Giảng viên: Ths. Hồ Kim Cường
Email: hocuongit@gmail.com
Di động: 0904 361 245
https://www.facebook.com/hocuong24

CHƯƠNG I: TỔNG QUAN VỀN AN TOÀN THÔNG TIN

1.1 Cập nhật tình hình ATTT ở VN và trên thế giới

1.2 Các khái niệm ATTT

1.3 Các giải pháp bảo đảm an toàn thông tin

1.4 Hệ thống văn bản QPPL về ATTT, ANM

Cập nhật tình hình ATTT ở VN và trên thế giới

TẠI VIỆT NAM

TRÊN THẾ GIỚI

Cập nhật tình hình ATTT ở VN và trên thế giới

- Số lượng địa chỉ IP Botnet: Trung bình đã giảm liên tiếp trong những năm qua. Cuối năm 2022 giảm xuống dưới 500.000 địa chỉ/tháng (479.115 địa chỉ/tháng), giảm gần 50% so với 2021.
- Tấn công mạng vào các HTTT Việt Nam: Ghi nhận, cảnh báo và hướng dẫn xử lý 11.213 cuộc (3.930 cuộc Phishing, 1.524 cuộc Deface, 5.759 cuộc Malware), tăng 44,2% so với 2021.
- Hành vi lừa đảo trực tuyến trên không gian mạng thời gian qua trở nên phổ biến hơn. Bằng nhiều thủ đoạn tinh vi, phức tạp, thu thập trái phép thông tin cá nhân của người dân hoặc giả mạo các tổ chức tài chính, ngân hàng để lừa đảo chiếm đoạt tiền...:
  - Giả mạo thương hiệu (72,6%), giả mạo chiếm đoạt tài khoản trực tuyến (11,4%), hình thức khác (16%) như lừa đảo trúng thưởng, việc làm online, app cho vay…
  - Hình thức chủ yếu: Lập website/blog giả mạo, thư điện tử giả mạo, giả mạo cá nhân qua tài khoản trực tuyến.
  - Cục An toàn thông tin đã điều phối ngăn chặn 2.328 website lừa đảo, vi phạm pháp luật (1.342 website lừa đảo trực tuyến, 986 web/blog vi phạm). Bảo vệ 4,33 triệu người dân (~6,8% người dùng Internet Việt Nam) không truy cập website lừa đảo.

6 tháng đầu năm 2023: Việt Nam

- Trong tháng 5/2023:
  - Số lượng địa chỉ IP Botnet:, ghi nhận có 512.712 địa chỉ IP của Việt Nam nằm trong mạng botnet (giảm 11% so với tháng 04/2023) trong đó có 160 địa chỉ IP của cơ quan, tổ chức nhà nước.
  - Ghi nhận có 58.100 điểm yếu, lỗ hổng an toàn thông tin tại các HTTT của các cơ quan, tổ chức nhà nước.

(Theo báo cáo số 12/BC-CATTT ngày 21/6/2023 của Cục An toàn thông tin)

- Tấn công mạng vào các HTTT Việt Nam: Ghi nhận, cảnh báo và hướng dẫn xử lý 6.362 cuộc, giảm 4,2% so với cùng kỳ năm 2022 (6.641 cuộc tấn công).
- Tình hình lừa đảo trực tuyến tại Việt Nam tăng 64,78% so với cùng kỳ năm ngoái; tăng 37,82 % so với 6 tháng cuối năm 2022.

(Theo báo cáo của Cục An toàn thông tin tại Hội nghị Sơ kết 6 tháng đầu năm 2023 của Bộ TT&TT)

