BỘ CÔNG AN
CỤC AN NINH MẠNG VÀ PHÒNG, CHỐNG TỘI PHẠM
SỬ DỤNG CÔNG NGHỆ CAO

AN NINH AN TOÀN THÔNG TIN TRONG CHUYỂN ĐỔI SỐ

MỤC TIÊU CHUYÊN ĐỀ

- Bối cảnh, tình hình an ninh mạng
- Rủi ro an toàn bảo mật dữ liệu
- Bảo vệ dữ liệu và quyền riêng tư
- Bảo vệ hệ thống thông tin, cơ sở dữ liệu, trang thông tin

"Hiểu rõ công việc, trí tuệ vượt máy móc
Công việc dập khuôn, máy móc vượt trí tuệ"

Bối cảnh Hiện tại và Mục tiêu

Tốc độ và Hiệu quả

Chuyển đổi số và AI mang lại khả năng xử lý nhanh chóng, tối ưu hóa quy trình và nâng cao hiệu suất hoạt động.

Rủi ro Tiềm ẩn

Song hành với lợi ích là các mối đe dọa bảo mật tinh vi hơn, đòi hỏi hệ thống phòng thủ vững chắc.

Dữ liệu là Tài sản

Mất dữ liệu không chỉ là thiệt hại tài chính mà còn ảnh hưởng đến uy tín và trách nhiệm pháp lý.

Mục tiêu của chuyên đề là nâng cao nhận thức về giá trị và rủi ro của dữ liệu, hiểu các mối đe dọa an ninh mạng mới trong bối cảnh AI, và nắm vững các biện pháp kỹ thuật, quản trị để bảo vệ hệ thống.

TẤN CÔNG MẠNG TĂNG MẠNH VỀ QUY MÔ VÀ SỐ LƯỢNG

Trong năm 2024 tại Việt Nam nhiều vụ việc nghiêm trọng đã xảy ra, nhắm vào các doanh nghiệp, tổ chức lớn như **VNDirect, PVOIL, Vietnam Post** và các cơ sở y tế, giáo dục....

- **46,15%** cơ quan, doanh nghiệp cho biết đã từng bị tấn công mạng ít nhất 1 lần trong năm
- **6,77%** thường xuyên bị tấn công
- **659.000** vụ tấn công mạng
- Các đơn vị trọng yếu đã có tới hơn **74.000 cảnh báo** tấn công mạng, **83 chiến dịch** tấn công có chủ đích APT

TẤN CÔNG CÓ CHỦ ĐÍCH APT LÀ HÌNH THỨC TẤN CÔNG PHỔ BIẾN NHẤT NĂM 2024.

26,14% các vụ tấn công trong năm là tấn công APT sử dụng mã độc gián điệp nằm vùng.

