DNS
- An toàn sử dụng các máy chủ proxy.

An toàn cho dịch vụ email

- Các giao thức vận hành dịch vụ email:
  - SMTP, POP, IMAP, HTTPS...
- Các vấn đề bảo mật đối với máy chủ email và dịch vụ email:
  - Truy cập trái phép vào email và gây rò rỉ dữ liệu
  - Thư rác và phishing
  - Mã độc
  - Tấn công DoS

An toàn cho dịch vụ email

- Các cơ chế bảo mật máy chủ email và dịch vụ email:
  - Sử dụng SMTP bảo mật (SMTPS - SMTP over SSL/TLS, S/MIME-Secure/Multipurpose Internet Mail Extensions)
  - Xác thực tài khoản và cấu hình máy chủ SMTP
  - Xác thực tên miền gửi email (Sender-ID, SPF, DKIM)
  - Giới hạn IP truy cập.

An toàn cho dịch vụ web

- Các giao thức vận hành dịch vụ web:
  - HTTP và HTTPS
- Các vấn đề bảo mật đối với máy chủ web, ứng dụng và trình duyệt web:
  - Tấn công khai thác các lỗ trong máy chủ web và các thành phần của máy chủ web (lỗi tràn bộ đệm, lỗi cấu hình, lỗi quản lý và sử dụng phiên web...)
  - Tấn công SQLi, CMDi, XSS, CSRF, SSRF, duyệt đường dẫn
  - Tấn công HTTP DoS/DDoS.

An toàn cho dịch vụ web

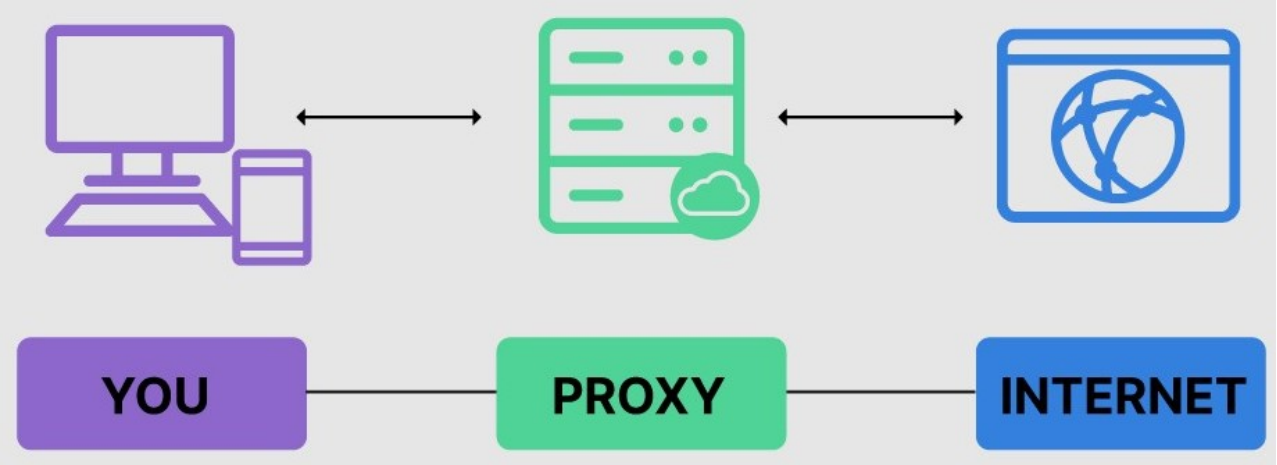
- Các cơ chế đảm bảo an toàn cho dịch vụ web:
  - Sử dụng quyền tối thiểu để chạy máy chủ web và các dịch vụ kèm theo
  - Cập nhật phần mềm máy chủ web, máy chủ ứng dụng và trình duyệt
  - Cấu hình an toàn
  - Sử dụng HTTPS thay cho HTTP
  - Sử dụng các bộ lọc dữ liệu đầu vào
  - Xác thực đa nhân tố.

An toàn cho dịch vụ DNS

- Các vấn đề bảo mật đối với máy chủ và dịch vụ DNS:
  - Tấn công đường hầm DNS (DNS Tunneling)
  - Tấn công khuếch đại DNS (DNS Amplification)
  - Tấn công ngập lụt DNS (DNS Flood Attack)
  - Tấn công giả mạo DNS (DNS Spoofing)
  - Tấn công NXDOMAIN.
- Các cơ chế đảm bảo an toàn cho máy chủ và dịch vụ DNS:
  - Cấu hình máy chủ DNS đúng chuẩn
  - Cập nhật HĐH và phần mềm dịch vụ DNS
  - Sử dụng DNSSEC.

An toàn sử dụng các máy chủ proxy

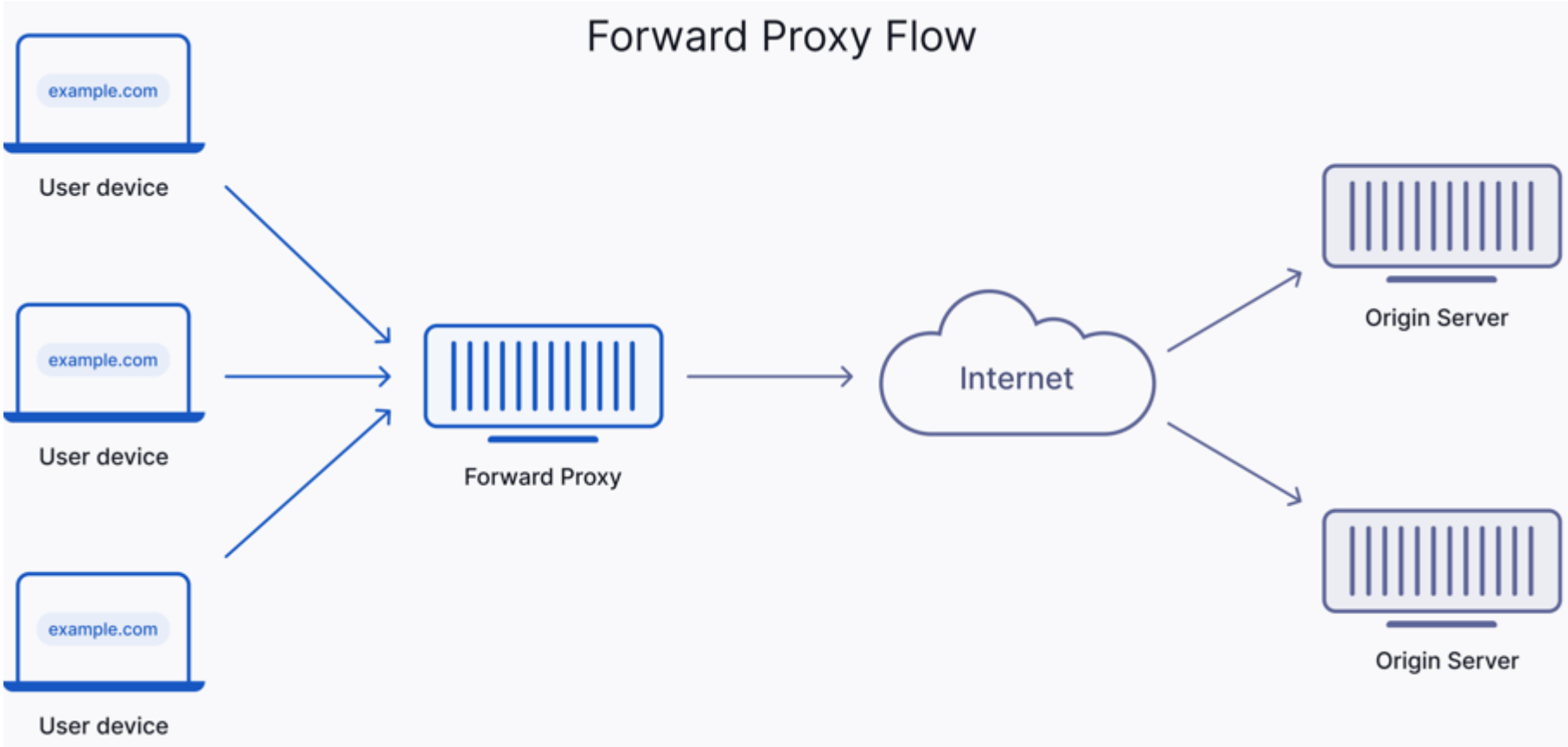
- Các máy chủ proxy được sử dụng khá phổ biến cho các dịch vụ web, DNS, FTP, email:
  - Giúp che giấu cấu hình mạng và địa chỉ IP của các máy thực (máy trạm, máy chủ)
  - Hỗ trợ cân bằng tải.