Tấn công Vietnamairlines ngày 29/7/2016

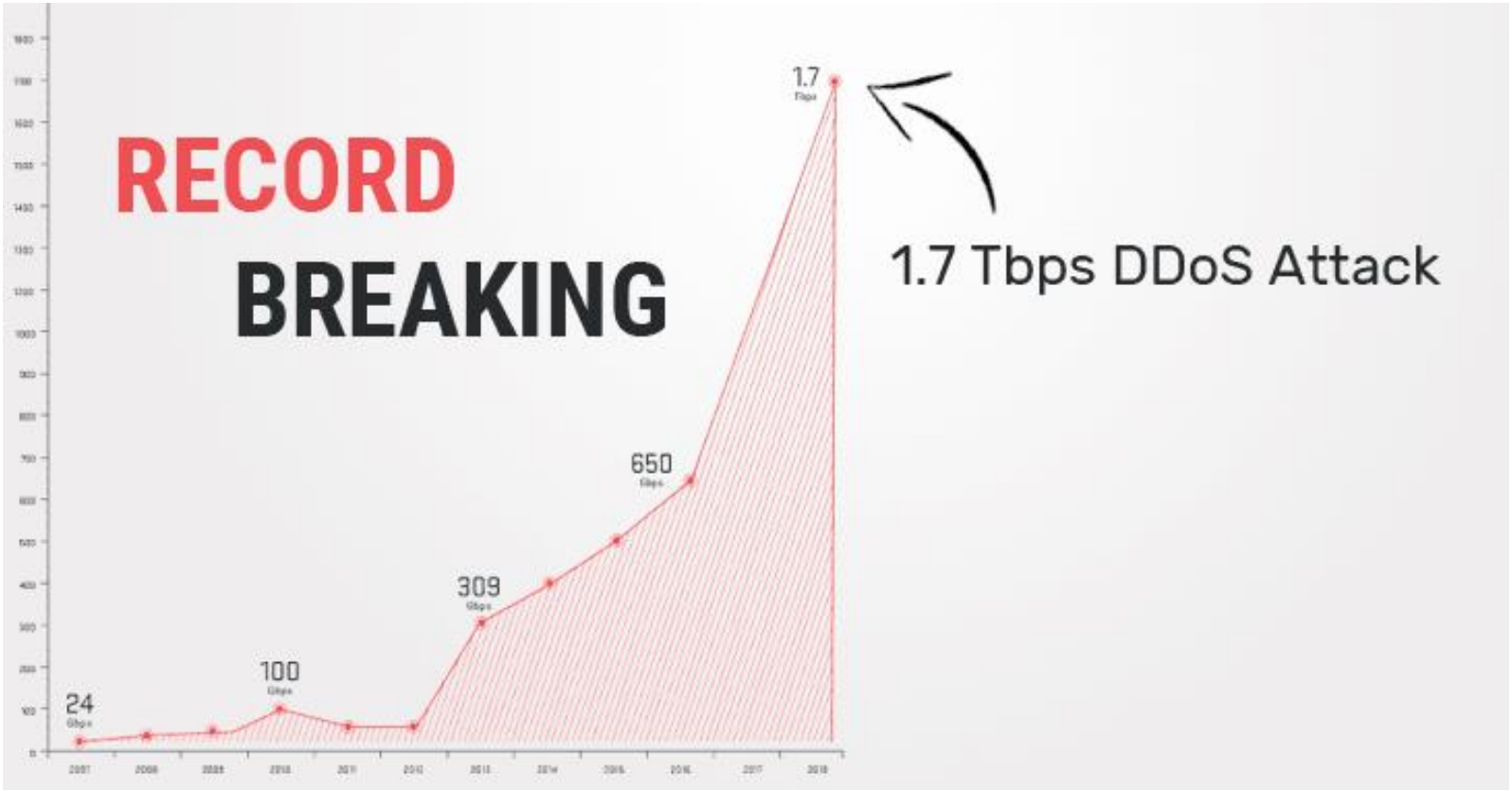
Tình hình ATTT trên thế giới

- Ngày 10/3/2021. Tờ báo Newsweek.com đăng tin. Quân đội Mỹ gửi các cảnh báo tới Trung Quốc về việc nước này sử dụng 1 triệu người làm "cỗ máy tin giả" nhằm phá hoại các giá trị của nền dân chủ Mỹ cũng như các nền dân chủ khác.

- Hành động được cho là nhằm chia cắt sợi dây liên kết giữa Mỹ với các nước châu Á và xây dựng quyền bá chủ của mình tại đây.

https://www.newsweek.com/chinas-1-million-strong-disinformation-machine-eroding-us-hegemony-admiral-1575057?utm_source=Flipboard&utm_medium=App&utm_campaign=Partnerships

TẤN CÔNG DDoS LỚN NHẤT TRONG LỊCH SỬ



Tấn công Memcached DDoS xảy ra vào tháng 3/2018

Nguồn: https://thehackernews.com/2018/03/ddos-attack-memcached.html

Các khái niệm ATTT

An toàn thông tin mạng là sự bảo vệ thông tin, hệ thống thông tin trên mạng tránh bị truy nhập, sử dụng, tiết lộ (Confidentiallity), gián đoạn (Availability), sửa đổi (Intergrity) hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin (Luật ATTT)