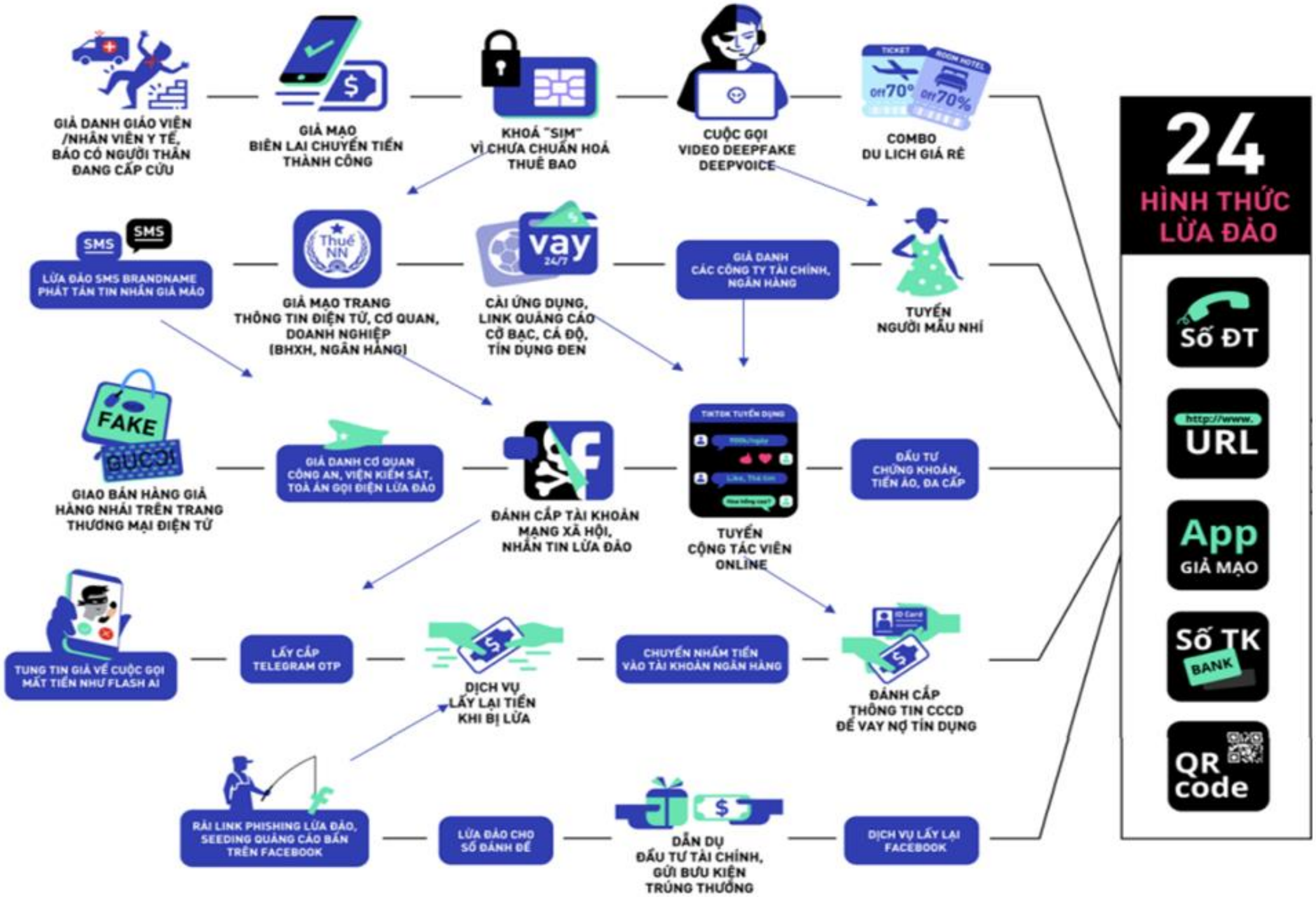
- Đánh cắp thông tin, dữ liệu
- Mối đe dọa bị mã hoá dữ liệu tống tiền

Theo khảo sát, có tới **14,59%** cơ quan, doanh nghiệp cho biết đã bị tấn công bằng mã độc ransomware trong năm qua

KHÔNG GIAN MẠNG

Không gian mạng **là mạng lưới kết nối của cơ sở hạ tầng công nghệ thông tin, bao gồm mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu; là nơi con người thực hiện các hành vi xã hội không bị giới hạn bởi không gian và thời gian**

