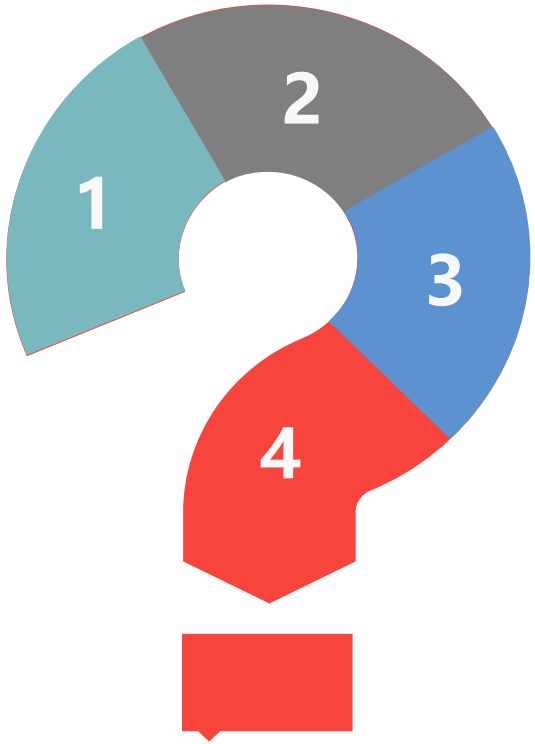
CỤC AN TOÀN THÔNG TIN
AUTHORITY OF INFORMATION SECURITY

AN TOÀN THÔNG TIN TRONG CHUYỂN ĐỔI SỐ

NỘI DUNG



1. Thực trạng

Tình hình an toàn thông tin Việt Nam, thế giới, những vấn đề hiện nay

2. Định hướng về an toàn thông tin trong chuyển đổi số

Chính sách, chủ trương về an toàn thông tin trong chuyển đổi số

3. Nội dung về an toàn thông tin trong chuyển đổi số

Triển khai đảm bảo an toàn thông tin theo cấp độ; Mô hình 4 lớp; DevSecops; Ứng cứu sự cố

4. Khuyến nghị

Một số giải pháp cần triển khai trong thời gian tới

01 Thực trạng

Dữ liệu là mục tiêu bảo vệ chính và cũng là mục tiêu tấn công của tội phạm mạng

THỰC TRẠNG

Tấn công mạng hiện đứng đầu danh sách các mối đe dọa hiện tại mà các cơ quan, tổ chức chính phủ, doanh nghiệp (*)

Các chiến dịch tấn công mạng được vận hành bởi:

NSO Group, DeathStalker, DarkBasin,…

APT27, APT29, Unit 8200, Lazarus Group,…

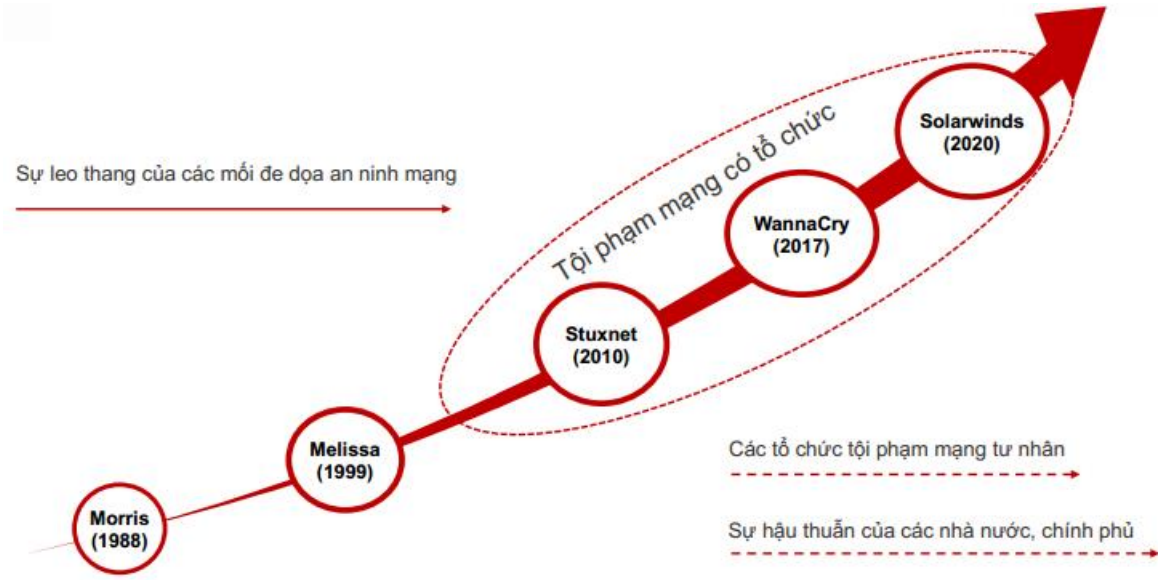
10 tỷ USD, 65 quốc gia

Chiến dịch tấn công Phishing nhằm vào 26 bank tại Việt Nam

18.000 khách hàng

2,5 tỷ USD, 150 quốc gia

Việt Nam là mục tiêu của các nhóm tấn công có chủ đích như nhóm APT10, APT37, GALLIUM, Mustang Panda...



THỰC TRẠNG

An toàn mạng đến 2025

DOANH THU (*)

- **352** tỷ USD.
- Tăng trưởng 14,5%/năm.

NHÂN LỰC

06 triệu
gấp 2 năm 2020

ĐỐI TƯỢNG

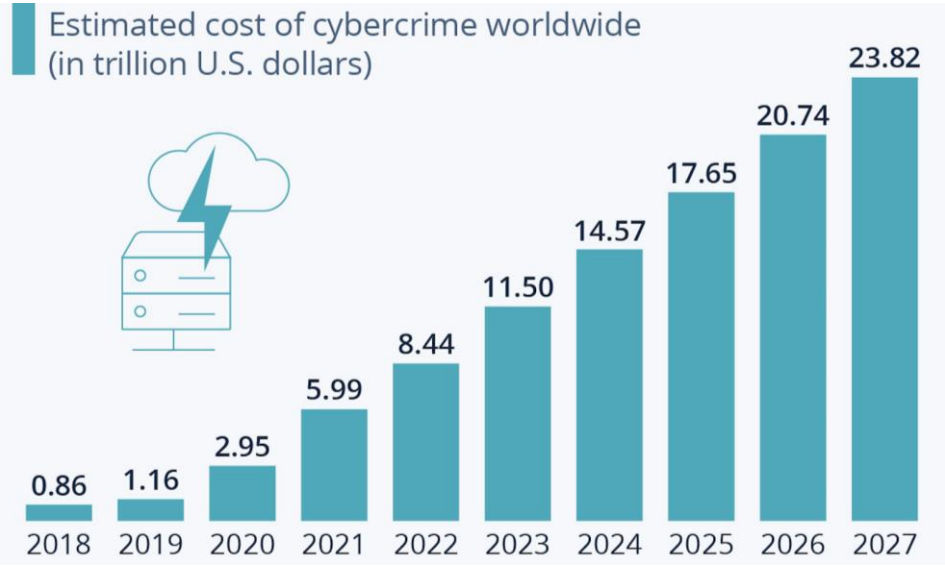
Đối tượng bị tấn công:
- **2025:** gấp 2,7 lần 2020.
- **2030:** gấp 7,5 lần 2020.

NGUY CƠ

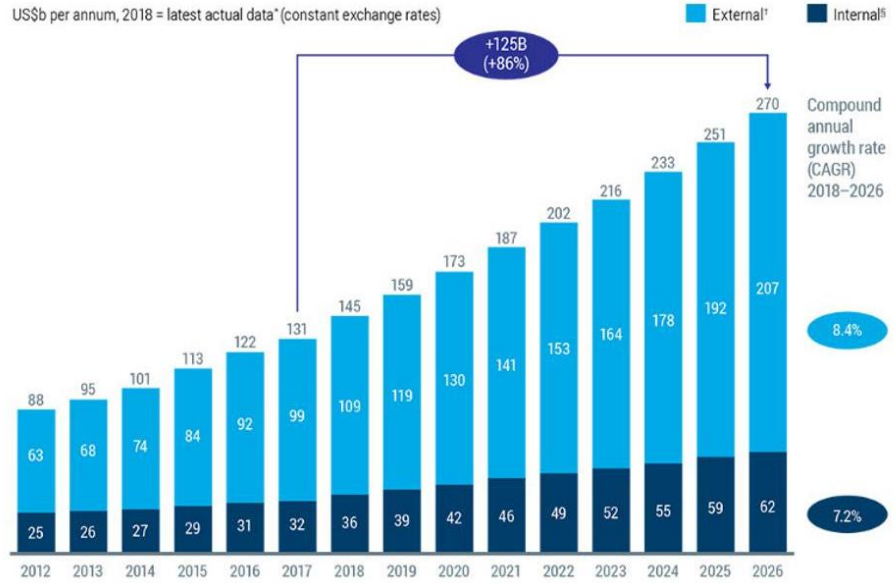
- **3.000** cuộc tấn công/giây <> 900
- **12** mã độc/giây <> 5
- **70** lỗ hổng mới/ngày <> 40

- Tấn công mạng quy mô lớn, chuyên nghiệp
- Tấn công mạng nhắm vào người dùng
- ATTT chuỗi cung ứng
- Ảnh hưởng của công nghệ
- Sự bùng nổ thiết bị
- Thiếu hụt nguồn nhân lực ATTT

Thiệt hại do tội phạm mạng



Chi tiêu cho an toàn thông tin mạng toàn cầu



10 MỐI ĐE DOẠ KHÔNG GIAN MẠNG HÀNG ĐẦU NĂM 2024

1 Social Engineering

Any network is hackable if an employee can be duped into sharing access.

2 Third-Party Exposure

Vendors, clients, and app integrations with poor security can provide access to an otherwise well-protected network.

3 Configuration Mistakes

Even the most cutting-edge security software only works if it's installed correctly.

4 Poor Cyber Hygiene

Employee training is essential to ensure those with network access maintain safe cyber practices.

5 Cloud Vulnerabilities

Online data storage and transfer provides increased opportunities for a potential hack.

6 Ransomware

Hackers can capture sensitive data or take down networks and demand payment for restored access.

7 Mobile Device Vulnerabilities

Devices that connect to multiple networks are exposed to more potential security threats.

8 Internet of Things

Smart technology users may not realize that any IoT device can be hacked to obtain network access.

9 Poor Data Management

When massive amounts of unnecessary data are kept, it's easier to lose and expose essential information.

