UBND TỈNH GIA LAI
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
Số: 168/QĐ-STTTT

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc
Gia Lai, ngày 01 tháng 8 năm 2019

QUYẾT ĐỊNH
Về việc ban hành Phương án ứng phó sự cố an toàn thông tin mạng trên địa bàn tỉnh Gia Lai

GIÁM ĐỐC SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Căn cứ Luật Tổ chức chính quyền địa phương;

Căn cứ Luật An toàn thông tin mạng;

Căn cứ 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;

Căn cứ Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ về ban hành quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia;

Căn cứ Thông tư số 03/2017/TT-BTTTT ngày 24/04/2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định về điều phối, ứng phó sự cố an toàn thông tin mạng trên toàn quốc;

Căn cứ Quyết định số 468/QĐ-UBND ngày 06/6/2017 của UBND tỉnh Gia Lai về việc ban hành Quy định về ứng phó sự cố an toàn thông tin mạng trên địa bàn tỉnh Gia Lai;

Căn cứ Quyết định số 468/QĐ-UBND ngày 12/7/2016 của UBND tỉnh Gia Lai về việc quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Sở Thông tin và Truyền thông tỉnh Gia Lai;

Căn cứ Kế hoạch số 2050/KH-UBND ngày 14/9/2018 của UBND tỉnh về việc ban hành Kế hoạch ứng phó sự cố bảo đảm an toàn thông tin mạng trên địa bàn tỉnh Gia Lai;

Theo đề nghị của Trưởng phòng Công nghệ thông tin,

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Phương án ứng phó sự cố an toàn thông tin mạng trên địa bàn tỉnh Gia Lai.

Điều 2. Các thành viên Đội ứng cứu sự cố an toàn thông tin mạng tỉnh Gia Lai (theo Quyết định số 1165/QĐ-UBND ngày 28/12/2017 của UBND tỉnh Gia Lai); Chánh Văn phòng, Trưởng các Phòng chuyên môn, Giám đốc Trung tâm Công nghệ thông tin và Truyền thông thuộc Sở Thông tin và Truyền thông tỉnh Gia Lai;

các đơn vị, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này.

Quyết định này có hiệu lực kể từ ngày ký./.

Nơi nhận:
- Như điều 3;
- UBND tỉnh (báo cáo);
- Văn phòng Tỉnh ủy;
- Văn phòng HĐND tỉnh;
- Công an tỉnh;
- Bộ Chỉ huy Quân sự tỉnh;
- Bộ Chỉ huy Bộ đội Biên phòng tỉnh;
- Các sở, ban, ngành;
- UBND các huyện, thị xã, thành phố;
- Bưu điện tỉnh;
- Các Doanh nghiệp Viễn thông trên địa bàn tỉnh;
- Báo Gia Lai; Đài PTTH tỉnh;
- Lưu: VT, P.CNTT.

GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH GIA LAI

Nguyễn Ngọc Hùng

UBND TỈNH GIA LAI
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

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

PHƯƠNG ÁN
Ứng phó sự cố an toàn thông tin mạng trên địa bàn tỉnh Gia Lai
(Ban hành kèm theo Quyết định số 168/QĐ-STTTT ngày 01 tháng 8 năm 2019 của Sở Thông tin và Truyền thông tỉnh Gia Lai)

CHƯƠNG I
SỰ CẦN THIẾT CỦA PHƯƠNG ÁN ỨNG CỨU SỰ CỐ

Căn cứ tình hình mất an toàn thông tin (ATTT) ở nước ta ngày càng diễn biến phức tạp, xuất hiện nhiều nguy cơ đe dọa nghiêm trọng đến việc ứng dụng công nghệ thông tin (CNTT) phục vụ phát triển kinh tế – xã hội và đảm bảo quốc phòng, an ninh. Theo số liệu thống kê, số vụ tấn công trên mạng và các vụ xâm nhập hệ thống CNTT nhằm do thám, trục lợi, phá hoại dữ liệu, ăn cắp tài sản, cạnh tranh không lành mạnh... đang gia tăng ở mức báo động về số lượng, đa dạng về hình thức và ngày càng tinh vi hơn về công nghệ. Kết quả nghiên cứu, khảo sát cũng cho thấy nhiều hệ thống CNTT của các cơ quan Nhà nước và doanh nghiệp, đặc biệt là các Cổng/Trang thông tin điện tử (TTĐT) có nhiều điểm yếu về ATTT, chưa được áp dụng các giải pháp đảm bảo an toàn và bảo mật thông tin phù hợp.

Bất kỳ một sự cố nào khi không được xử lý ngay có thể trở thành một vấn đề lớn trong an ninh mạng và cuối cùng nó có thể dẫn tới sự phá hủy dữ liệu hoặc làm sụp đổ hệ thống. Đối phó kịp thời với sự cố một cách nhanh chóng giúp tổ chức giảm thiểu sự thiệt hại, hạn chế các lỗ hổng, ngăn chặn mã độc tấn công, phục hồi các quy trình dịch vụ và giảm thiểu rủi ro an ninh mà các sự cố trong tương lai gây ra.

Căn cứ kết quả khảo sát tại Trung tâm Tích hợp dữ liệu của tỉnh (TTTHDL) và các sở, ban, ngành; UBND các huyện, thị xã, thành phố thuộc tỉnh, Sở Thông tin và Truyền thông có một số đánh giá như sau:

- Hệ thống thông tin của tỉnh được phân tán nhiều nơi, chứa các ứng dụng dùng chung, một số sở, ban, ngành có các ứng dụng chuyên ngành, đặc thù và ứng dụng tự quản với mức độ phức tạp cao. Vì vậy khi xảy ra các sự cố thường sẽ bị động trong phần lớn các tình huống. Một phần do các cán bộ quản trị hệ thống chưa được tham gia nhiều các khoá đào tạo về ứng cứu sự cố và còn bỡ ngỡ khi gặp các tình huống chưa dự phòng.

- Nhân sự quản trị hệ thống thông tin còn chưa được chú trọng, một số đơn vị chưa bố trí cán bộ chuyên trách về CNTT.

- Đội ứng cứu sự cố an toàn thông tin mạng của tỉnh đã được thành lập, ban hành quy chế hoạt động, tuy nhiên vẫn chưa có các phương án ứng cứu sự cố để đảm bảo công tác phối hợp giữa các cơ quan, đơn vị và thực hiện ứng cứu sự cố an toàn thông tin một cách hiệu quả.

Vì vậy, việc xây dựng các phương án ứng cứu sự cố là cần thiết trong công tác ứng cứu và xử lý sự cố an toàn thông tin trên địa bản tỉnh Gia Lai nhằm trang bị thêm các kiến thức cho đội ngũ cán bộ ứng cứu sự cố của tỉnh; đồng thời là căn cứ để Đội ứng cứu sự cố an toàn thông tin (ATTT) mạng tỉnh Gia Lai bảo đảm hoạt động có hiệu quả trong quá trình thực hiện công tác ứng cứu sự cố ATTT mạng trên địa bàn tỉnh.

CHƯƠNG II
PHÂN LOẠI SỰ CỐ AN TOÀN THÔNG TIN

I. CÁC NHÓM SỰ CỐ AN TOÀN THÔNG TIN

Các nhóm sự cố ATTT được chia theo các nhóm sau:

- Sự cố do bị tấn công mạng.
- Sự cố do lỗi của hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật hoặc do lỗi đường điện, đường truyền, hosting...
- Sự cố do lỗi của người quản trị, vận hành hệ thống.
- Sự cố liên quan đến các thảm họa tự nhiên như bão, lụt, động đất, hỏa hoạn v.v...

II. PHÂN LOẠI SỰ CỐ AN TOÀN THÔNG TIN

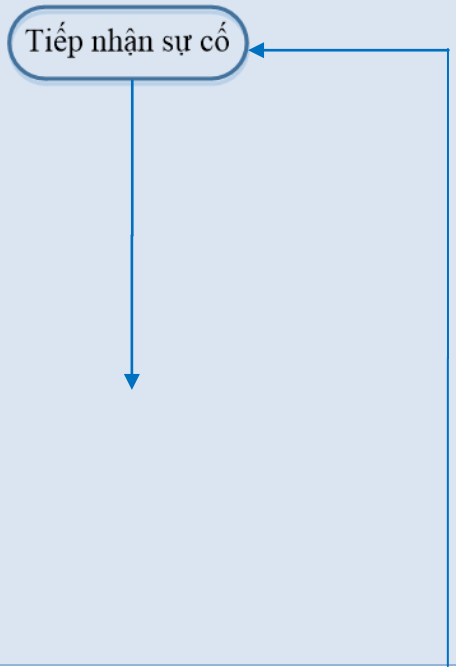
Để thực hiện tốt việc ứng cứu sự cố, cần thực hiện phân loại và lập bảng phân loại sự cố an toàn thông tin như bên dưới, từ đó xây dựng phương án cụ thể cho từng loại rủi ro sự cố:

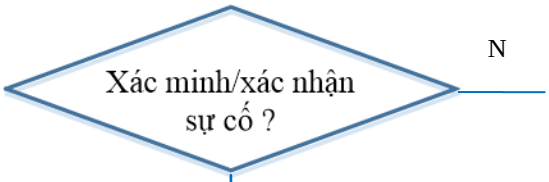
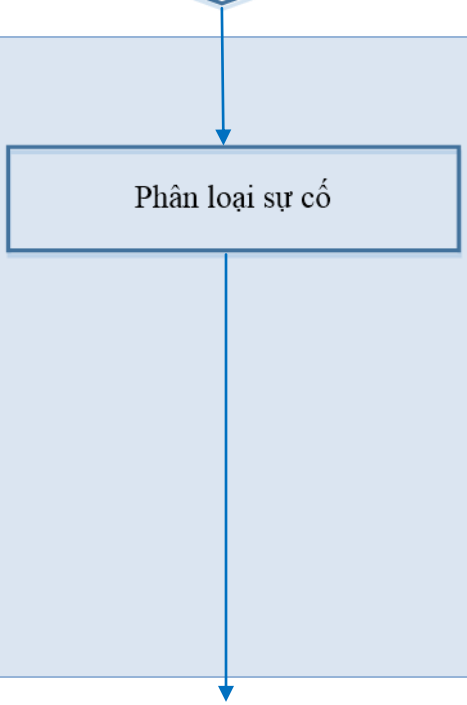
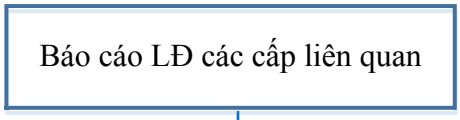
STT	Loại	Mô tả	Các sự cố
1	Sự cố do bị tấn công mạng	Các sự cố do tấn công mạng (từ internet hoặc từ mạng nội bộ)	- Tấn công từ chối dịch vụ; - Tấn công giả mạo; - Tấn công sử dụng mã độc; - Tấn công truy cập trái phép, chiếm quyền điều khiển; - Tấn công thay đổi giao diện; - Tấn công mã hóa phần mềm, dữ liệu, thiết bị; - Tấn công phá hoại thông tin, dữ liệu, phần mềm; - Tấn công nghe trộm, gián điệp, lấy cắp thông tin, dữ liệu; - Tấn công tổng hợp sử dụng kết hợp nhiều hình thức;
2	Sự cố do lỗi của hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật	Các lỗi xuất phát từ hệ thống (không phải do yếu tố con người)	- Sự cố nguồn điện; - Sự cố đường kết nối Internet; - Sự cố do lỗi phần mềm, phần cứng, ứng dụng của hệ thống thông tin;

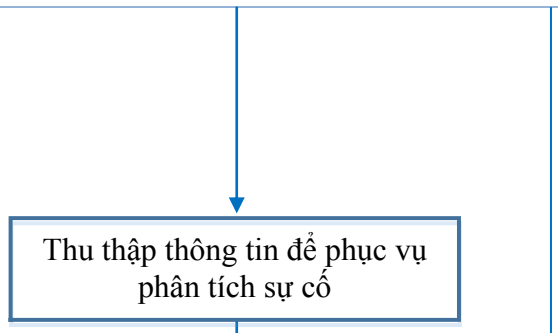
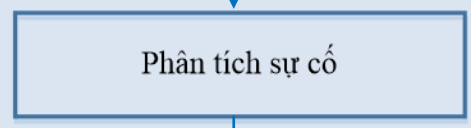
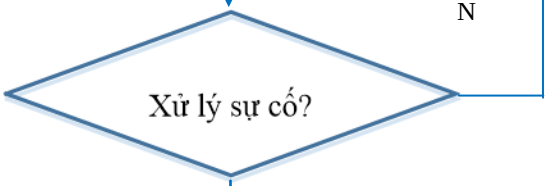
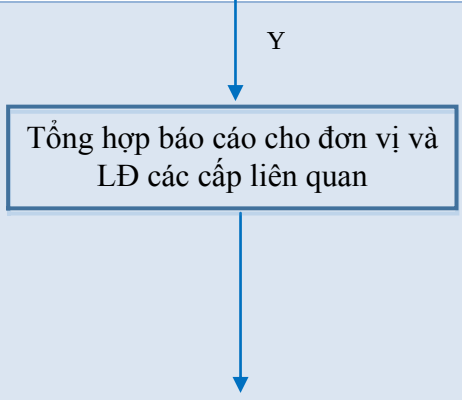
			- Sự cố liên quan đến quá tải hệ thống; - Sự cố khác do lỗi của hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật.
3	Sự cố do lỗi của người quản trị, vận hành hệ thống	Các lỗi xuất phát từ quá trình vận hành hệ thống, từ phía con người.	- Lỗi trong cập nhật, thay đổi, cấu hình phần cứng; - Lỗi trong cập nhật, thay đổi, cấu hình phần mềm; - Lỗi liên quan đến chính sách và thủ tục an toàn thông tin; - Lỗi liên quan đến việc dừng dịch vụ vì lý do bắt buộc; - Lỗi khác liên quan đến người quản trị, vận hành hệ thống.
4	Sự cố liên quan đến các thảm họa tự nhiên	Các sự cố về thảm họa tự nhiên	Bão lụt, động đất,...

