BỘ THÔNG TIN VÀ TRUYỀN THÔNG

TRUNG TÂM ỨNG CỨU SỰ CỐ MÁY TÍNH VIỆT NAM

HỆ THỐNG MẠNG LƯỚI GIÁM SÁT, CẢNH BÁO, ĐIỀU PHỐI, ỨNG CỨU SỰ CỐ ATTT QUỐC GIA

TS.Nguyễn Khắc Lịch

Nội dung

- Giới thiệu VNCERT
- Hoạt động Giám sát, Cảnh báo, Điều phối, Ứng cứu
- Đề xuất, kiến nghị

Giới thiệu VNCERT

- Trung tâm Ứng cứu Khẩn cấp Máy tính Việt nam - VNCERT được thành lập theo Quyết định số 339/2005/QĐ-TTg của Thủ tướng chính phủ ngày 20 tháng 12 năm 2005.
- Quyết định 1778/QĐ-BTTTT của Bộ trưởng Bộ Thông tin và Truyền thông ngày 26 tháng 10 năm 2015 quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam.
- **Chức năng chính:**
  - Giám sát an toàn thông tin đối với hệ thống, dịch vụ công nghệ thông tin của Chính phủ điện tử.
  - Cảnh báo các vấn đề về an toàn mạng.
  - Điều phối các hoạt động ứng cứu sự cố.
  - Thúc đẩy hình thành các tổ chức CERT trong nước và là đầu mối hợp tác với các tổ chức CERT nước ngoài.

Giới thiệu VNCERT

MIC

VNCERT

- Phòng Hành chính Tổng hợp
- Phòng Kế hoạch Tài chính
- Phòng Điều phối và Ứng cứu an toàn mạng
- Phòng Kỹ thuật Hệ thống
- Phòng Nghiên cứu và Phát triển
- Phòng Tư vấn Đào tạo
- Chi nhánh Đà Nẵng
- Chi nhánh TP. Hồ Chi Minh

Giới thiệu VNCERT

Các hoạt động chính trong thời gian qua:

- Xây dựng văn bản QPPL về an toàn thông tin (ATTT)
- Cảnh báo tấn công và sự cố an toàn mạng
- Điều phối ứng cứu – xử lý sự cố an toàn mạng
- Giám sát an toàn mạng
- Đầu mối nhóm ứng cứu sự cố (CSIRT) quốc gia
- Thúc đẩy và hỗ trợ thành lập các nhóm ứng cứu các tỉnh, địa phương
- Đầu mối CERT Việt Nam, làm việc và hợp các với các tổ chức CERT của các nước cũng như hợp tác quốc tế trong lĩnh vực an toàn thông tin
- Kiểm tra, đánh giá an toàn mạng và hệ thống thông tin
- Quản lý, phòng và chống tin nhắn rác
- Xây dựng các tiêu chuẩn kỹ thuật

Hoạt động

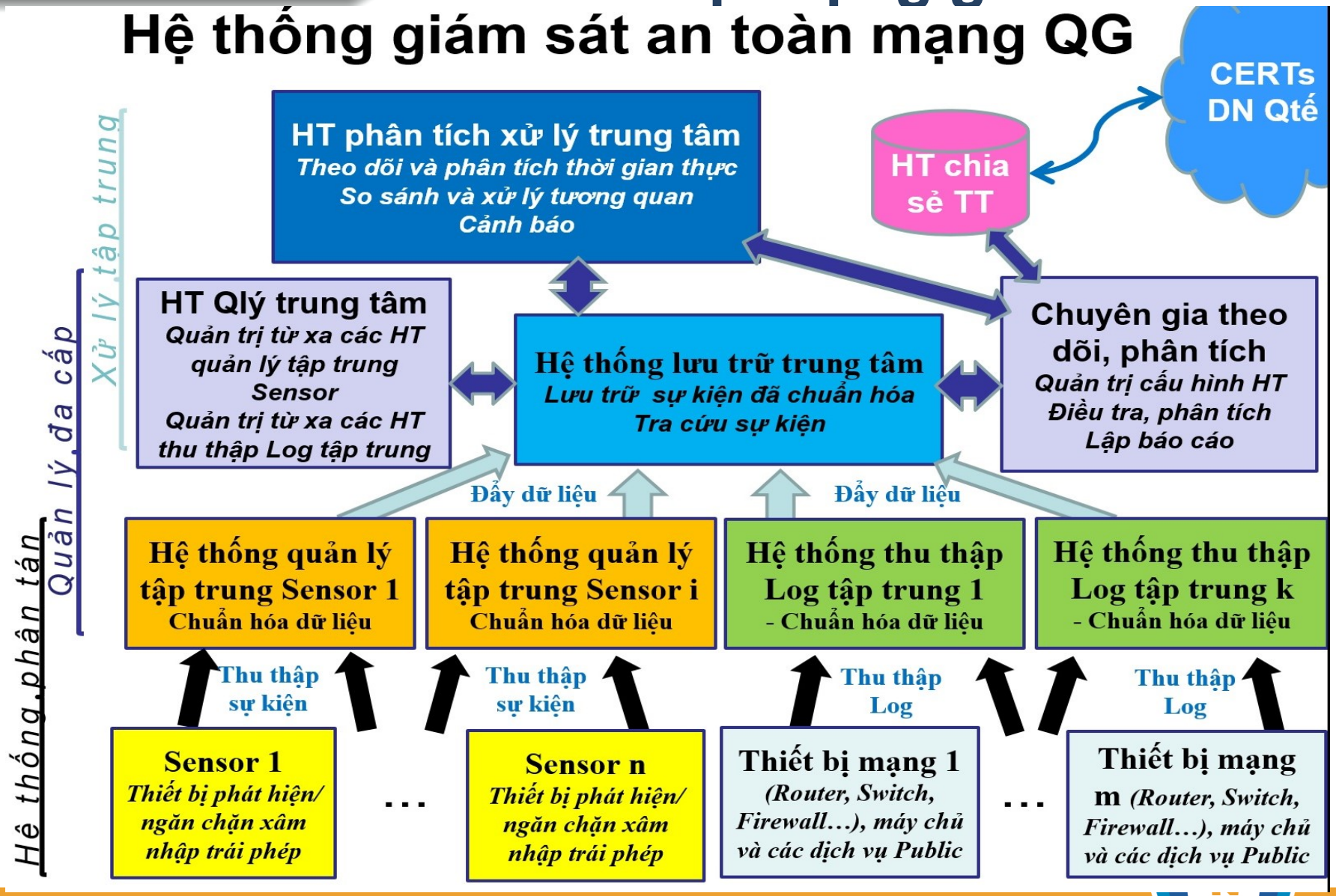
+ Giám sát
+ Cảnh báo
+ Điều phối
+ Ứng cứu