Khoản 3 Điều 2 - Luật An ninh mạng


GIẢ DANH GIÁO VIÊN /NHÂN VIÊN Y TẾ, BÁO CÓ NGƯỜI THÂN ĐANG CẤP CỨU
GIẢ MẠO BIÊN LAI CHUYỂN TIỀN THÀNH CÔNG
KHOÁ "SIM" VÌ CHƯA CHUẨN HOÁ THUÊ BAO
CUỘC GỌI VIDEO DEEPFAKE DEEPVOICE
COMBO DU LỊCH GIÁ RẺ
LỪA ĐẢO SMS BRANDNAME PHÁT TÁN TIN NHẮN GIẢ MẠO
GIẢ MẠO TRANG THÔNG TIN ĐIỆN TỬ, CƠ QUAN, DOANH NGHIỆP (BHXH, NGÂN HÀNG)
CÀI ỨNG DỤNG, LINK QUẢNG CÁO CỜ BẠC, CÁ ĐỘ, TÍN DỤNG ĐEN
GIẢ DANH CÁC CÔNG TY TÀI CHÍNH, NGÂN HÀNG
TUYỂN NGƯỜI MẪU NHÍ
GIAO BÁN HÀNG GIẢ HÀNG NHÁI TRÊN TRANG THƯƠNG MẠI ĐIỆN TỬ
GIẢ DANH CƠ QUAN CÔNG AN, VIỆN KIỂM SÁT, TOÀ ÁN GỌI ĐIỆN LỪA ĐẢO
ĐÁNH CẮP TÀI KHOẢN MẠNG XÃ HỘI, NHẮN TIN LỪA ĐẢO
TUYỂN CỘNG TÁC VIÊN ONLINE
ĐẦU TƯ CHỨNG KHOÁN, TIỀN ẢO, ĐA CẤP
TUNG TIN GIẢ VỀ CUỘC GỌI MẤT TIỀN NHƯ FLASH AI
LẤY CẮP TELEGRAM OTP
DỊCH VỤ LẤY LẠI TIỀN KHI BỊ LỪA
CHUYỂN NHẦM TIỀN VÀO TÀI KHOẢN NGÂN HÀNG
ĐÁNH CẮP THÔNG TIN CCCD ĐỂ VAY NỢ TÍN DỤNG
RẢI LINK PHISHING LỪA ĐẢO, SEEDING QUẢNG CÁO BẨN TRÊN FACEBOOK
LỪA ĐẢO CHO SỐ ĐÁNH ĐỀ
DẪN DỤ ĐẦU TƯ TÀI CHÍNH, GỬI BƯU KIỆN TRÚNG THƯỞNG
DỊCH VỤ LẤY LẠI FACEBOOK
24 HÌNH THỨC LỪA ĐẢO
Số ĐT
URL
App GIẢ MẠO
Số TK
QR code

BẢO VỆ DỮ LIỆU VÀ QUYỀN RIÊNG TƯ

CÁC LOẠI DỮ LIỆU CẦN BẢO VỆ

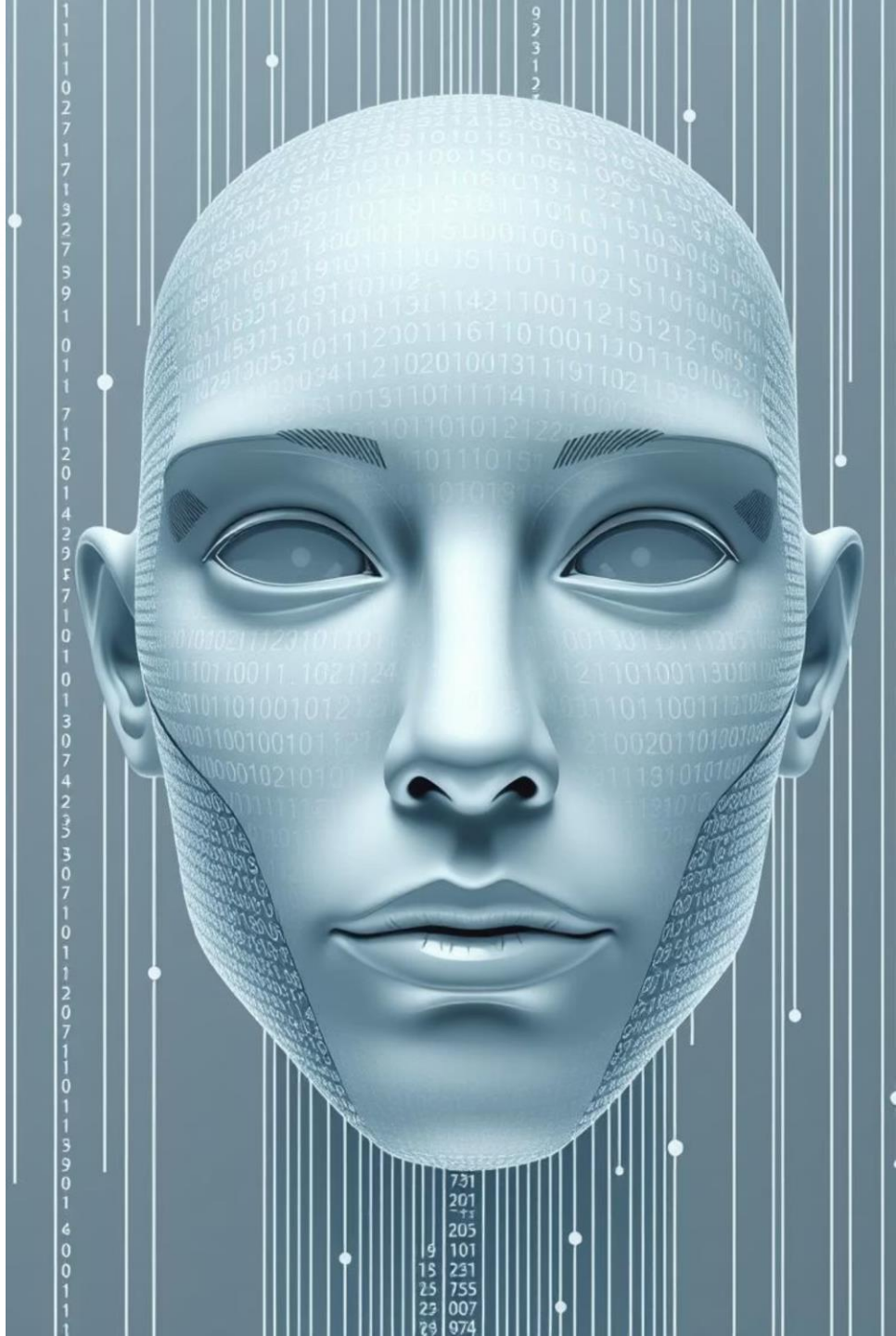
Để bảo vệ hiệu quả, chúng ta cần phân loại và nhận diện các nhóm dữ liệu có giá trị và mức độ nhạy cảm khác nhau.