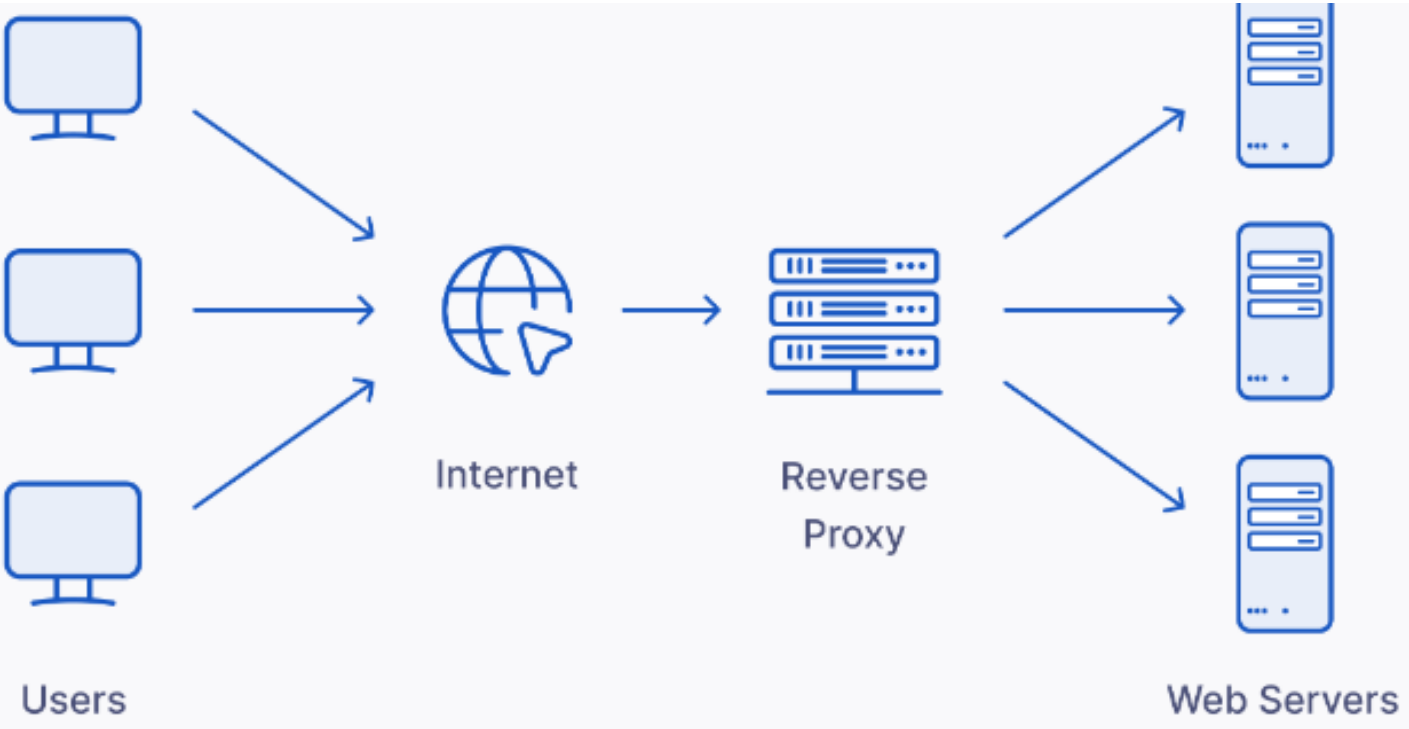
An toàn sử dụng các máy chủ proxy

- Các loại máy chủ proxy:
  - Foward proxy
  - Reverse proxy
  - Anonymous proxy

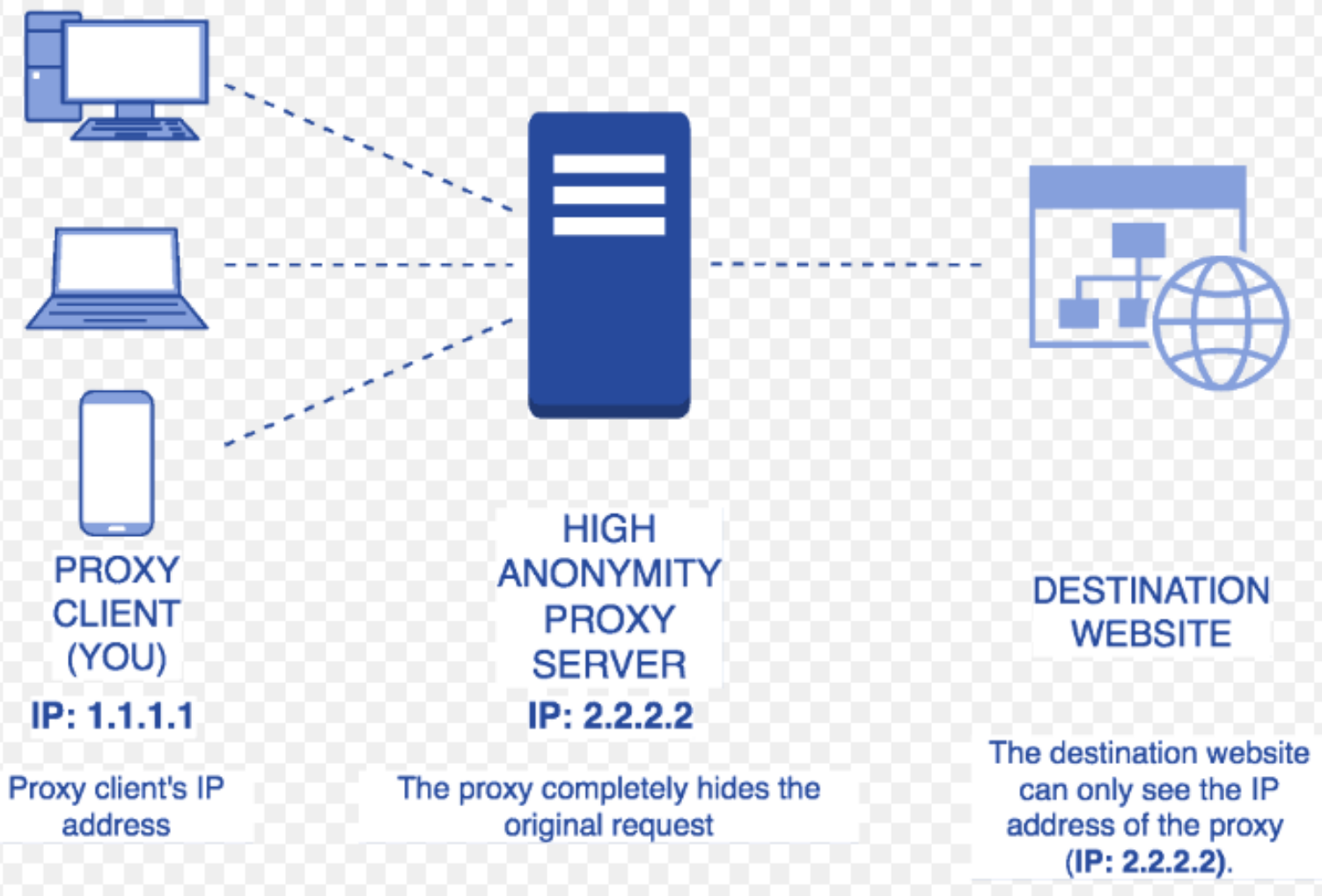
An toàn sử dụng các máy chủ proxy



An toàn sử dụng các máy chủ proxy



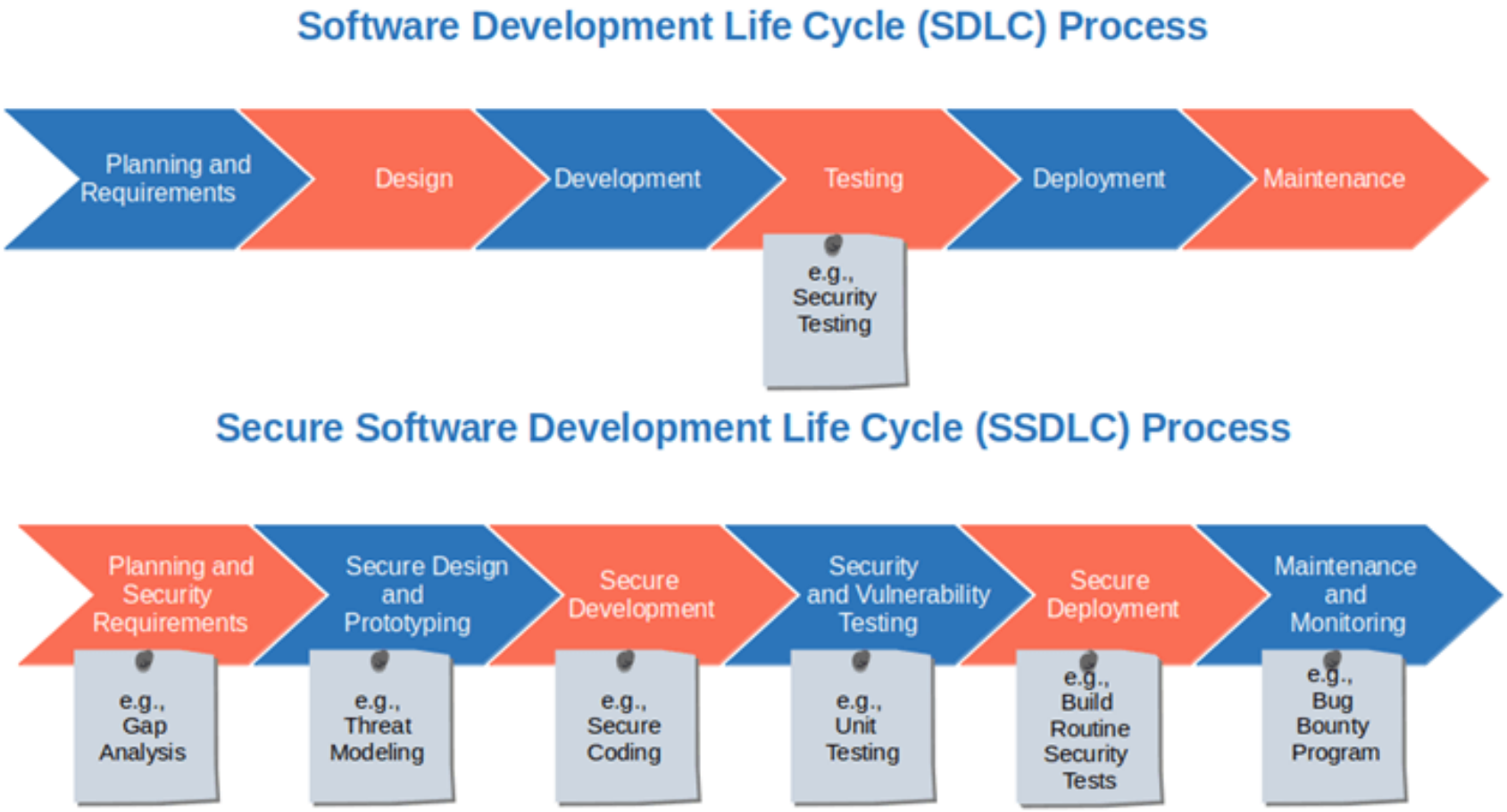
An toàn sử dụng các máy chủ proxy



An toàn cho các ứng dụng

- Đảm bảo an toàn cho các ứng dụng gồm các khâu:
  - Thiết kế và phát triển ứng dụng an toàn (sử dụng Secure Development Lifecycle)
  - Cài đặt, cấu hình ứng dụng an toàn
  - Vận hành ứng dụng an toàn
    - Cập nhật bản vá
    - Giám sát.

An toàn cho các ứng dụng



An toàn cho các ứng dụng

- Một số vấn đề thực tế về An toàn cho các ứng dụng:
  - Security Training: Đào tạo về an toàn cho nhóm phát triển ứng dụng
  - Secure Development Infrastructure: Cần có hạ tầng an toàn (máy chủ, hệ thống quản lý dự án...) cho phát triển ứng dụng
  - Security Requirements: Nêu rõ các yêu cầu đảm bảo an toàn
  - Secure Design: Thiết kế an toàn (bổ sung các thành phần cho đảm bảo an toàn từ khâu thiết kế)
  - Threat Modeling: Mô hình hóa các mối đe dọa (xem xét các thuộc tính bảo mật của thiết kế và xác định các vấn đề tiềm ẩn cũng như cách khắc phục)
  - Secure Coding: Viết mã an toàn (sử dụng các thư viện và phương pháp viết mã an toàn)

An toàn cho các ứng dụng

- Một số vấn đề thực tế về An toàn cho các ứng dụng:
  - Security Code Review: Đánh giá mã an toàn (thường sử dụng phương pháp phân tích tĩnh)
  - Security Testing: Kiểm thử an toàn (như Pentesting)
  - Security Documentation: Xây dựng tài liệu an toàn
  - Secure Release Management: Quản lý các phiên bản an toàn