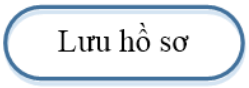
CHƯƠNG III
QUY TRÌNH VÀ BIỂU MẪU ỨNG CỨU

I. QUY TRÌNH TỔNG QUÁT VỀ ỨNG CỨU SỰ CỐ

Người thực hiện	Các bước thực hiện	Ghi chú, biểu mẫu
Viên chức, nhân viên thuộc Trung tâm Công nghệ thông tin và Truyền thông (TT.CNTT&TT) - Bộ phận giúp việc Đội ứng cứu sự số ATTT mạng – được giao tiếp nhận thông tin sự cố ATTT mạng của tỉnh (gọi tắt là Cán bộ TTTHDL)		- Thông báo sự cố (Công văn, email, điện thoại) - Phát hiện sự cố thông qua kiểm tra, rà soát, đánh giá

Cán bộ TTTHDL		Xem xét tình trạng, mức độ, phạm vi và độ ưu tiên xử lý
Cán bộ TTTHDL		- Sự cố do bị tấn công mạng - Sự cố do lỗi của hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật hoặc do lỗi đường điện, đường truyền, hosting, ...; - Sự cố do lỗi của người quản trị, vận hành hệ thống; - Sự cố liên quan đến các thảm họa tự nhiên như bão, lụt, động đất, hỏa hoạn v.v.... - Sự cố tấn công khác
Cán bộ TTTHDL		Chỉ đạo xử lý và phân công trách nhiệm xử lý
TT.CNTT&TT, Đội ứng cứu sự cố ATTT mạng tỉnh, chuyên gia ứng cứu sự cố, các đơn vị liên quan (Cơ quan điều phối quốc gia về ứng cứu sự cố để được hỗ trợ khắc phục các sự cố vượt quá khả năng xử lý của địa phương)		Bộ phận kỹ thuật liên quan và đơn vị hỗ trợ xử lý tiếp nhận thông tin sự cố

TT.CNTT&TT, Đội ứng cứu sự cố ATTT mạng tỉnh, các đơn vị liên quan và chuyên gia ứng cứu sự cố		- Thông tin về đầu mối liên hệ - Thu thập thông tin hệ thống - Thu thập chức năng của hệ thống - Thu thập cấu hình của hệ thống (OS, servise, version, network,...) - Thu thập các tập tin, hình ảnh, email, ... bị xóa, thời gian bị xóa - Thu thập bộ nhớ - Thu thập trạng thái network và các kết nối - Thu thập các tiến trình đang chạy - Thu thập log file
TT.CNTT&TT, Đội ứng cứu sự cố ATTT mạng tỉnh, các đơn vị liên quan và chuyên gia ứng cứu sự cố		- Phân tích dòng thời gian - Thời gian bị sửa đổi, truy cập, tạo hoặc thay đổi. - Thời gian thực hiện các cập nhật lớn đối với hệ thống - Thời điểm mà hệ thống sử dụng lần cuối cùng - Phân tích dữ liệu …
TT.CNTT&TT, Đội ứng cứu sự cố ATTT mạng tỉnh, các đơn vị liên quan và chuyên gia ứng cứu sự cố		- Loại bỏ tấn công - Khôi phục hệ thống - Khôi phục dữ liệu - Vá lỗi, cập nhật hệ thống
TT.CNTT&TT, Đội ứng cứu sự cố ATTT mạng tỉnh, các đơn vị liên quan và chuyên gia ứng cứu sự cố		- Báo cáo kết quả phân tích sự cố: mô tả chi tiết các bước quan trọng khi thực hiện xử lý sự cố. - Tổng hợp báo cáo gửi Lãnh đạo cấp cấp liên quan đến sự cố - Rút kinh nghiệm và ứng dụng cho các sự cố tương tự

Cán bộ TTTHDL		

II. CÁCH THỨC THU THẬP THÔNG TIN PHỤC VỤ PHÂN TÍCH SỰ CỐ

Khi xảy ra sự cố, các cán bộ TTTHDL, cán bộ quản trị hệ thống thông tin tại các đơn vị cần thực hiện việc thu thập các thông tin bên dưới để phục vụ các công tác ứng cứu, xử lý sự cố, lập báo cáo:

- Thông tin về đầu mối liên hệ;
- Thu thập thông tin hệ thống;
- Thu thập chức năng của hệ thống;
- Thu thập cấu hình của hệ thống (OS, servise, version, network, …);
- Thu thập chứng cứ;
- Thu thập bộ nhớ;
- Thu thập trạng thái hệ thống mạng và các kết nối;
- Thu thập các tiến trình đang chạy;
- Thu thập dữ liệu lưu trữ trên đĩa cứng;
- Thu thập dữ liệu trên hệ thống lưu trữ ngoài;
- Thu thập các nhật ký hệ thống (Log file).

III. CÁC BIỂU MẪU VỀ CÁCH THỨC XÁC ĐỊNH, PHÂN LOẠI SỰ CỐ

BIÊN BẢN GHI NHẬN VÀ XỬ LÝ SỰ CỐ

Số:…….

Cán bộ TTTHDL, cán bộ quản trị hệ thống thông tin tại các đơn vị	Hướng dẫn kịch bản ứng phó chống tấn công DDOS	Mã số: Ngày hiệu lực: Số trang: … trang
Biên soạn	Xem xét	Phê duyệt
Tên: Chức vụ: Chữ ký:	Tên: Chức vụ: Phụ trách quản lý TTTHDL, Phụ trách quản lý CNTT tại đơn vị Chữ ký:	Tên: Chức vụ: Lãnh đạo đơn vị Chữ ký:
Lần ban hành/sửa đổi	Mô tả sự thay đổi	
02	- Thay đổi tên, chức năng, nhiệm vụ được phân công tại đơn vị theo cấu trúc mới.	

Nội dung:

Nội dung thông báo sự cố:
Thời điểm xuất hiện sự cố (hh:mm-dd/mm/yyyy):
Người tiếp nhận:
Tiến hành các bước kiểm tra:
Nguyên nhân sự cố:

Các biện pháp khắc phục:
Thời điểm kết thúc sự cố (hh:mm-dd/mm/yyyy) (nếu xử lý xong):
Kiến nghị và đề xuất:
Kết quả: Hệ thống hoạt động tốt lúc … giờ … phút, ngày … tháng … năm... Biên bản được thành lập 02 bản có giá trị như nhau, mỗi bên giữ 01 bản Đại diện kỹ thuật hai Bên (người tiếp nhận và người biên soạn) cùng xác nhận:

MẪU BÁO BÁO CÁO SỰ CỐ ĐỘT XUẤT

Số: ……

Họ và tên người báo cáo: Đơn vị: Điện thoại: Fax: Thời điểm báo cáo: (hh:mmdd/mm/yyyy)	Nơi nhận: - - -	Fax: Fax: Fax:

Nội dung:

Tên sự cố:
Thời điểm xuất hiện sự cố (hh:mm-dd/mm/yyyy):
Thiết bị bị sự cố và sự ảnh hưởng đến hoạt động mạng lưới:
Mô tả chi tiết sự cố:
Nguyên nhân sự cố (nếu phát hiện được):
Các biện pháp khắc phục: Tình trạng hiện tại:
Thời điểm kết thúc sự cố (hh:mm-dd/mm/yyyy) (nếu xử lý xong):
Kiến nghị và đề xuất:

Ý kiến của Lãnh đạo (Ký và ghi rõ họ tên)	Người báo cáo (Ký và ghi rõ họ tên)

CHƯƠNG IV
CÁC TÌNH HUỐNG KHẨN CẤP VÀ PHƯƠNG ÁN ỨNG PHÓ

I. TÌNH HUỐNG TẤN CÔNG TỪ CHỐI DỊCH VỤ

1. Định nghĩa:

Tấn công từ chối dịch vụ hay DoS (Denial of Service) là một sự kiện bảo mật xảy ra khi kẻ tấn công có hành động ngăn cản người dùng hợp pháp truy cập hệ thống máy tính, thiết bị hoặc các tài nguyên mạng khác. Trong tấn công từ chối dịch vụ, kẻ tấn công nhằm vào các máy tính và sử dụng mạng máy tính mà người dùng đang dùng để ngăn cản truy cập email, website, tài khoản trực tuyến (ví dụ như ngân hàng) và các dịch vụ khác.

2. Phân loại:

- Tấn công SYN Flood:

SYN Flood khai thác điểm yếu trong chuỗi kết nối TCP, được gọi là bắt tay ba chiều. Máy chủ sẽ nhận được một thông điệp đồng bộ (SYN) để bắt đầu "bắt tay". Máy chủ nhận tin nhắn bằng cách gửi cờ báo nhận (ACK) tới máy lưu trữ ban đầu, sau đó đóng kết nối. Tuy nhiên, trong một SYN Flood, tin nhắn giả mạo được gửi đi và kết nối không đóng => dịch vụ sập.

- Tấn công UDP Flood:

User Datagram Protocol (UDP) là một giao thức mạng không session. Một UDP Flood nhắm đến các cổng ngẫu nhiên trên máy tính hoặc mạng với các gói tin UDP. Máy chủ kiểm tra ứng dụng tại các cổng đó nhưng không tìm thấy ứng dụng nào.

- HTTP Flood:

HTTP Flood gần giống như các yêu cầu GET hoặc POST hợp pháp được khai thác bởi một hacker. Nó sử dụng ít băng thông hơn các loại tấn công khác nhưng nó có thể buộc máy chủ sử dụng các nguồn lực tối đa.

- Ping of Death:

Ping of Death điều khiển các giao thức IP bằng cách gửi những đoạn mã độc đến một hệ thống. Đây là loại DDoS phổ biến cách đây hai thập kỷ nhưng đã không còn hiệu quả vào thời điểm hiện tại.

- Smurf Attack:

Smurf Attack khai thác giao thức Internet (IP) và ICMP (Internet Control Message Protocol) sử dụng một chương trình phần mềm độc hại gọi là smurf. Nó giả mạo một địa chỉ IP và sử dụng ICMP, sau đó ping các địa chỉ IP trên một mạng nhất định.

- Tấn công Fraggle Attack:

Fraggle Attack sử dụng một lượng lớn lưu lượng UDP vào mạng phát sóng của router. Nó giống như một cuộc tấn công Smurf, sử dụng UDP nhiều hơn là ICMP.

- *Tấn công Slowloris:*

Slowloris cho phép kẻ tấn công sử dụng nguồn lực tối thiểu trong một cuộc tấn công và các mục tiêu trên máy chủ web. Khi đã kết nối với mục tiêu mong muốn, Slowloris giữ liên kết đó mở càng lâu càng tốt với HTTP tràn ngập. Kiểu tấn công này đã được sử dụng trong một số DDoSing kiểu hacktivist (tấn công vì mục tiêu chính trị) cao cấp, bao gồm cuộc bầu cử tổng thống Iran năm 2009. Việc giảm thiểu ảnh hưởng với loại hình tấn công này là rất khó khăn.

- *Application Level Attacks:*

Application Level Attacks khai thác lỗ hổng trong các ứng dụng. Mục tiêu của loại tấn công này không phải là toàn bộ máy chủ, mà là các ứng dụng với những điểm yếu được biết đến.

- *NTP Amplification:*

NTPAmplification khai thác các máy chủ NTP (Network Time Protocol), một giao thức được sử dụng để đồng bộ thời gian mạng, làm tràn ngập lưu lượng UDP. Đây là reflection attack bị khuếch đại. Trong reflection attack bất kỳ nào đều sẽ có phản hồi từ máy chủ đến IP giả mạo, khi bị khuếch đại, thì phản hồi từ máy chủ sẽ không còn tương xứng với yêu cầu ban đầu. Vì sử dụng băng thông lớn khi bị DDoS nên loại tấn công này có tính phá hoại và volumne cao.

- *Advanced Persistent DoS (APDoS):*

Advanced Persistent DoS (APDoS) là một loại tấn công được sử dụng bởi hacker với mong muốn gây ra những thiệt hại nghiêm trọng. Nó sử dụng nhiều kiểu tấn công được đề cập trước đó HTTP Flood, SYN Flood, v.v...) và thường nhắm tấn công theo kiểu gửi hàng triệu yêu cầu/giây. Các cuộc tấn công của APDoS có thể kéo dài hàng tuần, phụ thuộc vào khả năng của hacker để chuyển đổi các chiến thuật bất cứ lúc nào và tạo ra sự đa dạng để tránh các bảo vệ an ninh.

- *Zero-day DDoS Attacks:*

Zero-day DDoS Attacks là tên được đặt cho các phương pháp tấn công DDoS mới, khai thác các lỗ hổng chưa được vá.