CƠ SỞ PHÁP LÝ

- **Luật**
  - Luật An toàn thông tin mạng, Luật Giao dịch điện tử, Luật Viễn thông, Luật Công nghệ thông tin, Luật Hình sự, Các điều 224-226b về ATTT số, Luật Cơ yếu
- **Nghị định**
  - NĐ 64/2007/NĐ-CP ngày 10/04/2007 - Ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước
  - NĐ 90/2008/NĐ-CP ngày 13/08/2008 – Chống thư rác và Nghị định 77/2012/NĐ-CP ngày 05/10/2012 Sửa đổi bổ sung một số điều trong nghị định 90 về Chống thư rác, thông tư 12/2008/TT-BTTTT về Chống thư rác
  - NĐ 72/2013/NĐ-CP ngày 15/07/2013 - Quy định về quản lý, cung cấp, sử dụng dịch vụ Internet và thông tin trên mạng
- **Nghị Quyết**
  - Nghị quyết 36a/NQ-CP ngày 14/10/2015 về xây dựng chính phủ điện tử, trong đó giao việc thực hiện giám sát an toàn thông tin đối với hệ thống, dịch vụ CNTT của Chính phủ điện tử cho Bộ Thông tin Truyền thông.
- **Thông tư**
  - TT 27/2011/TT-BTTTT ngày 04/10/2011 - Quy định về điều phối các hoạt động mạng lưới ứng cứu sự cố mạng Internet Việt Nam