  - Dependency Patch Monitoring: Giám sát sự phụ thuộc lẫn nhau của các bản vá
  - Product Security Incident Response: Phản hồi sự cố bảo mật với sản phẩm.

Đảm bảo an toàn cho các thiết bị di động

- Các thiết bị di động, gồm điện thoại thông minh, máy tính bảng và các thiết bị cá nhân khác được sử dụng ngày càng phổ biến;
- Đặc biệt, các thiết bị di động được kết nối vào hệ thống mạng của cơ quan, tổ chức, có thể chứa nhiều thông tin nhạy cảm, quan trọng, tiềm ẩn nhiều rủi ro có thể bị khai thác, kiểm soát nhằm đánh cắp thông tin nhạy cảm và làm cầu nối cho xâm nhập vào hệ thống mạng của cơ quan, tổ chức.

Đảm bảo an toàn cho các thiết bị di động

- Các rủi ro đối với các thiết bị di động:
  - Các rủi ro với thiết bị:
    - Các thiết bị di động về cơ bản có các thành phần và hoạt động tương tự máy tính nên cũng có các mối đe dọa tương tự máy tính.
    - Các mối đe dọa có thể khai thác các lỗ hổng tồn tại trong HĐH và các ứng dụng của thiết bị để xâm nhập, nhằm thay đổi các thông số cài đặt, đánh cắp thông tin lưu trong thiết bị.
    - Một số vấn đề bảo mật khác với thiết bị di động:
      - Thiết bị lưu trữ của các thiết bị di động có thể được truy cập dễ dàng thông qua cổng USB --> nguy cơ thông tin, dữ liệu bị đánh cắp.
      - Mật khẩu yếu (PIN, hình vẽ đều là các dạng mật khẩu yếu)
      - Chiếm quyền điều khiển Wi-Fi
      - Sử dụng như 1 wifi router mở
      - Xâm nhập vào băng tần cơ sở của thiết bị di động.

Đảm bảo an toàn cho các thiết bị di động

- Các rủi ro đối với các thiết bị di động:
  - Các rủi ro với ứng dụng:
    - Các ứng dụng trojan
    - Các URL độc hại ẩn (nhúng trong các tin nhắn, trang web để bẫy người dùng truy cập)
    - Phishing
    - Smishing (phishing qua tin nhắn).