- *HTTP GET:*

HTTP GET là một kiểu tấn công lớp ứng dụng (Application Layer attack), quy mô nhỏ hơn và được nhắm tới những mục tiêu hơn. Application Level Attacks khai thác lỗ hổng trong các ứng dụng. Mục tiêu của loại tấn công này không phải là toàn bộ máy chủ, mà là các ứng dụng với những điểm yếu được biết đến. HTTP GET khai thác quy trình trình của một trình duyệt web hoặc ứng dụng HTTP nào đó và yêu cầu một ứng dụng hoặc máy chủ cho mỗi yêu cầu HTTP, đó là GET hoặc POST. HTTP Flood gần giống như các yêu cầu GET hoặc POST hợp pháp được khai thác bởi một hacker. Nó sử dụng ít băng thông hơn các loại tấn công khác nhưng nó có thể buộc máy chủ sử dụng các nguồn lực tối đa. Rất khó

để chống lại kiểu tấn công này vì chúng sử dụng các yêu cầu URL_tiêu chuẩn, thay vì các tập lệnh bị hỏng hoặc khối lượng lớn.

3. Dấu hiệu nhận diện:

- Không phải sự sập đổ hoàn toàn nào của dịch vụ cũng là kết quả của một tấn công từ chối dịch vụ. Có nhiều vấn đề kỹ thuật với một mạng hoặc với các quản trị viên đang thực hiện việc bảo trì và quản lý. Mặc dù thế nhưng với các dấu hiệu dưới đây người dùng có thể nhận ra tấn công DoS hoặc DdoS:

- Thực thi mạng chậm một cách không bình thường (mở file hay truy cập website).

- Không vào được website người dùng vẫn xem.

- Không thể truy cập đến bất kỳ một website nào.

- Số lượng thư rác tăng một cách đột biến trong tài khoản của người dùng.

4. Phạm vi ảnh hưởng:

DoS có thể làm ngưng hoạt động của một máy tính, từ mạng nội bộ đến cả một hệ thống mạng lớn.

5. Phương án xử lý:

Bước	Nội dung thực hiện
1	Giám sát và thông báo khi tấn công DoS/DDoS xảy ra.
	Thông báo các bộ phận đơn vị liên quan khi thấy hiện tượng DoS/DDoS xảy ra: - Lãnh đạo Trung tâm CNTT&TT (đơn vị được giao quản lý trực tiếp TTTHDL) - TTTHDL; - Bộ phận kỹ thuật TTTHDL, cán bộ được giao tiếp nhận thông tin sự cố ATTT mạng của tỉnh tại TTTHDL (Trung tâm CNTT&TT); - Đơn vị quản lý website bị tấn công.
2	Phân tích log hệ thống để xác định nguồn tấn công, phạm vi và hình thức tấn công:
	- Phân tích log Router gateway và công cụ giám sát lưu lượng PRTG để xác định nguồn IP và hướng tấn công.
	- Phân tích log Firewall để xác định nguồn IP và hình thức tấn công.
	- Phân tích log system, dịch vụ và tài nguyên của server hosting website bị tấn công để xác định tình trạng hoạt động của hệ thống và dịch vụ.
3	Thực hiện các biện pháp ngăn chặn: - Nếu nguồn tấn công đến từ các IP nước ngoài, cần xử lý chặn các IP theo Geo Location. - Nếu nguồn tấn công đến từ các IP trong nước, cần thực hiện lọc các IP và gửi ISP liên quan để có phương án xử lý.
3.1	Xử lý nội bộ TTTHDL:

Bước	Nội dung thực hiện
	- Tạo route trên router gateway để định tuyến nguồn tấn công vào NULL0 nhằm giảm lưu lượng tấn công vào website. - Yêu cầu các ISP chặn (null-route) domain/IP các máy chủ CnC, các dải IP tham gia DdoS để block nguồn IP tấn công hoặc ngăn chặn lưu lượng tấn công vào Website.
	- Thực hiện cấu hình trên Firewall ngoài: + Tạo rule trên Firewall ngoài để ngăn nguồn IP tấn công. + Tăng số lượng giới hạn kết nối cho phép hiện tại lên tối đa 700.000 để có thể chịu được tấn công DDoS nhiều hơn (cân đối trên tổng giới hạn kết nối cho phép của hệ thống VSX là 1.200.000). + Bật các signatures lên quan đến tấn công tầng Network. + Thực hiện một số chính sách chống DoS của WAF để hạn chế tấn công và duy trì dịch vụ: + Khi tổng số các request vượt quá 500 trong vòng 10s đối với 1 IP, action ngăn chặn là block session. + Khi tổng số các request có mã lỗi trả về là 400,403,405, 500,501,503 vượt quá 150 trong vòng 5s, action ngăn chặn là block session. + Khi tổng số các request bất kỳ vượt quá 999 trong vòng 60s và thời gian hồi đáp vượt quá 9999ms, action ngăn chặn là block session.
	- Tăng tài nguyên CPU, RAM cho server hosting website bị tấn công (nếu quá tải) và chi tải các máy chủ nhằm duy trì dịch vụ. - Thực hiện các biện pháp kỹ thuật tối ưu đáp ứng của website.
3.2	Xử lý mở rộng nếu tấn công vẫn còn xảy ra:
	- Liên hệ với ISP có lưu lượng tấn cống DoS để mở rộng băng thông.
	- Liên hệ với ISP (VDC, FPT) triển khai giải pháp CDN để giảm lưu lượng vào server. - Tạo hệ thống server dự phòng thay thế và cô lập hệ thống hiện tại để phân tích vấn đề đang xảy ra.
	- Liên hệ với các chuyên gia ứng cứu sự cố tham gia phân tích và tìm biện pháp xử lý: + Truy tìm máy chủ CnC, truy tìm mã độc do hacker phát tán. + Phân tích mẫu mã độc và viết công cụ diệt các mã độc. + Theo dõi và cập nhật các mẫu mã độc mới.
4	Khôi phục lại trạng thái ban đầu khi tấn công đã chấm dứt:
	- Tiếp tục thep dõi giám sát để xác định tình trạng tấn công và khôi phục về trạng thái ban đầu khi đã chấm dứt.
	- Gửi email thông báo cho các ISP có nguồn IP tấn công để thông báo, yêu cầu họ ngăn chặn và xử lý hành vi tấn công.
	- Liên hệ với đơn vị an ninh quốc gia (nếu IP thuộc Viet Nam) để yêu cầu điều tra người thực hiện và xử lý theo phát luật.
5	Thực hiện các biện pháp phòng ngừa:
	Lập tài liệu quá trình tấn công khắc phục, thảo luận rút kinh nghiệm và thực hiện điều chỉnh kế hoạch/kịch bản phòng thủ phù hợp.

II. TÌNH HUỐNG TẤN CÔNG GIẢ MẠO

1. Định nghĩa:

Tấn công giả mạo (thuật ngữ gốc tiếng Anh: phishing, biến thể từ fishing, nghĩa là câu cá, có thể ảnh hưởng từ chữ phreaking, nghĩa là sử dụng điện thoại người khác không trả phí, ám chỉ việc "nhử" người dùng tiết lộ thông tin mật), trong lĩnh vực bảo mật máy tính, là một hành vi giả mạo ác ý nhằm lấy được các thông tin nhạy cảm như tên người dùng, mật khẩu và các chi tiết thẻ tín dụng bằng cách giả dạng thành một chủ thể tin cậy trong một giao dịch điện tử.

2. Phân loại:

- *Email and Spam:*

Nhúng một liên kết trong một email chuyển hướng tới một trang web không an toàn và yêu cầu người dùng cung cấp những thông tin nhạy cảm:

Giả mạo địa chỉ người gửi trong một email để xuất hiện như một nguồn đáng tin cậy và yêu cầu thông tin nhạy cảm.

Đặt một Trojan (mã độc) thông qua một tập tin đính kèm trong email hoặc quảng cáo thứ được gửi vào hòm thư của người dùng. Từ đó, kẻ xâm nhập có thể khai thác lỗ hổng và có được thông tin nhạy cảm.

- *Web-based Delivery:*

Bằng cách chèn vào trang web những banner hoặc những text quảng cáo có ý khiêu khích sự tò mò của người dùng. Ví dụ như những hình ảnh khiêu dâm, những nội dung đang nóng. Kết quả sau khi click vào đó thì máy tính của người dùng có thể bị nhiễm một loại malware nào đó, phục vụ cho một cộng tấn công khác.

3. Dấu hiệu nhận diện:

- Một địa chỉ lạ (tên miền không rõ ràng, dài ngoằn ngèo, có chứa link khác).

- Đường dẫn giả mạo thường chứa nhiều ký tự vô nghĩa hoặc các chuỗi văn bản bổ sung.

- SSL và chứng thứ số của website không có bảo mật (not secure).

- Mail nhận được từ những tài khoản vô danh.

4. Phạm vi ảnh hưởng:

- Lộ thông tin người dùng.

- Mất tài sản người dùng.

5. Phương án xử lý:

STT	Nội dung công việc
1	Thông báo các bộ phận, đơn vị liên quan khi thấy hiện tượng phát tán email giả

STT	Nội dung công việc
	mạo:
	- Lãnh đạo đơn vị vận hành, quản lí công nghệ thông tin. - Ban Giám đốc đơn vị. - Bộ phận, đơn vị liên quan.
2	Xử lý tạm thời:
	- Block email giả mạo có thông tin lạ. - Kiểm tra Log và xác định người dùng đã nhận email giả mạo email của hệ thống. - Thông báo và đề nghị người dùng kiểm tra lại tình trạng an toàn trên máy tính cá nhân, đề nghị người dùng thay đổi mật khẩu và kiểm tra thông tin cá nhân của mình. - Theo dõi tình trạng gửi nhận và đăng nhập của các người dùng nghi ngờ tài khoản của người dùng bị kẻ xấu lợi dụng. - Thông báo với người dùng và bộ phận Security nếu xảy ra các tình trạng bất thường. Block tạm thời chiều gửi của account người dùng để bộ phận Security xử lý.
3	Xử lý mở rộng:
	- Triển khai một bộ lọc SPAM phát hiện các mail giả mạo gửi đến người dùng và nhân viên nội bộ của cơ quan, đơn vị. - Mã hóa các thông tin quan trọng, nhạy cảm .
4	Khôi phục lại trạng thái ban đầu:
	Kiểm tra lại các thông tin của người dùng có trong danh sách nhận được thông tin giả mạo. Tiến hành thông báo cho người dùng đấy.
5	Thực hiện các biện pháp phòng ngừa:
	Lập tài liệu quá trình tấn công khắc phục, thảo luận rút kinh nghiệm và thực hiện điều chỉnh kế hoạch/kịch bản phòng thủ phù hợp.

5.1. Đối với cá nhân:

- Hãy cẩn thận và không nên trả lời bất kỳ thư rác nào yêu cầu người dùng xác nhận hoặc cập nhật bất kỳ thông tin nào về tài khoản của người dùng. Thậm chí có vẻ như được cung cấp bởi một tổ chức uy tín hoặc đó là yêu cầu hoàn lại tiền cho người dùng.

- Không nhấp bất kỳ liên kết đi kèm với thư rác, nếu người dùng không chắc chắn về nó.

- Không bao giờ gửi thông tin bí mật của người dùng về tài khoản của người dùng trong email.

- Không trả lời những thư lừa đảo đó, những kẻ gian lận thường gửi cho người dùng số điện thoại để người dùng gọi cho họ vì mục đích kinh doanh. Họ sử dụng công nghệ Voice over Internet Protocol. Với công nghệ này, các cuộc gọi của họ không bao giờ có thể được truy tìm.

- Để giảm thiểu rủi ro bởi những vụ lừa đảo phishing này người dùng nên sử dụng tường lửa, phần mềm chống gián điệp và phần mềm chống virus. Và phải đảm bảo cập nhật phần mềm này thường xuyên để bảo mật máy tính của người dùng.

- Hãy chuyển các thư rác đến spam@uce.gov. Người dùng cũng có thể gửi email tới reportphishing@antiphishing.org Tổ chức này giúp chống lại các phishing khác.

5.2. Đối với các cơ quan, tổ chức, doanh nghiệp:

- Đào tạo nhận thức của cán bộ và thực hiện các buổi tập huấn với các tình huống giả mạo giả mạo.

- Triển khai một bộ lọc SPAM để phát hiện vi rút, người gửi trống cho toàn bộ hệ thống mail của cơ quan, đơn vị.

- Giữ tất cả các hệ thống hiện tại với các bản vá lỗi bảo mật và cập nhật mới nhất. Cài đặt một giải pháp chống virus, lên lịch cập nhật chữ ký, và theo dõi trạng thái chống virus trên tất cả các thiết bị.

- Cùng với đó cơ quan, đơn vị phải mã hóa tất cả thông tin nhạy cảm, quan trọng.

III. TÌNH HUỐNG TẤN CÔNG SỬ DỤNG MÃ ĐỘC PHÁT TÁN QUA EMAIL

1. Giới thiệu:

Mã độc hay "Malicious software" là một loại phần mềm được tạo ra và chèn vào hệ thống một cách bí mật với mục đích thâm nhập, phá hoại hệ thống hoặc lấy cắp thông tin, làm gián đoạn, tổn hại tới tính bí mật, tính toàn vẹn và tính sẵn sàng của máy tính nạn nhân.

