**BỘ THÔNG TIN VÀ TRUYỀN THÔNG**

**CỤC AN TOÀN THÔNG TIN**

**CHƯƠNG TRÌNH KHUNG “ĐÀO TẠO NGẮN HẠN VỀ AN TOÀN THÔNG TIN CHO CÁN BỘ QUẢN LÝ - MỨC CƠ BẢN”**

Nội dung

[1. Tổng quan và các khái niệm cơ bản 5](#_Toc422135930)

[1.1. Kiến trúc và dịch vụ của mạng Internet 5](#_Toc422135931)

[1.1.1. Kiến trúc mạng Internet 5](#_Toc422135932)

[1.1.2. Mô hình tham chiếu OSI và bộ giao thức TCP/IP 6](#_Toc422135933)

[1.3.4. Intranet và Extranet 11](#_Toc422135934)

[1.2. Các vấn đề chung về rủi ro trên Internet 11](#_Toc422135935)

[1.2.1. Đánh cắp định danh. 11](#_Toc422135936)

[1.2.2. Khai thác lỗ hổng. 14](#_Toc422135937)

[1.2.3. Khai thác lỗi vận hành. 15](#_Toc422135938)

[1.2.4. Tấn công từ chối dịch vụ 17](#_Toc422135939)

[1.2.5. Virus và các mã độc hại trên Internet 20](#_Toc422135940)

[1.2.6. Các mối đe doạ khác 22](#_Toc422135941)

[1.3. Các thuộc tính và nguyên tắc cơ bản của an toàn thông tin 26](#_Toc422135942)

[1.3.1. Các thuộc tính cơ bản 26](#_Toc422135943)

[1.3.2. Các nguyên tắc trong an toàn thông tin 27](#_Toc422135944)

[1.4. Tình hình an toàn thông tin tại Việt Nam và trên thế giới 31](#_Toc422135945)

[2. Quản lý nhà nước trong lĩnh vực an toàn thông tin 34](#_Toc422135946)

[2.1. An toàn thông tin quốc gia 34](#_Toc422135947)

[2.2. Văn bản pháp lý của một số quốc gia và Việt Nam 35](#_Toc422135948)

[2.2.1. Văn bản pháp lý của một số quốc gia 35](#_Toc422135949)

[2.2.2. Một số văn bản pháp luật về ATTT ban hành tại Việt Nam. 42](#_Toc422135950)

[2.3. Giới thiệu các cơ quan, tổ chức, đầu mối đảm bảo an toàn thông tin trong nước 46](#_Toc422135951)

[2.4. Nhận dạng tội phạm mạng và vấn đề hình sự trong an toàn thông tin. 47](#_Toc422135952)

[2.4.1. Đánh cắp định danh 47](#_Toc422135953)

[2.4.2. Rình rập, quấy rối 53](#_Toc422135954)

[2.4.3. Truy cập bất hợp pháp tới hệ thốngmáy tính và các dữ liệu nhạy cảm 56](#_Toc422135955)

[2.4.4. Lừa đảo trực tuyến 56](#_Toc422135956)

[2.4.5. Phát tán tin rác, mã độc hại 60](#_Toc422135957)

[2.5. Phân biệt hacker mũ trắng, hacker mũ đen và vấn đề đạo đức trong an toàn thông tin 60](#_Toc422135958)

[3. Hệ thốngtiêu chuẩn an toàn thông tin 63](#_Toc422135959)

[3.1. Giới thiệu hệ thốngtiêu chuẩn ISO/IEC 27000 về quản lý an toàn thông tin 63](#_Toc422135960)

[3.2. Vấn đề kiểm định và đánh giá mức độ an toàn thông tin. 68](#_Toc422135961)

[3.2.1. Khái niệm đánh giá an toàn hệ thốngthông tin 68](#_Toc422135962)

[3.2.2. Khái niệm kiểm định an toàn hệ thốngthông tin 70](#_Toc422135963)

[3.2.3. Phân biệt đánh giá và kiểm định an toàn hệ thốngthông tin 70](#_Toc422135964)