Đảm bảo an toàn cho các thiết bị di động

- Các cơ chế / biện pháp đảm bảo an toàn cho thiết bị di động:
  - Các tính năng an toàn có sẵn:
    - Tách biệt/cô lập không gian làm việc của các ứng dụng --> giảm thiểu việc đánh cắp dữ liệu của ứng dụng khác
    - Hạn chế người dùng có thể tự cài đặt lại HĐH, hoặc chỉnh sửa sâu các tham số hệ thống.
    - Hỗ trợ các cơ chế xác thực các ứng dụng trước khi có thể được tải và chạy trên các thiết bị.
  - Mật khẩu an toàn (đủ độ dài, đảm bảo độ khó, sử dụng xác thực sinh trắc)
  - Sử dụng mã hóa dữ liệu.

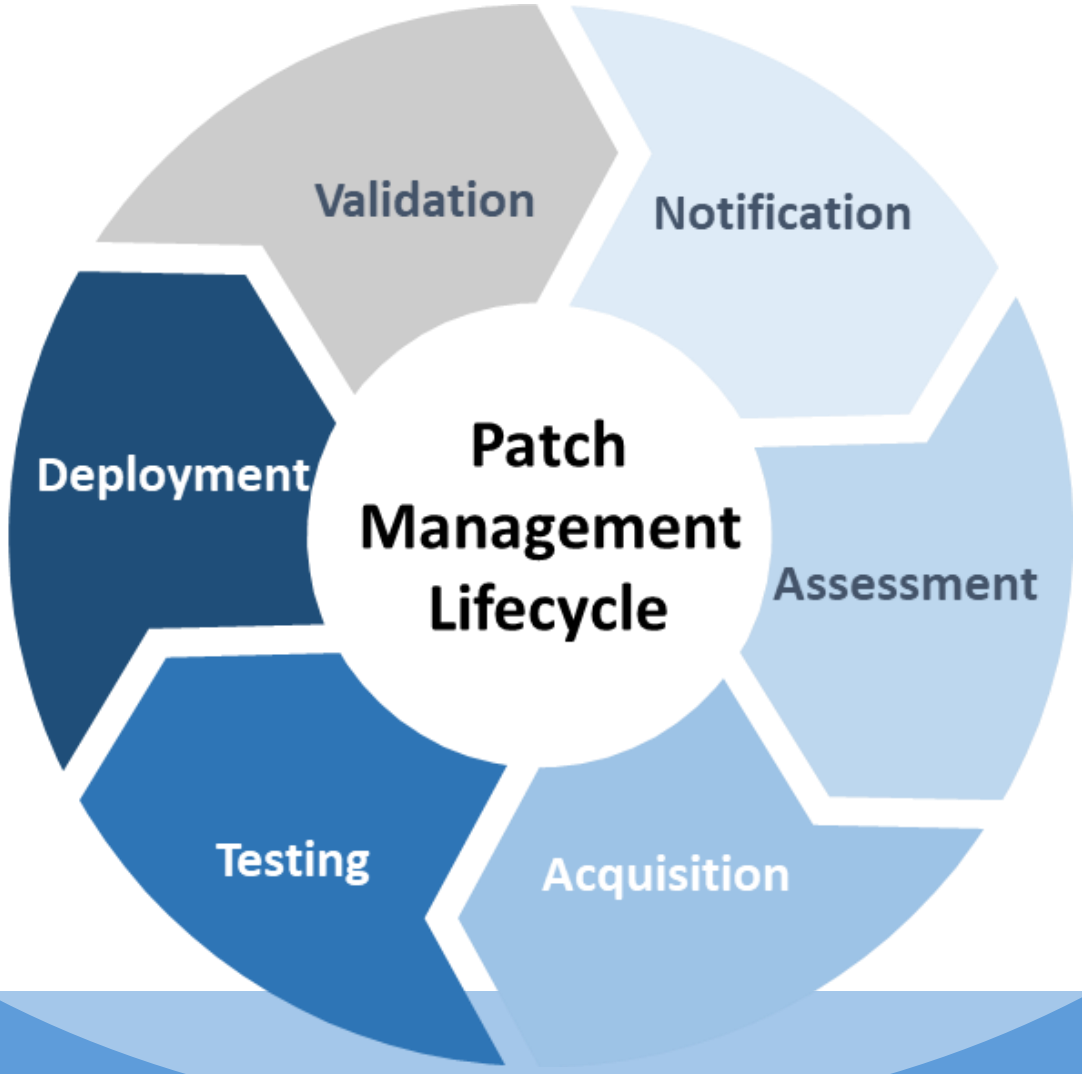
Quản lý bản vá

- Quản lý bản vá là quá trình phân phối và áp dụng các bản cập nhật cho phần mềm;
  - Những bản vá này thường cần thiết để sửa các "lỗ hổng" hoặc "lỗi" tồn tại trong phần mềm.
- Các thành phần hệ thống cần bản vá bao gồm: hệ điều hành, ứng dụng và hệ thống nhúng (như thiết bị mạng).
- Khi một lỗ hổng được tìm thấy sau khi phát hành một phần mềm, một bản vá có thể được sử dụng để khắc phục.
  - Cập nhật sẽ giúp đảm bảo rằng các tài sản CNTT không bị khai thác.

Quản lý bản vá

- Tầm quan trọng của Quản lý bản vá:
  - Bảo mật: Quản lý bản vá khắc phục các lỗ hổng trong các thành phần phần mềm dễ bị tấn công mạng, giúp giảm thiểu rủi ro bảo mật.
  - Thời gian hoạt động của hệ thống: Quản lý bản vá đảm bảo phần mềm và ứng dụng luôn cập nhật và chạy trơn tru, đảm bảo thời gian hoạt động của hệ thống.
  - Tuân thủ: Với sự gia tăng liên tục của các cuộc tấn công mạng, các tổ chức thường được các cơ quan quản lý yêu cầu duy trì mức độ tuân thủ nhất định. Quản lý bản vá là một phần cần thiết để tuân thủ các tiêu chuẩn.
  - Cải tiến tính năng: Quản lý bản vá có thể vượt ra ngoài việc sửa lỗi phần mềm để bao gồm cả các bản cập nhật tính năng/chức năng. Các bản vá có thể rất quan trọng để đảm bảo rằng bạn có phiên bản mới nhất và tốt nhất mà sản phẩm cung cấp.