2. Phân loại:

- Trojan:

Đặc tính phá hoại máy tính, thực hiện các hành vi phá hoại như: xóa file, làm đổ vỡ các chương trình thông thường, ngăn chặn người dùng kết nối internet…

- Worm:

Cùng với các loại mã độc máy tính như Trojan, WannaCry, Worm (sâu máy tính) là loại virus phát triển và lây lan mạnh mẽ nhất hiện nay nhờ mạng Internet. Vào thời điểm ban đầu, Worm được tạo ra chỉ với mục đích phát tán qua thư điện tử – email. Khi lây vào máy tính, chúng thực hiện tìm kiếm các sổ địa chỉ, danh sách email trên máy nạn nhân rồi giả mạo các email để gửi bản thân chúng tới các địa chỉ thu thập được. Các email do worm tạo ra thường có nội dung "giật gân", hoặc "hấp dẫn", hoặc trích dẫn một email nào đó ở máy nạn nhân để ngụy trang. Điều này khiến các email giả mạo trở nên "thật" hơn và người nhận dễ bị đánh lừa hơn. Nhờ những email giả mạo đó mà Worm lây lan mạnh mẽ trên mạng Internet theo cấp số nhân.

Bên cạnh Worm lây lan theo cách truyền thống sử dụng email, Worm hiện nay còn sử dụng phương pháp lân lan qua ổ USB. Thiết bị nhớ USB đã trở nên phổ biến trên toàn thế giới do lợi thế kích thước nhỏ, cơ động và trở thành phương tiện lây lan lý tưởng cho Worm.

Dựa đặc điểm lây lan mạnh mẽ của Worm, những kẻ viết virus đã đưa thêm vào Worm các tính năng phá hoại, ăn cắp thông tin…, Worm đã trở thành "người dùng đồng hành" của những phần mềm độc hại khác như BackDoor, Adware…

- *Spyware:*

Là phần mềm cài đặt trên máy tính người dùng nhằm thu thập các thông tin người dùng một cách bí mật, không được sự cho phép của người dùng.

- *Adware:*

Phần mềm quảng cáo, hỗ trợ quảng cáo, là các phần mềm tự động tải, pop up, hiển thị hình ảnh và các thông tin quảng cáo để ép người dùng đọc, xem các thông tin quảng cáo. Các phần mềm này không có tính phá hoại nhưng nó làm ảnh hưởng tới hiệu năng của thiết bị và gây khó chịu cho người dùng.

- *Ransomware:*

Đây là phần mềm khi lây nhiễm vào máy tính nó sẽ kiểm soát hệ thống hoặc kiểm soát máy tính và yêu cầu nạn nhân phải trả tiền để có thể khôi phục lại điều khiển với hệ thống.

- *Virus Hoax:*

Virus Hoax là các cảnh báo giả về virus. Các cảnh bảo giả này thường núp dưới dạng một yêu cầu khẩn cấp để bảo vệ hệ thống. Mục tiêu của cảnh báo virus giả là cố gắng lôi kéo mọi người gửi cảnh báo càng nhiều càng tốt qua email.

Bản thân cảnh báo giả là không gây nguy hiểm trực tiếp nhưng những thư gửi để cảnh báo có thể chứa mã độc hại hoặc trong cảnh báo giả có chứa các chỉ dẫn về thiết lập lại hệ điều hành, xoá file làm nguy hại tới hệ thống. Kiểu cảnh báo giả này cũng gây tốn thời gian và quấy rối bộ phận hỗ trợ kỹ thuật khi có quá nhiều người gọi đến và yêu cầu dịch vụ.

- *Rootkit:*

Rootkit ra đời sau các loại virus khác, nhưng rootkit lại được coi là một trong những loại virus nguy hiểm nhất.

Bản thân rootkit không thực sự là virus, đây là phần mềm hoặc một nhóm các phần mềm máy tính được giải pháp để can thiệp sâu vào hệ thống máy tính (nhân của hệ điều hành hoặc thậm chí là phần cứng của máy tính) với mục tiêu che giấu bản thân nó và các loại phần mềm độc hại khác.

Với sự xuất hiện của rootkit, các phần mềm độc hại như trở nên "vô hình" trước những công cụ thông thường thậm chí vô hình cả với các phần mềm diệt virus. Việc phát hiện_mã độc và tiêu diệt virus trở nên khó khăn hơn rất nhiều trước sự bảo vệ của rootkit – vốn được trang bị nhiều kĩ thuật mới hiện đại.

Xuất hiện lần đầu trên hệ thống Unix từ khá lâu, nhưng kể từ lần xuất hiện "chính thức" trên hệ điều hành Windows vào năm 2005, Rootkit đang dần trở nên phổ biến và trở thành công cụ che giấu hữu hiệu cho các loại phần mềm độc hại khác.

3. Dấu hiện nhận diện:

- Máy tính xuất hiện các dấu hiệu bất thường khi sử dụng là các dấu hiệu đầu tiên chúng ta cần quan tâm. Các chuyện bất thường có nguy cơ cao:

- Máy tính đang sử dụng bị chậm, các tác vụ và ứng dụng không hoạt động bình thường.

- Có chương trình lạ bật các thông báo, tự động bật, tự động tắt.

- Máy tính tự động khởi động lại, màn hình, Webcam tự dưng bật sáng.

- Chuột tự động điều khiển như có người đang sử dụng máy tính.

- Trình duyệt xuất hiện các plugin lạ, thường xuyên bật quảng cáo không mong muốn.

- Khi kiểm tra kĩ hơn bằng các công cụ giám sát, máy tính đang chạy các tiến trình lạ, các chương trình không được cài đặt hoặc không có nguồn gốc rõ ràng.

- Băng thông mạng lớn, ổ cứng hoạt động với tốc độ cao.

- Xuất hiện các chương trình hỗ trợ điều khiển từ xa được cài đặt hoặc được bật.

- Nhiều tệp tin bị mã hóa, bị thay đổi định dạng, thay đổi phần mở rộng.

- Chương trình duyệt tập tin trên windows (Window Explorer) bị biến mất hoặc không thể sử dụng được.

4. Phạm vi ảnh hưởng:

- Một cuộc tấn công mã độc lây lan rất nhanh trong một khoảng thời gian ngắn gây thiệt hại nghiêm trọng cho các cá nhân, tổ chức.

- Các máy chủ khi bị hacker nắm giữ sẽ bị lợi dụng để làm "bàn đạp" tấn công sang các hệ thống máy tính khác. Không chỉ bị tấn công, nắm giữ, nhiều máy chủ của các cơ quan chính phủ còn bị rao bán trên các chợ đen của hacker. Nhiều máy chủ của các cơ quan chính phủ cũng bị tấn công, nắm giữ nhiều lần vì tồn tại các lỗ hổng bảo mật đơn giản nhưng nhiều cơ quan không khắc phục. Đây là lỗ hổng rất đáng lo ngại cho hệ thống máy tính của các cơ quan chính phủ tại Việt Nam.

5. Phương án xử lý:

- Để xử lí nhanh với các dấu hiệu nghi ngờ mã độc, phương pháp tốt nhất là tìm tới sự hỗ trợ từ các chuyên gia, những người có kinh nghiệm. Tuy nhiên, trước khi nhờ tới các chuyên gia giúp đỡ, bản thân mỗi người cần tự chủ động trang bị và thực hiện một số bước để đảm bảo an ninh thông tin cho cá nhân:

- Theo dõi kĩ và ghi nhận các dấu hiệu bất thường.

- Sử dụng một thiết bị tin tưởng khác, thực hiện thay đổi, cập nhật mật khẩu các dịch vụ quan trọng, thiết lập xác thực hai bước cho Gmail, Facebook và các tài khoản quan trọng.

- Backup (sao lưu) lại các dữ liệu quan trọng.

- Sau khi xử lí sơ bộ, người dùng tốt nhất nên liên hệ với các chuyên gia để nhận được tư vấn cụ thể cho từng trường hợp.

- Để tránh các nguy cơ mã độc lây nhiễm, gây ảnh hưởng tới hệ thống và dữ liệu, thay vì đợi đến khi mã độc lây nhiễm mới xử lí chúng ta cần trang bị trước các phương pháp phòng tránh. Có một số phương pháp cần lưu ý:

- Luôn luôn cài đặt và sử dụng một phần mềm diệt virus chính hãng. Ví dụ: Kaspersky, CyStack, Bitdifender, Avast, Norton, Bkav, … Việc xuất hiện một phần mềm diệt virus có thể chúng ta rất ít khi thấy mã độc nào được phát hiện hay diệt, tuy nhiên nó giúp chúng ta phòng tránh mã độc được các hiểm họa xâu xa và giúp chúng ta yên tâm hơn khi duyệt web hoặc download các phần mềm.

- Xây dựng chính sách với các thiết bị PnP: Với các thiết bị loại này: USB, CD/DVD, … virus có thể lợi dụng để thực thi mà không cần sự cho phép của người dùng. Do đó, cần thiết lập lại chế độ cho các thiết bị và chương trình này để hạn chế sự thực thi không kiểm soát của mã độc. Ngoài ra, trong quá trình sử dụng các thiết bị như USB, chúng ta không nên mở trực tiếp bằng cách chọn ổ đĩa rồi nhấn phím Enter, hoặc nhấp đôi chuột vào biểu tượng mà nên bấm chuột phải rồi click vào explore.

- Thiết lập quy tắc đối xử với các file: Không nên mở hoặc tải về các file không rõ nguồn gốc, đăc biệt là các file thực thi (các file có đuôi .exe, .dll, …). Với các file không rõ nguồn gốc này, tốt nhất chúng ta nên tiến hành quét bằng phần mềm diệt virus hoặc thực hiện kiểm tra trực tiếp trên website: https://www.virustotal.com Khi có nghi ngờ được cảnh báo cần dừng việc thực thi file lại để đảm bảo an toàn.

- Truy cập web an toàn: Quá trình truy cập web là nguyên nhân khiến máy tính dễ dàng bị nhiễm mã độc nếu người dùng không có nhận thực đúng đắn. Khi truy cập web cần chú ý: Không nên truy cập vào các trang web đen, các trang web độc hại, có nội dung không lành mạnh, không tuy tiện click vào các url từ các email hoặc từ nội dung chat, trên các website, … Các website và url như trên thường xuyên ẩn chứa các mã độc và chỉ đợi người dùng click, nó sẽ tự động tải về, thiết lập cài đặt để thực thi hợp pháp trên máy tính người dùng. Một ví dụ tiêu biểu đó là khi chúng ta phân tích và theo dõi các máy của các nhân viên văn phòng, các máy tính này hầu hết đều bị cài đặt các addon hoặc các phần mềm quản cáo do quá trình duyệt web chính bản thân người sử dụng đã cho phép addon hoặc phần mềm đó thực thi.

- Cập nhật máy tính, phần mềm: Thường xuyên cập nhật các bản vá được cung cấp từ hệ điều hành, các bản vá cho các ứng dụng đang sử dụng và đặc biệt là cập nhật chương trình diệt virus. Đây là yếu tố quan trọng để tránh được các loại mã độc lợi dụng các lỗ hổng để lây lan, đồng thời cũng cập nhật được các mẫu mã độc mới để giúp phần mềm diệt virus làm việc hiệu quả hơn.

- Nhờ chuyên gia can thiệp: Khi thấy máy tính có các dấu hiệu bị lây nhiễm cần tiến hành quét ngay bằng phần mềm diệt virus, nếu vẫn không có tiến triển tốt, cần nhờ sự giúp

đỡ của các chuyên gia để kiểm tra máy tính, phát hiện và tiêu diệt mã độc ngay. Có thể việc này sẽ làm tốn thời gian và tiền bạc nhưng nó thật sự cần thiết vì rất có thể tác hại của việc để nguyên máy tính còn tốn kém và thiệt hại hơn rất nhiều lần.

IV. TÌNH HUỐNG TẤN CÔNG TRUY CẬP TRÁI PHÉP, CHIẾM QUYỀN ĐIỀU KHIỂN

1. Giới thiệu:

Tấn công truy cập trái phép, chiếm quyền điều khiển là kiểu tấn công mà hacker tấn công để truy cập vào những nơi có tính riêng tư, tài sản riêng. Mục đích là để đánh cắp thông tin, phá hoại hệ thống, cài đặt các phần mềm độc hại: virus, spyware, keylogger, backdoor, sniffer… Một số hình thức điển hình là:

- *Session Hijacking:*

Thuật ngữ chiếm quyền điều khiển session (session hijacking) chứa đựng một loạt các tấn công khác nhau. Nhìn chung, các tấn công có liên quan đến sự khai thác session giữa các thiết bị đều được coi là chiếm quyền điều khiển session. Khi đề cập đến một session, chúng ta sẽ nói về kết nối giữa các thiết bị mà trong đó có trạng thái đàm thoại được thiết lập khi kết nối chính thức được tạo, kết nối này được duy trì và phải sử dụng một quá trình nào đó để ngắt nó.

Có hai dạng Session Hijacking đó là chủ động và bị động. Khác biệt chính giữa hai hình thức hijacking này phụ thuộc vào sự tác động của hacker lên phiên làm việc của người sử dụng trong môi trường mạng. Ở trạng thái chủ động hacker sẽ tìm các phiên làm việc đang hoạt động và chiếm đoạt nó thông qua các công cụ và tính toán các giá trị tuần tự của gói tin trong TCP session. Ngược lại, ở tình huống tấn công hijacking thụ động thì các kẻ tấn công chỉ theo dõi và ghi lại tất cả những truyền thông được gởi bởi người sử dụng hợp lệ.