Hoạt động giám sát

Hệ thống giám sát an toàn mạng QG

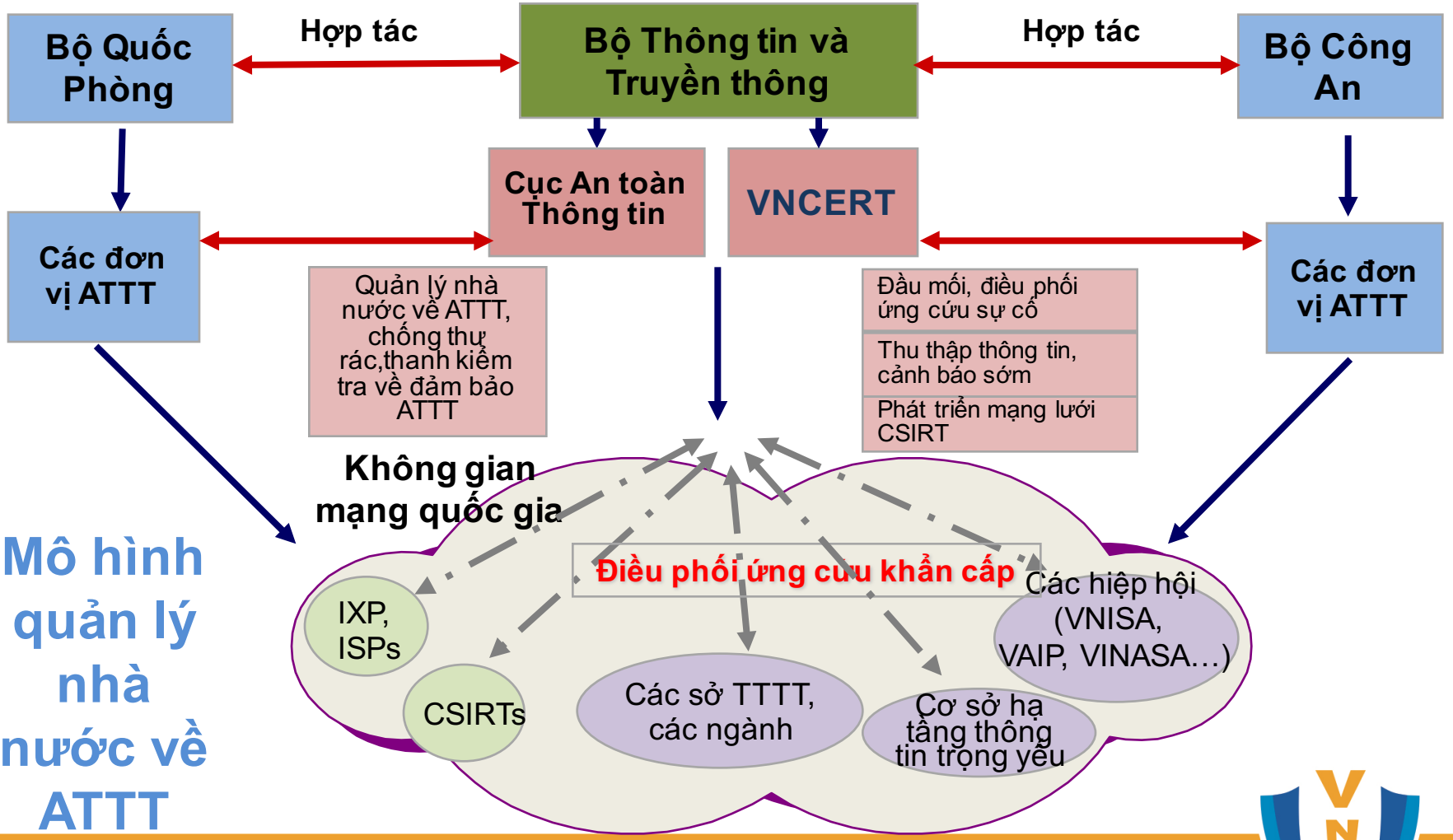


Hoạt động Cảnh báo

- **Cảnh báo, hướng dẫn xử lý các sự cố về an toàn mạng:**
  - ✓ Mã độc, phần mềm gián điệp
  - ✓ Tấn công thay đổi giao diện
  - ✓ Lừa đảo – Phishing
  - ✓ Mạng máy tính ma, DDoS
  - ✓ Các địa chỉ IP nhiễm mã độc botnet

- **Cảnh báo kỹ thuật:**
  - ✓ Cảnh báo lỗ hổng bảo mật
  - ✓ Các biện pháp kỹ thuật hạn chế rủi ro

