Góc nhìn toàn cảnh an toàn thông tin năm 2024

Cần Thơ, ngày 05/12/2024

Phạm Tuấn An
Cục An toàn thông tin

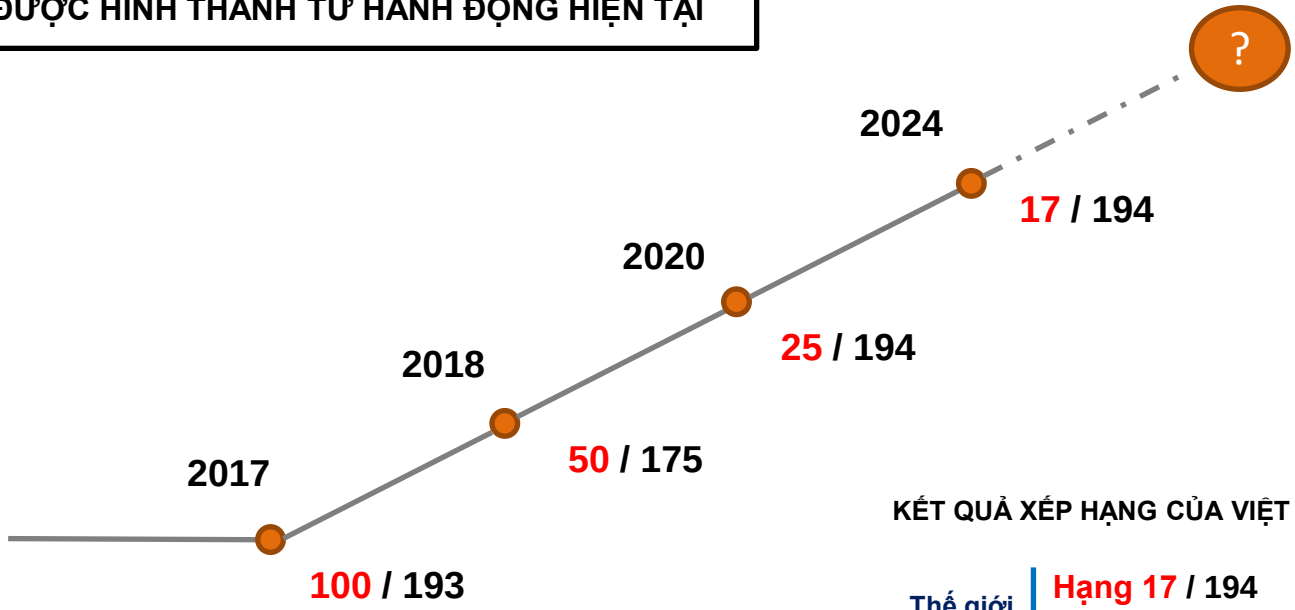
CỤC AN TOÀN THÔNG TIN
AUTHORITY OF INFORMATION SECURITY

NỘI DUNG

1. TÌNH HÌNH ATTTM 2024
2. HIỆN TRẠNG ATTT CỦA BỘ TN&MT
3. ĐỊNH HƯỚNG NĂM 2025

CHỈ SỐ AN TOÀN THÔNG TIN MẠNG TOÀN CẦU GCI 2024

**KẾT QUẢ XẾP HẠNG TRONG TƯƠNG LAI,
ĐƯỢC HÌNH THÀNH TỪ HÀNH ĐỘNG HIỆN TẠI**



KẾT QUẢ XẾP HẠNG CỦA VIỆT NAM: 99,74 / 100 ĐIỂM

Thế giới
Hạng 17 / 194
Nhóm 1 - Hình mẫu (46 quốc gia)

Khu vực Châu Á & TBD
04 / 38
Sau Hàn Quốc (100), Indonesia (100) và Singapore (99,86).

TÌNH HÌNH AN TOÀN THÔNG TIN MẠNG NĂM 2024

- Lừa đảo trực tuyến gia tăng.
- Tấn công mạng quy mô lớn, chuyên nghiệp.
- Phần mềm mã độc, ransomware.
- An toàn dữ liệu, xâm phạm quyền riêng tư.
- Thiếu tuân thủ quy định pháp luật về ATTTM.
- Thiếu hụt nguồn lực bảo đảm ATTTM.