- *Local Attack:*

Là một phương pháp rất phổ biến dùng để tấn công 1 website nào đó trên cùng 1 server. Công cụ của việc tấn công này là dùng các đoạn mã khai thác được viết bằng 1 số ngôn ngữ lập trình như: PHP, ASP.Net, Python… Các đoạn mã đó được gọi là Shell. Khi một hosting trên server bị upload lên đoạn file shell này, người tấn công có thể dùng các câu lệnh khai thác để thâm nhập qua các tài khoản hosting cùng server để đọc các thông tin nhạy cảm như: Email, thông tin Database *(username, password..)* một cách dễ dàng. Từ đó người tấn công có thể làm mọi điều họ muốn. Công việc đầu tiên của người hack local attack là tìm hiểu thông tin mục tiêu. Họ sẽ quét sơ qua trước thông tin về domain, ip hosting của người dùng đang sử dụng. Họ sẽ vào và xem website của người dùng đang chạy mã nguồn gì, có sử dụng plugin hay code gì có lỗi dễ khai thác hay không…Nếu website của người dùng tồn tại các lỗi như SQL Injection hoặc XSS hoặc 1 số lỗi phổ biến khác thì họ sẽ tấn công trực tiếp vào. Còn ngược lại, khi họ đã kiểm tra qua website của người dùng, có vẻ như không có lỗi để khai thác, họ sẽ bắt đầu Reverse IP hosting của người dùng. Thuật ngữ

này dùng để quét ra tất cả website đang chạy cùng IP server với người dùng – hàng xóm của người dùng. Tùy theo Server mà họ setup cho server đó chạy bao nhiêu website cùng lúc. Sau khi đã có danh sách website đó, họ lại tiếp tục rà soát xem có bao nhiêu web hàng xóm của người dùng dính lỗi để upload shell.

Nếu một trong các website đó dính lỗi SQL Injection hoặc các lỗi khác có thể khai thác để lấy và chiếm quyền Admin vào để upload shell thì từ đó sẽ là bàn đạp cho việc hacker tấn công qua website của người dùng. Một phương pháp tuy không hay lắm nhưng cũng được xem là lợi hại là:

- *Kỹ thuật tấn công Brute Force:*

Hiện vẫn còn rất nhiều ứng dụng để mật khẩu và username mặc định sau khi cài đặt hoặc đặt các mật khẩu quá dễ đoán như: 123456, admin, 123456789, 123abc…. Từ đó họ có quyền upload file shell lên hosting kia và thực thi các lệnh để lấy thông tin từ website của người dùng và phá hoại hệ thống.

2. Dấu hiệu nhận diện:

- Dựa vào lịch sử truy cập trong ứng dụng.

- Dựa vào nhật ký truy cập ứng dụng (thông qua các địa chỉ IP lạ).

- Dựa vào dấu hiệu khi có xác thực 2 bước.

3. Phạm vi ảnh hưởng:

- Hacker có thể đánh cắp những thông tin nhạy cảm về cá nhân người dùng, cơ quan, đơn vị hoặc chính phủ.

- Tê liệt, phá hủy hệ thống.

- Những phần mềm được hacker cài vào có mối nguy hại lâu dài nếu không phát hiện kịp thời.

4. Phương án xử lý

Để phòng chống không bị tấn công Session Hijacking thì chúng ta cần phòng tránh bị nghe lén, một khi hacker không thể nghe lén được thì cũng koh6ng thể tấn công vào session của người dùng. Một torng các giải pháp đế tránh các sniffer chính là mã hóa dữ liệu, mã hóa đường truyền với các kỹ thuật như dùng Secure Shell (SSH thay cho Telnet thông thường) khi quản trị từ xa hay áp dụng Secure Socket Layer (SSL dùng cho truyền thông qua HTTPS). Ngoài ra, chúng ta có thể ngăn không cho hacker tương tác vào đường truyền cũng giúp loại bỏ nguy cơ bị tấn công này, với những giải pháp hữu hiệu như dùng mạng riêng ảo (VPN), hay áp dụng IPSEC. Sau đây là một số khuyến nghị nhằm ngăn ngừa:

- *Session Hijacking:*

+ Sử dụng mã hóa.

+ Ứng dụng các giao thức an toàn.

+ Hạn chế các kết nối đầu vào.

+ Giảm các truy cập từ xa.

+ Có chế độ xác thực mạnh mẽ.

+ Huấn luyện cho người dùng, nâng cao nhận thức an toàn thông tin.

+ Sử dụng các thông tin truy cập khác nhau cho các tài khoản khác nhau.

- *Local Attack:*

+ Không sử dụng các mã nguồn không rõ nguồn gốc vì có thể có nhiều lỗi hoặc bị chèn mã độc vào sẵn.

+ Thường xuyên update các phiên bản mới của các loại mã nguồn mở để vá lỗi.

+ Không đặt password quá dễ đoán, hãy tập thói quen cho mình dùng password kết hợp ký tự in hoa, số và ký tự đặc biệt.

+ Không đặt trùng 1 password cho nhiều loại tài khoản. Vì bị mất cái này có thể mất luôn cái khác.

+ CHMOD 400 cho các file có thông tin nhạy cảm, 101 cho folder.

+ Sử dụng VPS thay vì dùng hosting để loại bỏ khả năng hack qua Local attack.

+ Thường xuyên backup dữ liệu và quét dữ liệu xem có chứa mã độc hay không.

V. TÌNH HUỐNG TẤN CÔNG THAY ĐỔI GIAO DIỆN

1. Định nghĩa:

Deface được định nghĩa là tấn công thay đổi nội dung website, thông qua một điểm yếu nào đó của website, hacker sẽ thay đổi nội dung website của nạn nhân. Việc thay đổi nội dung này nhằm một số mục đích :

- Mục đích tốt: cảnh báo quản trị viên biết website đang tồn tại lỗ hỏng bảo mật/ điểm yếu nghiêm trọng…

- Mục đích không tốt: chứng tỏ năng lực bản thân, dạng này rất dễ gặp như kiểu hacked by…

- Mục đích xấu: thù hằn, nội dung thay đổi thường là lăng mạ nạn nhân hoặc nội dung liên quan đến chính trị, tôn giáo, quốc gia…

2. Phân loại:

- *Lỗi SQL injection:*

SQL injection là một kỹ thuật cho phép những kẻ tấn công lợi dụng lỗ hổng của việc kiểm tra dữ liệu đầu vào trong các ứng dụng web và các thông báo lỗi của hệ quản trị cơ sở dữ liệu trả về để inject (tiêm vào) và thi hành các câu lệnh SQL bất hợp pháp.

SQL injection có thể cho phép những kẻ tấn công thực hiện các thao tác, delete, insert, update, v.v. trên cơ sở dữ liệu của ứng dụng, thậm chí là server mà ứng dụng đó đang chạy.

SQL injection thường được biết đến như là một vật trung gian tấn công trên các ứng dụng web có dữ liệu được quản lý bằng các hệ quản trị cơ sở dữ liệu như SQL Server, MySQL, Oracle, DB2, Sysbase...

- *Lỗi XSS (Cross Site Scripting):*

XSS (Cross Site Scripting) là một kiểu tấn công cho phép hacker chèn những đoạn script độc hại (thông thường là javascript hoặc HTML) vào website và sẽ được thực thi ở phía người dùng (trong trình duyệt của người dùng). Ví dụ tại các form tìm kiếm, comment, form đăng nhập. Đối với XSS, người bị tấn công là người dùng chứ không phải website, hacker có thể dùng XSS để gửi những đoạn script độc hại tới một người dùng bất kỳ, và trình duyệt của người dùng sẽ thực thi những đoạn script đó và gửi về cho hacker những thông tin của người dùng thông qua email hoặc server do hacker định sẵn từ trước.

- *Lỗ hổng Remote File Include:*

Kiểu tấn công này, cho phép tin tặc include và thực thi trên máy chủ mục tiêu một tệp tin được lưu trữ từ xa. Tin tặc có thể sử dụng RFI để chạy một mã độc trên cả máy của người dùng và phía máy chủ. Ảnh hưởng của kiểu tấn công này thay đổi từ đánh cắp tạm thời session token hoặc các dữ liệu của người dùng cho đến việc tải lên các webshell, mã độc nhằm đến xâm hại hoàn toàn hệ thống máy chủ.

PHP có nguy cơ cao bị tấn công RFI do việc sử dụng lệnh include rất nhiều và thiết đặt mặc định của server cũng ảnh hưởng một phần nào đó. Để bắt đầu chúng ta cần tìm nơi chứa file include trong ứng dụng phụ thuộc vào dữ liệu đầu vào người dùng.

- *Lỗ hổng Local file inclusion:*

Lỗ hổng này nằm trong quá trình include file cục bộ có sẵn trên server. Lỗ hổng xảy ra khi đầu vào người dùng chứa đường dẫn đến file bắt buộc phải include. Khi đầu vào này không được kiểm tra, tin tặc có thể sử dụng những tên file mặc định và truy cập trái phép đến chúng, tin tặc cũng có thể lợi dụng các thông tin trả về trên để đọc được những tệp tin nhạy cảm trên các thư mục khác nhau bằng cách chèn các ký tự đặc biệt như "/", "../", "-". Không cập nhật phiên bản, mật khẩu quản trị yếu.

Đặt mật khẩu quản trị quá yếu (không đủ độ dài ký tự, không có các ký tự viết hoa, ký tự đặc biệt,...), thiếu cơ chế chống brute force khiến kẻ tấn công có thể dò password admin. Cài đặt các module, plugin, extension, đều đã cũ bị dính các lỗi bảo mật đã được công bố (CVE) hoặc không cập nhật mới khi dùng các mã nguồn mở hiện nay thường là joomla, wordpress, ...

3. Dấu hiệu nhận biết:

Thông thường tấn công Deface chủ yếu là vào các trang mặc định như: index.php, index.html, home.html, default.html, trangchu.html..... thì chỉ cần xử lý các trang mặc định này website sẽ hoạt động lại. Nhưng nếu hacker không thay đổi nội dung những file trên thì

người dùng khó thể phát hiện và người dùng sẽ nhận được cảnh báo từ việc truy cập website hoặc nhà quản lý hosting.

4. Phạm vi ảnh hưởng:

Ảnh hưởng giao diện ứng dụng

5. Phương án xử lý:

Bước	Nội dung thực hiện
1	Giám sát và thông báo khi website bị deface:
	Thông báo các bộ phận đơn vị liên quan khi thấy hiện tượng deface website xảy ra: Đơn vị quản lý website bị tấn công.
2	Thực hiện các biện pháp ngăn chặn.
2.1	Xử lý nội bộ:
	- Gỡ bỏ ngay lập tức trang website bị deface thay đổi nội dung. - Thực hiện chuyển đổi domain website về trang tạm HTML có nội dung trang index giống với trang homepage của trang chủ. - Sao lưu toàn bộ log và backup lại dữ liệu website bị deface để bộ phận Security phân tích kiểm tra - Thực hiện khôi phục lại data sao lưu gần nhất và kiểm tra phục hồi dữ liệu website. - Thực hiện chuyển đổi domain website về trang chính.
	- Phân tích log Firewall và WAF để xác định nguồn IP, hình thức tấn công và thực hiện ngăn chặn IP tấn công và đặt rule fix lỗ hổng của website.
	- Tạo access list trên router gateway để ngăn chặn các IP tấn công vào website.
2.2	Xử lý mở rộng nếu website bị deface liên tục:
	Liên hệ với các chuyên gia ứng cứu tham gia phân tích và tìm biện pháp xử lý: - Truy tìm mã độc do hacker upload lên server. - Phân tích mẫu mã độc và viết công cụ diệt các mã độc. - Theo dõi và cập nhật các mẫu mã độc mới
3	Phân tích log hệ thống để xác định nguồn tấn công, phạm vi và hình thức tấn công:
	- Dò quét mã độc trên server hosting website bị deface. Nếu phát hiện file lạ mà phần mềm antivirus không nhận biết là virus thì upload file đó lên website https://www.virustotal.com/en/ để kiểm tra virus.
	- Kiểm tra network infomation. Sử dụng lệnh nbtstat liệt kê bảng NETBIOS name chứa danh sách các kết nối trên hệ thống sử dụng NETBIOS. Thu thập chi tiết các kết nối mạng ảnh hưởng đến hệ thống máy chủ. Sử dụng lệnh netstat–ao có thể giúp truy tìm logged attacker, giao tiếp IRCbot comminication và Worm logging. - Kiểm tra các tài khoản người dung mới lạ, nhất là với các tài khoản có ID bằng không.

	- Kiểm tra liệt kê thông tin user tồn tại trên hệ thống máy chủ bằng cách sử dụng công cụ UserProfileView. - Kiểm tra truy nhập hệ thống bằng các tài khoản thông thường, đề phòng trường hợp các tài khoản này bị truy nhập trái phép và thay đổi quyền hạn mà người sử dụng hợp pháp không kiểm soát được. - Kiểm tra loggon của user. Sử dụng công cụ Psloggedon Tool và Logonsessions Tool kiểm tra loại logon và thời điểm mà các user remote vào máy chủ.
	- Dựa vào các thông tin thu thập và được phân tích của bộ phận system và security sẽ đưa ra phương án khắc phục phòng ngừa như: đóng port upload fck của Tomcat, xoá user mặc định, đổi port dịch vụ mặc định…
4	Khôi phục lại trạng thái ban đầu khi tấn công đã chấm dứt:
	- Tiếp tục theo dõi giám sát để xác định tình trạng tấn công và khôi phục website về trạng thái ban đầu khi tấn công đã chấm dứt.
	- Gửi email thông báo cho các ISP có nguồn IP tấn công để thông báo, yêu cầu họ ngăn chặn và xử lý hành vi tấn công.
	- Liên hệ với đơn vị an ninh quốc gia (nếu IP thuộc Viet Nam) để yêu cầu điều tra người thực hiện và xử lý theo phát luật.
5	Thực hiện các biện pháp phòng ngừa:
	- Lập tài liệu quá trình tấn công khắc phục, thảo luận rút kinh nghiệm và thực hiện điều chỉnh kế hoạch/kịch bản phòng thủ phù hợp. - Tăng cường công tác giám sát. - Tự động việc giám sát nội dung (tính bảo toàn nội dung) website thông qua phần mềm Website Watcher, giúp phát hiện và cảnh báo deface website sớm. - Giám sát tính bảo toàn nội dung của trang chính (có thể nhận biết deface khi thay đổi files index), kiểm tra thay đổi banner và một số tính năng khác. - Cảnh báo thông qua sound, sms, email. - Thông báo với các đơn vị phát triển website về các lỗ hổng source code để fix lỗi. - Cập nhật tin lên website bằng tài khoản VPN. - Phối hợp với các đơn vị liên quan tổ chức đánh giá định kỳ lỗ hổng của website.