Nói cách khác, đảm bảo an toàn thông tin là đảm bảo ba thuộc tính sau:

- Tính bí mật (Confidentiallity)
- Tính toàn vẹn (Intergrity)
- Tính sẵn sàng (Availability)

Các khái niệm ATTT

- Tính bí mật (Confidentiality): Là đảm bảo thông tin chỉ được truy xuất bởi những đối tượng được cấp quyền.
- Tính toàn vẹn (Integrity): Là duy trì và đảm bảo tính chính xác và nhất quán của dữ liệu trên toàn bộ vòng đời của nó.
- Tính sẵn sàng (Availability): Thông tin phải sẵn có khi cần thiết, không bị gián đoạn đối với đối tượng có quyền truy xuất.

- An ninh mạng: là sự bảo đảm hoạt động trên không gian mạng không gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân. (Luật ANM)

Các khái niệm

Lỗ hổng bảo mật (vulnerable): Là điểm yếu của phần mềm, phần cứng, dữ liệu, quy trình, con người và các tài sản khác trong tổ chức, nó có thể bị khai thác bởi một hoặc nhiều mối đe dọa.

Mối đe doạ (Threat): là tác nhân gây ra sự cố an toàn thông tin cho hệ thống hoặc tổ chức.

Rủi ro (Risk): là khả năng (hay xác suất) xảy ra một sự cố an toàn thông tin và tác động (thiệt hại) mà sự cố đó để lại. Khả năng xảy ra một sự cố là do tác nhân đe dọa tác động đến các lỗ hổng bảo mật. Tác động là sự ảnh hưởng đến các thuộc tính C-I-A.

Một số ví dụ

Ví dụ về lỗ hổng bảo mật

- Người dùng, nhân viên kém nhận thức về ATTT
- Quy trình, chính sách thiếu, yếu, tuân thủ kém
- Các thành phần thiết bị công nghệ không được cập nhật, nâng cấp, rà soát lỗ hổng hoặc không được trang bị để bảo vệ theo nhiều lớp
- Thiếu các biện pháp kiểm soát vật lý, môi trường …

Ví dụ về mối đe dọa

- Lây nhiễm mã độc, hoặc các công cụ tấn công tinh vi
- Nhân viên vô tình hoặc cố ý trở thành mối đe dọa (kẻ tấn công),
- Attacker tấn công từ bên ngoài hoặc bên trong
- Trộm đột nhập đánh cắp tài sản thông tin
- Thiên tai, hỏa hoạn, động đất …

Một số ví dụ

(Bài tập: hãy cho biết đâu là ví dụ về vul/threat)