Việc phân loại giúp ưu tiên các biện pháp bảo vệ phù hợp với từng loại dữ liệu, từ thông tin cá nhân cơ bản đến dữ liệu có tầm quan trọng chiến lược.

RỦI RO TỪ AI ĐỐI VỚI QUYỀN RIÊNG TƯ

AI, dù mang lại nhiều lợi ích, cũng tiềm ẩn những rủi ro đáng kể đối với quyền riêng tư cá nhân và dữ liệu.

- Deepfake & Giả mạo giọng nói: Công nghệ tổng hợp hình ảnh và âm thanh giả mạo ngày càng tinh vi, được sử dụng cho mục đích lừa đảo, gây tổn hại uy tín cá nhân và tổ chức.
- Data Poisoning: Kẻ tấn công chèn dữ liệu độc hại vào tập huấn luyện AI, làm sai lệch mô hình hoặc tạo lỗ hổng bảo mật để khai thác sau này.
- Model Inversion: Kỹ thuật này cho phép trích xuất thông tin nhạy cảm hoặc cá nhân từ mô hình AI đã được huấn luyện, ngay cả khi dữ liệu gốc đã được ẩn danh.



BIỆN PHÁP BẢO VỆ DỮ LIỆU & QUYỀN RIÊNG TƯ

1

Mã hóa Dữ liệu

Áp dụng mã hóa mạnh cho dữ liệu khi lưu trữ (data at rest) và khi truyền tải (data in transit) để ngăn chặn truy cập trái phép.

2

Ẩn danh hóa

Thực hiện các kỹ thuật ẩn danh hóa (anonymization) hoặc giả danh hóa (pseudonymization) dữ liệu trước khi sử dụng trong các mô hình AI hoặc phân tích.

3

Kiểm soát Truy cập

Triển khai kiểm soát truy cập dựa trên vai trò (RBAC), thuộc tính (ABAC) và xác thực đa yếu tố (MFA) để hạn chế quyền truy cập.

4

Chính sách Dữ liệu

Xây dựng và tuân thủ chính sách rõ ràng về lưu trữ, sao lưu và hủy dữ liệu an toàn, đảm bảo tuân thủ các quy định pháp luật.

RỦI RO BẢO MẬT TRONG CHUYỂN ĐỔI SỐ

Quá trình chuyển đổi số mở ra nhiều cánh cửa cho các mối đe dọa an ninh mạng truyền thống và mới nổi.

- Tấn công Phishing, Ransomware, Malware: Các hình thức tấn công phổ biến, nhằm lừa đảo thông tin, mã hóa dữ liệu đòi tiền chuộc, hoặc lây nhiễm phần mềm độc hại.
- Lỗ hổng Ứng dụng: Lỗ hổng trong API, SQL Injection, Cross-Site Scripting (XSS) là những điểm yếu thường bị khai thác để xâm nhập hệ thống và lấy cắp dữ liệu.
- Mối nguy từ Nhân viên Nội bộ: Các mối đe dọa đến từ nội bộ tổ chức, có thể do sơ suất, bất mãn hoặc bị lợi dụng, gây rò rỉ hoặc phá hoại dữ liệu.