VI. TÌNH HUỐNG TẤN CÔNG MÃ HÓA PHẦN MỀM, DỮ LIỆU, THIẾT BỊ

1. Định nghĩa:

- *Ransomware:*

Đây là cách gọi tên của dạng mã độc mới nhất và có tính nguy hiểm cao độ đối với nhân viên văn phòng, bởi nó sẽ mã hóa toàn bộ các file word, excel và các tập tin khác trên máy tính bị nhiễm làm cho nạn nhân không thể mở được file. Các chuyên gia của Kaspersky Lab nhận dạng các trường hợp bị nhiễm nhiều nhất tại Việt Nam là do một thành viên của Ransomware – Trojan-Ransom.Win32.Onion gây nên.

2. Phân loại:

- Trojans: Thay đổi mã hóa nhằm đánh cắp mật khẩu của người dùng.

- Password Cracker: hình thức tấn công làm vô hiệu hóa chức năng bảo vệ mật khẩu của hệ thống cơ quan, đơn vị sau đó bẻ khóa để truy cập.

- Virus: xóa dữ liệu.

3. Phạm vi ảnh hưởng:

- Một khi kẻ xấu, tin tặc hay hacker biết được dữ liệu liên quan tới cơ quan, đơn vị người dùng, chúng có thể bôi xấu trên các mạng xã hội, trên phương diện truyền thông báo chí.

- Nguy hiểm nhất là trong trường hợp cơ quan, đơn vị bị hacker chiếm toàn quyền kiểm soát hệ thống của cơ quan, đơn vị thì người dùng sẽ rất khó lấy lại được dữ liệu của mình. Lúc này người dùng cần phải nhờ tới sự giúp đỡ của những cơ quan, đơn vị an ninh mạng, cơ quan, đơn vị bảo mật. Chúng tôi sẽ ứng cứu, xử lý sự cố về bảo mật, lỗ hổng, an ninh mạng một cách an toàn và chuyên nghiệp, đảm bảo dữ liệu của cơ quan, đơn vị được an toàn nhất.

- Ngoài ra, nếu việc bảo mật dữ liệu của cơ quan, đơn vị người dùng chưa tốt, hacker có thể tấn công và thay đổi cấu hình website, giao diện phần mềm, xóa dữ liệu….

4. Phương án xử lý:

Giải pháp phần cứng: giải pháp này tập trung vào các hệ thống máy chuyên dụng, hệ thống máy tính hay những mô hình mạng riêng biệt.

Giải pháp bảo mật phần mềm: hiện nay phần mềm, công cụ được sử dụng trong cơ quan, đơn vị rất nhiều do đó cần có những giải pháp bảo mật cho phần mềm của cơ quan, đơn vị như quản lý người dùng tốt, xác thực 2 yếu tố, kiểm soát thiết bị đầu vào đầu ra, cập nhật bản vá lỗi phần mềm…

Giải pháp về con người: Thường xuyên tổ chức các buổi tập huấn hoặc đào tạo kiến thức bảo mật dữ liệu, an ninh mạng, các phương pháp kiểm tra lỗ hổng bảo mật cơ bản…

VII. TÌNH HUỐNG TẤN CÔNG PHÁ HOẠI THÔNG TIN, DỮ LIỆU, PHẦN MỀM

1. Giới thiệu:

Đây là cuộc tấn công có hình thức phá hoại, nhằm xóa dữ liệu từ các máy và khiến một số mạng nội bộ của hang không thể hoạt động Phá huỷ dữ liệu đòi hỏi ít thách thức về mặt kỹ thuật hơn so với xâm nhập vào một mạng lưới, do vậy, các sự cố được công bố không xảy ra thường xuyên thường là do tin tặc thiếu động lực để hành động. Hiện nay, công cụ hack đang được lan truyền rộng rãi hơn, và càng có nhiều tội phạm mạng, nhà hoạt động, gián điệp và các đối thủ kinh doanh thử nghiệm những phương pháp này.

2. Phân loại:

- *Gửi email chứa phần mềm gián điệp:*

Trước hết hacker sẽ thu thập thông tin về đối tượng cần tấn công bằng nhiều cách thức khác nhau: qua đài báo, phương tiện xã hội, qua mối quan hệ, qua mạng internet, thậm chí là tới tận nơi để tìm hiểu…

Hacker sẽ thu thập càng nhiều thông tin càng tốt: web, email, điện thoại, nhân sự, hoạt động kinh doanh, sơ đồ hệ thống… Sau đó họ dùng công cụ kỹ thuật để tìm lỗ hổng. Đôi khi họ chưa tiến hành trực tiếp vào hệ thống mà tập trung tấn công vào máy tính, điện thoại, email… của một nhân viên nào đó trong tổ chức hoặc tổ chức liên quan (tìm hiểu gián tiếp). Thông qua những bước trung gian như vậy để lấy thông tin cần.

Cung cấp thiết bị có chứa sẵn mã độc một kịch bản tấn công đơn giản thường được hacker sử dụng để phát tán phần mềm gián điệp là gửi email đính kèm file văn bản.

Nội dung và địa chỉ của các email này là có thật, nội dung file đính kèm cũng là có thật nhưng máy tính người dùng bị nhiễm virus do trong file có chứa sẵn phần mềm gián điệp. Khi các file văn bản này được mở, phần mềm gián điệp sẽ xâm nhập, kiểm soát máy tính. Chúng ẩn náu bằng cách giả dạng các phần mềm phổ biến như Windows Update, Adobe Flash, Bộ gõ Unikey, Từ điển… và chỉ hoạt động khi có lệnh của những kẻ điều khiển nên rất khó phát hiện. Các mã độc này âm thầm đánh cắp thông tin gửi về máy chủ điều khiển hoặc nhận lệnh để thực hiện các hành vi phá hoại khác.

3. Dấu hiện nhận diện:

Kiểm tra Internet Gateway các IP độc hại, giám sát từ các hệ thống kiểm soát truy cập Internet.

4. Phương án xử lý:

- Ngăn chặn các địa chỉ độc hại, cô lập máy tính ra khỏi mạng.

- Thực hiện lấy mẫu để xác định các hành vi.

- Liên hệ đội ứng cứu để phục vụ các công tác điều tra chuyên sâu.

VIII. TÌNH HUỐNG TẤN CÔNG NGHE TRỘM, GIÁN ĐIỆP, LẤY CẮP THÔNG TIN, DỮ LIỆU

1. Định nghĩa

Các phần mềm gián điệp bằng cách nào đó được cài đặt vào thiết bị của người dùng chúng nằm vùng và thực hiện các cuộc tấn công có chủ đích thông qua các thiết bị bị nhiễm, hiện tại mục tiêu tấn công phổ biến là các thiết bị IoT.

2. Phân loại:

- WildTangent: phần mềm này được cài đặt thông qua American Online Instant Messenger (AIM). Một khi được cài đặt, nó sẽ lấy các thông tin về tên họ, số điện thoại, địa chỉ thư điện tử cũng như là tốc độ của CPU, các tham số của video card và DirectX. Các thông tin này có thể bị chia sẻ cho các nơi khác chiếm dụng.

- Xupiter: chương trình này sẽ tự nảy các bảng quảng cáo. Nó thêm các chỗ đánh dấu (*bookmark*) lên trên menu của chương trình duyệt và, nguy hại hơn, nó thay đổi cài đặt của

trang chủ. Xupiter còn chuyển các thói quen xài Internet (*surfing*) về xupiter.com và do đó làm chậm máy. Ngoài ra nó còn đọc cả địa chỉ IP và các tin tức khác.

- DoubleClick: dùng một tệp nhỏ gọi là cookies theo dõi hoạt động trực tuyến của người dùng.

- WinWhatWhere: thông báo cho người khác biết về các tổ hợp phím (*keystroke*) mà người dùng gõ.

- Gator và eWallet: ăn cắp tên, quốc gia, mã vùng bưu điện và nhiều thứ khác.

3. Dấu hiệu nhận diện:

- Khi người dùng gõ tìm một địa chỉ trên "Internet Explorer" và nhấn nút "Enter" để bắt tìm kiếm thì trang "search" thường dùng bị thay bởi một trang search lạ.

- Các chương trình chống spyware không hoạt động được. Nó có thể báo lỗi mất những tệp tin cần thiết, ngay cả sau khi cài đặt trở lại thì vẫn không hoạt động. Nguyên do là các phần mềm gián điệp đã ngăn chặn không cho cài các chương trình chống gián điệp hoạt động hữu hiệu.

- Người dùng tìm thấy những tên địa chỉ lạ trong danh sách "Favorites" mặc dù người dùng chưa hề đặt nó vào trong mục này.

- Máy tự nhiên chạy chậm hơn thường nhật, có những tiến trình không quen biết dùng gần như 100% thời lượng của CPU.

- Ở thời điểm mà người dùng không hề làm gì với mạng mà vẫn thấy đèn gửi/nhận chớp sáng trên "dial-up" hay "board band modem" giống như là khi đang tải một phần mềm về máy hay là các biểu tượng "network/modem" nhấp nháy nhanh khi mà người dùng không hề nối máy vào mạng.

- Một "search toolbar" hay "browser toolbar" xuất hiện mặc dù người dùng không hề ra lệnh để cài đặt nó và không thể xoá chúng, hay là chúng xuất hiện trở lại sau khi xoá.

- Người dùng nhận một cửa sổ quảng cáo khi trình duyệt chưa hề chạy và ngay cả khi máy chưa nối kết với Internet hay là người dùng nhận được các quảng cáo có đề tên người dùng trong đó.

- Trang chủ của bạn bị đổi một cách kì cục. Bạn đổi nó lại bằng tay nhưng nó lại bị sửa...

- Gõ vào các địa chỉ quen biết mà chỉ nhận được trang trống không hay bị báo lỗi "*404 Page cannot be Found*".

4. Phạm vi ảnh hưởng:

- Từ cá nhân người dùng cho đến doanh nghiệp, tổ chức chính phủ,… đều có thể là nạn nhân của hình thức tấn công này

- Sự phát triển mạnh mẽ của IoT càng làm cho mức độ ảnh hưởng của hình thức tấn công này nhân rộng.

5. Phương án xử lý

- Cần xây dựng hệ thống giám sát để nhận biết các cuộc tấn công sử dụng các thiết bị IoT một cách nhanh nhất, sau đó tiến hành vô hiệu hóa máy chủ điều khiển để ngăn chặn hành vi tấn công này.

- Hệ thống giám sát an toàn mạng đóng vai trò quan trọng, không thể thiếu trong hạ tầng công nghệ thông tin (CNTT) của các cơ quan, đơn vị, tổ chức. Hệ thống này cho phép thu thập, chuẩn hóa, lưu trữ và phân tích tương quan toàn bộ các sự kiện an toàn mạng được sinh ra trong hệ thống CNTT của tổ chức.

- Ngoài ra, hệ thống giám sát an toàn mạng phát hiện kịp thời các tấn công mạng, các điểm yếu, lỗ hổng bảo mật của các thiết bị, ứng dụng và dịch vụ trong hệ thống. Phát hiện kịp thời sự bùng nổ virus trong hệ thống mạng, các máy tính bị nhiễm mã độc, các máy tính bị nghi ngờ là thành viên của mạng máy tính ma (botnet).

XI. TÌNH HUỐNG TẤN CÔNG TỔNG HỢP SỬ DỤNG KẾT HỢP NHIỀU HÌNH THỨC

1. Định nghĩa:

Phần lớn các kỹ thuật tấn công đã được nhận diện ở các mục trên, nhưng một cuộc tấn công thường trải qua nhiều quá trình và kết hợp nhiều hình thức với nhau. Từ đó sẽ để lại nhiều thông tin trên các vùng mạng từ phía ngoài vào phía trong. Từ đó mỗi phân vùng mạng cần trang bị đầy đủ các giải pháp để có được đầy đủ thông tin khi có bất kỳ thay đổi, và đưa ra phương án xử lý.

2. Phân loại:

Các hình thức tấn công chính:

- Tấn công kết hợp lừa đảo thông qua mạng xã hội.

- Tấn công thông qua các mã khai thác mà hệ thống chưa nhận diện.
- Thông qua các tài khoản được cung cấp từ trong nội bộ.

3. Phương án xử lý:

- Kết hợp với các biện pháp đã xây dựng bên trên để cùng xử lý, phân tách vai trò từng vùng mạng và cán bộ xử lý riêng.

- Thu thập các nguồn dữ liệu để phục vụ phân tích sau này.