Vòng đời quản lý bản vá

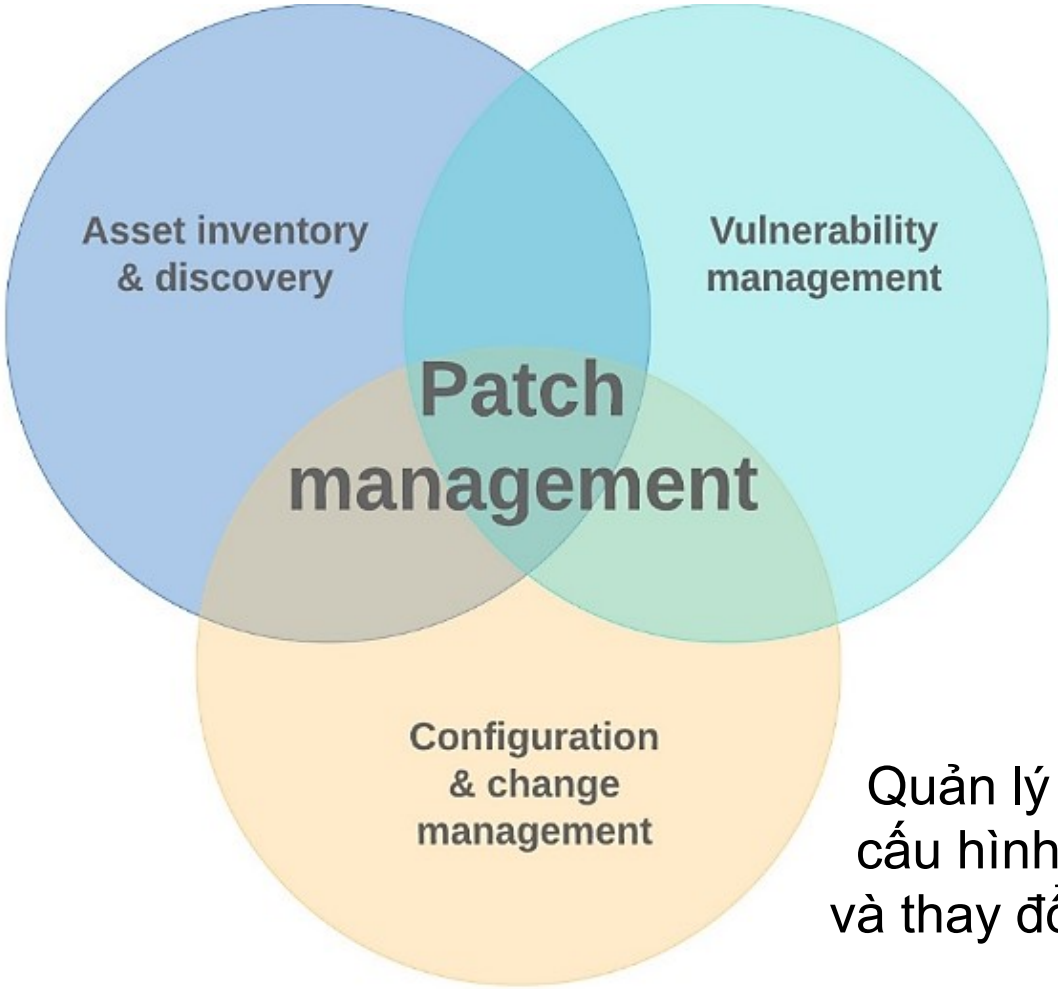


Vòng đời quản lý bản vá

- B1-Notification (Thông báo): Nhận thông báo về các bản vá từ nhiều nguồn khác nhau.
- B2-Assessment (Đánh giá): Đánh giá/xếp hạng mức độ nghiêm trọng của lỗ hổng --> lựa chọn triển khai
- B3-Acquisition (Thu nhận/Tải về): Thu nhận hoặc tải bản vá từ nhà cung cấp hoặc nguồn tin cậy.
- B4-Testing (Kiểm tra): Các bản vá nên được thử nghiệm ở các hệ thống mẫu, hoặc phạm vị hẹp trước khi triển khai.
- B5-Deployment (Triển khai): Triển khai bản vá trên hệ thống thực.
- B6-Validation (Xác minh): Các bản vá sau triển khai cần được kiểm tra, xác minh để đảm bảo lỗi được khắc phục và hệ thống hoạt động ổn định.

Các phần phụ thuộc cơ bản của quản lý bản vá

Kiểm kê và khám phá tài sản



Quản lý lỗ hổng bảo mật

Quản lý cấu hình và thay đổi

Các thực tế tốt nhất trong quản lý bản vá

Đảm bảo an toàn cho người dùng

- Các mối đe dọa thường gặp với người dùng:
  - Mã độc (virus, worm, ransomware...)
  - Phishing / Social engineering
  - Tấn công người đứng giữa (MITM)
  - Spaming (Email, messenging spams...)
  - Mất dữ liệu do tấn công mạng, hoặc hỏng hóc phần cứng/phần mềm
  - Bắt nạt trên mạng xã hội / không gian mạng.
- Đảm bảo an toàn cho người dùng là 1 khâu quan trọng trong giải pháp đảm bảo an toàn cho thông tin và hệ thống mạng của cơ quan, tổ chức.

Các biện pháp đảm bảo an toàn cho người dùng

Các biện pháp đảm bảo an toàn cho người dùng

- Các biện pháp đảm bảo an toàn cho người dùng gồm:
  - Đào tạo ý thức
  - Sử dụng mật khẩu mạnh, xác thực đa nhân tố
  - Cập nhật phần mềm (phiên bản mới + bản vá)
  - Sao lưu dữ liệu
  - Sử dụng tường lửa và các cơ chế kiểm soát truy cập.

4.3 Ứng phó sự cố

- Mục tiêu cuối cùng của ứng phó sự cố (Incident Response) là ngăn chặn, phục hồi và tiếp tục các hoạt động bình thường nhanh chóng và suôn sẻ nhất có thể.
- Để có thể ứng phó sự cố hiệu quả, cần có kế hoạch ứng phó sự cố (Incident Response Plan), hay kế hoạch quản lý sự cố (Incident Management Plan);
  - Kế hoạch ứng phó sự cố đề cập đến các quy trình và công cụ mà tổ chức sử dụng để phát hiện, loại bỏ và khắc phục các mối đe dọa và tấn công an ninh mạng.
  - Kế hoạch này hỗ trợ tổ chức và nhóm của tổ chức đảm bảo phản ứng nhanh chóng trước mọi mối đe dọa từ môi trường bên ngoài.

4.3 Ứng phó sự cố

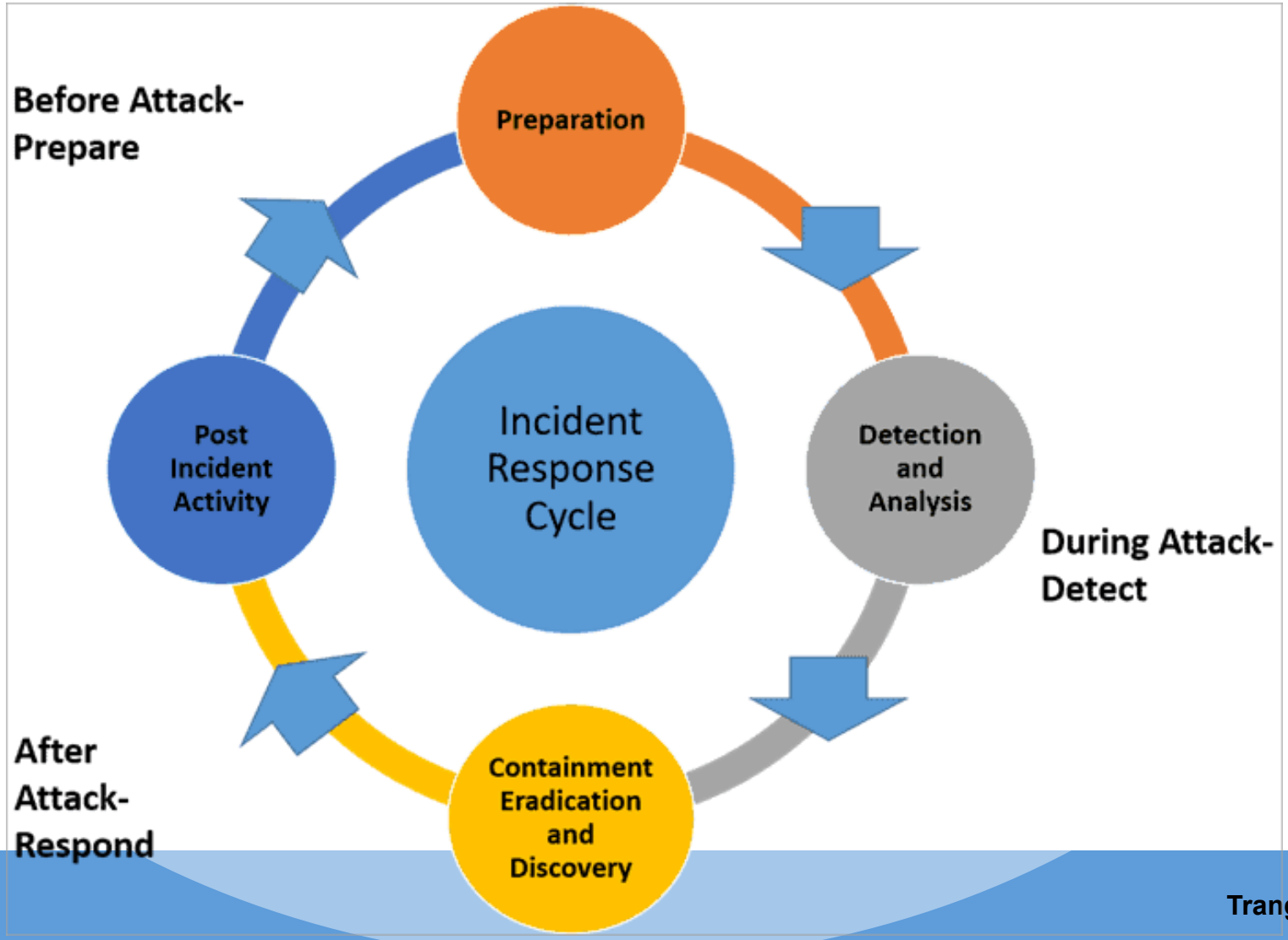
- Kế hoạch ứng phó sự cố cũng đảm bảo rằng quá trình ứng phó với các mối đe dọa có hiệu quả.
  - Những kế hoạch hiệu quả này cũng đảm bảo giảm thiểu tác động của cuộc tấn công.
  - Một kế hoạch ứng phó toàn diện và hiệu quả có thể vạch ra kế hoạch hành động cho mọi sự cố.
  - Kế hoạch phải xác định rõ ràng quy trình cần tuân thủ trong trường hợp xảy ra sự cố và đề cập cụ thể đến các đội sẽ hành động để khắc phục sự cố.