GIẢM THIỂU RỦI RO BẢO MẬT DỮ LIỆU

1 Defense in Depth

Áp dụng nguyên tắc phòng thủ nhiều lớp, từ tường lửa, hệ thống phát hiện xâm nhập đến kiểm soát truy cập vật lý, để tạo ra các hàng rào bảo vệ vững chắc.

2 Zero Trust

Không tin tưởng bất kỳ ai hay bất kỳ thứ gì mặc định, mọi truy cập đều phải được xác minh nghiêm ngặt, áp dụng kiểm soát truy cập nhỏ nhất.

3 Đào tạo Nhận thức

Thường xuyên tổ chức các buổi đào tạo, nâng cao nhận thức về an toàn thông tin cho toàn bộ nhân viên, giúp họ nhận diện và phòng tránh các mối đe dọa.

4 Diễn tập & Đánh giá

Tổ chức diễn tập xử lý sự cố định kỳ và thực hiện đánh giá rủi ro thường xuyên để xác định, khắc phục lỗ hổng và cải thiện khả năng ứng phó.

BẢO VỆ HỆ THỐNG THÔNG TIN, CƠ SỞ DỮ LIỆU, TRANG THÔNG TIN

FIREWALL

- **Kiểm soát truy cập**, phân vùng mạng, ngăn chặn truy cập trái phép.
- Các loại tường lửa (**phần cứng, phần mềm, thế hệ mới** - NGFW).

HỆ THỐNG PHÁT HIỆN VÀ NGĂN CHẶN XÂM NHẬP (IDS/IPS)

- **IDS:** Giám sát lưu lượng mạng hoặc hoạt động hệ thống để phát hiện các hành vi bất thường, tấn công, xâm nhập nhưng không tự động ngăn chặn (chỉ cảnh báo).
- **IPS:** Ngoài việc phát hiện, còn có khả năng chặn ngay các cuộc tấn công hoặc hành vi xâm nhập trong thời gian thực.

SIEM (SECURITY INFORMATION AND EVENT MANAGEMENT)

- **Thu thập, lưu trữ, phân tích log** và sự kiện bảo mật từ nhiều nguồn trong hệ thống.
- Tự động **phát hiện các dấu hiệu bất thường, cảnh báo sự cố** bảo mật dựa trên quy tắc và phân tích hành vi

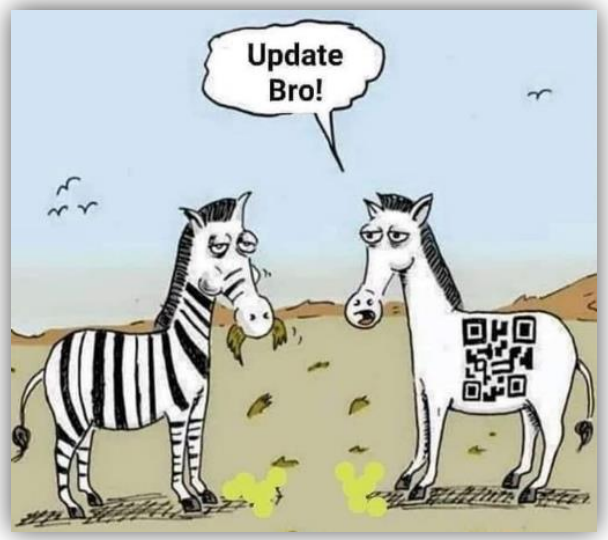
GIÁM SÁT VÀ KIỂM TRA AN NINH MẠNG

SOC (Security Operations Center)

- Đơn vị hoặc phòng ban chuyên trách giám sát, phát hiện và phản ứng với các sự cố an ninh mạng.
- Đội ngũ con người vận hành các công cụ như **SIEM, IDS/IPS, firewall** để giám sát và xử lý.

KIỂM TRA XÂM NHẬP PENETRATION TESTING

- **Mô phỏng tấn công** để đánh giá mức độ an toàn của hệ thống.
- **Phát hiện điểm yếu** để khắc phục trước khi bị khai thác thực tế



CẬP NHẬT VÁ LỖ HỔNG BẢO MẬT

- Duy trì hệ thống **luôn được cập nhật.**
- **Có quy trình quản lý** bản vá, tránh bị khai thác lỗ hổng.