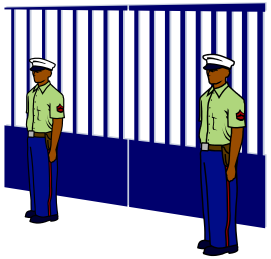
(1) Người dùng thiếu hiểu biết

(2) Trộm cắp. Phá hoại

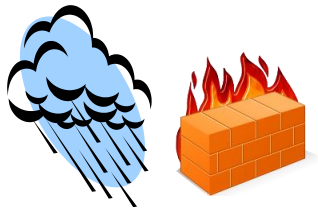
(3) Malware

(4) Lỗi hệ thống

(5) Lack Of Documentation



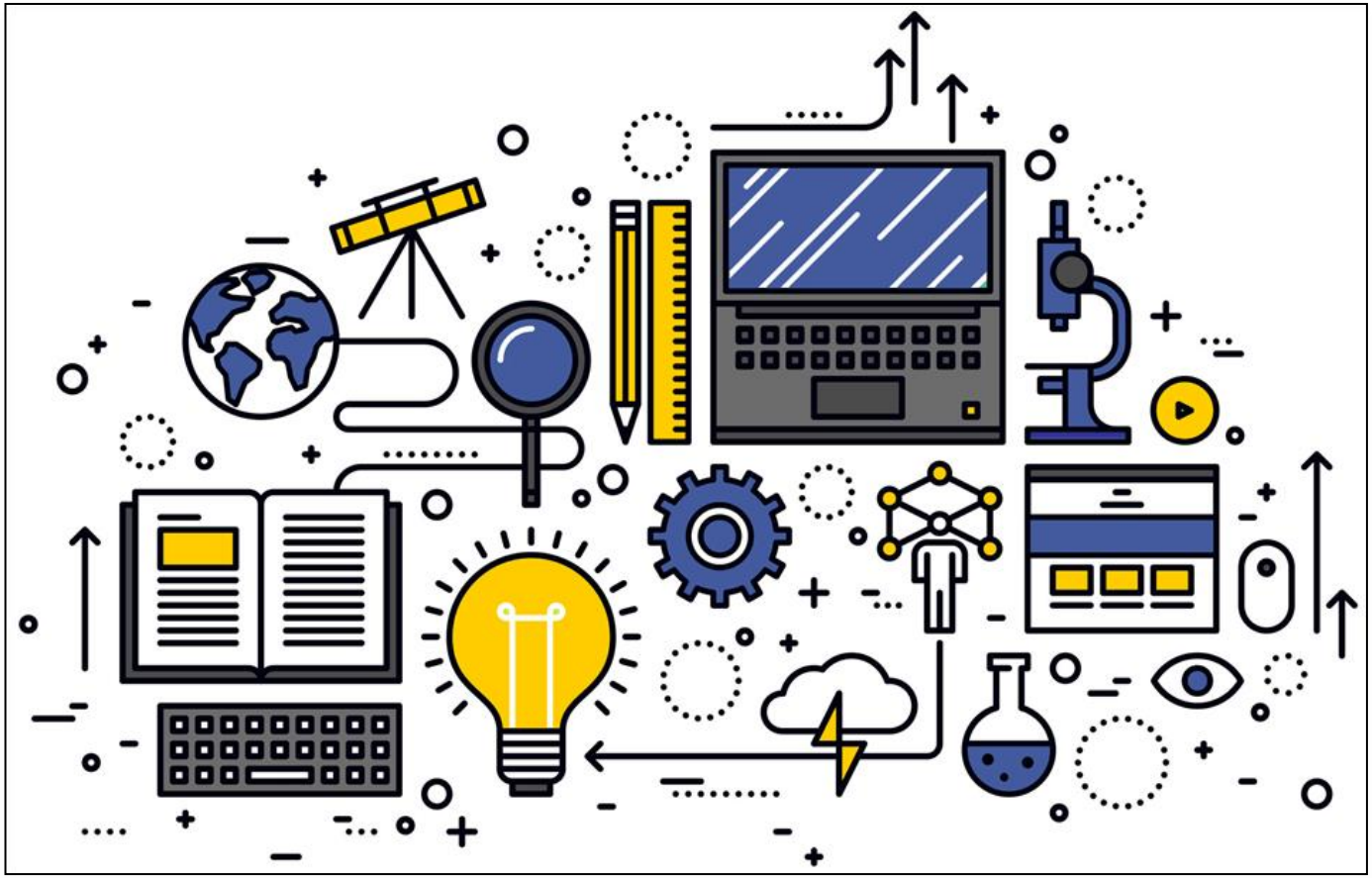
(6) Mất cảnh giác trong việc bảo vệ phần vật lý



(7) Thảm hoạ thiên nhiên, cháy nổ

Chuyển đổi số

Chuyển đổi số là quá trình thay đổi tổng thể và toàn diện của cá nhân, tổ chức về cách sống, cách làm việc và phương thức sản xuất dựa trên các công nghệ số.