X. TÌNH HUỐNG CÁC HÌNH THỨC TẤN CÔNG MẠNG KHÁC

1. Định nghĩa:

Trên thực tế, hiện nay có rất nhiều dạng, phương thức tấn công mạng. Các tin tặc có thể cài mã độc vào bên trong file hoặc ứng dụng phần mềm của hệ thống hoặc tấn công từ wifi bên ngoài…; các hoạt động xâm nhập ngày càng tinh vi, đa chiều vì vậy "phòng bệnh tốt hơn chữa bệnh".

2. Phân loại:

- *Tấn công mạng với hình thức Phishing:*

Người dùng rất dễ bị lừa nếu không để ý tới trang web mà mình đang truy cập bởi vì Phishing là kiểu tấn công người dùng bằng cách tạo ra 1 trang web với địa chỉ giả mạo. Chẳng hạn như www.google.com thành www.gugle.com. Thông thường với hình thức này,

các tin tặc sẽ gửi tới người dùng 1 email đăng nhập để người dùng đăng nhập và click vào đó, tiếp theo sẽ sử dụng kỹ thuật điều hướng để điều sang website chứa mã độc. Và vô tình, khi người dùng đăng nhập thông tin tài khoản gmail của mình vào web giả mạo đó, người dùng đã bị mất tài khoản.

- *Tấn công mạng trực tiếp từ bên trong nội bộ:*

Tin tặc có thể cài gắm máy tính trực tiếp của họ vào máy tính của người khác hoặc lấy được tài khoản và mật khẩu của người khác sau đó thực hiện hành vi tấn công của mình

Tấn công gián tiếp. Các hacker có thể nghe trộm những thông tin khi truy cập vào hệ thống máy tính người dùng để đánh cắp dữ liệu cá nhân như hình ảnh, file, video…

Tấn công theo tệp đính kèm. Ví dụ như Email, file đính kèm chẳng hạn. Sau khi người dùng click vào tệp đính kèm thì lập tức máy tính bị nhiễm virus. Case Study điển hình trong thời gian quý I năm 2017 là hàng loạt vụ xảy ra liên quan tới mã độc tống tiến Ransomware khi người dùng Click vào tệp đính kèm trong email. Hoặc mã độc tống tiền Ransomware có thể ẩn trong quảng cáo Skype, phần mềm trên điện thoại iPhone, Android.

Tấn công ẩn danh. Virus có thể xâm nhập vào máy tính bằng những phần mềm độc hại như những phần mềm diệt virus, phần mềm học tập hay các trình duyệt, plug in ẩn danh, ẩn trong quảng cáo của trình duyệt và phần mềm

- *Tấn công vào con người:*

Kẻ tấn công có thể liên lạc với người quản trị hệ thống, tạo nên 1 hộp thoại đăng nhập sau đó yêu cầu người dùng thay đổi mật khẩu, thay đổi cấu hình hệ thống. Phương tức tấn công mạng này rất khó tìm ra giải pháp ngăn chặn triệt để ngoài giáo dục nhận thức của người dùng.

Một số hình thức, phương thức tấn công vào hệ thống mạng, máy tính khác như: thông qua usb, đĩa CD, địa chỉ IP, server, qua đầu vào của máy in….

- *Giải pháp:*

Bảo vệ tài khoản cá nhân của mình bằng xác thực mật khẩu 2 lớp . Hiện tại những trang web như facebook, gmail, những trang web với giao thức https cũng đã hỗ trợ người dùng bảo mật mật khẩu 2 lớp.

Không nên sử dụng những USB không rõ nguồn gốc hay đã cắm vào nhiều máy tính khác nhau. Nếu tốc độ copy hoặc paste file trong USB của người dùng chậm thì nên thay cái mới với dung lượng lớn hơn

Để tránh bị tấn công mạng, người dùng cũng không nên click vào những đường link lạ hoặc những trang web đen

Dùng những phần mềm diệt virus uy tín

Nâng cấp các trình duyệt, phần mềm và ứng dụng một cách thường xuyên

Đối với các doanh nghiệp, để tránh lại những phương thức tấn công mạng đa dạng của hackers cần phải kiểm tra, nâng cấp hệ thống, có những giải pháp, chiến lược an ninh mạng rõ ràng. Đồng thời việc bảo trì hệ thống mạng, máy tính cần được thực hiện một cách đều đặn.

3. Dấu hiệu nhận diện:

Theo từng loại tấn công sẽ có dấu hiệu nhận diện khác nhau, tuỳ tình huống đội ứng phó sẽ có những sự kiện tương ứng.

4. Phạm vi ảnh hưởng:

Từ cá nhân người dùng cho đến doanh nghiệp, tổ chức chính phủ,… đều có thể là nạn nhân của hình thức tấn công này

5. Phương án xử lý:

Xây dựng quy trình chung và áp dụng cho các loại hình thức tấn công, từ đó đưa ra phương án xử lý cụ thể.

XI. TÌNH HUỐNG SỰ CỐ NGUỒN ĐIỆN

1. Định nghĩa:

Nguồn điện bị mất đột ngột do hoạt động cắt điện đột xuất của điện lực, sự cố chạm chập trên đường dẫn làm nhảy Ap-to-mat. Nguồn điện bị tăng giảm áp đột ngột xuất phát từ sự cố thiết bị phụ tải xảy ra ở trạm phát hay trên đường dẫn, có thể do sét đánh. Các sự cố nguồn điện có thể làm thiết bị điện tử ngừng hoạt động đột ngột hoặc hoạt động không ổn định gây ảnh hưởng, lỗi cả hệ thống phần mềm lần phần cứng dẫn đến mất dữ liệu, hư ổ cứng, giảm tuổi thọ của thiết bị.

2. Phương án xử lý:

- Trang bị thiết bị UPS để lưu điện và có thời gian chuyển đổi nguồn dự phòng.

- Trạng bị máy phát điện để trong trường hợp nguồn điện dự phòng không hoạt động.

Bước	Nội dung thực hiện
1	Kiểm tra nguồn đã được tự động chuyển sang đường dự phòng.
2	Chuẩn bị máy phát trong trường hợp đường dự phòng cũng ảnh hưởng.
3	Đội vận hành kiểm tra hoạt động của hệ thống.
4	Theo dõi và chuyển nguồn về nguồn chính, theo dõi trạng thái hoạt động của máy phát.

XII. TÌNH HUỐNG SỰ CỐ ĐƯỜNG KẾT NỐI INTERNET

1. Định nghĩa:

Sự cố về đường truyền Internet xuất phát chủ yếu từ việc đứt cáp quang đi quốc tế trên biển. Các sự cố do đứt cáp gây tình trạng chập chờn khi kết nối Internet và không thể khắc

phục chủ động mà phải đợi nhà cung cấp hoàn tất sửa chữa. Việc truy cập chậm kết nối Internet cũng do các thiết bị modem, switch hay card mạng bị lỗi. Ngoài ra, sự cố liên quan đến kết nối Internet cũng có thể do có virus trong hệ thống hoặc các ứng dụng không cần thiết truy cập Internet liên tục chiếm băng thông, làm trì hoãn truy cập internet của hệ thống.

2. Phương án xử lý:

Trang bị thêm tối thiểu 01 đường Internet, cần có giải pháp Fail Over khi xảy ra mất kết nối đầu Internet, các thiết bị Router, Moderm phải được trang bị dự phòng, phòng trường hợp thiết bị hư hỏng.

XIII. TÌNH HUỐNG SỰ CỐ DO LỖI PHẦN MỀM, PHẦN CỨNG, ỨNG DỤNG CỦA HỆ THỐNG THÔNG TIN

1. Định nghĩa:

Phần mềm, phần cứng, ứng dụng của hệ thống thông tin chưa được cập nhật, tồn tại lỗ hỏng người dùng vô tình truy cập vào lỗ hỏng này, hoặc kẻ tấn công có chủ đích khai thác lỗ hỏng này. Các sự cố này dẫn đến truy cập tài nguyên của người dùng gặp khó khăn, trì trệ công việc hoặc nguy hiểm hơn nếu kẻ tấn công khai thác thành công để xâm nhập vào hệ thống gây hậu quả nặng nề hơn.

2. Phương án xử lý:

- Liên hệ nhà cung cấp phần mềm (nếu còn trong thời hạn hợp đồng).

- Trang bị các giải pháp phòng thủ để hạn chế tấn công trong trường hợp tồn tại lỗ hổng nhưng không có mã nguồn để khắc phục.

- Cần trang bị, mua thêm bản quyền nếu ứng dụng đã hết hạn.

XIV. TÌNH HUỐNG SỰ CỐ LIÊN QUAN ĐẾN QUÁ TẢI HỆ THỐNG

1. Định nghĩa:

Việc hệ thống phải hoạt động liên tục dẫn đến đôi khi bị quá tải, có thể do truy cập và hoạt động tăng cao bất thường lên máy chủ vượt quá khả năng tải, cũng xuất phát từ các yếu tố liên quan đến phần cứng cũ, xuống cấp không còn xử lý mạnh mẽ như thời gian ban đầu. Ngoài ra các lỗ hỏng xuất phát từ các phần mềm đang chạy gây chiếm tài nguyên lớn gây treo đứng hệ thống. Các sự cố quá tải hệ thống dễ gây hiện tương trì trệ hoạt động của doanh nghiệp và cơ sở, đôi khi hệ thống bị sụp rất khó khắc phục.

2. Phương án xử lý:

- Xác định nguồn đang quá tải (máy chủ, tiến trình, kết nối).

- Xác định phạm vi ảnh hưởng.

- Liên hệ với quản trị, chủ quản của hệ thống để kiểm tra các nguồn gốc.

- Xác định nguồn gốc, nếu sự cố đến từ bên ngoài -> có dấu hiệu bị tấn công từ chối dịch vụ, xem phương án xử lý tình huống tấn công DoS.

- Nếu nguồn gốc từ quá trình vận hành, kiểm tra các thay đổi trên máy chủ/thiết bị để xác định nguyên nhân (tiến trình chiếm nhiều CPU, RAM, băng thông).

- Nếu thiết bị vận hành tăng cao về lưu lượng, kiểm tra các Log kết nối qua thiết bị để nhận diện nguyên nhân và cách xử lý.

- Liên hệ cơ quan chức năng nếu xảy ra tấn công.

XV. TÌNH HUỐNG SỰ CỐ KHÁC DO LỖI CỦA HỆ THỐNG, THIẾT BỊ, PHẦN MỀM, HẠ TẦNG KỸ THUẬT

1. Định nghĩa:

Ngoài ra trong khi vận hành với các hạ tầng kỹ thuật, việc xảy ra va chạm lên thiết bị ngoài ý muốn, như vô tình làm rơi, ngã, làm đổ nước vào gây hư hỏng thiết bị. Đối với phần mềm, việc cập nhật phiên bản mới đôi khi gây hiện tượng xung đột và không tương thích, ảnh hưởng dịch vụ đang chạy, thậm chí gây sụp máy chủ.

2. Phương án xử lý:

- Cần xây dựng hồ sơ kiểm soát vòng đời thiết bị, máy chủ, phần mềm.

- Lập kế hoạch nâng cấp theo thời gian hiệu lực và vòng đời.

- Trang bị thiết bị thay thế nóng.

- Trong trường hợp thiết bị Inline xảy ra hư hỏng có thể bypass qua thiết bị (cần module bypass) hoặc thay đổi kết nối vật lý.

- Khi thực hiện nâng cấp thiết bị cần có thiết bị dự phòng, sao lưu các cấu hình trước khi nâng cấp, cần có phương án roll back khi xảy ra sự cố không tương thích.

XVI. TÌNH HUỐNG SỰ CỐ DO LỖI CỦA NGƯỜI QUẢN TRỊ, VẬN HÀNH HỆ THỐNG

1. Định nghĩa:

- Lỗi trong cập nhật, thay đổi, cấu hình phần cứng:

Khi cập nhật, thay đổi cấu hình phần cứng, người quản trị đôi khi sai thao tác hoặc sai cú pháp dẫn đến thiết bị chạy không ổn định, chết dịch vụ hoặc xung đột cấu hình với các thiết bị khác. Các lỗi liên quan cấu hình phần cứng gây trì trệ, thiếu ổn định trên hệ thống nếu xảy ra.

- Lỗi trong cập nhật, thay đổi, cấu hình phần mềm:

Việc cập nhật, thay đổi cấu hình trên phần mềm là cần thiết, tuy nhiên đôi khi thực hiện sai thao tác và cú pháp dẫn đến lỗi hoặc không chuẩn. Các lỗi liên quan đến cập nhật thay đổi cấu hình phần mềm gây trì trệ truy cập từ phía người dùng, có thể xuất hiện hiện tượng không tương thích với các phần mềm tích hợp khác.

- Lỗi liên quan đến chính sách và thủ tục an toàn thông tin:

Quy định chính sách và thủ tục an toàn thông tin là bắt buộc, nhưng đôi khi xuất hiện các lỗ hổng và thiếu chặt chẽ dẫn đến các lỗi liên quan. Việc này gây ra các hành vi sai trái có thể được thực hiện trong hệ thống, hoặc sự chủ quan cả phía người dùng và quản trị gây thiếu sót trong khâu vận hành và sử dụng, gây các thao tác thiếu an toàn.

- *Lỗi liên quan đến việc dừng dịch vụ vì lý do bắt buộc:*

Việc dừng dịch vụ đôi khi xảy ra để thực hiện bảo trì, tuy nhiên khi thực hiện ngưng chạy dịch vụ gây ra hiện tượng dịch vụ vẫn chạy nhưng chạy sai, hoặc dịch vụ không thể khởi chạy lại được nữa. Các lỗi này rất khó khắc phục nếu không có thao tác dự phòng, dịch vụ bị trì hoãn lâu dài và có thể gây ảnh hưởng các dịch vụ khác trong hệ thống.