NGUY CƠ

2025:

- 3.000 cuộc tấn công/giây.
- 12 mã độc/giây.
- 70 lỗ hổng/điểm yếu mới/ngày.

ĐỐI TƯỢNG

Đối tượng bị tấn công:

- **2025:** gấp 2,7 lần 2020.
- **2030:** gấp 7,5 lần 2020.

CÔNG NGHỆ

- **Lượng tử:** 100% ứng dụng mật mã phi đối xứng có thể bị phá vỡ.
- **AI:** dần thay thế con người. AI lĩnh vực ATTT đạt 38,2 tỉ $ năm 2026

CHỈ ĐẠO CỦA THỦ THƯỚNG CHÍNH PHỦ

Chỉ thị số 09/CT-TTg
Công điện 33/CĐ-TTg

(1) ATTT là bắt buộc, chiếm tối thiểu 10% kinh phí CĐS, CNTT;
(2) Hoàn thành phê duyệt cấp độ (9/2024) và triển khai đầy đủ phương án ATTT (12/2024) cho 100% HTTT;
(3) Tuân thủ quy định, quy trình ứng cứu sự cố, khôi phục hoạt động HTTT và chia sẻ kinh nghiệm, bài học.

(1) ATTT là bắt buộc, chiếm tối thiểu 10% kinh phí CĐS, CNTT;

(2) Hoàn thành phê duyệt cấp độ (9/2024) và triển khai đầy đủ phương án ATTT (12/2024) cho 100% HTTT;

(3) Tuân thủ quy định, quy trình ứng cứu sự cố, khôi phục hoạt động HTTT và chia sẻ kinh nghiệm, bài học.

Để đẩy mạnh công tác tuân thủ quy định pháp luật và tăng cường bảo đảm an toàn hệ thống thông tin theo cấp độ, Thủ tướng Chính phủ yêu cầu:

1. Bộ trưởng, Thủ trưởng cơ quan ngang bộ, cơ quan thuộc Chính phủ; Chủ tịch Ủy ban nhân dân các tỉnh, thành phố trực thuộc trung ương; Chủ tịch Hội đồng quản trị, Hội đồng thành viên, Tổng Giám đốc các tập đoàn, tổng công ty nhà nước, ngân hàng thương mại nhà nước, Ngân hàng Phát triển Việt Nam, Ngân hàng Chính sách xã hội, Ngân hàng Hợp tác xã Việt Nam và tổ chức tín dụng, tài chính nhà nước khác trên toàn quốc tập trung chỉ đạo thực hiện đồng bộ các giải pháp sau đây:

a) Trực tiếp chỉ đạo và phụ trách công tác bảo đảm an toàn thông tin trong hoạt động của cơ quan, địa phương mình; chịu trách nhiệm trước Thủ tướng Chính phủ và pháp luật nếu các đơn vị thuộc phạm vi quản lý không tuân thủ các quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ hoặc để xảy ra mất an toàn thông tin, lộ lọt thông tin, dữ liệu cá nhân, bí mật nhà nước.

d) Tổ chức rà soát, thống kê, cập nhật danh mục hệ thống thông tin thuộc phạm vi quản lý; bảo đảm 100% hệ thống thông tin từ cấp độ 1 đến cấp độ 5 (nếu có) đang vận hành phải được phê duyệt cấp độ an toàn hệ thống thông tin chậm nhất trong tháng 9 năm 2024 và triển khai đầy đủ phương án bảo đảm an toàn thông tin theo hồ sơ đề xuất cấp độ được phê duyệt chậm nhất trong tháng 12 năm 2024.

h) Định kỳ tổ chức hoạt động thanh tra, kiểm tra, đánh giá tuân thủ các quy định, giám sát việc thực hiện công tác bảo đảm an toàn thông tin theo cấp độ trong phạm vi quản lý, tối thiểu 01 lần/01 năm. Báo cáo kết quả thực hiện về Bộ Thông tin và Truyền thông trước ngày 25 tháng 12 hàng năm để tổng hợp, báo cáo Thủ tướng Chính phủ.