10 Inadequate Post-Attack Procedures

Security patches must be as strong as the rest of your cybersecurity protections.

CÁC VỤ TẤN CÔNG GẦN ĐÂY

24/03/2024

Sự cố VNDIRECT

Mã hóa hạ tầng ảo hóa và sao lưu

- ~ 1000 máy chủ đã bị mã hóa
- ~ 1 tuần để VNDIRECT khôi phục các chức năng cơ bản
- ~ 0,6% thị phần bị mất sau sự cố

02/04/2024

Sự cố PVOIL

Mã hóa toàn bộ máy chủ windows

- 80 máy chủ windows bị mã hóa
- 3 ngày để khôi phục các chức năng cơ bản
- 7/9 hệ thống bị mã hóa hoàn toàn
- 6/9 hệ thống có backup có thể phục hồi

04/06/2024

Sự cố VNPOST

Mã hóa hạ tầng ảo hóa và sao lưu

- Ảnh hưởng tới 109 host, 530 VM
- 1 tuần khôi phục các chức năng cơ bản
- 10% Cloud, 35TB dữ liệu đã bị mã hóa hoàn toàn

13/06/2024

Sự cố của một tổ chức y tế

Mã hóa hạ tầng ảo hóa và sao lưu

- 21 host, 105 VM bị ảnh hưởng
- 5 ngày để khôi phục các chức năng cơ bản
- 21 dịch vụ ngừng hoạt động

Nguyên nhân chủ yếu:

1. ***Chưa thực hiện đầy đủ các quy định về đảm bảo an toàn thông tin***
2. ***Sai sót trong thiết kế hệ thống, không phân vùng mạng chặt chẽ***
3. ***Quản lý, kiểm soát truy cập lỏng lẻo***
4. ***Chưa triển khai hệ thống SOC, các hệ thống bảo vệ***
5. ***Các tài khoản đặc quyền sử dụng chung mật khẩu; chưa có quy định về việc quản lý, cấp và thu hồi tài khoản***

Tạo điều kiện cho kẻ tấn công chiếm được tài khoản quan trọng và mở rộng phạm vi tấn công

NGUY CƠ MẤT AN TOÀN THÔNG TIN

Lỗ hổng

Tháng 6/2024: **90.033** điểm yếu, lỗ hổng an toàn thông tin tại các cơ quan, tổ chức tại Việt Nam

Sự cố

06 tháng đầu năm 2024, số sự cố nghiêm trọng mà Cục ATTT xử lý đã tăng gần **60%** so với năm 2023

Lộ lọt dữ liệu

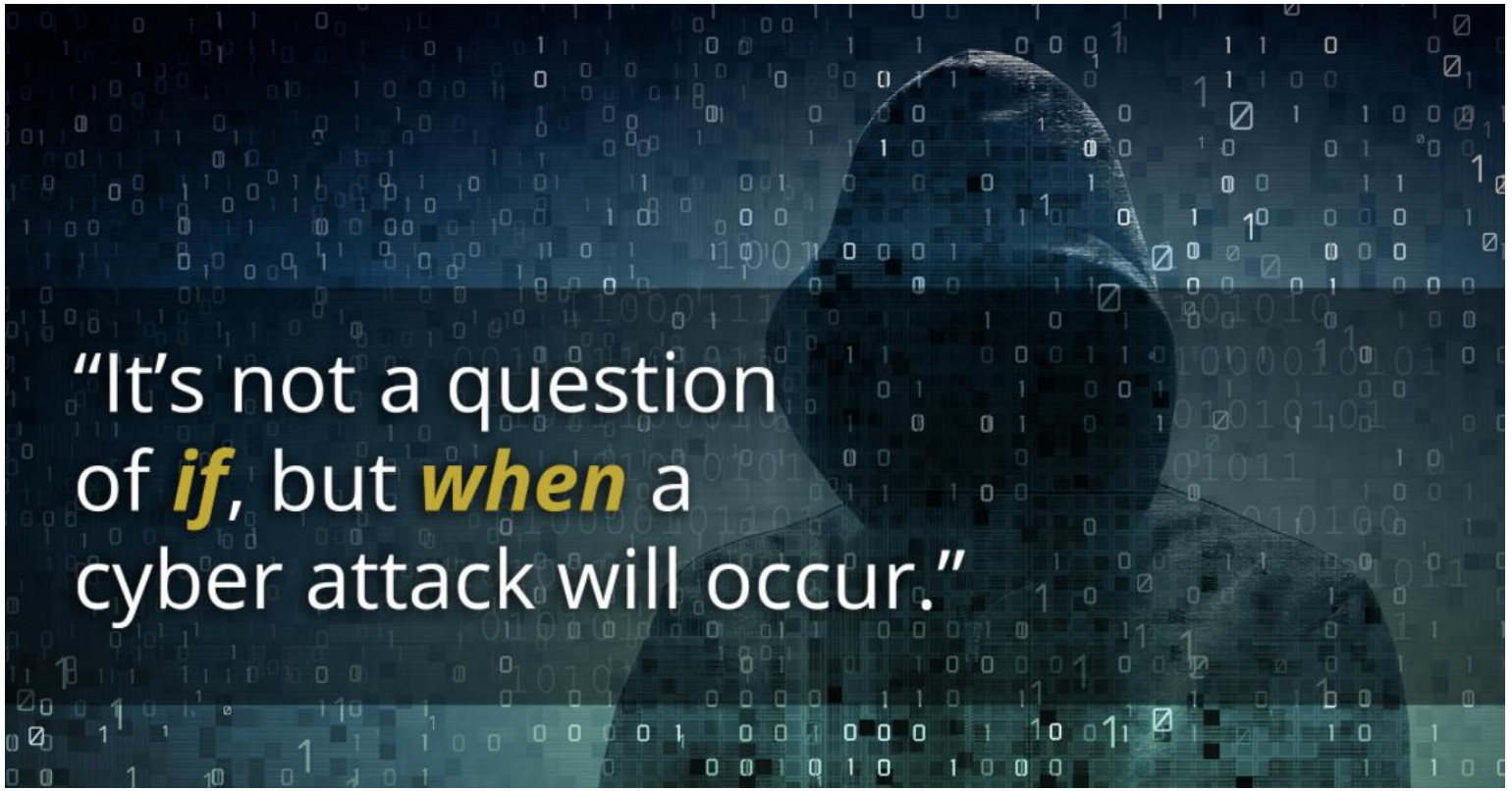
Tài khoản lộ lọt do nhiễm mã độc tại Việt Nam năm 2023 gấp **31** lần so với năm 2020

Lừa đảo trực tuyến

Cục ATTT đã ngăn chặn **3.170** website lừa đảo trực tuyến, bảo vệ hơn **10,981** triệu người dân

Nguy cơ ngày càng gia tăng

Không còn là "nếu" bị tấn công mạng, mà là "khi nào" bị tấn công



Hãy chuẩn bị !
Hãy tổ chức !
Hãy sẵn sàng !
Đôi khi, bạn chỉ có 1 cơ hội ?

02 Định hướng về an toàn thông tin trong chuyển đổi số

QUAN ĐIỂM VỀ ĐẢM BẢO AN TOÀN THÔNG TIN TRONG CHUYỂN ĐỔI SỐ

Quyết định 749/QĐ-TTg ngày 03/6/2020 Chương trình Chuyển đổi số quốc gia đến năm 2025, định hướng đến năm 2030

1. Bảo đảm an toàn, an ninh mạng là **then chốt** để chuyển đổi số **thành công** và **bền vững**, đồng thời là phần **xuyên suốt**, không thể tách rời của chuyển đổi số.
2. Mọi thiết bị, sản phẩm, phần mềm, hệ thống thông tin, dự án đầu tư về công nghệ thông tin đều có **cấu phần bắt buộc về an toàn, an ninh mạng** ngay **từ khi thiết kế**.

Quyết định 964/QĐ-TTg ngày 10/08/2022 Phê duyệt Chiến lược An toàn, an ninh mạng quốc gia, chủ động ứng phó với các thách thức từ không gian mạng đến năm 2025, tầm nhìn 2030

1. An toàn, an ninh mạng là **trọng tâm** của quá trình chuyển đổi số, là trụ cột quan trọng tạo lập niềm tin số và sự phát triển thịnh vượng trong kỷ nguyên số.
2. An toàn, an ninh mạng là nhiệm vụ **trọng yếu**, **thường xuyên, lâu dài** nhằm khởi tạo và duy trì môi trường mạng an toàn, lành mạnh, tin cậy cho các cơ quan, tổ chức, doanh nghiệp và mỗi người dân.
3. Đầu tư cho an toàn, an ninh mạng là đầu tư cho **phát triển bền vững** và **tạo ra giá trị**.

HÀNH LANG PHÁP LÝ VỀ CÔNG TÁC BẢO ĐẢM AN TOÀN THÔNG TIN

1. Luật An toàn thông tin mạng
2. Nghị định số 85/2016/NĐ-CP về bảo đảm an toàn hệ thống thông tin theo cấp độ
3. Nghị định số 15/2020/NĐ-CP 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
4. Quyết định số 05/2017/QĐ-TTg Ban hành quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia
5. Thông tư số 20/2017/TT-BTTTT của Bộ Thông tin và Truyền thông quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc
6. Thông tư số 31/2017/TT-BTTTT của Bộ Thông tin và Truyền thông quy định hoạt động giám sát an toàn hệ thống thông tin
7. Thông tư số 12/2022/TT-BTTTT quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 về bảo đảm an toàn hệ thống thông tin theo cấp độ