4.3 Ứng phó sự cố

- Kế hoạch ứng phó sự cố cần có câu trả lời cho câu hỏi "Ai chịu trách nhiệm ứng phó khi xảy ra sự cố?"

  ==> Nhóm ứng phó sự cố (Incident Response Team).
- Kế hoạch ứng phó sự cố cũng nên tính đến việc người phát hiện ra vấn đề rất có thể không có khả năng khắc phục nó và do đó, người đó sẽ cần phải báo cáo vấn đề.
- Việc chỉ định cách thức và địa điểm báo cáo sự cố là điểm khởi đầu tốt cho nhiều kế hoạch ứng phó sự cố.
- Chu kỳ ứng phó sự cố thường gồm 3 giai đoạn:
  - Chuẩn bị (Prepare): thực hiện trước khi tấn công/xâm nhập xảy ra
  - Phát hiện (Detect): thực hiện trong khi tấn công/xâm nhập xảy ra
  - Ứng phó (Respond): thực hiện sau khi tấn công/xâm nhập xảy ra.

Chu kỳ ứng phó sự cố



Chu kỳ ứng phó sự cố

- Các bước của Chu kỳ ứng phó sự cố:
  - Preparation (Chuẩn bị):
    - Xem xét, đánh giá kỹ lưỡng các chính sách bảo mật chịu trách nhiệm cung cấp thông tin cho kế hoạch ứng phó sự cố;
    - Gồm việc đánh giá rủi ro với các tài sản quan trọng
    - Vạch ra một kế hoạch liên lạc rõ ràng và một tài liệu nêu rõ vai trò và trách nhiệm được phân công rõ ràng trong trường hợp xảy ra sự cố an ninh
    - Xây dựng Nhóm ứng phó sự cố.

Chu kỳ ứng phó sự cố

- Các bước của Chu kỳ ứng phó sự cố:
  - Detection (Phát hiện):
    - Thực hiện giám sát, phân tích và phát hiện các vi phạm và sự cố bảo mật
    - Ngay khi phát hiện được một sự cố tiềm ẩn, Nhóm ứng phó sự cố phải tìm thêm bằng chứng giúp hiểu được bản chất, loại hình và mức độ nghiêm trọng của sự cố.
    - Nhóm cũng phải ghi lại tất cả các hành động được thực hiện.
      - Tài liệu ghi chép phải chi tiết và chứa thông tin rõ ràng như “ai, khi nào, ở đâu, tại sao và như thế nào” về vụ việc.

Chu kỳ ứng phó sự cố

- Các bước của Chu kỳ ứng phó sự cố:
  - Containment (Ngăn chặn):
    - Ngay sau khi nhóm phát hiện ra sự cố, hành động tiếp theo là ngăn chặn sự cố để có thể ngăn chặn mọi thiệt hại thêm.
    - Việc ngăn chặn có thể là ngắn hạn hoặc dài hạn:
      - Ngăn chặn ngắn hạn có thể là một bước đơn giản để cô lập một mạng cụ thể nơi xảy ra cuộc tấn công.
      - Ngăn chặn dài hạn có thể bao gồm việc sử dụng các bản sửa lỗi ngắn hạn và áp dụng chúng cho mạng bị ảnh hưởng để đảm bảo tính liên tục của quá trình vận hành trong khi các hệ thống mới được xây dựng lại.

Chu kỳ ứng phó sự cố

- Các bước của Chu kỳ ứng phó sự cố:
  - Eradication (Loại bỏ):
    - Bước tiếp theo của nhóm ứng phó sự cố là xác định nguyên nhân cốt lõi của sự cố hoặc mối đe dọa và thực hiện các hành động khắc phục nhanh chóng để ngăn chặn bất kỳ sự cố nào xảy ra trong tương lai.
    - Ví dụ: nếu lỗi xảy ra do quy trình xác thực yếu thì quy trình xác thực cần được thực hiện mạnh mẽ ngay lập tức.

Chu kỳ ứng phó sự cố

- Các bước của Chu kỳ ứng phó sự cố:
  - Recovery (Phục hồi):
    - Thực hiện các bước để khôi phục hệ thống bị ảnh hưởng và tiếp tục hoạt động có giám sát kỹ lưỡng để ngăn chặn bất kỳ sự cố nào tái diễn.
    - Giai đoạn này cũng liên quan đến việc đưa ra các quyết định quan trọng về thời điểm thích hợp để khôi phục hoạt động, phương pháp và thời gian giám sát hệ thống bị ảnh hưởng trong quá trình sản xuất để đảm bảo hoạt động bình thường.

Chu kỳ ứng phó sự cố

- Các bước của Chu kỳ ứng phó sự cố:
  - Post-incident follow-up (Xử lý sau sự cố):
    - Đây là giai đoạn phải được hoàn thành trong vòng 2 tuần kể từ khi xảy ra sự cố.
    - Giai đoạn này nhằm mục đích vá mọi lỗ hổng đã liệt kê mà không thể vá trước đó và đưa ra đánh giá toàn diện về sự cố về lý do xảy ra cũng như các hành động được thực hiện để khắc phục và loại bỏ sự cố.
    - Gồm các phân tích, đánh giá về các hành động được thực hiện để xác định rõ ràng hành động nào hiệu quả và hành động nào là cải tiến.

7 gợi ý xây dựng kế hoạch ứng phó sự cố

7 gợi ý xây dựng kế hoạch ứng phó sự cố

- Establish an IR Team (Thành lập nhóm ứng phó sự cố)
- Conduct Threat Analysis (Phân tích các mối đe dọa)
- Outline Quick Response Guidelines (Phác thảo các định hướng phản ứng nhanh)
- Develop Procedures for External Communication (Xây dựng quy trình trao đổi thông tin với bên ngoài)
- Train Employees (Đào tạo nhân viên)
- Test IR Plan (Kiểm tra kế hoạch ứng phó sự cố)
- Learn (Rút kinh nghiệm từ các sự cố trong quá khứ).