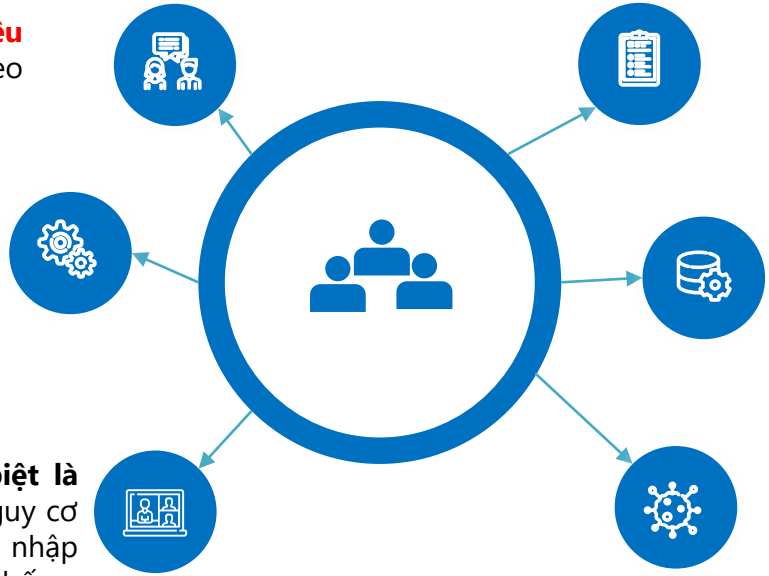
Công văn số 2516/BTTTT-CATTT ngày 27/6/2024 của Bộ trưởng B.TTTT gửi Bộ trưởng các bộ: Từ THỰC TIỄN rút ra NHẬN THỨC MỚI:

=> HTTT có thể bị tấn công mạng, xảy ra sự cố bất cứ kỳ lúc nào, để chủ động bảo vệ HTTT an toàn tuyệt đối là bất khả thi và vô cùng tốn kém. Vì vậy, B.TTTT hướng dẫn **06** giải pháp và trong đó có **02 trọng tâm**:

Định kỳ thực hiện sao lưu dữ liệu ngoại tuyến (offline). Sao lưu theo nguyên tắc 3-2-1

Triển khai giải pháp để sẵn sàng phục hồi nhanh. Đưa HTTT trở lại hoạt động bình thường trong vòng 24h

Triển kahi các giải pháp, đặc biệt là giám sát ATTT. Sớm phát hiện nguy cơ tấn công với 3 giai đoạn (1)xâm nhập HT; (2) nằm gián điệp trong hệ thống; (3) khởi tạo quá trình phá hoại hệ thống.



Phân tách, kiểm soát truy cập giữa các vùng mạng. Chuyển đổi sang hư ứng dùng các nền tảng, ứng dụng.

Giám sát, quản lý tài khoản quan trọng , quản trị HT bằng xác thực 2 lớp. Giảm thiểu thiệt hại trong trường hợp kẻ tấn c ông có được mật khẩu của tài khoản quả n trị nhưng cũng không thể chiếm quyền điều khiển HT

Rà soát, khắc phục các lỗi cơ bản Bộ TT&TT khuyến nghị lưu ý, khắc phục 14 lỗi cơ bản thường mắc phải để giải thiểu nguy cơ mất an toàn HTTT

HIỆN TRẠNG PHÊ DUYỆT HSĐXCĐ BỘ TN&MT

Số lượng HTTT: **101 HTTT** **01 HTTT cấp độ 4 chưa được vận hành (Quản lý đất đai MPLIS)**

Tỷ lệ phê duyệt HSĐXCĐ: **39%** **(39 HTTT/100 HTTT đang hoạt động)**

Tỷ lệ triển khai đầy đủ phương án bảo đảm ATHTTT theo cấp độ: **28%** **(28 HTTT/100 HTTT đang hoạt động)**

ĐỀ NGHỊ

- **Khẩn trương Phê duyệt và triển khai đầy đủ phướng án bảo đảm ATTT**
  - ❑ Phương án về quản lý
  - ❑ Phương án về kỹ thuật
- **Bảo đảm an toàn thông tin theo mô hình 4 lớp**
  - ❑ Giám sát, bảo vệ chuyên nghiệp
  - ❑ Định kỳ kiểm tra, đánh giá
- **Triển khai phương án sao lưu dự phòng và sẵn sàng phục hồi nhanh**
  - ❑ Sao lưu theo 3-2-1
  - ❑ Xây dựng phương án phục hồi nhanh trong 24h
- **Diễn tập thực chiến**
  - ❑ HTTT cấp độ 3 tối thiểu tổ chức diễn tập thực chiến 01 lần/ năm