1.2. Các giải pháp bảo đảm an toàn thông tin

Các giải pháp bảo đảm an toàn thông tin mạng

03 giải pháp bảo đảm an toàn hệ thống thông tin

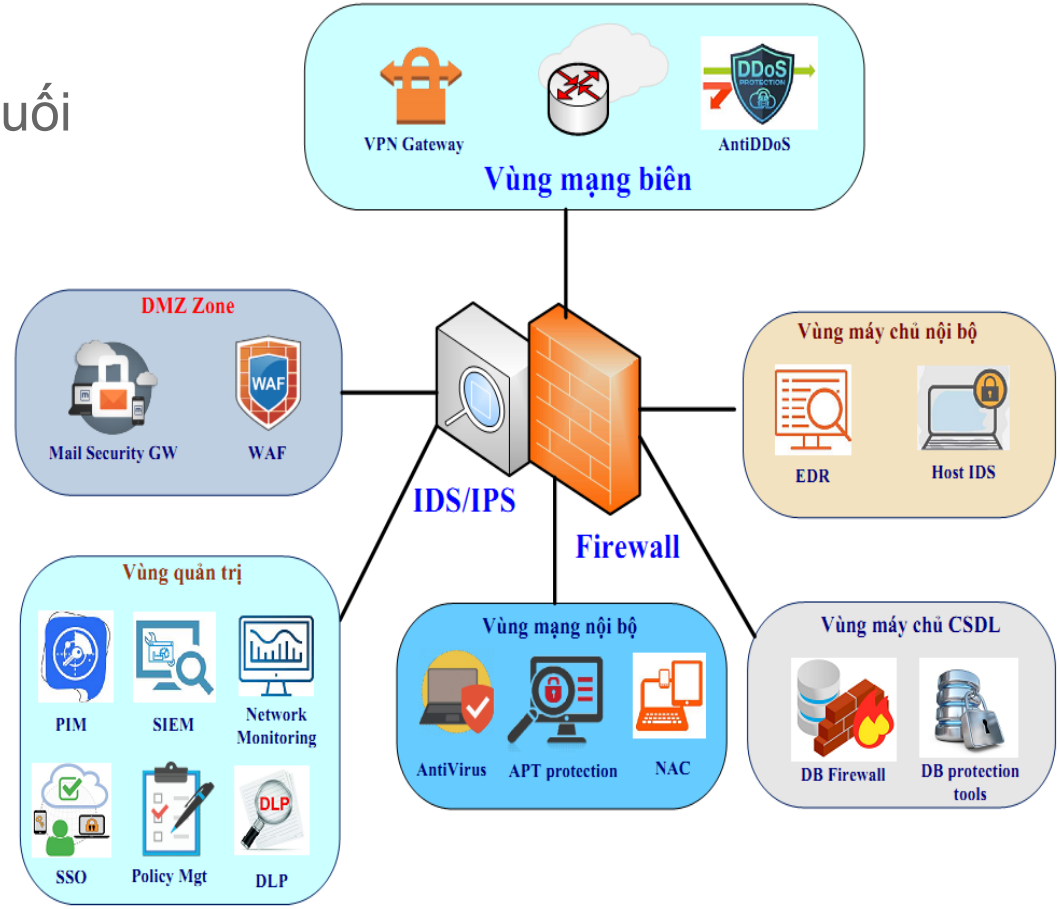
Công nghệ: là các phương án, giải pháp kỹ thuật được sử dụng để bảo đảm an tòa cho hệ thống thông tin.

Quy trình/Chính sách: bao gồm các quy trình, chính sách, quy định về ATTT (dựa trên các tiêu chuẩn và hiện trạng ATTT) được ban hành và tuân thủ bởi tổ chức.

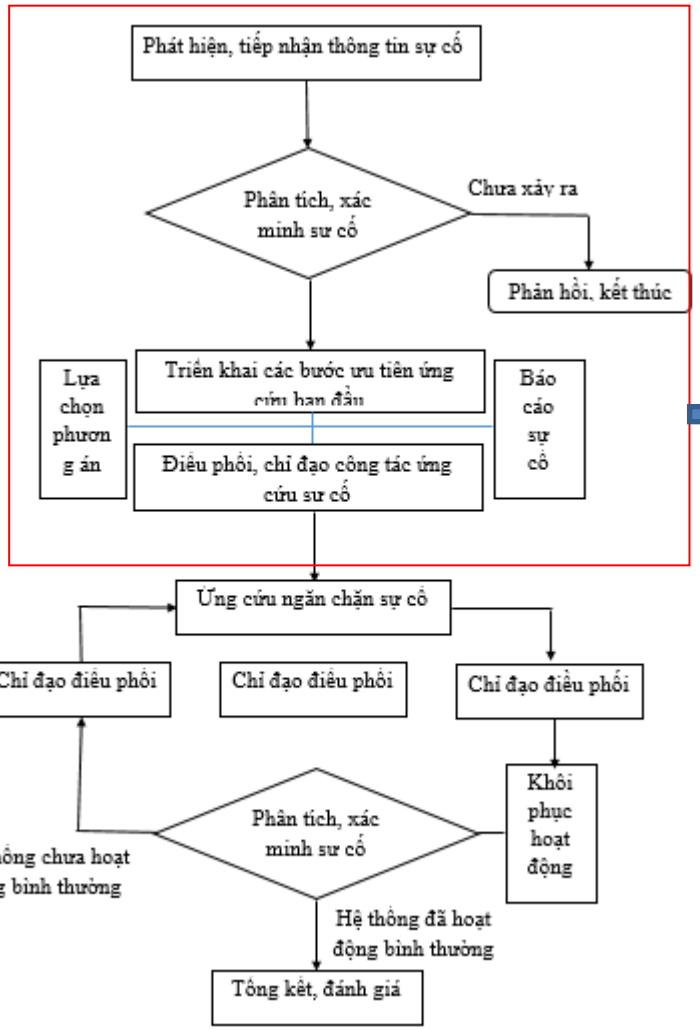
Con người: bao gồm lãnh đạo, người dùng, cán bộ kỹ thuật ATTT cần có kiến thức và kỹ năng phù hợp để thiết lập, tuân thủ quy trình/Chính sách, và áp dụng, vận hành các giải pháp công nghệ được triển khai bởi tổ chức.