CHỈ ĐẠO TRIỂN KHAI BẢO ĐẢM ATTT

1. Quyết định 632/QĐ-TTg năm 2017 ban hành danh mục lĩnh vực quan trọng cần ưu tiên bảo đảm an toàn thông tin mạng và hệ thống thông tin quan trọng quốc gia
2. Quyết định 1622/QĐ-TTg năm 2017 đẩy mạnh hoạt động của mạng lưới ứng cứu sự cố, tăng cường năng lực cho các cán bộ, bộ phận chuyên trách ứng cứu sự cố an toàn thông tin mạng trên toàn quốc đến 2020, định hướng đến 2025
3. Chỉ thị 14/CT-TTg năm 2018 về việc nâng cao năng lực phòng, chống phần mềm độc hại
4. Chỉ thị 14/CT-TTg năm 2019 về việc tăng cường bảo đảm an toàn, an ninh mạng nhằm cải thiện chỉ số xếp hạng của Việt Nam
5. Chỉ thị 18/CT-TTg năm 2022 về đẩy mạnh triển khai các hoạt động ứng cứu sự cố an toàn thông tin mạng Việt Nam
6. Quyết định 749/QĐ-TTg ngày 03/6/2020 Chương trình Chuyển đổi số quốc gia đến năm 2025, định hướng đến năm 2030
7. Chỉ thị 02/CT-TTg ngày 26/4/2022 về phát triển chính phủ điện tử hướng tới chính phủ số, thúc đẩy chuyển đổi số quốc gia
8. Quyết định 964/QĐ-TTg ngày 10/08/2022 Phê duyệt Chiến lược An toàn, An ninh mạng quốc gia, chủ động ứng phó với các thách thức từ không gian mạng đến năm 2025, tầm nhìn 2030
9. Chỉ thị 09/CT-TTg năm 2024 về việc tuân thủ quy định pháp luật và tăng cường bảo đảm an toàn hệ thống thông tin theo cấp độ
10. Công điện 33/CĐ-TTg năm 2024 về việc tăng cường bảo đảm an toàn thông tin mạng

VAI TRÒ CỦA NGƯỜI ĐỨNG ĐẦU

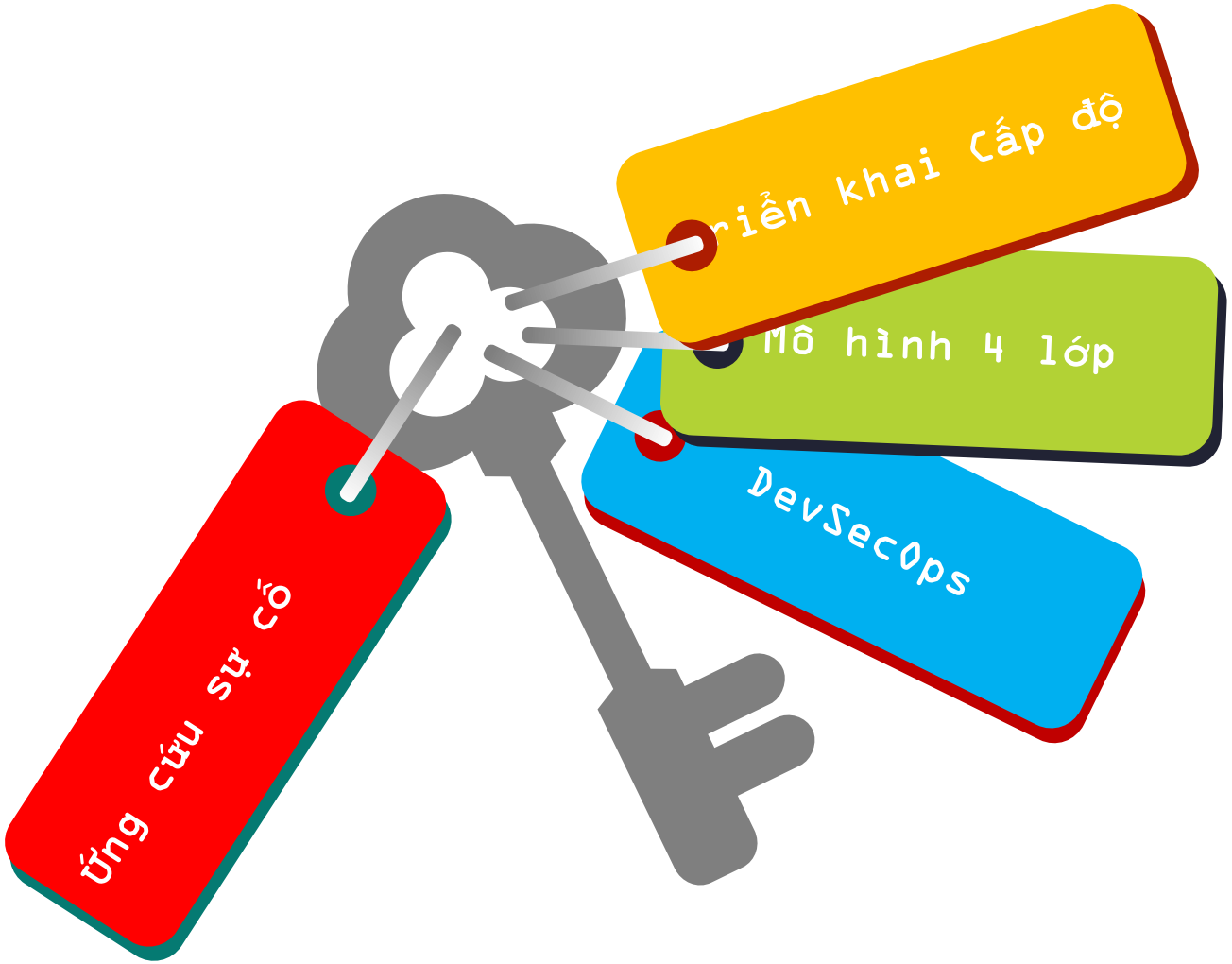
1. Chỉ thị 18/CT-TTg năm 2022: **Người đứng đầu** chịu trách nhiệm trước Thủ tướng Chính phủ nếu lơ là trong công tác ứng cứu sự cố an toàn thông tin mạng, để xảy ra hậu quả, thiệt hại nghiêm trọng tại cơ quan, đơn vị thuộc phạm vi quản lý.

2. Chỉ thị 09/CT-TTg năm 2024: **Người đứng đầu** 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.

3. Công điện 33/CĐ-TTg năm 2024: **Người đứng đầu** trực tiếp chỉ đạo và phụ trách công tác bảo đảm an toàn thông tin mạng; chịu trách nhiệm trước pháp luật và Thủ tướng Chính phủ nếu để hệ thống thông tin thuộc phạm vi quản lý không bảo đảm an toàn thông tin mạng, để xảy ra sự cố nghiêm trọng.

03 Nội dung về an toàn thông tin trong chuyển đổi số

NỘI DUNG VỀ ĐẢM BẢO AN TOÀN THÔNG TIN TRONG CHUYỂN ĐỔI SỐ



- Hệ thống thông tin cần **triển khai đầy đủ** phương án bảo đảm an toàn thông tin theo cấp độ
- Hệ thống thông tin được quản lý, vận hành theo **mô hình 4 lớp**
- Phần mềm nội bộ phải **do đơn vị chuyên nghiệp** phát triển, tuân thủ Khung phát triển phần mềm an toàn DevSecOps
- Hoạt động ứng cứu sự cố phải chuyển từ **bị động** sang **chủ động**

1. ĐẢM BẢO AN TOÀN THÔNG TIN THEO CẤP ĐỘ

1. Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 về bảo đảm an toàn hệ thống thông tin theo cấp độ
2. Thông tư 12/2022/TT-BTTTT ngày 12/8/2022 Quy định chi tiết và hướng dẫn một số điều của Nghị định 85
3. Tiêu chuẩn quốc gia TCVN 11930: 2017
4. Chỉ thị 09/CT-TTg ngày 23/02/2024 của Thủ tướng Chính phủ Về tuân thủ quy định pháp luật và tăng cường bảo đảm an toàn hệ thống thông tin theo cấp độ
5. Công văn 708/BTTTT-CATTT hướng dẫn kỹ thuật triển khai Đề án 06
6. Công văn 2596/BTTTT-CATTT hướng dẫn bảo đảm an toàn thông tin mạng cho các hệ thống thông tin thuộc phạm vi quản lý cấp bộ, tỉnh

ĐẢM BẢO AN TOÀN THÔNG TIN THEO CẤP ĐỘ

Tiêu chí: Điều 7 Nghị định 85
Yêu cầu: Phụ lục 1 Thông tư 12

Tiêu chí: Điều 8 Nghị định 85
Yêu cầu: Phụ lục 2 Thông tư 12

Tiêu chí: Điều 9 Nghị định 85
Yêu cầu: Phụ lục 3 Thông tư 12

Tiêu chí: Điều 10 Nghị định 85
Yêu cầu: Phụ lục 4 Thông tư 12

Tiêu chí: Điều 11 Nghị định 85
Yêu cầu: Phụ lục 5 Thông tư 12

ĐẢM BẢO AN TOÀN THÔNG TIN THEO CẤP ĐỘ

Chỉ thị 09/CT-TTg ngày 23/02/2024 của Thủ tướng Chính phủ Về tuân thủ quy định pháp luật và tăng cường bảo đảm an toàn hệ thống thông tin theo cấp độ:

1. Người đứng đầu trực tiếp chỉ đạo và phụ trách công tác đảm bảo an toàn thông tin, chịu trách nhiệm nếu không tuân thủ quy định về đảm bảo an toàn thông tin theo cấp độ.
2. Phổ biến, quán triệt các đơn vị trực thuộc nghiêm túc tuân thủ các quy định của Pháp luật về bảo đảm an toàn thông tin.
3. 100% hệ thống thông tin đang thiết kế, xây dựng, nâng cấp, mở rộng phải được phê duyệt cấp độ và triển khai phương án đảm bảo an toàn thông tin theo cấp độ trước khi đưa vào vận hành.
4. 100% các hệ thống thông tin từ cấp độ 1 đến cấp độ 5 (nếu có) đang vận hành phải được phê duyệt cấp độ chậm nhất trong tháng 9/2024 & triển khai đầy đủ phương án đảm bảo an toàn thông tin theo cấp độ trong tháng 12/2024.
5. Ưu tiên bố trí nguồn lực để triển khai và thực thi hiệu quả.