Hoạt động Điều phối - Ứng cứu



Mô hình quản lý nhà nước về ATTT

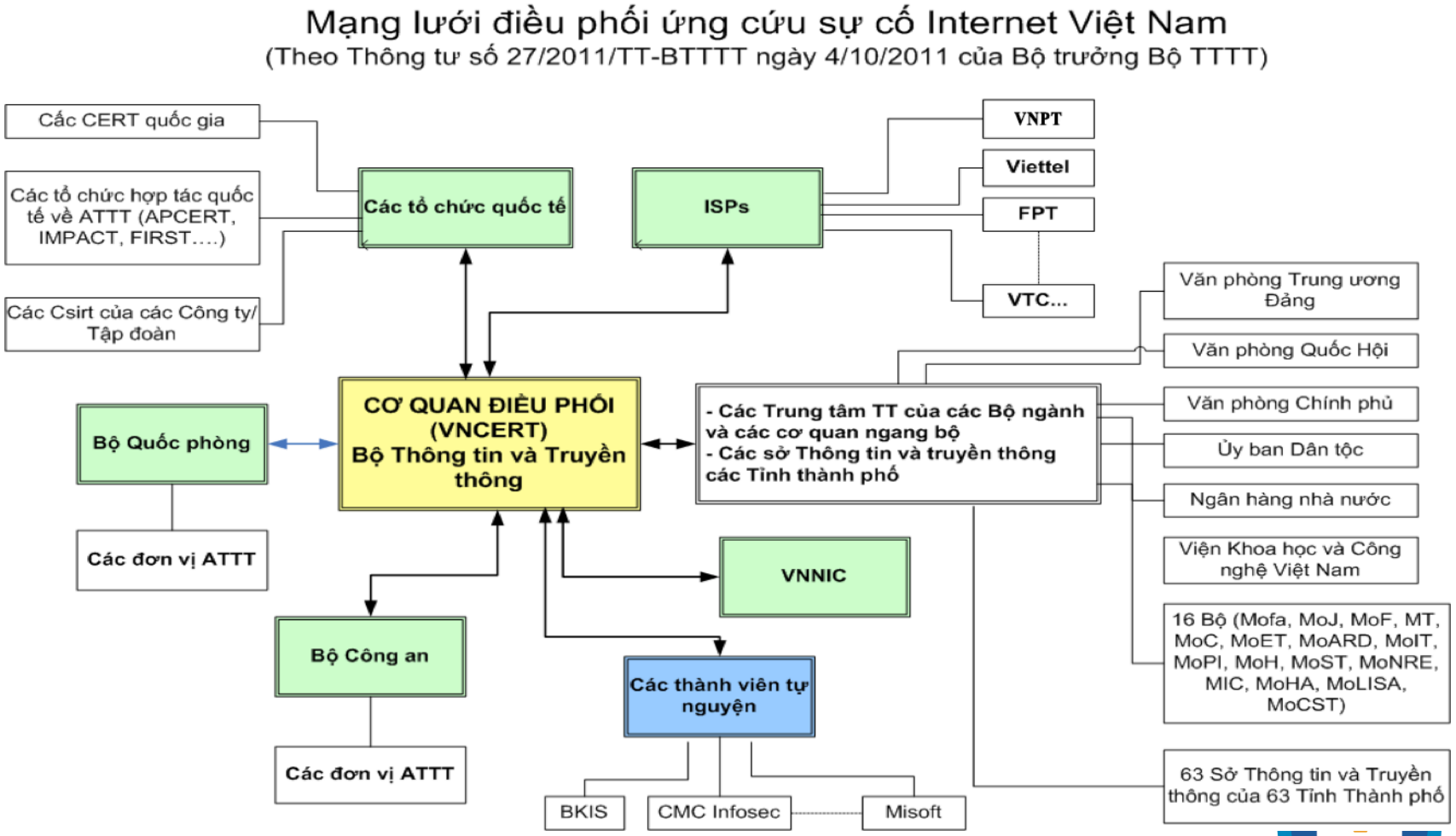
Hoạt động Điều phối - Ứng cứu

Mạng lưới ứng cứu sự cố bảo mật CSIRT (Computer Security Incident Response Team)

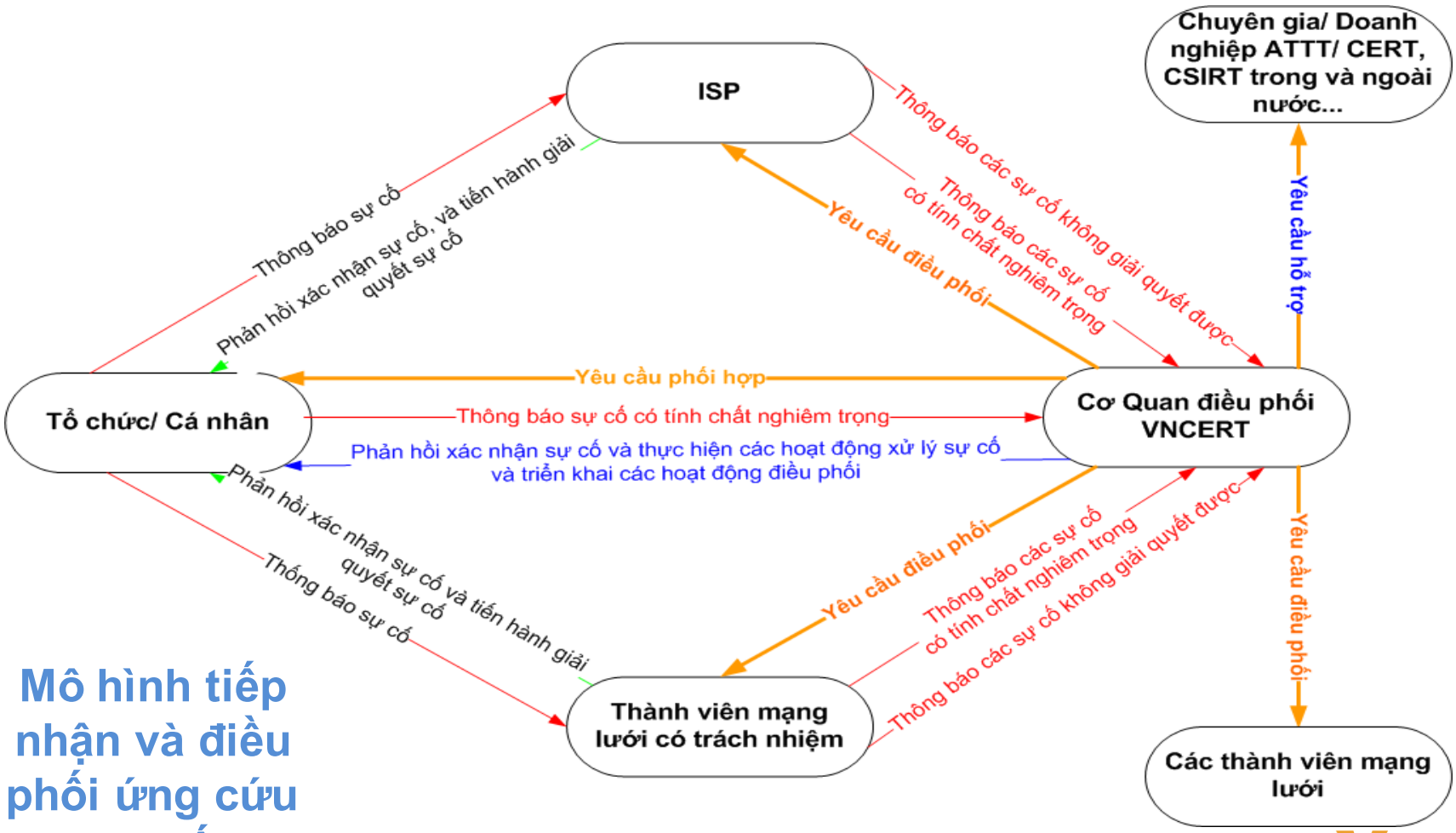
- **Cơ quan điều phối quốc gia: VNCERT**
  - Điều phối các hoạt động ứng cứu sự cố trên toàn quốc và có quyền điều động các tổ chức khác trong mạng lưới phối hợp ngăn chặn, xử lý và khắc phục sự cố mạng Internet tại Việt Nam;
  - Quyết định hình thức điều phối các hoạt động ứng cứu sự cố và chịu trách nhiệm về các yêu cầu điều phối;
  - Đầu mối trao đổi thông tin về hợp tác ứng cứu sự cố với các tổ chức ứng cứu khẩn cấp máy tính quốc tế
- **Các nguyên tắc hoạt động của mạng lưới điều phối ứng cứu:**
  - Bảo mật, bảo vệ thông tin riêng của các tổ chức
  - Chấp nhận chia sẻ thông tin qua tài liệu, thư điện tử, điện thoại, fax. Các thông tin sẽ được kiểm tra và xác nhận
  - Các thành viên sẽ nhận các thông tin chia sẻ, các kinh nghiệm và tham gia các diễn tập, các khoá huấn luyện về phản ứng các sự cố