- *Lỗi khác liên quan đến người quản trị, vận hành hệ thống:*

Sự chủ quan và lơ là của người quản trị và vận hành hệ thống dễ gây ra các thao tác sai dễ dẫn đến các dịch vụ chạy lỗi, các thiết bị chạy sai và các lỗ hổng có thể bị xâm nhập.

2. Phương án xử lý:

STT	Nội dung	Công việc	Ghi chú
1	Giám sát và phát hiện	- Giám sát và phát hiện các dịch vụ, ứng dụng có bị gián đoạn hay không. - Nhận định nguyên nhân và xác định sự cố an toàn thông tin theo danh mục.	
2	Phối hợp các đơn vị ứng cứu	Phối hợp các đơn vị ứng cứu chuyên trách của Tỉnh và các đơn vị khác	
3	Các bước xử lý	- Tiến hành phục hồi dữ liệu sao lưu. - Tiến hành thay thế thiết bị. - Tiến hành sử dụng ứng dụng, thiết bị dự phòng.	- Cần tiến hành sao lưu backup định kỳ - Cần chuẩn bị các thiết bị hoặc phương án mượn thiết bị đối với các thành phần quan trọng của hệ thống CNTT
4	Báo cáo	- Báo cáo cho ban lãnh đạo đơn vị. - Báo cáo cho đơn vị chuyên trách về CNTT của tỉnh.	Bằng văn bản hoặc Email để ghi nhận sự cố

XVII. TÌNH HUỐNG SỰ CỐ LIÊN QUAN ĐẾN CÁC THẢM HỌA TỰ NHIÊN NHƯ BÃO, LỤT, ĐỘNG ĐẤT, HỎA HOẠN V.V....

1. Phân loại:

Danh mục các sự cố trong nhóm này:

- Bão, lụt;

- Thiên tai, động đất, hỏa hoạn…

2. Phương án xử lý:

STT	Nội dung	Công việc	Ghi chú
1	Giám sát và phát hiện	Thường xuyên theo dõi các tin tức dự báo về thảm họa tự nhiên	Nên có phương án sao lưu dự phòng đặt tại trung tâm dữ liệu khác khu vực địa lý.
2	Phối hợp các đơn vị ứng cứu	Phối hợp các đơn vị ứng cứu chuyên trách của tỉnh và các đơn vị khác	
3	Các bước xử lý	- Tiến hành sử dụng các hệ thống tạm để duy trì công việc. - Tiến hành xây dựng phục hồi hệ thống hạ tầng sau thảm họa. - Phục hồi dữ liệu từ các bản sao lưu.	Cần tiến hành sao lưu backup định kỳ Xem xét chuẩn bị phương án các hệ thống dự phòng cho các ứng dụng quan trọng.
4	Báo cáo	- Báo cáo cho ban lãnh đạo đơn vị. - Báo cáo cho đơn vị chuyên trách về CNTT của tỉnh.	Bằng văn bản hoặc Email để ghi nhận sự cố.

CHƯƠNG V
CÔNG TÁC TỔ CHỨC, ĐIỀU HÀNH, PHỐI HỢP TRONG ĐỐI PHÓ, NGĂN CHẶN, ỨNG CỨU, KHẮC PHỤC SỰ CỐ

I. CÔNG TÁC PHỐI HỢP

Khi có sự cố nghiêm trọng, cần thực hiện các công tác phối hợp, kết hợp với các đơn vị chức năng để hạn chế về thiệt hại, từ đó Đội ứng cứu ATTT mạng tỉnh đưa ra một cách thức xử lý chung cho các trường hợp khẩn:

1. Ghi nhận tấn công:

Khi phát hiện hệ thống có nguy cơ mất an toàn thông tin như: hệ thống hoạt động chậm bất thường, không truy cập được hệ thống ứng dụng, nội dung Cổng/Trang thông tin điện tử hoặc giao diện ứng dụng bị thay đổi, các sự cố khác có liên quan,… các đơn vị thực hiện các bước cơ bản:

Bước 1: Ngắt kết nối hệ thống máy chủ ra khỏi hệ thống mạng, báo cáo sự cố đến Thủ trưởng cơ quan, đơn vị;

Bước 2: Sao chép nhật ký truy cập của người dùng (logfile) và toàn bộ dữ liệu của hệ thống ra thiết bị lưu trữ (phục vụ cho công tác phân tích);

Bước 3: Khôi phục lại hệ thống, hoặc sử dụng hệ thống dự phòng và chuyển dữ liệu sao lưu dự phòng (backup) mới nhất để hệ thống hoạt động;

Bước 4: Tổng hợp, báo cáo sự cố và nội dung khắc phục gửi về Đội ứng cứu sự cố ATTT mạng tỉnh để tổng hợp.

2. Nguyên tắc phối hợp trong ứng cứu sự cố:

a) Đơn vị vận hành hệ thống thông tin:

- Thực hiện các bước khắc phục sự cố theo bước 1 tại Mục 1 Phần I của Phương án này.

- Các sự cố vượt quá khả năng xử lý, đơn vị thông báo đến Đội ứng cứu để hỗ trợ khắc phục và thực hiện báo cáo sự cố ATTT mạng (theo mẫu).

- Tổng hợp, báo cáo gửi đơn vị chuyên trách CNTT (Sở Thông tin và Truyền thông) theo định kỳ 06 tháng một lần và báo cáo đột xuất khi có yêu cầu.

b) Đội ứng cứu sự cố ATTT mạng tỉnh:

- Tiếp nhận thông tin, báo cáo sự cố mất an toàn thông tin của đơn vị.

- Phản hồi cho đơn vị, cá nhân gửi thông báo, báo cáo ban đầu ngay sau khi nhận được để xác nhận về việc đã nhận được thông báo, báo cáo sự cố.

- Thẩm tra, xác minh và phân loại sự cố an toàn thông tin mạng để lựa chọn phương án ứng cứu phù hợp hoặc đề xuất với Ban chỉ đạo xây dựng Chính quyền điện tử tỉnh chịu trách nhiệm chỉ đạo ứng cứu khẩn cấp sự cố ATTT trong phạm vi trên địa bàn tỉnh đối với các biện pháp giải quyết vượt thẩm quyền.

- Chủ động hỗ trợ ngay đơn vị cần ứng cứu, xử lý sự cố trong khả năng và trách nhiệm của mình, cử cán bộ kỹ thuật của Đội ứng cứu phối hợp với cán bộ phụ trách về lĩnh vực CNTT tại đơn vị để ghi nhận, hướng dẫn giải quyết sự cố trong trường hợp sự cố phức tạp, nguy cơ cao về an toàn thông tin mà không thể hướng dẫn, trao đổi qua điện thoại, email với đơn vị bị sự cố.

- Giám sát diễn biến tình hình ứng cứu sự cố và báo cáo Ban chỉ đạo xây dựng Chính quyền điện tử tỉnh và đề xuất, xin ý kiến chỉ đạo trong trường hợp không thuộc thẩm quyền, phạm vi trách nhiệm hoặc vượt khả năng xử lý của mình.

- Tổng hợp, báo cáo Trung tâm Ứng cứu khẩn cấp Máy tính Việt Nam - Cơ quan điều phối quốc gia về ứng cứu sự cố theo quy định và báo cáo đột xuất khi có yêu cầu.

- Sở Thông tin và Truyền thông – Cơ quan thường trực của Đội ứng cứu báo cáo về Ủy ban nhân dân tỉnh đồng thời báo cáo đến Bộ Thông tin và Truyền thông thông qua Trung tâm Ứng cứu khẩn cấp Máy tính Việt Nam - Cơ quan điều phối quốc gia về ứng cứu sự cố, để được hỗ trợ khắc phục các sự cố vượt quá khả năng xử lý của địa phương.

II. VAI TRÒ, NHIỆM VỤ CỦA CÁC ĐƠN VỊ, BỘ PHẬN LIÊN QUAN

Căn cứ Quyết định số 1165/QĐ-UBND ngày 28/12/2017 của Ủy ban nhân dân tỉnh Gia Lai về việc thành lập Đội ứng cứu an toàn thông tin mạng tỉnh Gia Lai và Quy chế hoạt động của Đội ứng cứu sự cố an toàn thông tin mạng tỉnh Gia Lai, trong đó đã nêu rõ vai trò và nhiệm vụ của từng đơn vị chức năng tham gia vào các công tác phối hợp qui định như sau:

STT	Đơn vị	Vai trò	Thông tin liên hệ
1	Đơn vị, cá nhân vận hành hệ thống thông tin	Phát hiện sự cố ATTT; báo cáo sự cố ATTT theo Phương án này (trong trường hợp không thể tự khắc phục)	Các cơ quan, đơn vị liên quan
2	Nhà thầu cung cấp dịch vụ an toàn thông tin mạng (nếu có)	Hỗ trợ phân tích thông tin sự cố	Chuyên gia ứng cứu sự cố ATTT mạng (theo phạm vi dịch vụ nếu có)
3	Đơn vị chuyên trách ứng cứu sự cố	Xử lý chính trong các trường hợp xảy ra sự cố	Đội ứng cứu sự cố ATTT mạng tỉnh

4	Cơ quan thường trực về ứng cứu sự cố ATTT mạng	Đảm bảo các điều kiện cho công tác ứng cứu sự số	Sở TT&TT tỉnh Gia Lai
5	Bộ phận giúp việc Đội ứng cứu sự cố ATTT mạng tỉnh	Tổ chức các hoạt động ứng cứu; đề xuất kế hoạch, biện pháp kỹ thuật phòng ngừa, ngăn chặn và xử lý, khắc phục sự cố để đảm bảo ATTT mạng	Trung tâm CNTT&TT
6	Cơ quan điều phối quốc gia	Tiếp nhận các báo cáo về sự cố ATTT từ địa phương; phối hợp, hỗ trợ thực hiện ứng cứu sự cố.	VNCERT
7	Cơ quan liên quan đến sự cố ATTT mạng	Phối hợp với cơ quan chuyên trách về ATTT để khắc phục các sự cố	Trung tâm CNTT&TT
8	Các đơn vị liên quan khác.	Phối hợp thực hiện ứng cứu sự cố	Các đơn vị có liên quan

CHƯƠNG VI
TỔ CHỨC THỰC HIỆN

I. TRIỂN KHAI THỰC HIỆN

1. Đội ứng cứu sự cố an toàn thông tin mạng:

- Trung tâm Công nghệ thông tin và Truyền thông thuộc Sở Thông tin và Truyền thông tỉnh Gia Lai (Bộ phận giúp việc Đội ứng cứu sự cố):

+ Chủ trì, phối hợp với các cá nhân, đơn vị liên quan tổ chức thực hiện Phương án ứng phó sự cố an toàn thông tin mạng trên địa bàn tỉnh Gia Lai;

+ Tổng hợp, tham mưu giải quyết các vướng mắc, tồn tại, phát sinh trong quá trình triển khai thực hiện Phương án;

+ Hằng năm, Trung tâm CNTT&TT báo cáo, tham mưu Sở Thông tin và Truyền thông sửa đổi, bổ sung Phương án ứng phó sự cố bảo đảm an toàn thông tin mạng trên địa bàn tỉnh Gia Lai cho phù hợp với tình hình thực tế.

- Cơ quan Thường trực Đội ứng cứu sự cố ATTT mạng (Sở Thông tin và Truyền thông):

+ Đảm bảo các điều kiện để Đội ứng cứu sự cố ATTT mạng thực hiện các nhiệm vụ ứng cứu sự cố theo Phương án này.

+ Làm đầu mối phối hợp với các cơ quan chuyên môn về ATTT ở cấp Trung ương liên quan đến công tác ứng cứu sự cố.

+ Hướng dẫn các cơ quan, đơn vị thực hiện tốt công tác đảm bảo ATTT; cập nhật các phương thức tấn công, cảnh báo tình huống gây ra sự cố hệ thống thông tin và phương án xử lý trên chuyên mục An toàn thông tin mạng của Trang Thông tin điện tử Sở Thông tin và

Truyền thông để các cơ quan, đơn vị, địa phương chủ động nghiên cứu, triển khai thực hiện.

+ Thực hiện công tác báo cáo định kỳ (hằng năm) hoặc đột xuất theo yêu cầu của các cơ quan cấp trên về tình hình thực hiện công tác bảo đảm an toàn thông tin mạng, ứng phó sự cố an toàn thông tin mạng trên địa bàn tỉnh.

4. Đề nghị Giám đốc các sở, ban, ngành, Chủ tịch UBND các huyện, thị xã, thành phố và Thủ trưởng các cơ quan, đơn vị có liên quan phổ biến, quán triệt và tổ chức việc thực hiện việc ứng phó sự cố về ATTT mạng theo Phương án này và các quy định có khác liên quan.

II. SỬA ĐỔI, BỔ SUNG PHƯƠNG ÁN

Trong quá trình tổ chức triển khai thực hiện Phương án, nếu có khó khăn, vướng mắc hoặc vấn đề mới phát sinh cần sửa đổi, bổ sung thì các cơ quan, đơn vị phản ánh về Sở Thông tin và Truyền thông để tổng hợp, xem xét, sửa đổi, bổ sung cho phù hợp./.

GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH GIA LAI

Nguyễn Ngọc Hùng