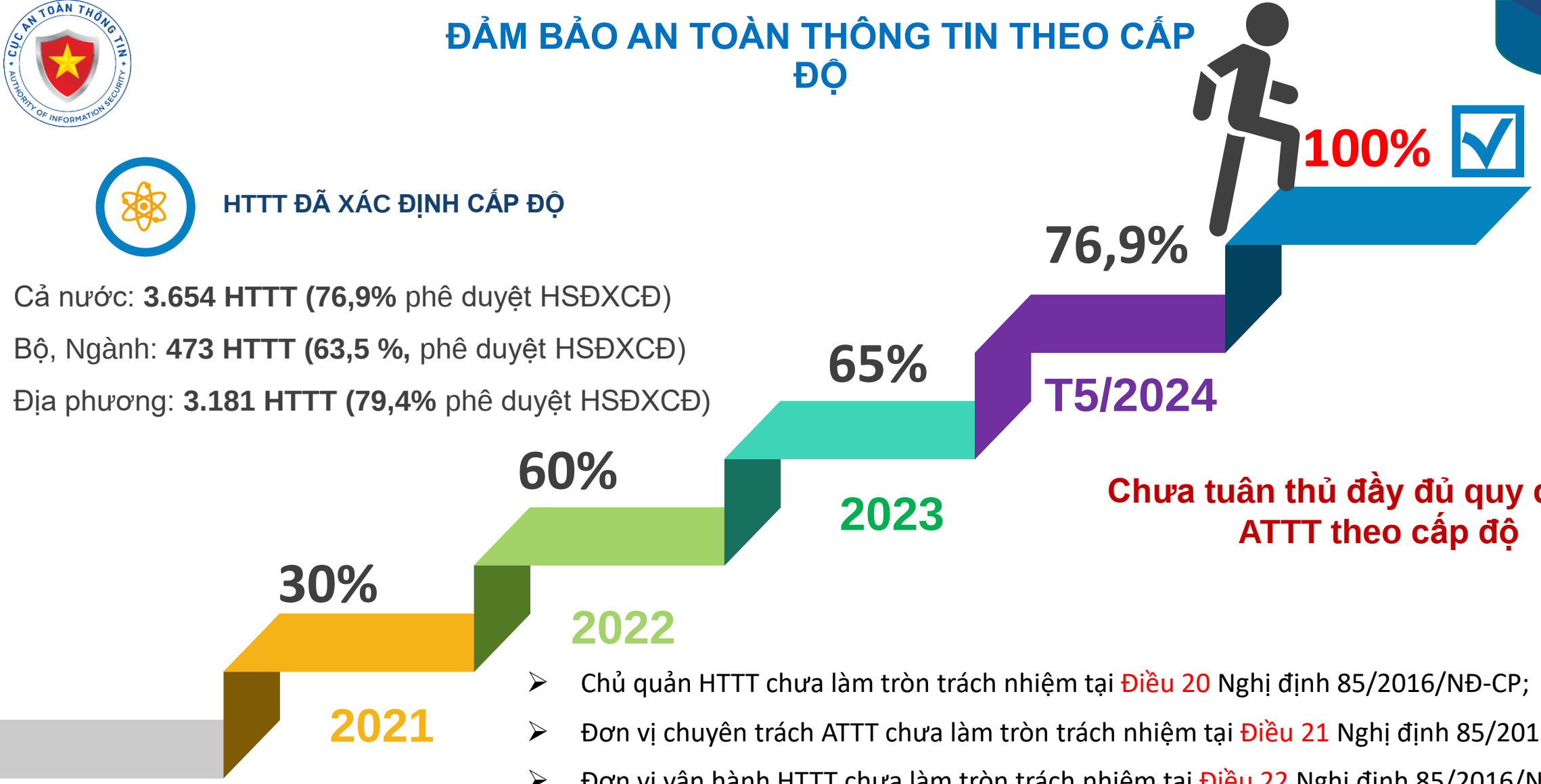
ĐẢM BẢO AN TOÀN THÔNG TIN THEO CẤP ĐỘ

HTTT ĐÃ XÁC ĐỊNH CẤP ĐỘ

Cả nước: **3.654 HTTT (76,9%** phê duyệt HSĐXCĐ)

Bộ, Ngành: **473 HTTT (63,5 %,** phê duyệt HSĐXCĐ)

Địa phương: **3.181 HTTT (79,4%** phê duyệt HSĐXCĐ)

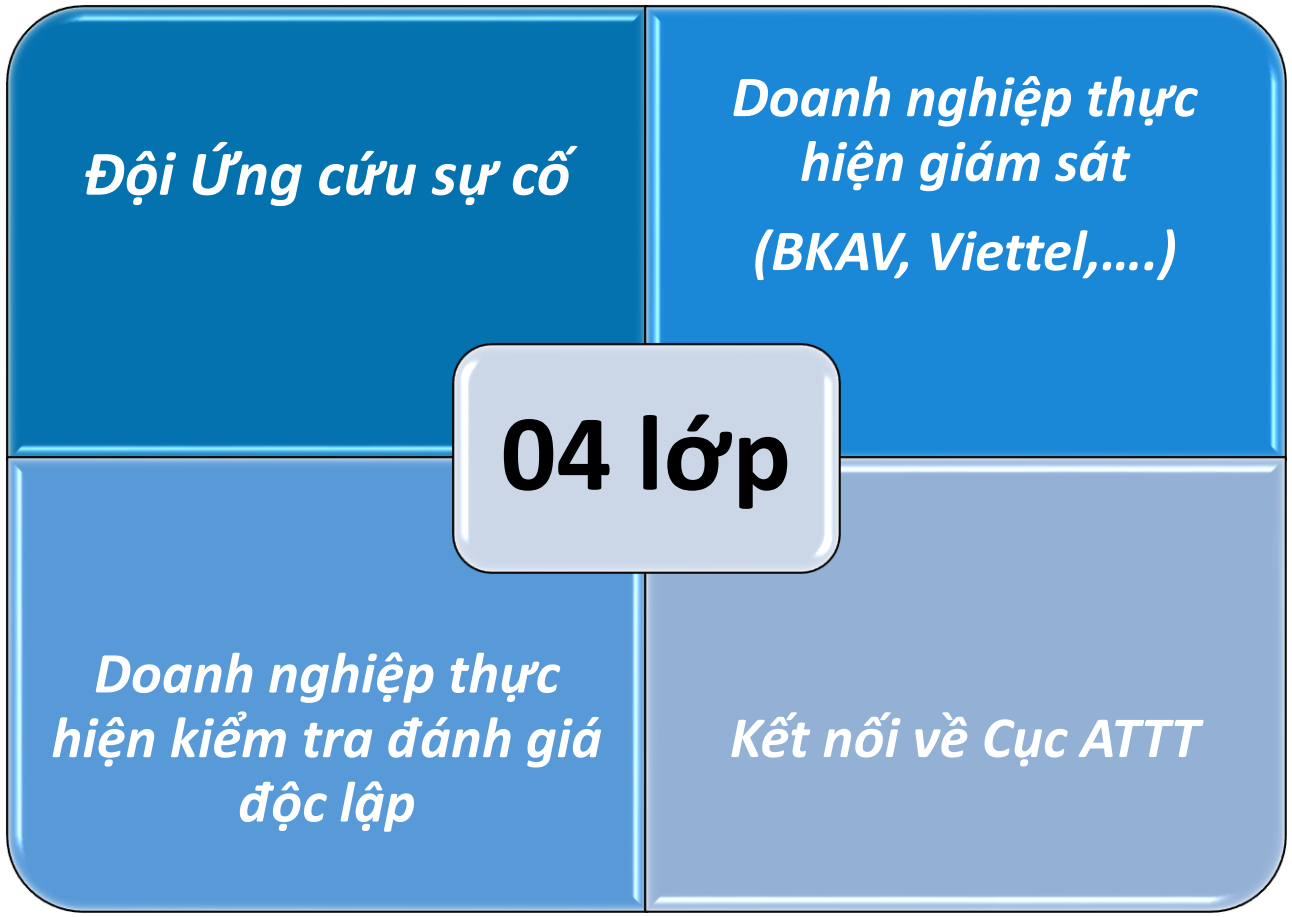


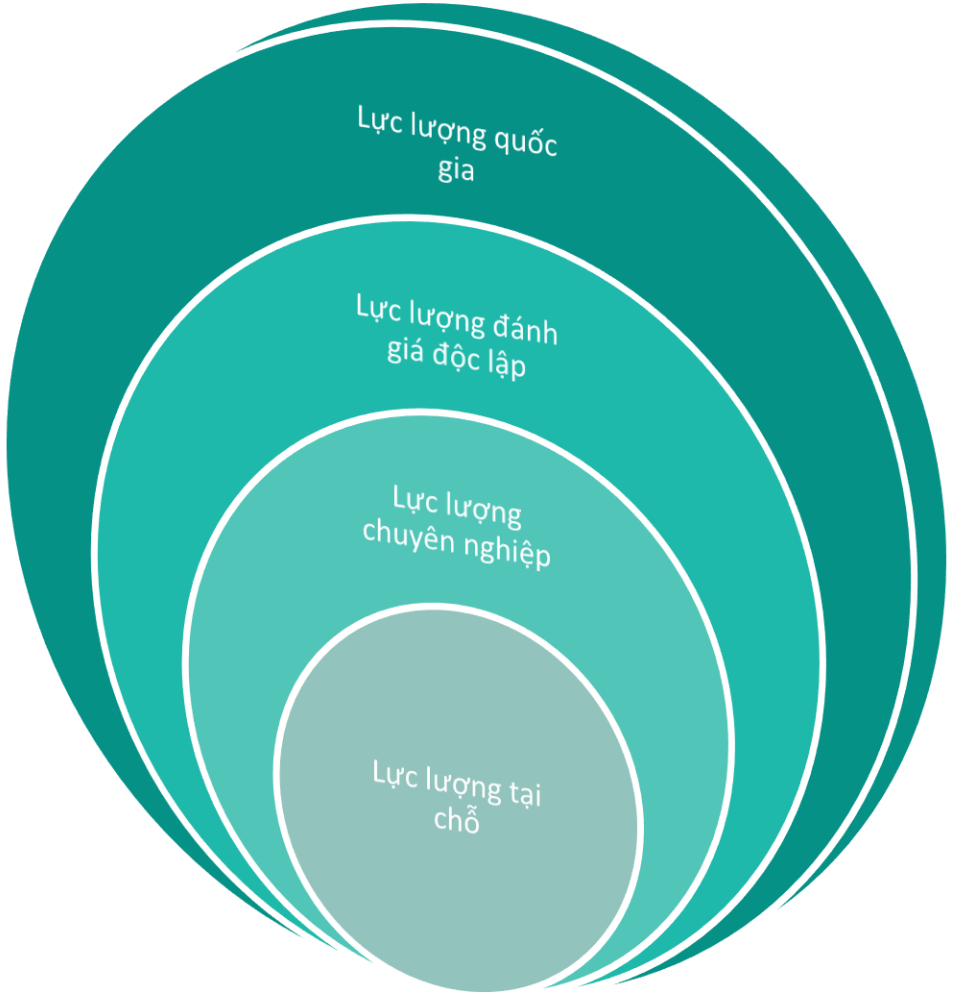
Chưa tuân thủ đầy đủ quy định về ATTT theo cấp độ

- Chủ quản HTTT chưa làm tròn trách nhiệm tại Điều 20 Nghị định 85/2016/NĐ-CP;
- Đơn vị chuyên trách ATTT chưa làm tròn trách nhiệm tại Điều 21 Nghị định 85/2016/NĐ-CP;
- Đơn vị vận hành HTTT chưa làm tròn trách nhiệm tại Điều 22 Nghị định 85/2016/NĐ-CP.