Hoạt động Điều phối - Ứng cứu

(120 thành viên cơ quan, tổ chức với hơn 1000 thành viên cá nhân)



Hoạt động Điều phối - Ứng cứu



Mô hình tiếp nhận và điều phối ứng cứu sự cố

Hoạt động Điều phối - Ứng cứu

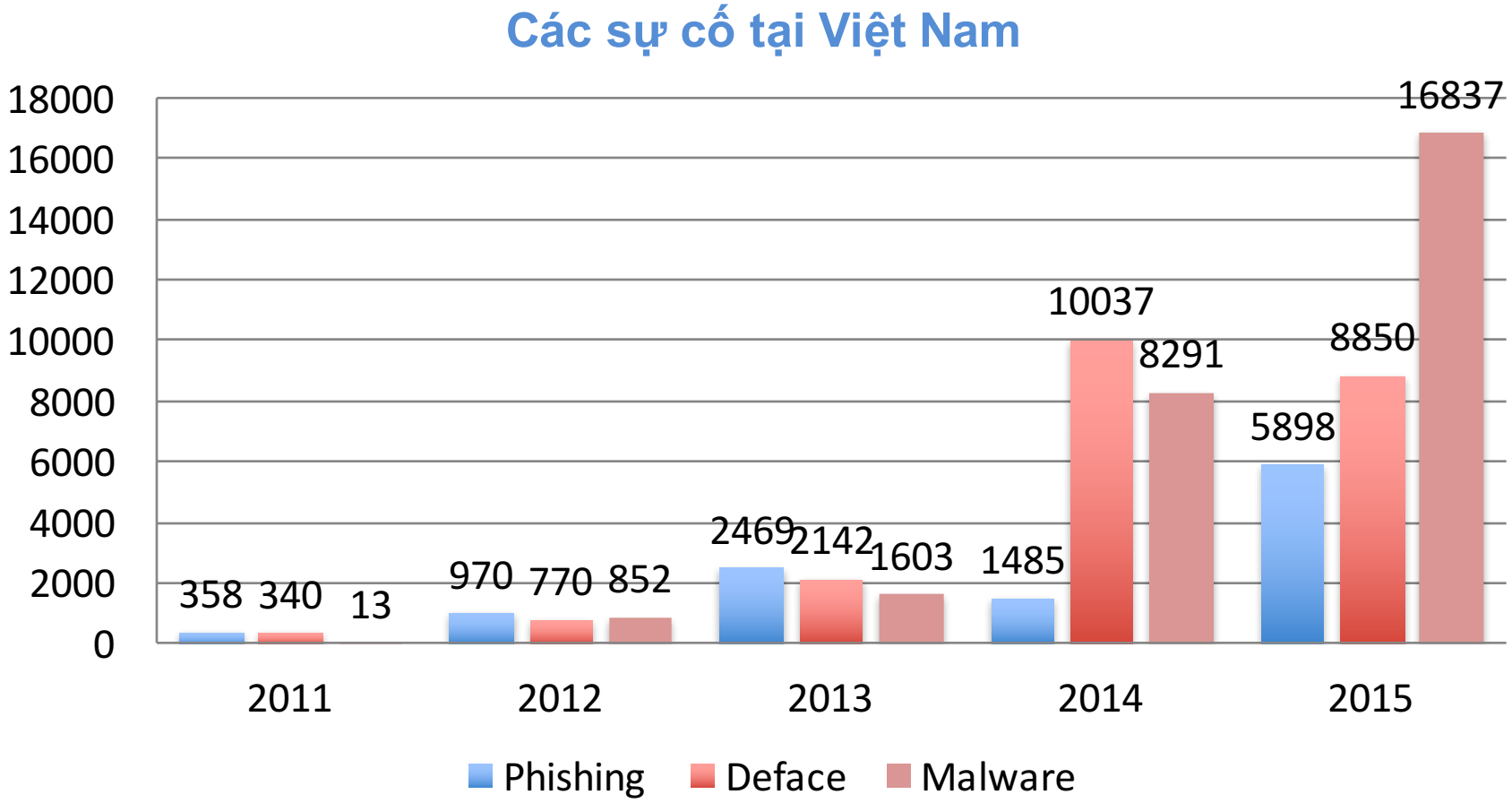
- Thành viên chính thức của APCERT (2008)
- Thoả thuận hợp tác (MoU) với JPCERT/CC (2009), KISA (2009), Bộ Viễn thông và Internet Lào (2010)
- Phối hợp với KISDI, Microsoft, Google, TWCERT, USCERT, CERT-Brazil và nhiều tổ chức CERT của các nước trên thế giới
- Tổ chức cho mạng lưới ứng cứu sự cố quốc gia tham gia thường niên 03 tập trận về An toàn mạng quốc tế:
  - Tập trận hàng năm của APCERT, bao gồm 20 quốc gia và vùng lãnh thổ thuộc khu vực Châu Á, Thái bình dương
  - Tập trận hàng năm của 11 Quốc gia ASEAN - Nhật Bản
  - Tập trận hàng năm của CERT 10 Quốc gia ASEAN và các quốc gia đối thoại
- Tổ chức 01 tập trận toàn quốc về an toàn mạng cho các thành viên mạng lưới ứng cứu sự cố quốc gia.