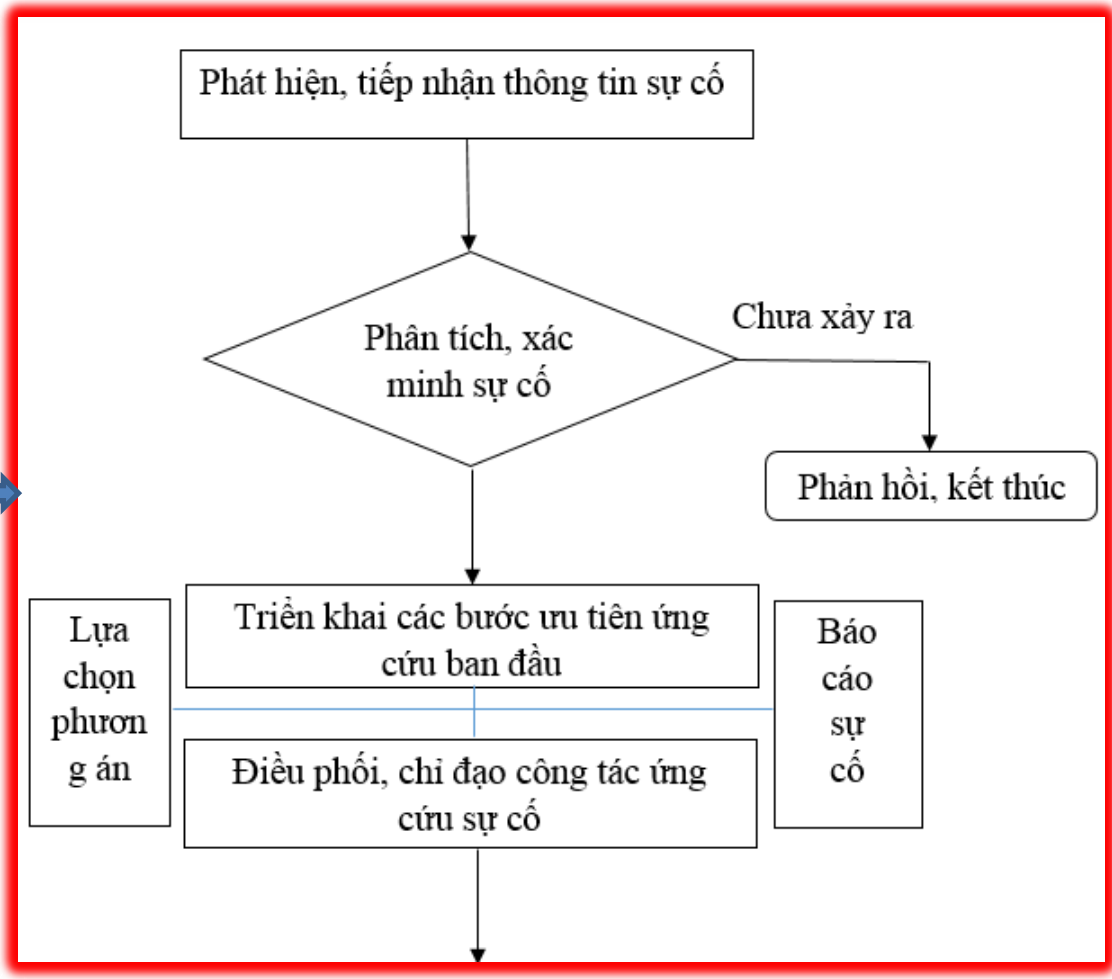
Giải pháp công nghệ

- An toàn cho thiết bị đầu cuối
- An toàn lớp mạng
- An toàn lớp ứng dụng
- Bảo vệ dữ liệu