[4. Nhận biết các nguy cơ mất an toàn thông tin 72](#_Toc422135965)

[4.1. Khái niệm các hiểm họa an toàn thông tin 72](#_Toc422135966)

[4.1. Các hiểm họa điển hình gây mất an toàn thông tin 72](#_Toc422135967)

[4.2. Kỹ thuật tấn công Social engineering 76](#_Toc422135968)

[4.2.1. Tấn công lừa đảo dựa vào các kỹ thuật về con người (Human-based) 76](#_Toc422135969)

[4.2.2. Tấn công lừa đảo dựa vào các kỹ thuật máy tính (Computer-based) 79](#_Toc422135970)

[4.1. Đánh giá rủi ro internet 82](#_Toc422135971)

[4.2. Nguy cơ mất an toàn thông tin do các yếu tố vật lý 84](#_Toc422135972)

[5. Quản lý và xử lý sự cố mất an toàn thông tin 86](#_Toc422135973)

[5.1. Tổng quan về sự cố an toàn thông tin 86](#_Toc422135974)

[5.2. Sự cố an ninh là gì ? 86](#_Toc422135975)

[5.2.1. Ứng phó sự số là gì ? 86](#_Toc422135976)

[5.2.2. Phân loại sự cố 87](#_Toc422135977)

[5.2.3. Phân loại mức nghiêm trọng của sự cố 89](#_Toc422135978)

[5.3. Chính sách, kế hoạch và thủ tục xử lý sự cố an toàn thông tin 89](#_Toc422135979)

[5.3.1. Chính sách 89](#_Toc422135980)

[5.3.2. Kế hoạch 90](#_Toc422135981)

[5.3.3. Thủ tục 90](#_Toc422135982)

[5.4. Quy trình xử lý sự cố mất an toàn thông tin. 95](#_Toc422135983)

[5.4.1. Chuẩn bị 95](#_Toc422135984)

[5.4.2. Phát hiện và phân tích 98](#_Toc422135985)

[5.4.3. Ngăn chặn, Loại bỏ và Phục hồi 104](#_Toc422135986)

[5.4.4. Hoạt động sau sự cố 107](#_Toc422135987)

[5.5. Tổ chức nhóm CSIRT. 108](#_Toc422135988)

[5.5.1. Mô hình 108](#_Toc422135989)

[5.5.2. Lựa chọn mô hình phù hợp 109](#_Toc422135990)

[5.5.3. Thành viên trong đội ứng phó sự cố 112](#_Toc422135991)

[5.5.4. Sự phụ thuộc bên trong tổ chức 113](#_Toc422135992)

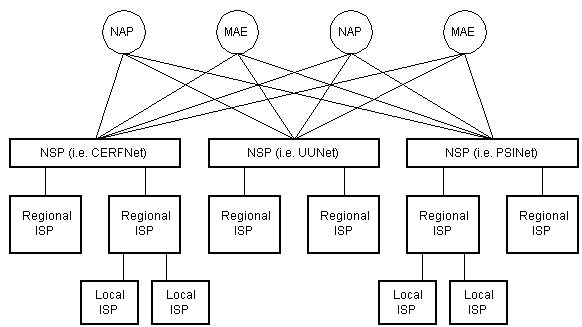
[5.5.5. Các dịch vụ của đội ứng phó sự cố 115](#_Toc422135993)