Hoạt động Điều phối - Ứng cứu

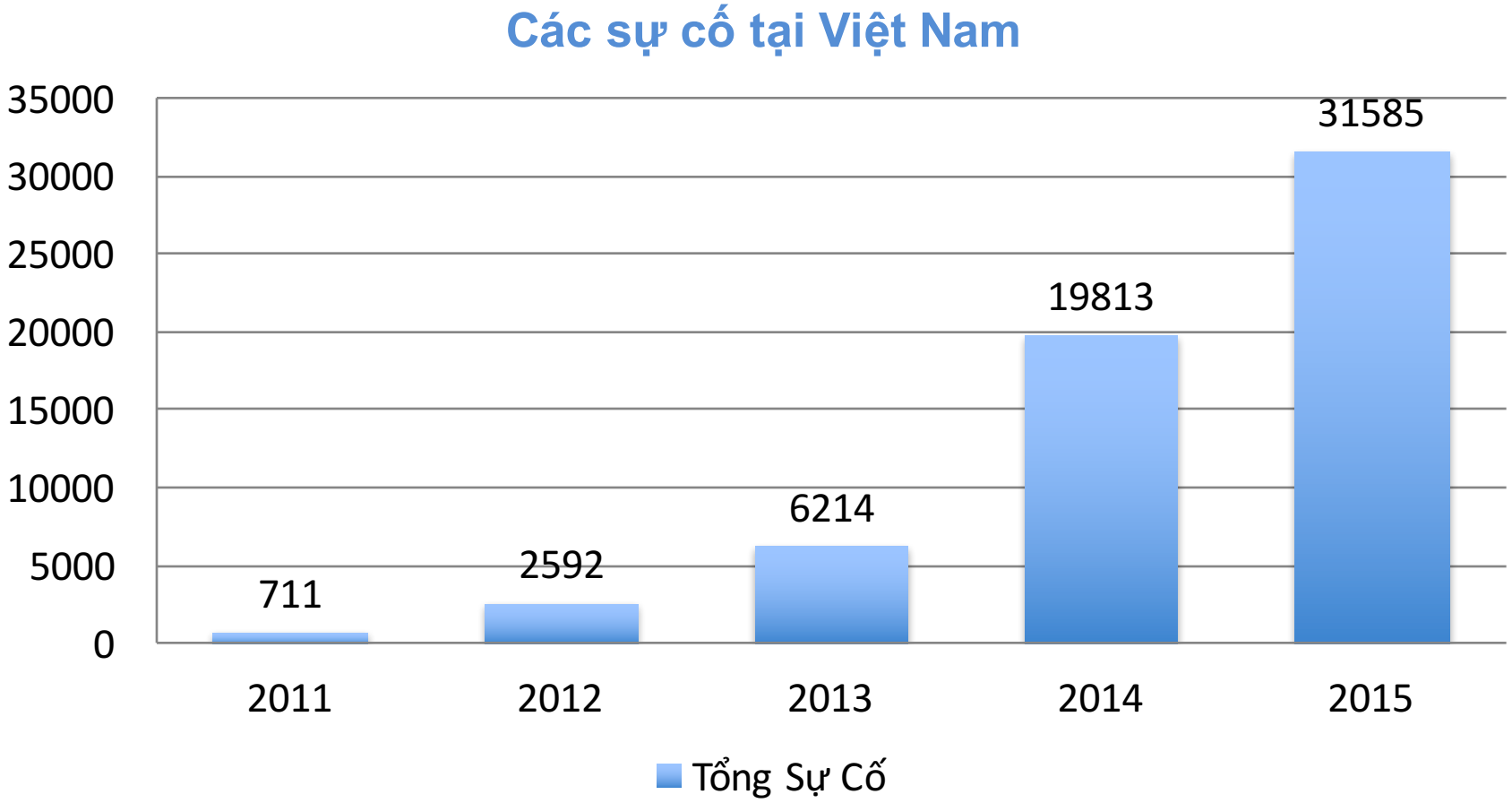
Các sự cố và điều phối 2015

- 16.837 website bị nhiễm mã độc và lây lan mã độc đến các máy tính, trong đó có 87 website/cổng thông tin điện tử của các CQNN
- 5.898 website bị tấn công và cài mã phishing
- 8.850 tấn công thay đổi giao diện (deface), trong đó có 252 website/cổng thông tin điện tử của các CQNN
- 1.451.997 lượt địa chỉ IP tham gia các mạng botnet, trong đó có 3.779 IP từ các cơ quan Nhà nước
- Điều phối và ngăn chặn 7.540 máy chủ điều khiển mã độc (C&C Server).
- Phối hợp với các CERT quốc tế để ngăn chặn hơn 200 website giả mạo: các website giả mạo giấy phép do Bộ TTTT cấp, giả mạo webmail của VNN, VDC; giả mạo website Ngân hàng Nhà nước.