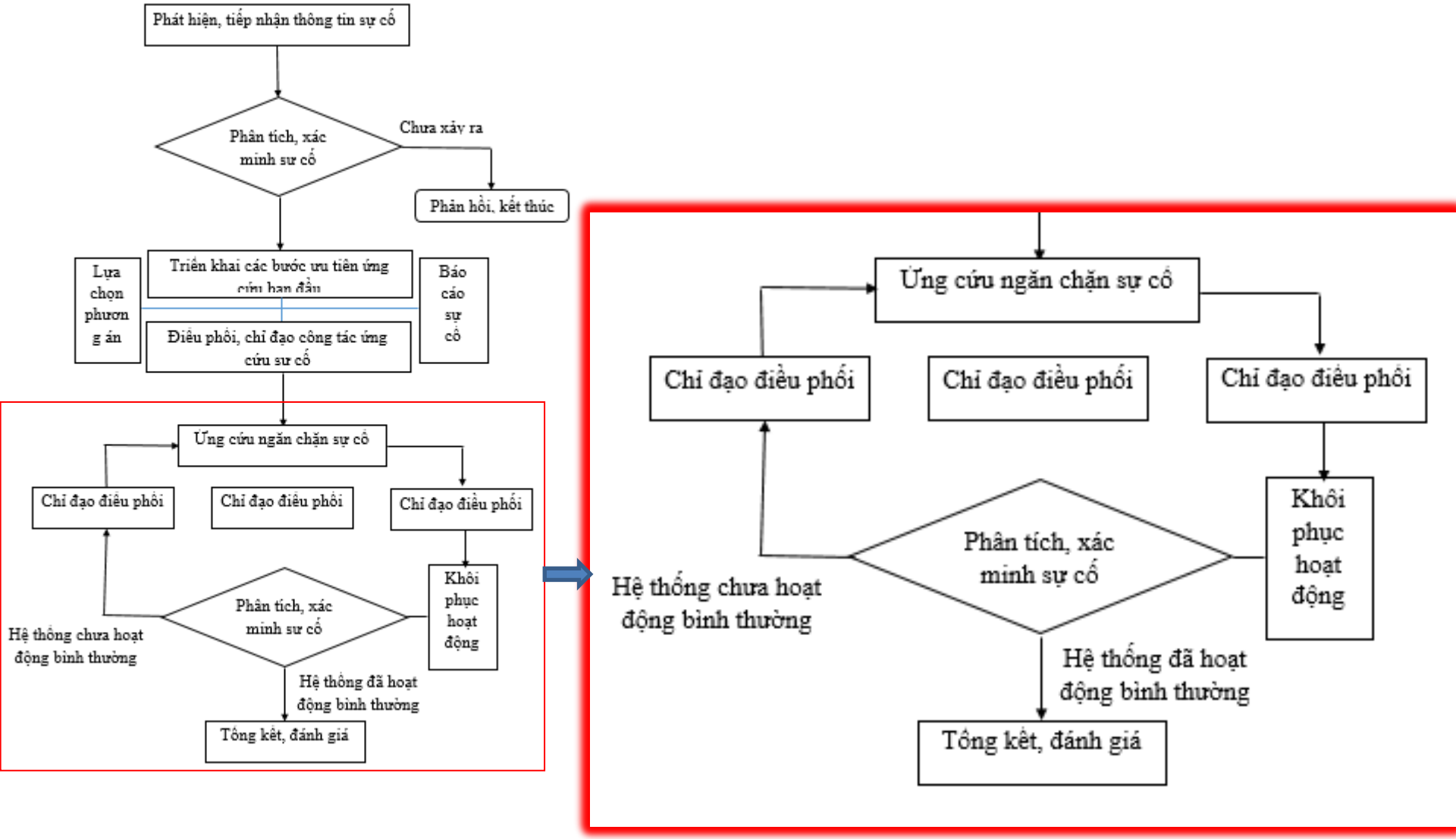


Quy trình ứng cứu sự cố (1)





Quy trình ứng cứu sự cố (2)



Chính sách ATTT

1. **Chính Sách Bảo Vệ Mật Khẩu (Password Protection Policy)**: Đặt ra các yêu cầu mật khẩu mạnh, xác định chu kỳ thay đổi mật khẩu và quy định việc sử dụng mật khẩu an toàn.
2. **Chính Sách Bảo Vệ Dữ Liệu (Data Protection Policy)**: Xác định cách tổ chức bảo vệ dữ liệu nhạy cảm và dữ liệu cá nhân thông qua việc áp dụng mã hóa, xác thực và kiểm soát truy cập.
3. **Chính Sách Quản Lý Thiết Bị Di Động (Mobile Device Management Policy)**: Điều này đặt ra hướng dẫn về việc sử dụng và bảo mật các thiết bị di động như điện thoại thông minh và máy tính bảng trong tổ chức.
4. **Chính Sách Quản Lý Sự Cố Bảo Mật (Incident Management Policy)**: Xác định cách tổ chức xử lý và phản ứng khi xảy ra sự cố bảo mật, bao gồm cách báo cáo, đánh giá và khắc phục sự cố.