# Tổng quan và các khái niệm cơ bản

## Kiến trúc và dịch vụ của mạng Internet

### Kiến trúc mạng Internet

Mạng đường trục Internet do nhiều mạng lớn kết nối với nhau. Các mạng lớn này thuộc nhà cung cấp dịch vụ mạng **Network Service Providers (NSP)**. Một số NSP lớn có thể kể ra ở đây là UUNet, CerfNet, IBM, BBN Planet, SprintNet, PSINet… Các mạng này là ngang hàng với nhau trong việc trao đổi thông lượng gói tin. Mỗi NSP phải kết nối với 3 điểm truy cập mạng Network **Access Points (NAP)**. Tại NAP, gói tin dữ liệu nhảy từ mạng trục của NSP này sang mạng trục của NSP khác. NSP còn kết nối với mạng đô thị **Metropolitan Area Exchanges (MAE)**. MAE cũng có cùng nhiệm vụ như NSP nhưng không phải là mạng công cộng. Cả NAP và MAE đều được coi là điểm chuyển vận Internet: **Internet Exchange Points (IX)**. NSP còn bán lại băng thông cho các mạng nhỏ hơn như ISP, và các nhà cung cấp băng thông nhỏ hơn.



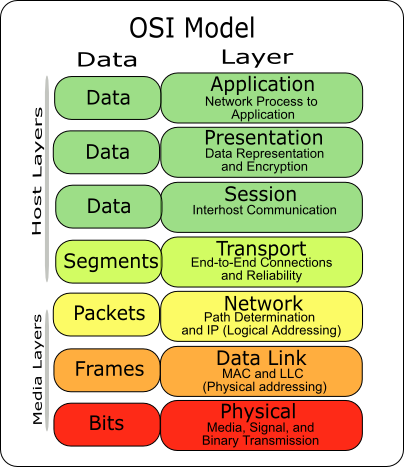
Hình 1.1: Kiến trúc phân cấp của mạng Internet

Các ISP Việt Nam cũng thuê lại kênh truyền của các NSP để kết nối tới Internet toàn cầu. Định tuyến dữ liệu truyền giữa các máy trong mạng Internet cũng theo cấu trúc phân cấp nêu trên.

### Mô hình tham chiếu OSI và bộ giao thức TCP/IP

**Mô hình tham chiếu OSI**

Để dễ hình dung hơn về cơ chế truyền tin giữa các máy tính với nhau thì tổ chức ISO và IUT-T đề ra một “Mô hình tham chiếu kết nối các hệ thống mở” OSI (Open Systems Interconnection) hay còn được gọi là “Mô hình tham chiếu 7 tầng OSI”. Mô hình OSI mô tả cách thức truyền tin từ các chương trình ứng dụng của một hệ thống máy tính đến các chương trình ứng dụng của một hệ thống khác thông qua các phương tiện truyền thông vật lý.

[](http://1.bp.blogspot.com/-dEPOLAvxsek/UzQcvDS44KI/AAAAAAAAACw/c_Fxrkuul7k/s1600/Osi-model-jb.png)

*Hình 1.2: Mô hình OSI*

Mô hình OSI bao gồm 7 tầng. Mỗi một tầng đều có đặc tính là nó chỉ sử dụng chức năng của tầng dưới nó, đồng thời chỉ cho phép tầng trên sử dụng các chức năng của mình. Mô hình OSI cho phép chia nhỏ hoạt động phức tạp của mạng thành các phần công việc đơn giản, trừu tượng, dễ hình dung hơn. Dựa vào mô hình OSI các nhà thiết kế có khả năng phát triển trên từng module chức năng, cùng với các chuẩn giao tiếp chung cung cấp khả năng “plug and play” và tích hợp nhiều nhà cung cấp sản phẩm.

Trong 7 tầng của OSI có 3 tầng dưới được thực hiện trên kênh truyền, định nghĩa cách thức thiết lập đầu cuối trên thiết bị phần cứng cho kết nối, 4 tầng trên được thực hiện trên host, phục vụ cho việc định nghĩa các chuẩn chung phát triển trên ứng dụng, giao tiếp người dùng.

Tầng 1 : Physical Layer (tầng vật lý) Điều khiển việc truyền tải các bit trên đường truyền vật lý. Tầng vật lý định nghĩa các tín hiệu điện, trạng thái đường truyền, phương pháp mã hóa dữ liệu, các loại đầu nối được sử dụng …

Tầng 2 : Data-link Layer (tầng liên kết dữ liệu ) Đảm bảo việc truyền các frame(Khung dữ liệu) giữa hai máy tính có đường truyền vật lý nối trực tiếp với nhau. Tầng liên kết dữ liệu hỗ trợ cơ chế phát hiện và xử lý lỗi dữ liệu.