Hoạt động Điều phối - Ứng cứu



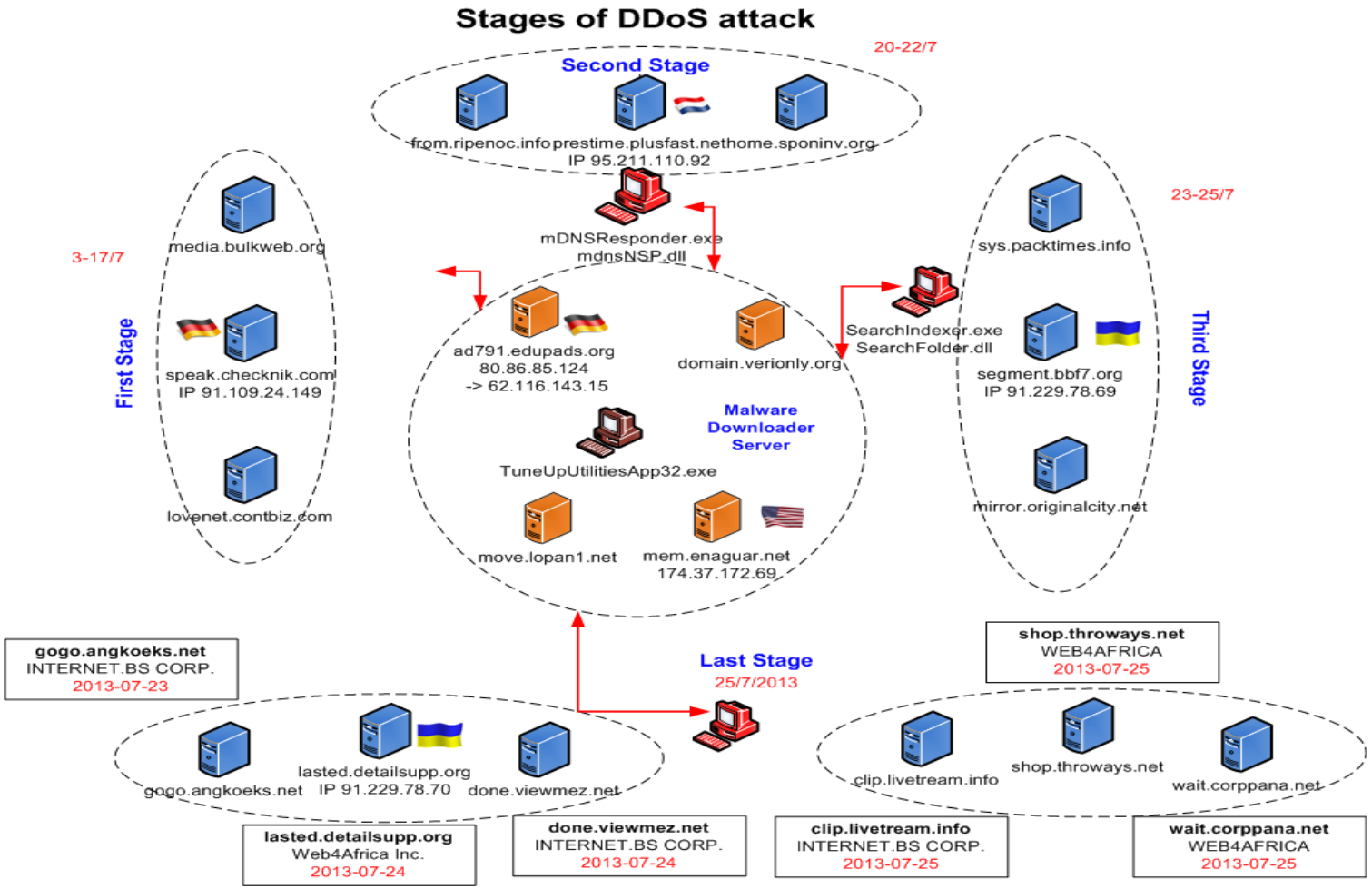
Hoạt động Điều phối - Ứng cứu



Hoạt động Điều phối - Ứng cứu

Các cuộc tấn công lớn và điển hình

Hoạt động Điều phối - Ứng cứu



Hoạt động Điều phối - Ứng cứu

Từ tháng 7/2015 đến 8/2015, Trung tâm VNCERT thực thi **chiến dịch ngăn chặn, phòng chống mã độc, mạng máy tính ma, và đề phòng các cuộc tấn công có chủ đích được hỗ trợ từ các tổ chức, Chính phủ nước ngoài**