- Việc này **có thể bị xử phạt** theo quy định tại Điều 88 của Nghị định số 15/2020/NĐ-CP.
- Cục ATTT đã đưa hệ thống quản lý cấp độ hệ thống thông tin vào khai thác, sử dụng
- Cục ATTT cung cấp hồ sơ mẫu https://ais.gov.vn/thong-tin-tham-khao/mau-hsdxcd.htm

2. MÔ HÌNH BẢO ĐẢM AN TOÀN THÔNG TIN 4 LỚP





LỚP 1 - NĂNG LỰC ĐỘI ỨNG CỨU SỰ CỐ

ĐỘI ỨNG CỨU SỰ CỐ

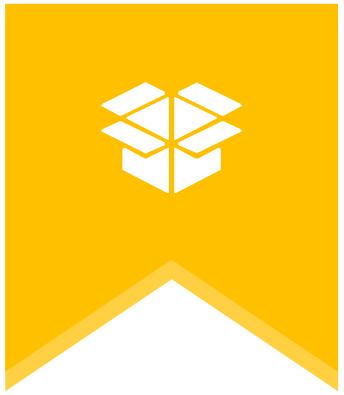
100% Đội tại các cơ quan, tổ chức nhà nước theo mô hình kiêm nhiệm, năng lực hạn chế

70% đơn vị chưa tuân thủ nghiêm túc việc khắc phục các lỗ hổng

Chỉ thị 18/CT-TTg về tăng cường năng lực ứng cứu sự cố.

- Coi ứng cứu sự cố là **chốt chặn cuối cùng** của an toàn thông tin, không được phép lơ là.
- Đội Ứng cứu sự cố phải được tổ chức theo hướng **chuyên nghiệp**, **cơ động**
- Đội Ứng cứu sự cố có **tối thiểu 05 (năm) chuyên gia** an toàn thông tin mạng
- Đội Ứng cứu sự cố đảm trách các **nhiệm vụ thường xuyên**

LỚP 1: NÂNG CAO NĂNG LỰC LỰC LƯỢNG TẠI CHỖ



Kiện toàn lực lượng

- Người đứng đầu cơ quan, tổ chức trực tiếp chỉ đạo.
- Chỉ định bộ phận chuyên trách về an toàn thông tin.
- Thành lập Đội Ứng cứu sự cố. Tối thiểu 05 chuyên gia an toàn thông tin mạng

Nâng cao năng lực

- Gắn với nhiệm vụ thường xuyên
- Đào tạo, huấn luyện chuyên sâu cho nhân sự chuyên trách
- Diễn tập thực chiến tối thiểu 01 lần/năm (cấp độ 3 trở lên)
- Khai thác hiệu quả các nền tảng hỗ trợ.
- Tuyên truyền, phổ biến kiến thức tới nhân viên

Tham gia VNCSIRT

- Nhận các thông tin cảnh báo
- Tham gia các chương trình diễn tập, huấn luyện
- .....

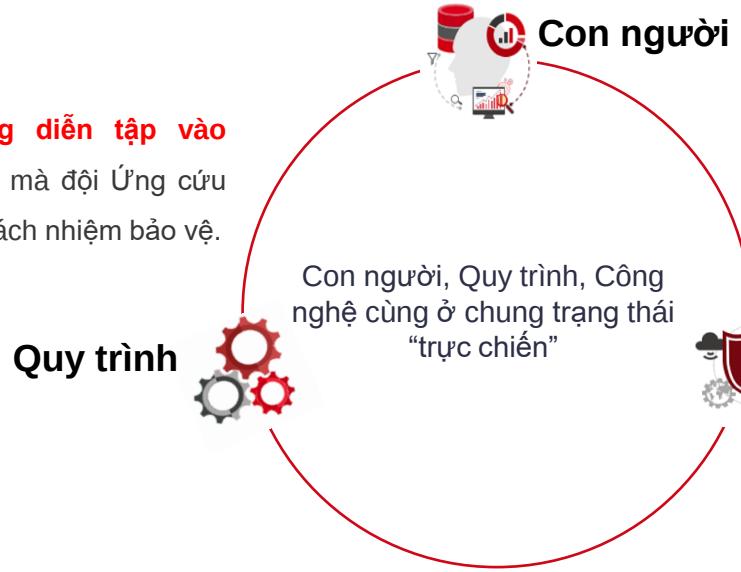
LỚP 1 - DIỄN TẬP THỰC CHIẾN AN TOÀN THÔNG TIN

DIỄN TẬP THỰC CHIẾN AN TOÀN THÔNG TIN

Chỉ thị 18/CT-TTg yêu cầu các tổ chức phải định kỳ thực hiện diễn tập thực chiến

Bộ TT&TT ban hành Chỉ thị 60/CT-BTTTT năm 2021 về diễn tập thực chiến.

Gắn hoạt động diễn tập vào chính hệ thống mà đội Ứng cứu sự cố đang có trách nhiệm bảo vệ.



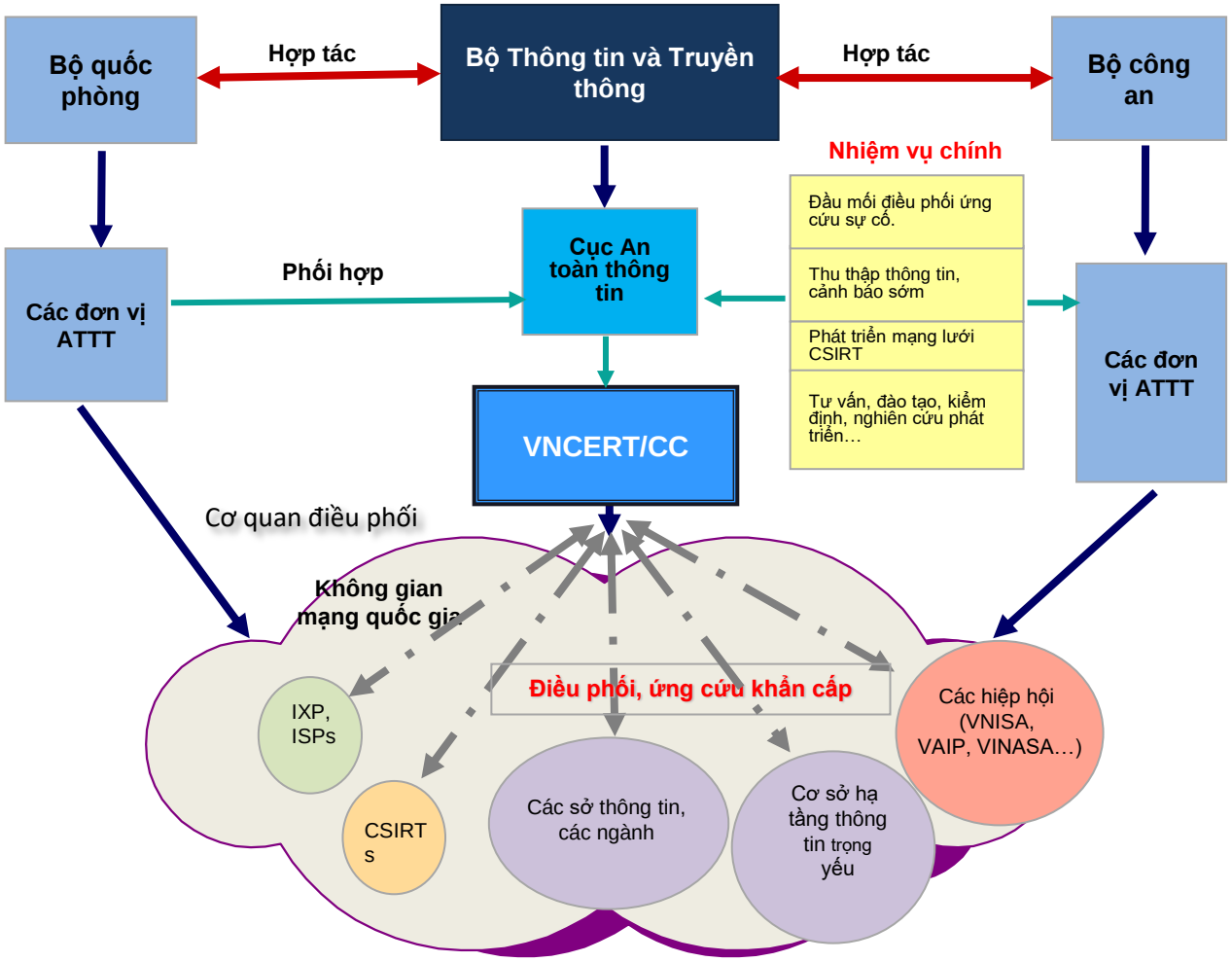
Giúp các tổ chức đánh giá được khả năng ứng phó trong trạng thái đang bị tấn công, **xác định các điểm yếu đang tồn tại liên quan đến con người, quy trình, công nghệ** để cải thiện.

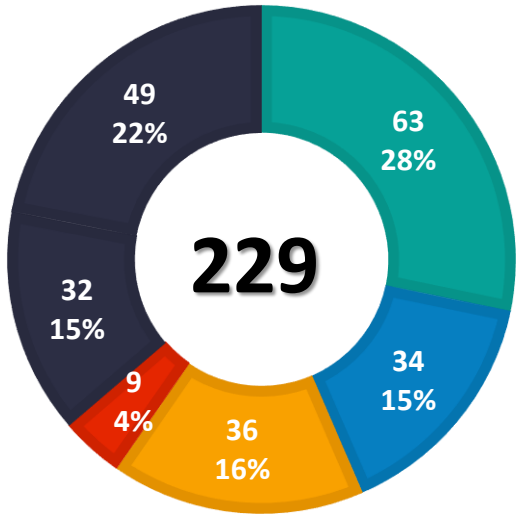
Chuyển từ diễn tập theo kịch bản sẵn có sang **tấn công với nhiều chiến thuật linh hoạt**, trong **thời gian kéo dài** và đặt toàn bộ hệ thống của tổ chức trong trạng thái bất ngờ.