NGÀNH TÀI NGUYÊN VÀ MÔI TRƯỜNG

Kinh doanh có điều kiện

Kinh doanh dịch vụ tư vấn điều tra, đánh giá đất đai

Kinh doanh dịch vụ xác định giá đất

Kinh doanh dịch vụ xác định giá đất

Kinh doanh dịch vụ khai thác, sử dụng tài nguyên nước, xả nước thải vào nguồn nước

Kinh doanh dịch vụ điều tra cơ bản, tư vấn lập quy hoạch, đề án, báo cáo tài nguyên nước

Điều 9. Tiêu chí xác định cấp độ 3

Hệ thống thông tin cấp độ 3 là hệ thống thông tin có một trong các tiêu chí cụ thể như sau:

1. Hệ thống thông tin xử lý thông tin bí mật nhà nước hoặc hệ thống phục vụ quốc phòng, an ninh khi bị phá hoại sẽ làm tổn hại tới quốc phòng, an ninh quốc gia.

2. Hệ thống thông tin phục vụ người dân, doanh nghiệp thuộc một trong các loại hình như sau:

a) Cung cấp thông tin và dịch vụ công trực tuyến từ mức độ 3 trở lên theo quy định của pháp luật;

b) Cung cấp dịch vụ trực tuyến thuộc danh Mục dịch vụ kinh doanh có Điều kiện;

c) Cung cấp dịch vụ trực tuyến khác có xử lý thông tin riêng, thông tin cá nhân của từ 10.000 người sử dụng trở lên.

3. Hệ thống cơ sở hạ tầng thông tin dùng chung phục vụ hoạt động của các cơ quan, tổ chức trong phạm vi một ngành, một tỉnh hoặc một số tỉnh.

[i] Lưu ý: *Căn cứ quy định tại mục 25 Phụ lục IV Luật đầu tư năm 2020 và khoản 2 Điểm b khoản 2 Điều 9 Nghị định 85/2016/NĐ-CP, các hệ thống thông tin cung cấp dịch vụ chứng khoán cần triển khai bảo đảm an toàn hệ thống thông tin theo cấp độ quy định tại Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ và Thông tư 12/2022/tt-bttt ngày 12/8/2022 của Bộ trưởng Bộ Thông tin và Truyền thông. Việc không triển khai bảo đảm an toàn hệ thống thông tin theo cấp độ là vi phạm quy định pháp luật và bị xử phạt hành chính theo Điều 88 và Điều 89 Nghị định số 15/2020/NĐ-CP ngày 03/02/2020 của Chính phủ quy định xử phạt vi phạm hành chính trong lĩnh vực bưu chính, viễn thông, tần số vô tuyến điện, công nghệ thông tin và giao dịch điện tử.*

MỤC TIÊU NĂM 2025

KHÔNG GIAN MẠNG QUỐC GIA ĐƯỢC ĐẢM BẢO AN TOÀN.

DUY TRÌ NIỀM TIN SỐ - KHÔNG GIAN MẠNG VĂN MINH, LÀNH MẠNH

MỤC TIÊU CỤ THỂ:

1. Duy trì thứ hạng của Việt Nam trong top 20 về Chỉ số an toàn, an ninh mạng theo đánh giá của Liên minh Viễn thông quốc tế (Chỉ số GCI).
2. **Đôn đốc, giám sát** việc tuân thủ quy định pháp luật về cấp độ ATHTTT và bảo đảm ATTT thực chất theo mô hình 4 lớp.
3. Bảo vệ cơ sở hạ tầng thông tin trong 11 lĩnh vực quan trọng, các **sự kiện quan trọng của quốc gia**
4. **Thanh tra, kiểm tra các cơ quan, doanh nghiệp tuân thủ quy định về ATTT**

Trân trọng cảm ơn
Quý vị đã lắng nghe !