- VNCERT phối hợp các CERT Quốc tế thu thập, phân tích, phát hiện 7.540 máy chủ đặt tại nhiều Quốc gia trực tiếp điều khiển hơn 1 triệu địa chỉ IP bị lây nhiễm mã độc.
- Đã gửi lệnh điều phối đến:
  - Viettel
  - VNPT
  - FPT
  - SCTV
  - …
- Ngăn chặn thành công 7.540 địa chỉ máy chủ điều khiển
- Yêu cầu các ISP hỗ trợ hơn 1.000.000 khách hàng gỡ bỏ các máy tính nhiễm mã độc botnet (địa chỉ IP)

Hoạt động Cảnh báo nổi bật

Năm 2015:

- VNCERT đã kiểm tra, đánh giá và đưa ra cảnh báo lỗ hổng an toàn thông tin của phần mềm phân giải tên miền BIND.
- Lỗ hổng này ảnh hưởng 70% số máy chủ trên thế giới và Việt Nam.
- Phần mềm BIND hiện đang được sử dụng khá phổ biến tại các hệ thống thông tin trọng điểm (Trung tâm hạ tầng CNTT, Trung tâm dữ liệu v.v..) của Tỉnh, Thành phố, Bộ, ngành, đoàn thể Trung ương v.v.

Trong 03 tháng đầu năm 2016:

- Gửi điều phối và cảnh báo về mã độc Ransomware (đòi tiền chuộc) có biến thể và hành vi lây nhiễm mới
- Gửi điều phối và cảnh báo về máy chủ có lỗ hổng DNS tại Việt nam bị lợi dụng để tấn công DDoS số lượng lớn

Thông tin chi tiết tại http://www.vncert.gov.vn

Phương hướng – Đề xuất Kiến nghị

Phương hướng quốc gia:

- Triển khai Nghị quyết 36a/NQ-CP ngày 14/10/2015 của Chính phủ về Chính phủ điện tử:
  - ✓ Thực hiện giám sát an toàn thông tin đối với hệ thống, dịch vụ CNTT của Chính phủ điện tử trên phạm vi toàn quốc;
  - ✓ Đẩy mạnh hoạt động của Mạng lưới Ứng cứu sự cố, hướng dẫn triển khai các biện pháp nhằm tăng cường năng lực cho các cán bộ, bộ phận chuyên trách ứng cứu sự cố mạng (CERT);
  - ✓ Đề xuất cơ chế ưu đãi thí điểm cho các cán bộ kỹ thuật an toàn thông tin và lực lượng ứng cứu sự cố an toàn mạng.
- Hoàn thiện môi trường pháp lý và cơ chế chính sách về giám sát, cảnh báo, điều phối và ứng cứu sự cố an toàn thông tin.
  - ✓ Xây dựng và hoàn thiện Thông tư Giám sát.
  - ✓ Xây dựng Quy trình và hướng dẫn hoạt động giám sát. cảnh báo, điều phối, ứng cứu.
  - ✓ Xây dựng các định mức kinh tế kỹ thuật về các hoạt động giám sát. cảnh báo, điều phối, ứng cứu.

Phương hướng – Đề xuất Kiến nghị

Phương hướng quốc gia (tiếp):

- Hoàn thiện các hệ thống kỹ thuật về:
  + Giám sát an toàn mạng quốc gia
  + Chống, ngăn chặn thư rác, tin nhắn rác
- Tăng cường đào tạo, huấn luyện kỹ năng và hoạt động tập trận an toàn thông tin cho các thành viên mạng lưới ứng cứu sự cố quốc gia.
- Hỗ trợ triển khai hệ thống quản lý an toàn thông tin tuân thủ theo tiêu chuẩn TCVN ISO/ IEC 27001.

Phương hướng – Đề xuất Kiến nghị

Kiến nghị địa phương:

- Thành lập và vận hành đội ứng cứu khẩn cấp sự cố an toàn mạng của tỉnh, khuyến khích xây dựng các tổ/đội ứng cứu khẩn cấp của các đơn vị, tổ chức lớn và có điều kiện;
- Có kế hoạch định biên nhân sự chuyên trách về ATTT, cấp tỉnh –> sở ngành –> quận huyện, làm nòng cốt cho hoạt động ATTT và các đội ứng cứu khẩn cấp sự cố mạng
- Bổ sung các giải pháp để bảo mật hệ thống toàn diện: ngăn chặn – phòng chống – phát hiện lỗ hổng – phân tích đánh giá – cảnh báo .

Phương hướng – Đề xuất Kiến nghị

Kiến nghị địa phương:

- Đào tạo, tập huấn kỹ năng về bảo mật ATM cho lực lượng CNTT Nâng cao nhận thức về an toàn TT cho cán bộ lãnh đạo, công chức viên chức và nhân dân trên địa bàn
- Bố trí ngân sách tương xứng cho hoạt động an toàn thông tin hàng năm: đào tạo, thiết bị / giải pháp, vận hành
- Phối hợp với VNCERT trong các hoạt động giám sát, cảnh báo, ứng cứu sự cố, đảm bảo an toàn thông tin trong các hoạt động tại địa phương và các hoạt động cung cấp dịch vụ về an toàn thông tin cho các tổ chức, doanh nghiệp và cá nhân trên địa bàn

TS.Nguyễn Khắc Lịch
Phó Giám đốc Trung tâm VNCERT
ĐT: 0912571223
Email: nklich@vncert.gov.vn