ANTIVIRUS

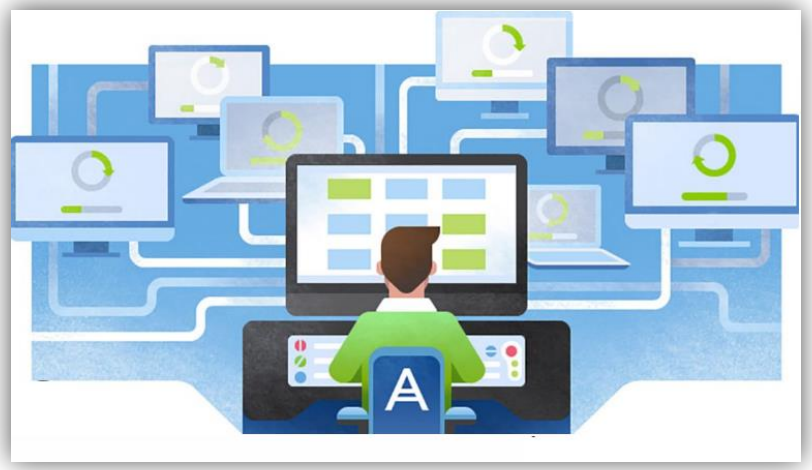
- **Phát hiện, ngăn chặn** virus, mã độc, ransomware...
- **Cập nhật** virus mới thường xuyên.

MÃ HÓA DỮ LIỆU

- Mã hóa khi **lưu trữ**, mã hóa khi **truyền tải**
- **Bảo mật** thông tin, bảo vệ bí mật doanh nghiệp, tuân thủ quy định pháp luật
- Đảm bảo **tính toàn vẹn và xác thực**
- **Ngăn chặn** tấn công và truy cập trái phép

XÁC THỰC HAI YẾU TỐ (2FA)

- **Tăng cường bảo vệ** tài khoản và hệ thống bằng lớp bảo mật thứ hai. Ví dụ 2FA: **SMS, app xác thực, token**
- **Ngăn lộ lọt dữ liệu** nếu mật khẩu bị đánh cắp.
- **Giảm thiểu nguy cơ tấn công** brute-force hoặc phishing
- **Bắt buộc** trong nhiều tiêu chuẩn an ninh (ISO 27001, PCI DSS, NIST...).



SAO LƯU DỮ LIỆU

- Đảm bảo **an toàn** dữ liệu, đảm bảo tính **toàn vẹn** của dữ liệu sao lưu, **phân loại** dữ liệu cần sao lưu
- Đảm bảo dữ **liệu luôn có bản sao dự phòng**.
- **Quy trình, tần suất** sao lưu, kiểm tra phục hồi dữ liệu.

BẢO VỆ HỆ THỐNG THÔNG TIN & CƠ SỞ DỮ LIỆU

1

Quản lý Tài khoản & Mật khẩu

Sử dụng mật khẩu mạnh, duy nhất và kích hoạt xác thực đa yếu tố (MFA) cho tất cả các tài khoản quan trọng.

2

Cập nhật & Vá lỗi

Thường xuyên cập nhật phần mềm, hệ điều hành và ứng dụng để vá các lỗ hổng bảo mật đã biết.

3

Mã hóa & Backup DB

Mã hóa cơ sở dữ liệu và thực hiện sao lưu định kỳ, đảm bảo khả năng phục hồi dữ liệu khi có sự cố.

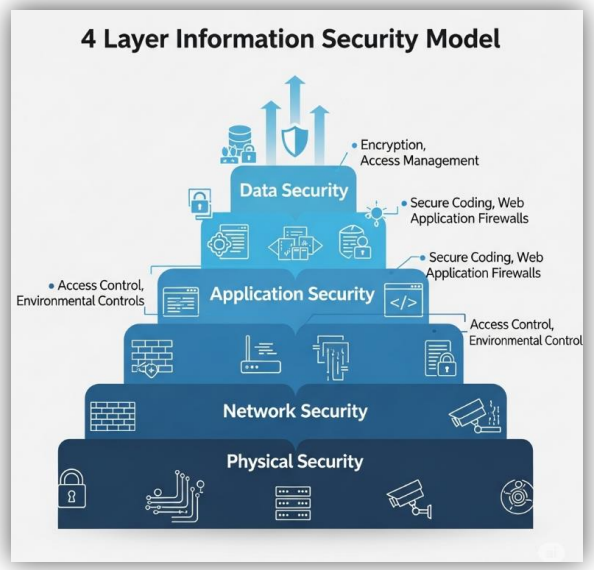
4

Giám sát Nhật ký

Thiết lập hệ thống giám sát nhật ký truy cập (logging) để phát hiện và cảnh báo kịp thời các hoạt động bất thường.