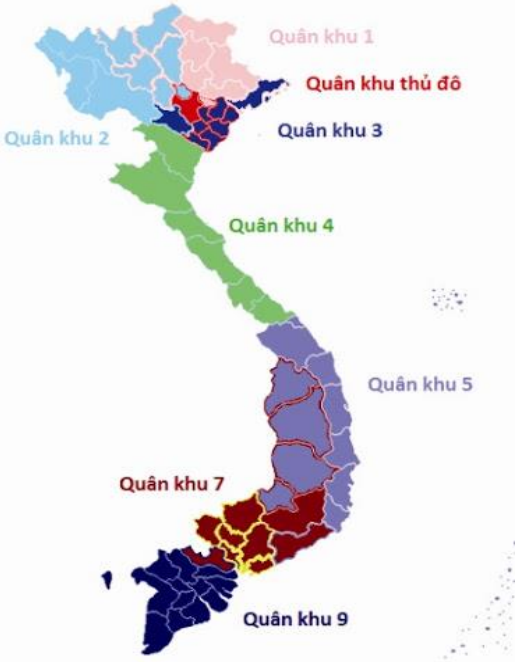
Đánh giá Đội tấn công	Đánh giá Đội phòng thủ
Số lượng và mức độ nghiêm trọng của lỗ hổng, điểm yếu phát hiện được	Đánh giá hiện trạng
Mức độ phức tạp của kỹ thuật tấn công	Năng lực phát hiện tấn công
Khuyến nghị hướng khắc phục	Khả năng ngăn chặn, ứng cứu sự cố

LỚP 1 - MẠNG LƯỚI ỨNG CỨU SỰ CỐ QUỐC GIA

Quyết định 05/2017/QĐ-TTg Ban hành quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia.







- Cụm 8: Doanh nghiệp viễn thông, hạ tầng và Cục BĐTƯ, VNNIC
- Cụm 6: Hà Nội và các Bộ, Ngành
- Cụm 10: Ngân hàng, tài chính, kho bạc, thuế, hải quan
- Cụm 11: Doanh nghiệp CNTT, ATTT

LỚP 1: HOẠT ĐỘNG MẠNG LƯỚI ƯCSC ATTTM QUỐC GIA

Diễn tập

3 diễn tập quốc tế: ASEAN-Nhật Bản, APCERT, ACID

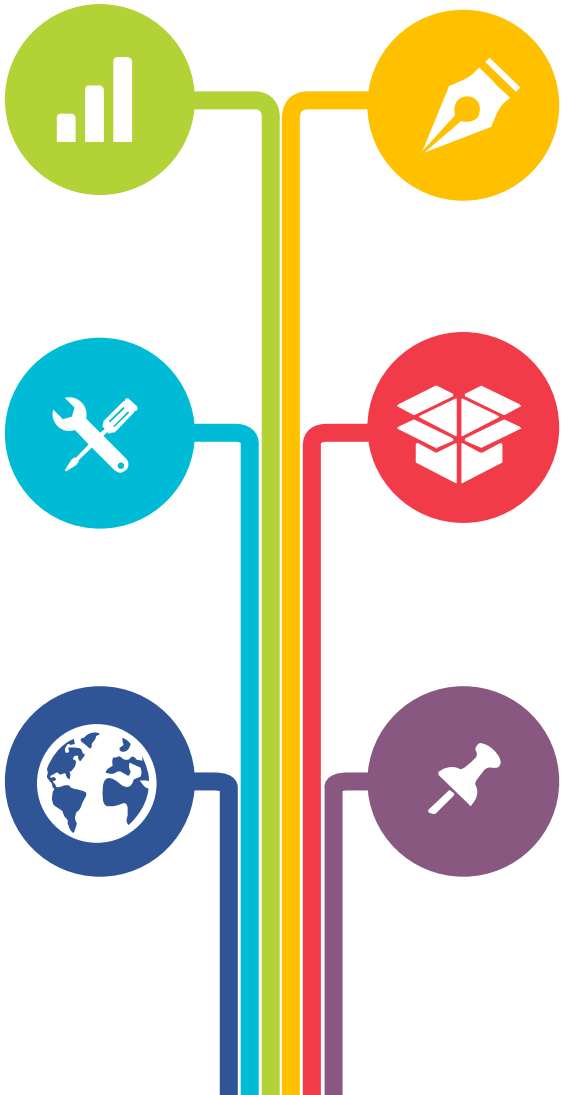
3 diễn tập thực chiến quốc gia

Webinar về bảo đảm ATTT

Duy trì thường xuyên tổ chức webinar chuyên sâu về an toàn thông tin

Duy trì nhóm hoạt động

Nhóm cán bộ đầu mối và kỹ thuật với ~ 1.075 thành viên



Hội nghị Giao ban mạng lưới ƯCSC

Đánh giá hoạt động mạng lưới; hoạt động Cụm

Đánh giá mức độ trưởng thành

Mô hình trưởng thành quản lý ứng cứu sự cố ATTT (SIM3)

Nền tảng

Nền tảng (1) Irlab; (2) DF Lab; (3) Nền tảng hỗ trợ diễn tập; (4) Nền tảng đánh giá mức độ trưởng thành đội UCSC

LỚP 2: LỰC LƯỢNG GIÁM SÁT, BẢO VỆ CHUYÊN NGHIỆP

1. Tự thực hiện giám sát, ứng cứu sự cố, bảo vệ HTTT thuộc quyền quản lý hoặc lựa chọn/thuê tổ chức, DN có đủ năng lực để thực hiện cung cấp dịch vụ giám sát, ứng cứu sự cố, bảo vệ.
2. Lực lượng chuyên nghiệp có thể là doanh nghiệp được Bộ TT&TT cấp phép hoặc đơn vị chuyên trách của Bộ Quốc phòng (Bộ Tư lệnh 86), Ban Cơ yếu Chính phủ, Bộ Công an (Cục ANM và phòng chống tội phạm CNC), Bộ TT&TT (Cục ATTT).
3. Giám sát 4 lớp kỹ thuật:
    1. Giám sát lớp mạng: Tổ chức giám sát các thiết bị mạng, thiết bị bảo mật như Router, Switch, Firewall/IPS/IDS, Sandbox, WAF, Network APT...
    2. Giám sát lớp máy chủ: Tổ chức giám sát các máy chủ hệ thống (cả máy chủ vật lý và ảo hóa) trên các nền tảng khác nhau: Windows, Linux, Unix…
    3. Giám sát lớp ứng dụng: (1) Ứng dụng phục vụ hoạt động của hệ thống: DHCP, DNS, NTP, VPN, Proxy Server…; (2) Ứng dụng cung cấp dịch vụ: Web, Mail, FTP, TFTP và các hệ quản trị cơ sở dữ liệu Oracle, SQL, MySQL...
    4. Giám sát lớp thiết bị đầu cuối: Máy tính người dùng, máy in, máy fax, IP Phone, Camera IP…
5. Triển khai một Trung tâm giám sát, điều hành an toàn, an ninh mạng (SOC) theo chỉ đạo của Thủ tướng Chính phủ tại Quyết định 942/QĐ-TTg ngày 15/6/2021

LỚP 2 – TRUNG TÂM GIÁM SÁT ĐIỀU HÀNH AN TOÀN, AN NINH MẠNG

TRUNG TÂM GIÁM SÁT ĐIỀU HÀNH AN TOÀN, AN NINH MẠNG

Bộ Thông tin và Truyền thông ban hành Quyết định 1356/QĐ-BTTTT về tiêu chí giải pháp đánh giá giải pháp, dịch vụ Trung tâm SOC

I. Tiêu chí về công nghệ

1. **Tiêu chí đánh giá từng thành phần:**

   Cơ bản (SIEM, NIPS, Antivirus, EDR) ➔ ***Theo tiêu chí của Bộ TTTT***

   Nâng cao (WAF, SOAR, TI) ➔ ***Theo tiêu chí của Bộ TTTT***

2. **Tiêu chí đánh giá tính hiệu quả:** Kiểm tra, thử nghiệm

II. Tiêu chí về chất lượng dịch vụ

1. **Quy trình:** đánh giá hồ sơ, thử nghiệm quy trình
2. **Con người:** tối thiểu 12 nhân sự với các mức yêu cầu khác nhau

LỚP 3: KIỂM TRA, ĐÁNH GIÁ AN TOÀN HỆ THỐNG THÔNG TIN

1. **Hệ thống thông tin chưa kết luận bảo đảm an toàn thông tin mạng thì chưa đưa vào sử dụng.**
2. **Phải lựa chọn/thuê tổ chức, doanh nghiệp độc lập với tổ chức, doanh nghiệp tại lớp 2 để định kỳ kiểm tra, đánh giá**

Nội dung kiểm tra, đánh giá

- Kiểm tra, đánh giá việc tuân thủ quy định của pháp luật về bảo đảm ATHTTT theo cấp độ;
- Kiểm tra, đánh giá hiệu quả của các biện pháp bảo đảm ATTT theo phương án bảo đảm ATTT được phê duyệt;
- Kiểm tra, đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập HTTT (có đánh giá mã nguồn).

Tần suất kiểm tra, đánh giá

- Đối với các HTTT cấp độ 3 và cấp độ 4, định kỳ hàng năm;
- Đối với HTTT quan trọng QG (cấp độ 5), định kỳ 06 tháng/01 lần;
- Kiểm tra, đánh giá đột xuất theo yêu cầu của cấp có thẩm quyền.

Hình thức kiểm tra, đánh giá

- Kiểm tra, đánh giá hộp đen (Black box);
- Kiểm tra, đánh giá hộp xám (Gray box);
- Kiểm tra, đánh giá hộp trắng (White box).