4.4 Phục hồi sau sự cố và tiếp tục hoạt động

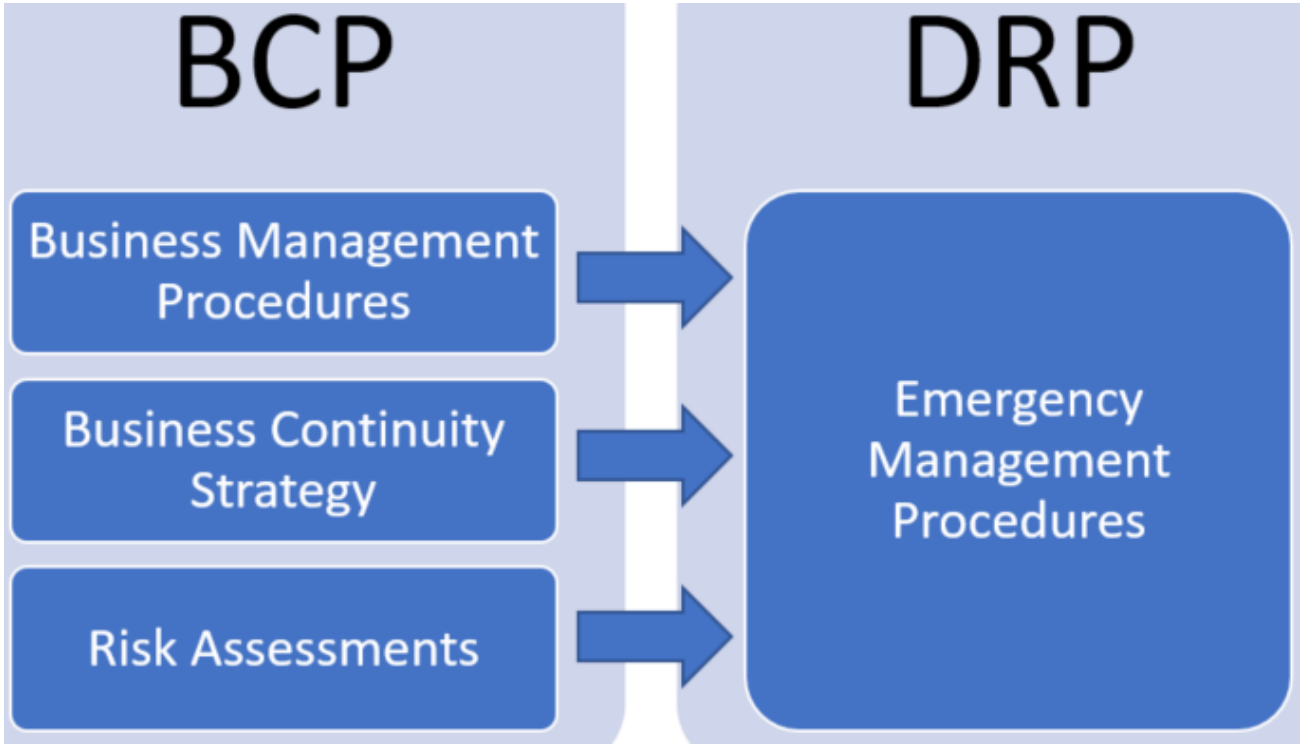
- Giới thiệu
- Phục hồi sau sự cố (Disaster recovery)
- Lập kế hoạch tiếp tục hoạt động (Business continuity planning)
- Sao lưu dữ liệu (Backup).

Phục hồi sau sự cố và tiếp tục hoạt động - Giới thiệu

- Phục hồi sau sự cố liên quan đến việc khôi phục các hệ thống kỹ thuật của tổ chức, như máy tính, phần mềm, mạng, dữ liệu sau khi sự cố xảy ra.
- Lập kế hoạch tiếp tục hoạt động liên quan đến các qui trình khôi phục hoạt động bình thường của tổ chức, các chức năng của hạ tầng nghiệp vụ và khôi phục hoạt động của nhân viên tại văn phòng.
  - Kế hoạch phục hồi sau sự cố là 1 phần của Kế hoạch tiếp tục hoạt động.

Phục hồi sau sự cố và tiếp tục hoạt động - Giới thiệu

Phục hồi sau sự cố và tiếp tục hoạt động - Giới thiệu



Phục hồi sau sự cố và tiếp tục hoạt động - Giới thiệu

Phục hồi sau sự cố

- Để có thể phục hồi sau sự cố một cách hiệu quả, cần lập kế hoạch phục hồi sau sự cố (Disaster recovery plan - DRP).
- Kế hoạch phục hồi sau sự cố là một cách tiếp cận có cấu trúc, được ghi thành văn bản, mô tả cách một tổ chức có thể nhanh chóng tiếp tục công việc sau một sự cố ngoài ý muốn.
- DRP là một phần thiết yếu của kế hoạch kinh doanh liên tục (Business continuity plan - BCP).
  - Nó được áp dụng cho các khía cạnh của một tổ chức phụ thuộc vào cơ sở hạ tầng CNTT.
  - DRP nhằm mục đích giúp tổ chức giải quyết tình trạng mất dữ liệu và khôi phục chức năng hệ thống để tổ chức có thể hoạt động sau sự cố, ngay cả khi tổ chức đó hoạt động ở mức tối thiểu.

Phục hồi sau sự cố

- Kế hoạch bao gồm các bước nhằm giảm thiểu ảnh hưởng của sự cố để tổ chức có thể tiếp tục hoạt động hoặc nhanh chóng khôi phục các chức năng quan trọng.
- Thông thường, DRP liên quan đến việc phân tích các quy trình kinh doanh và nhu cầu liên tục.
- Trước khi lập kế hoạch chi tiết, tổ chức thường thực hiện phân tích tác động kinh doanh (BIA) và phân tích rủi ro (RA), đồng thời thiết lập các mục tiêu phục hồi.

Kế hoạch phục hồi sau sự cố

- Kế hoạch phục hồi sau sự cố gồm các bước:
  - Risk Assessment (Đánh giá rủi ro):
  - Business Impact Analysis (Phân tích tác động kinh doanh):
  - Plan Development (Xây dựng kế hoạch):
  - Plan Testing (Kiểm tra kế hoạch):
  - Plan Maintenance (Bảo trì kế hoạch):

Kế hoạch phục hồi sau sự cố

- Kế hoạch phục hồi sau sự cố gồm các bước:
  - Risk Assessment (Đánh giá rủi ro):
    - Nhận dạng các rủi ro, đe dọa có thể gây gián đoạn hoạt động bình thường của tổ chức, như thảm họa tự nhiên, tấn công mạng, mất điện...
    - Giúp phân loại, xếp hạng rủi ro và các chức năng trọng yếu.
  - Business Impact Analysis (BIA - Phân tích tác động kinh doanh):
    - Đánh giá ảnh hưởng của các rủi ro, đe dọa đối với các chức năng trọng yếu của tổ chức
    - Phân tích này giúp xác định mục tiêu về thời gian và điểm phục hồi của từng vị trí được yêu cầu.

Kế hoạch phục hồi sau sự cố

- Kế hoạch phục hồi sau sự cố gồm các bước:
  - Plan Development (Xây dựng kế hoạch):
    - Tùy thuộc vào đánh giá rủi ro và BIA, kế hoạch này phác thảo các thủ tục, chính sách và chiến lược trước, trong và sau sự cố.
    - Kế hoạch này bao gồm các bước sao lưu và khôi phục dữ liệu chi tiết, khôi phục cơ sở hạ tầng, kế hoạch liên lạc, kế hoạch sơ tán và ứng phó khẩn cấp cũng như thử nghiệm và cập nhật chúng.
  - Plan Testing (Kiểm tra kế hoạch):
    - Đảm bảo tính hiệu quả trong các tình huống thực tế.
    - Các bài kiểm tra bao gồm các bài tập trên bàn, hướng dẫn từng bước, mô phỏng và thử nghiệm toàn diện.
    - Kết quả kiểm tra xác định những lỗ hổng trong đó và thực hiện những cải tiến cần thiết.

Kế hoạch phục hồi sau sự cố

- Kế hoạch phục hồi sau sự cố gồm các bước:
  - Plan Maintenance (Bảo trì kế hoạch):
    - Kế hoạch cần được xem xét và cập nhật thường xuyên để duy trì tính phù hợp và thiết thực.
    - Điều này bao gồm cập nhật thông tin liên hệ, sửa đổi quy trình khôi phục dựa trên những thay đổi trong cơ sở hạ tầng CNTT của tổ chức và kết hợp các bài học rút ra từ các thử nghiệm trước đó hoặc sự cố thực tế.

Kế hoạch phục hồi sau sự cố

- Một số mục cần thiết trong Kế hoạch phục hồi sau sự cố:
  - Thông tin liên hệ khẩn cấp : Bao gồm danh sách các liên hệ khẩn cấp của nhân viên, nhà cung cấp và khách hàng, cùng với vai trò và trách nhiệm của họ trong sự cố.
  - Dữ liệu và chức năng quan trọng : Xác định các chức năng và dữ liệu thiết yếu và ưu tiên theo tầm quan trọng của chúng đối với tổ chức. Điều này sẽ giúp xác định mục tiêu thời gian phục hồi (RTO) và mục tiêu điểm khôi phục (RPO) của từng chức năng.
  - Quy trình sao lưu : Xác định quy trình sao lưu cho dữ liệu và hệ thống quan trọng, bao gồm tần suất, thời gian lưu giữ và vị trí lưu trữ. Điều này sẽ bao gồm cả bản sao lưu tại chỗ và ngoại vi.