…

Giải pháp con người trong bảo đảm ATTT

- **Nhận Thức và Đào Tạo**: Cung cấp đào tạo về an toàn thông tin cho nhân viên ở mọi cấp độ (gồm các cấp quản lý, người dùng, kỹ thuật IT & Security, khách hàng…). Giúp họ nhận biết các nguy cơ, hiểu về cách thức tấn công và biết cách ứng phó với chúng; biết vận hành và áp dụng các giải pháp kỹ thuật ATTT.
- **Cảnh Báo và Báo Cáo**: Khuyến khích người dùng cảnh giác và báo cáo ngay khi phát hiện sự bất thường hoặc nghi ngờ về vấn đề an toàn thông tin.
- **Xây dựng quy trình, chính sách:** bộ phận chuyên môn ATTT, Lãnh đạo của tổ chức xây dựng, ban hành quy trình chính sách phù hợp với các yêu cầu thực tế của tổ chức và tiêu chuẩn ATTT
- **Tuân Thủ Chính Sách**: Người dùng cần hiểu và tuân thủ các quy tắc và chính sách an toàn thông tin của tổ chức.
- **Kiểm Tra Kiến Thức:** Đánh giá, cập nhật kiến thức ATTT định kỳ để đảm bảo rằng mọi cấp độ luôn được trang bị hiểu biết mới nhất.

1.4 Hệ thống văn bản QPPL về ATTT, ANM

Hệ thống văn bản quy phạm pháp luật về an toàn thông tin

01 **Luật An toàn thông tin mạng (2015)**
86/2015/QH13.

07 **Nghị định của Chính phủ**
58/2016/NĐ-CP; 85/2016/NĐ-CP; 101/2016/NĐ-CP; 108/2016/NĐ-CP; 142/2016/NĐ-CP; 53/2018/NĐ-CP; 91/2020/NĐ-CP.

07 **Quyết định của Thủ tướng Chính phủ**
05/2017/QĐ-TTg; 632+1622/QĐ-TTg (2017); 1017/QĐ-TTg (2018); 1907/QĐ-TTg (2020); 21+830/QĐ-TTg (2021).

04 **Chỉ thị của Thủ tướng Chính phủ**
14/CT-TTg (2018); 14/CT-TTg (2019); 18/CT-TTg (2022); 23/CT-TTg (2022).

13 **Thông tư của các Bộ: TT&TT, QP, TC và NHNN**
20/2017/TT-BTTTT; 27/2017/TT-BTTTT; 31/2017/TT-BTTTT; 13/2018/TT-BTTTT; 121/2018/TT-BTC; 12/2019/TT-BTTTT; 09/2020/TT-NHNN; 95/2021/TT-BTC; 23/2022/TT-BQP; 10/2022/TT-BTTTT; 12/2022/TT-BTTTT.

01 **Luật An an ninh mạng (2018)**
24/2018/QH14.

03 **Nghị định của Chính phủ**
04/2019/NĐ-CP (m); 53/2022/NĐ-CP; 13/2023/NĐ-CP.

01 **Chiến lược An toàn, An ninh mạng quốc gia đến năm 2025, tầm nhìn 2030**
964/QĐ-TTg (2022).

LUẬT AN TOÀN THÔNG TIN MẠNG

Luật an toàn thông tin mạng gồm 08 Chương và 54 Điều quy định về hoạt động an toàn thông tin mạng, gồm:

Chương I. Những quy định chung

Chương II. Bảo đảm an toàn thông tin mạng

Chương III. Mật mã dân sự

Chương IV. Tiêu chuẩn, quy chuẩn kỹ thuật an toàn thông tin mạng

Chương V. Kinh doanh trong lĩnh vực an toàn thông tin mạng

Chương VI.Phát triển nguồn nhân lực an toàn thông tin mạng

Chương VII. Quản lý nhà nước về an toàn thông tin mạng

Chương VIII. Điều khoản thi hành