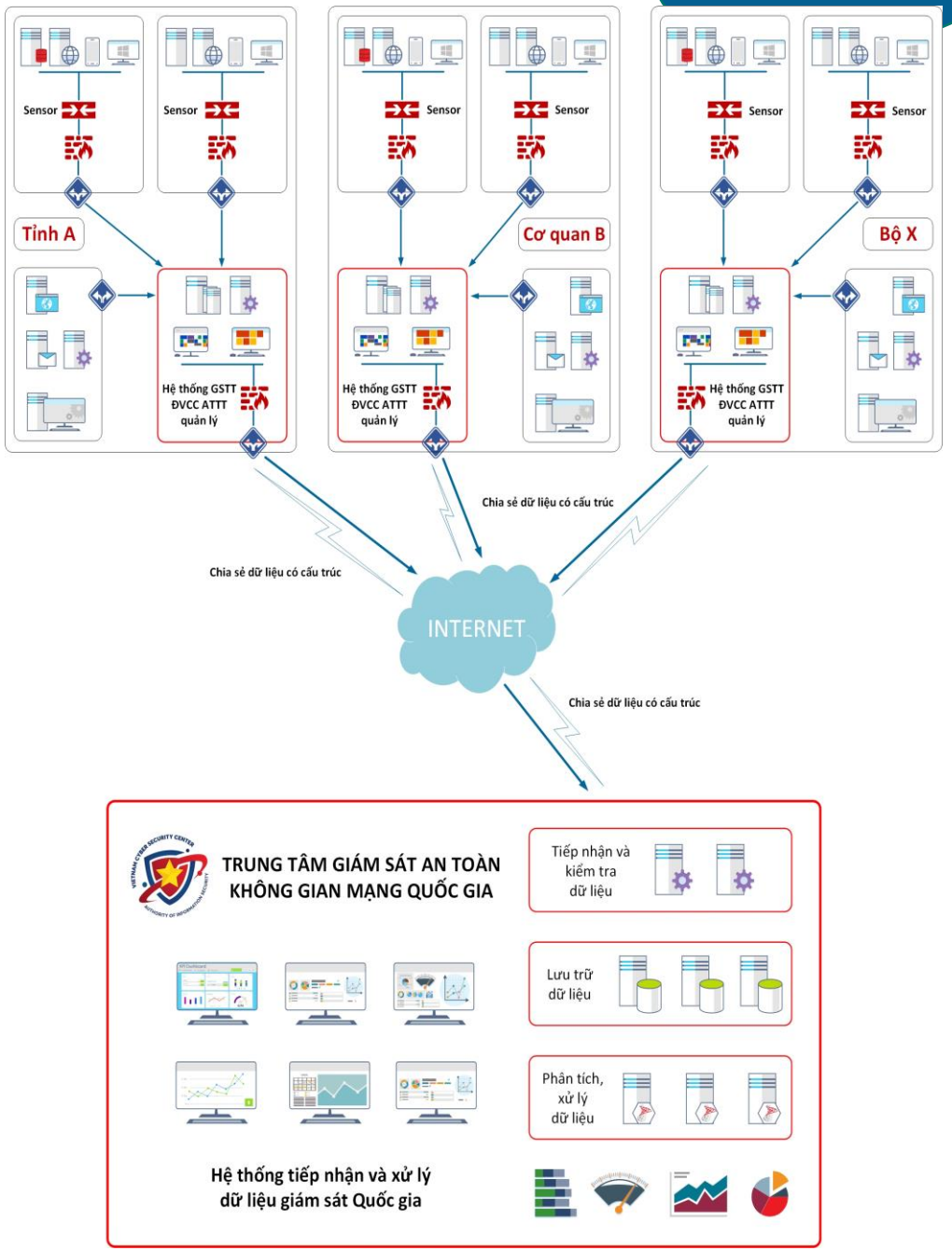
LỚP 4: LỰC LƯỢNG QUỐC GIA

1. Mục đích: Giúp phát hiện và cảnh báo sớm nguy cơ mất an toàn thông tin có thể xảy ra với cơ quan, tổ chức và phục vụ công tác quản lý nhà nước của Bộ TT&TT.

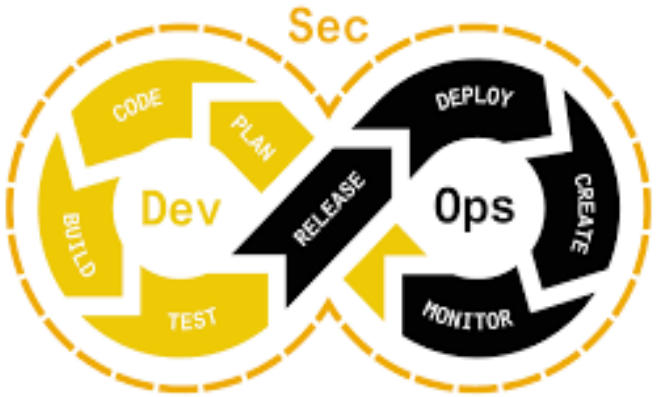
2. Nội dung: Kết nối, chia sẻ thông tin giám sát an toàn thông tin với Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) trực thuộc Cục ATTT.

3. Hướng dẫn kết nối: Văn bản số 2973/BTTTT-CATTT ngày 04/9/2019 về việc hướng dẫn triển khai hoạt động giám sát ATTT trong cơ quan, tổ chức nhà nước.

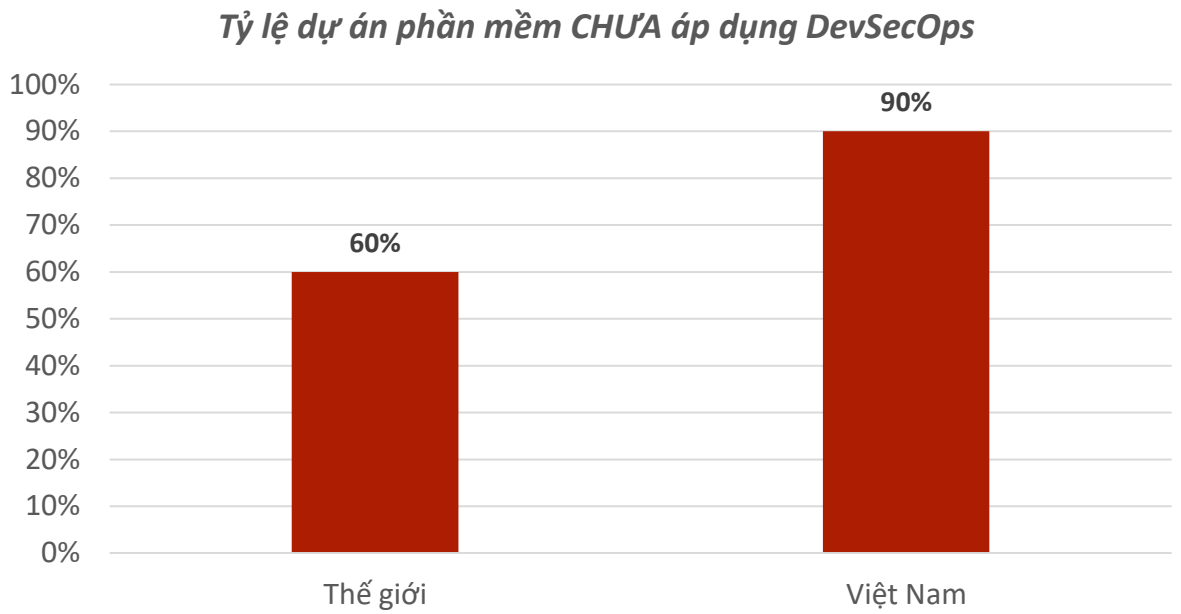
4. Định kỳ hàng tháng, Cục ATTT sẽ có báo cáo tình hình an toàn thông tin và thống kê kết nối chia sẻ dữ liệu về mã độc, giám sát.



3. KHUNG PHÁT TRIỂN PHẦN MỀM AN TOÀN (DEVSECOPS)



Tất cả mọi thành phần đều có trách nhiệm với bảo mật



- Áp dụng DevSecOps khi phát triển phần mềm tăng lên **40%** năm 2024 (*)
- **90%** dự án phần mềm yêu cầu tuân theo DevSecOps trước năm 2022, tăng **42%** so 2019 (**)

Công văn số 166 /CATTT-ATHTTT Ban hành hướng dẫn "Khung phát triển phần mềm an toàn (phiên bản 1.0)"

Xây dựng theo NIST Special Publication 800-218, Secure Software Development Framework (SSDF) Version 1.1

4. ỨNG CỨU SỰ CỐ

Chỉ thị 18/CT-TTg yêu cầu ứng cứu sự cố phải chuyển từ "bị động" sang "chủ động"

1. Tổ chức hiệu quả hoạt động của Đội ứng cứu sự cố, tự đánh giá mức độ trưởng thành của Đội

2. Quy định trách nhiệm và quy trình phối hợp giữa các lực lượng tham gia ứng cứu sự cố

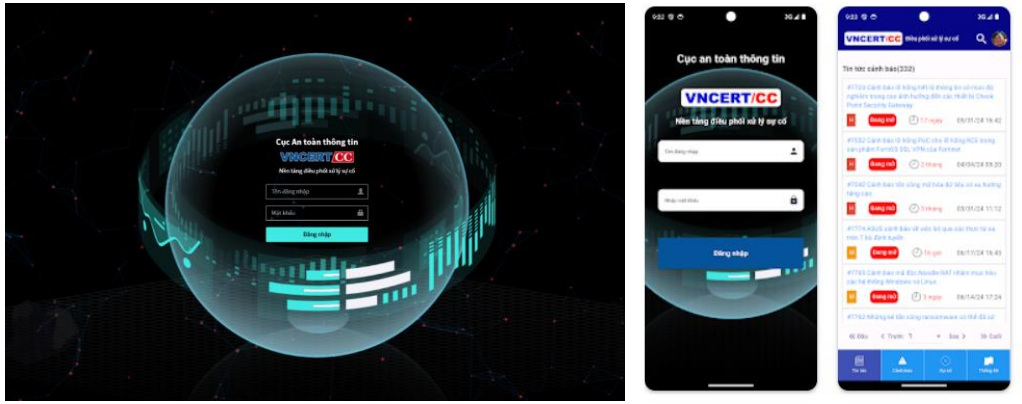
3. Xây dựng sẵn kịch bản, quy trình ứng cứu sự cố cho một số sự cố tấn công mạng

4. Chủ động thực hiện săn lùng mối nguy hại và rà quét lỗ hổng trên các hệ thống

5. Tổ chức huấn luyện, diễn tập ứng cứu sự cố trên các hệ thống thông tin, khai thác hiệu quả các công cụ, nền tảng

ĐIỀU PHỐI XỬ LÝ SỰ CỐ QUA NỀN TẢNG KỸ THUẬT

“Năm 2023, công tác quản lý nhà nước về ứng cứu sự cố cơ bản được chuyển dịch lên môi trường số”



Cảnh báo sự cố ATTT

Theo dõi danh sách địa chỉ IP public của tổ chức.