Kế hoạch phục hồi sau sự cố

- Một số mục cần thiết trong Kế hoạch phục hồi sau sự cố:
  - Quy trình khôi phục : Phát triển các quy trình khôi phục chi tiết cho từng chức năng quan trọng, bao gồm trình tự khôi phục, các nguồn lực cần thiết và nhân sự chịu trách nhiệm cho từng bước.
  - Kế hoạch liên lạc : Nêu rõ cách liên lạc với nhân viên, khách hàng, nhà cung cấp và các bên liên quan trước, trong và sau thảm họa. Điều này nên bao gồm các phương pháp liên lạc thay thế và hệ thống liên lạc dự phòng.
  - Quy trình kiểm tra và bảo trì : Kiểm tra kế hoạch thường xuyên để đảm bảo rằng nó hiệu quả và cập nhật. Điều này sẽ bao gồm cả bài tập trên bàn và mô phỏng thực tế. Kế hoạch cũng cần được xem xét và cập nhật định kỳ để phản ánh những thay đổi trong môi trường hoạt động.

Kế hoạch phục hồi sau sự cố

- Yêu cầu về nguồn lực : Xác định các nguồn lực cần thiết, chẳng hạn như thiết bị, phần mềm và nhân sự, cần thiết để thực hiện kế hoạch. Điều này bao gồm việc xác định các nhà cung cấp và nhà cung cấp dự phòng cũng như mọi hợp đồng và thỏa thuận.
- Đào tạo và nâng cao nhận thức : Đào tạo nhân viên về vấn đề phục hồi sau sự cố cũng như vai trò và trách nhiệm của họ trong khi sự cố xảy ra. Điều này nên bao gồm các buổi đào tạo thường xuyên và các chiến dịch nâng cao nhận thức.
- Đánh giá rủi ro : Xác định các mối đe dọa và phát triển chiến lược quản lý rủi ro bổ sung cho các mối đe dọa.

Lập kế hoạch tiếp tục hoạt động

- Các thành phần chính của Lập kế hoạch tiếp tục hoạt động:
  - Khởi động kế hoạch
  - Phân tích tác động hoặc đánh giá rủi ro kinh doanh
  - Phát triển các chiến lược phục hồi
  - Diễn tập hoặc thực hành kế hoạch khắc phục sự cố và kinh doanh liên tục.

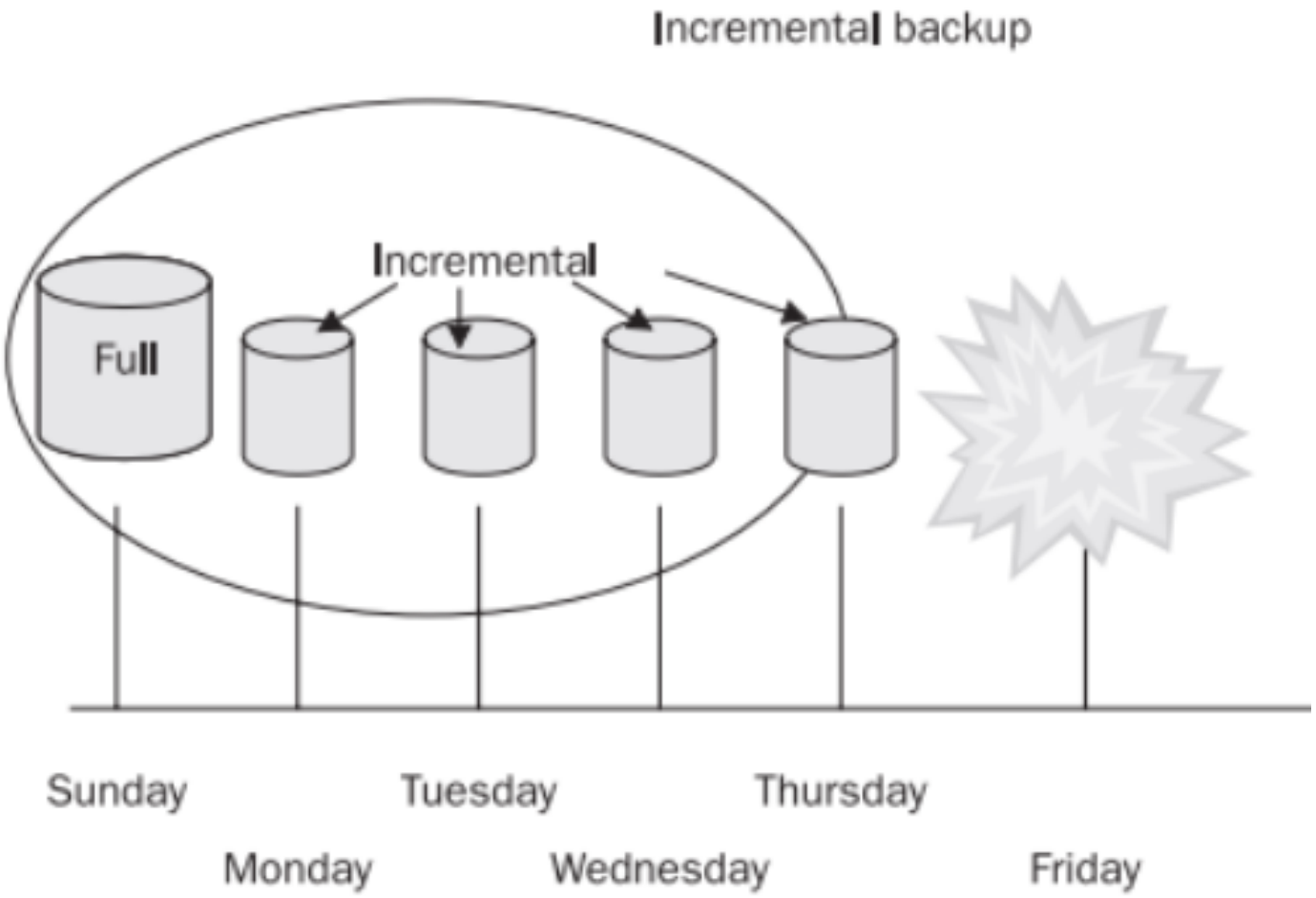
Sao lưu dữ liệu (Backup)

- Sao lưu dữ liệu là chủ động thực hiện việc sao chép dữ liệu của cá nhân, tổ chức sang một phương tiện lưu trữ vật lý khác nhằm chủ động đối phó với các sự cố về phần cứng, phần mềm, thao tác gây mất mát dữ liệu.
- Yêu cầu:
  - Sao lưu cần thực hiện định kỳ, tự động
  - Cần kiểm tra, đảm bảo chất lượng và an toàn của dữ liệu sao lưu.

Sao lưu dữ liệu

- Các dạng sao lưu:
  - Full (sao lưu đầy đủ): sao lưu toàn bộ dữ liệu, kể cả không có thay đổi.
  - Copy (sao chép): thực hiện sao chép dữ liệu trực tiếp từ đĩa này sang đĩa khác.
  - Incremental (sao lưu tăng dần): chỉ sao lưu phần thay đổi so với lần sao lưu gần nhất.
    - Sao lưu nhanh, nhưng khi khôi phục chậm do phải khôi phục lần lượt theo số lần sao lưu.
  - Differential (sao lưu thay đổi): chỉ sao lưu phần thay đổi so với lần sao lưu gần nhất có khởi tạo lại bit lưu trữ.
    - Sao lưu chậm hơn Incremental, nhưng khi khôi phục lại nhanh hơn do chỉ cần khôi phục sao lưu full và lần sao lưu cuối.

Sao lưu dữ liệu



Sao lưu dữ liệu