BẢO VỆ WEBSITE VÀ VẬN HÀNH AN TOÀN

- HTTPS & Chứng chỉ số: Luôn sử dụng HTTPS và đảm bảo chứng chỉ SSL/TLS hợp lệ để mã hóa lưu lượng truy cập web.
- Chống Tấn công Web: Triển khai các biện pháp bảo vệ chống DDoS, XSS, SQL Injection và các cuộc tấn công web phổ biến
- Kiểm duyệt & Quét mã độc: Thường xuyên kiểm tra nội dung và quét mã độc trên website
- Kế hoạch BCP/DRP: Xây dựng Quy trình vận hành chuẩn (SOP), hệ thống SIEM và Kế hoạch kinh doanh liên tục (BCP)/Phục hồi sau thảm họa (DRP).



ĐẢM BẢO AN TOÀN, AN NINH THÔNG TIN THEO MÔ HÌNH 4 LỚP

- **Lớp vật lý:** bảo vệ thiết bị, hạ tầng mạng, trung tâm dữ liệu.
- **Lớp mạng:** bảo vệ luồng dữ liệu, kiểm soát truy cập mạng, tường lửa, IDS/IPS.
- **Lớp ứng dụng:** bảo vệ phần mềm, hệ thống thông tin, bảo mật ứng dụng.
- **Lớp dữ liệu:** mã hóa, quản lý quyền truy cập, sao lưu dữ liệu.

CẤP ĐỘ	Ý NGHĨA	MỨC ĐỘ ẢNH HƯỞNG KHI BỊ TẤN CÔNG	VÍ DỤ HỆ THỐNG
CẤP 1	Thấp nhất	Ảnh hưởng không đáng kể đến hoạt động của cơ quan	Website giới thiệu thông tin công khai
CẤP 2	Trung bình	Ảnh hưởng giới hạn trong một bộ phận/cơ quan	Cổng dịch vụ công cấp sở, ngành
CẤP 3	Cao	Ảnh hưởng toàn bộ cơ quan, tác động đáng kể đến người dân	Hệ thống quản lý dữ liệu ngành y tế, giáo dục
CẤP 4	Rất cao	Ảnh hưởng phạm vi quốc gia, an ninh – quốc phòng	Cơ sở dữ liệu dân cư, tài chính quốc gia

ĐẢM BẢO AN TOÀN THÔNG TIN THEO CẤP ĐỘ

YÊU CẦU BẢO MẬT	CẤP 1–2	CẤP 3	CẤP 4
BẢO MẬT (CONFIDENTIALITY)	Phân quyền cơ bản, mật khẩu mạnh	Xác thực đa yếu tố (MFA), mã hóa dữ liệu	Mã hóa toàn diện, quản lý khóa chuyên biệt, kiểm soát truy cập nghiêm ngặt
TOÀN VẸN (INTEGRITY)	Kiểm tra checksum, sao lưu định kỳ	Giám sát thay đổi dữ liệu, chữ ký số	Hệ thống chống giả mạo, cơ chế kiểm soát thay đổi 4 mắt
SẴN SÀNG (AVAILABILITY)	Sao lưu cơ bản, dự phòng đơn giản	Dự phòng nóng/lạnh, giám sát 24/7	Trung tâm dữ liệu song song, khả năng chuyển đổi dự phòng tức thì
KIỂM SOÁT TRUY CẬP	Danh sách kiểm soát truy cập	RBAC/ABAC, định danh tập trung	Xác thực đa yếu tố kết hợp sinh trắc học
GIÁM SÁT AN NINH	IDS/Firewall cơ bản	SIEM + SOC giám sát liên tục	SOC quốc gia + phân tích mối đe dọa nâng cao (Threat Intelligence)


TRÂN TRỌNG CẢM ƠN