Cập nhật thông tin hàng ngày

Lỗ hổng bảo mật mới nhất, các bài phân tích chuyên sâu, các công cụ, kỹ thuật khai thác…

Báo cáo sự cố ATTT

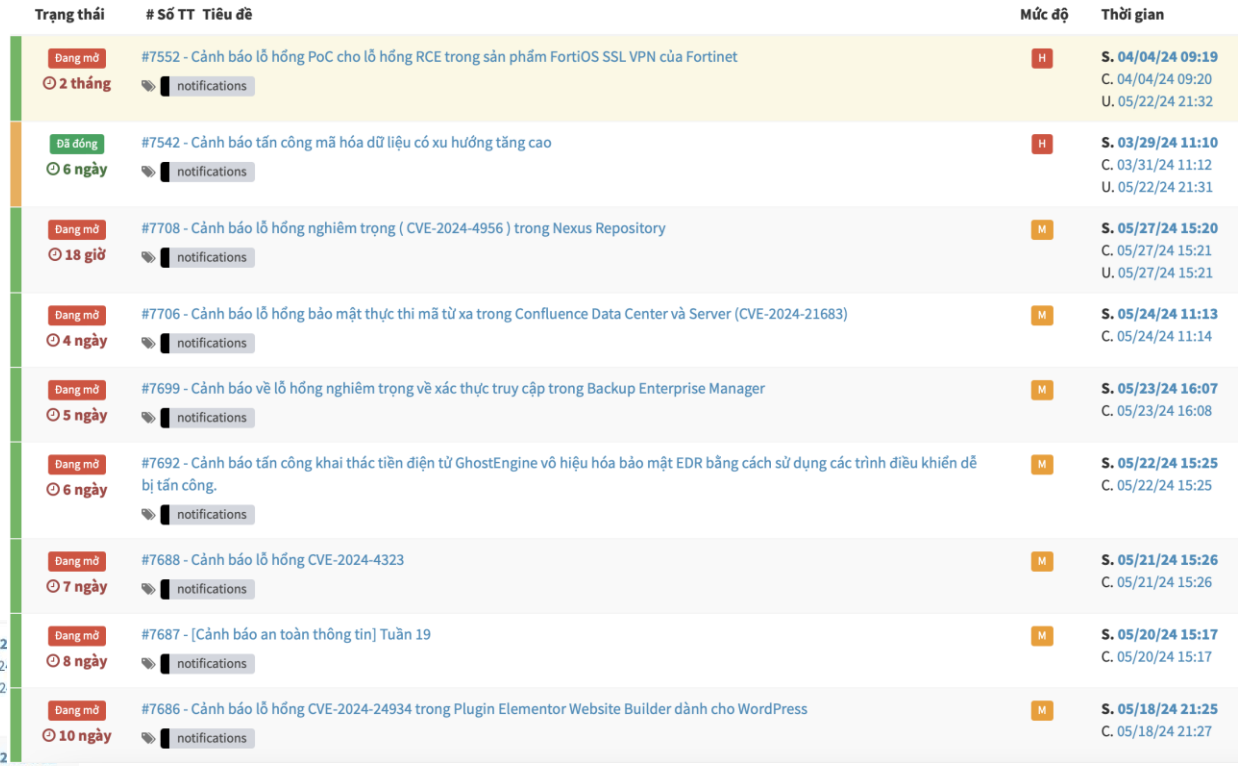
Báo cáo sự cố, hỗ trợ điều phối, xử lý sự cố từ xa.

Liên thông các nền tảng

Cung cấp hệ thống nghiệp vụ và chuyên biệt về điều tra số.

ĐIỀU PHỐI XỬ LÝ SỰ CỐ QUA NỀN TẢNG KỸ THUẬT

- Cảnh báo 50.763 cho các tổ chức,
- Điều phối xử lý 5.726 sự cố, tập trung vào sự cố liên quan đến mã độc, phishing và lỗ hổng bảo mật
- 1145/3961 tổ chức/cá nhân sử dụng



ỨNG CỨU XỬ LÝ SỰ CỐ QUA NỀN TẢNG KỸ THUẬT

Nền tảng DFLab được đưa vào vận hành cho phép các chuyên gia của Cục ATTT ngồi tập trung một chỗ để thực hiện phân tích, điều tra số từ xa và không phụ thuộc khoảng cách địa lý.

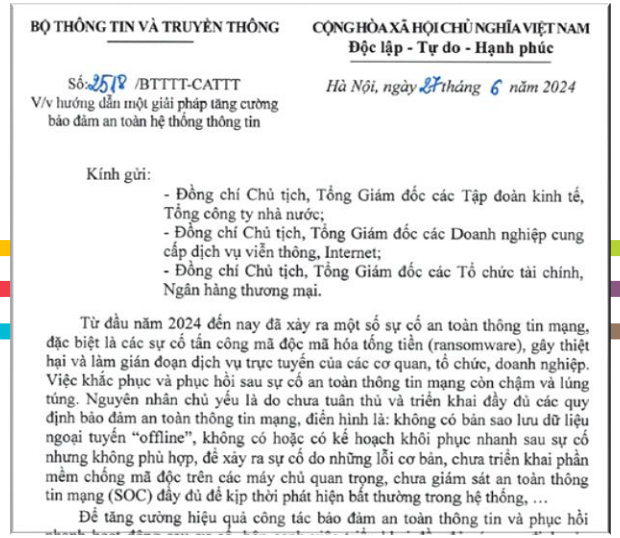
DFLab cho phép phân tích, điều tra số trên một phạm vi rộng lớn lên đến hàng trăm, hàng ngàn máy tính với nguồn lực chuyên gia ít, thời gian ngắn. DF Lab rút ngắn được khoảng 70% thời gian, công sức

MỘT SỐ BIỆN PHÁP CẦN TRIỂN KHAI ĐỂ TĂNG CƯỜNG BẢO ĐẢM AN TOÀN THÔNG TIN CHO HỆ THỐNG THÔNG TIN

1
Định kỳ thực hiện sao lưu dữ liệu ngoại tuyến "offline" theo chiến lược 3-2-1

2
Triển khai giải pháp để sẵn sàng phục hồi nhanh hoạt động của hệ thống

3
Triển khai các giải pháp ngăn ngừa, phát hiện sớm nguy cơ tấn công mạng



BỘ THÔNG TIN VÀ TRUYỀN THÔNG

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Số: 2518 /BTTTT-CATTT
V/v hướng dẫn một giải pháp tăng cường bảo đảm an toàn hệ thống thông tin

Hà Nội, ngày 27 tháng 6 năm 2024

Kính gửi:
- Đồng chí Chủ tịch, Tổng Giám đốc các Tập đoàn kinh tế, Tổng công ty nhà nước;
- Đồng chí Chủ tịch, Tổng Giám đốc các Doanh nghiệp cung cấp dịch vụ viễn thông, Internet;
- Đồng chí Chủ tịch, Tổng Giám đốc các Tổ chức tài chính, Ngân hàng thương mại.

Từ đầu năm 2024 đến nay đã xảy ra một số sự cố an toàn thông tin mạng, đặc biệt là các sự cố tấn công mã độc mã hóa tống tiền (ransomware), gây thiệt hại và làm gián đoạn dịch vụ trực tuyến của các cơ quan, tổ chức, doanh nghiệp. Việc khắc phục và phục hồi sau sự cố an toàn thông tin mạng còn chậm và lúng túng. Nguyên nhân chủ yếu là do chưa tuân thủ và triển khai đầy đủ các quy định bảo đảm an toàn thông tin mạng, điển hình là: không có bản sao lưu dữ liệu ngoại tuyến "offline", không có hoặc có kế hoạch khôi phục nhanh sau sự cố nhưng không phù hợp, để xảy ra sự cố do những lỗi cơ bản, chưa triển khai phần mềm chống mã độc trên các máy chủ quan trọng, chưa giám sát an toàn thông tin mạng (SOC) đầy đủ để kịp thời phát hiện bất thường trong hệ thống, …

Để tăng cường hiệu quả công tác bảo đảm an toàn thông tin và phục hồi

4
Phân tách, tăng cường kiểm soát truy cập giữa các vùng mạng

5
Tăng cường giám sát, quản lý các tài khoản quan trọng/quản trị

6
Rà soát, khắc phục và không để xảy ra các lỗi cơ bản dẫn đến mất an toàn

04 Khuyến nghị

KHUYẾN NGHỊ

Yêu cầu các tổ chức, doanh nghiệp phần mềm áp dụng mô hình DevSecOps khi xây dựng, phát triển ứng dụng

Thực hiện và duy trì hoạt động sao lưu, dự phòng dữ liệu đầy đủ, an toàn

Kiểm tra, đánh giá an toàn thông tin mạng các hệ thống thông tin trước và trong khi sử dụng, mỗi khi có nâng cấp, thay đổi

Xây dựng và phát triển Đội ứng cứu sự cố

Phê duyệt và triển khai các biện pháp đảm bảo an toàn thông tin cấp độ.

Duy trì đầy đủ các hoạt động đảm bảo an toàn thông tin: giám sát, kiểm tra đánh giá, diễn tập thực chiến, săn lùng mối nguy hại

Người đứng đầu chịu trách nhiệm chỉ đạo nội dung về an toàn thông tin

Nâng cao nhận thức cho nhân viên để mỗi người đều trở thành "thành trì" trong công tác đảm bảo an toàn thông tin cho tổ chức

KIỂM TRA TUÂN THỦ QUY ĐỊNH CỦA PHÁP LUẬT

An toàn thông tin mạng là yêu cầu **“bắt buộc”,** không phải là yếu tố để **“lựa chọn”**. Cục An toàn thông tin sẽ đề nghị:

1. 100% bộ, ngành, địa phương cần tổ chức kiểm tra, đánh giá tuân thủ quy định của pháp luật về an toàn thông tin:

2. Ưu tiên, tập trung kiểm tra tuân thủ quy định pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ và bảo vệ thông tin, dữ liệu cá nhân

3. Ưu tiên kiểm tra, đánh giá đối với các đơn vị, tổ chức, doanh nghiệp đang được giao quản lý, vận hành nhiều hệ thống thông tin hoặc hệ thống thông tin quan trọng, dùng chung.

“Cùng với phát triển dữ liệu, chuyển đổi số, chúng ta cũng cần chú trọng đến an toàn, an ninh mạng ngay từ đầu. Chúng tôi vẫn nói và lặp đi lặp lại rằng chuyển đổi số cần an toàn, an ninh mạng giống như một chiếc xe cần có phanh. Phanh không phải để dừng chiếc xe lại, mà để chúng ta yên tâm nhấn ga đi nhanh hơn. Chuyển đổi số muốn nhanh, bền vững thì an toàn, an ninh mạng phải song hành và trở thành một phần không thể tách rời”.

Thứ trưởng Bộ Thông tin và Truyền thông Nguyễn Huy Dũng

CỤC AN TOÀN THÔNG TIN
AUTHORITY OF INFORMATION SECURITY

CỤC AN TOÀN THÔNG TIN

Chính sách tốt. Thực thi tốt

Trân trọng cảm ơn!