Tầng 3 : Network Layer (tầng mạng ) Đảm bảo cho việc truyền packet (gói dữ liệu) giữa hai máy tính bất kỳ trong mạng máy tính (có thể có hoặc không có kết nối đường truyền vật lý trực tiếp). Hay nói cách khác, tầng mạng có nhiệm vụ tìm đường đi cho dữ liệu truyền thông giữa hai máy bất kỳ.

Tầng 4 : Transport Layer (tầng vận chuyển) Tầng vận chuyển làm nhiệm vụ phân nhỏ các gói tin có kích thước lớn khi gửi và tập hợp lại khi nhận, đảm bảo tính toàn vẹn cho dữ liệu (không lỗi,không mất, không lặp, đúng thứ tự).

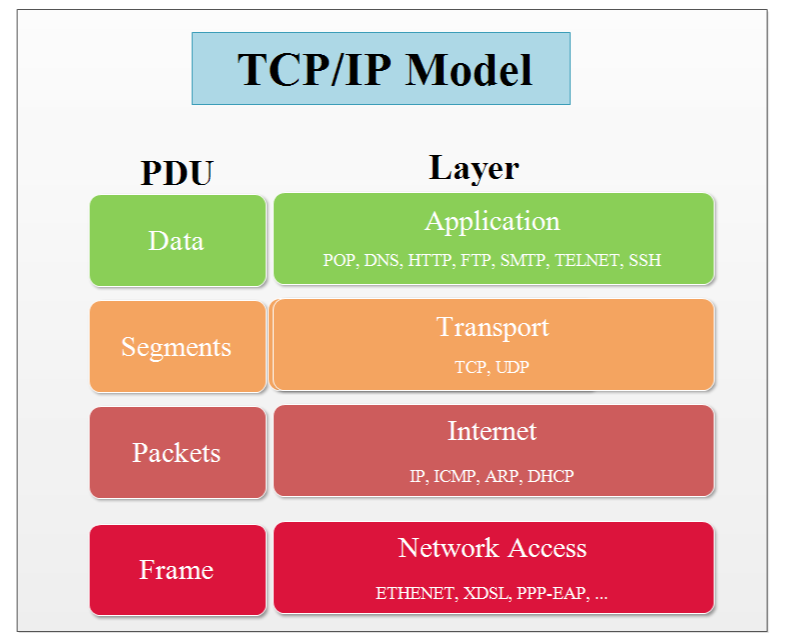
Tầng 5 : Session Layer (tầng phiên) Quản lý các phiên làm việc giữa các người sử dụng. Tầng phiên cung cấp cơ chế nhận biết tên và chức năng về bảo mật thông tin khi truyền qua mạng máy tính.

Tầng 6 : Presentation Layer (tầng trình bày) Cung cấp định dạng dữ liệu cho ứng dụng. Trong quá trình truyền dữ liệu, trên tầng trình bày bên máy gửi có nhiệm vụ dịch dữ liệu từ định dạng riêng sang định dạng chung và quá trình ngược lại trên tâng trình bày bên máy nhận. Tầng trình bày đảm bảo cho các máy tính có định dạng dữ liệu khác nhau vẫn có thể truyền thông tin với nhau bình thường.

Tầng 7 : Application Layer (tầng ứng dụng) Cung cấp các ứng dụng truy xuất đến các dịch vụ mạng như Web Browser, Mail User Agent … hoặc các chương trình làm server cung cấp các dịch vụ mạng như Web Server, FTP Server, Mail server …

**Bộ giao thức TCP/IP**

Mô hình TCP/IP là mô hình có trước so với mô hình OSI, mục đích mô hình OSI để tham chiếu làm rõ ràng cách thức trao đổi thông tin giữa các máy tính với nhau, hay nói cách khác là mô hình OSI mang tính chất dùng cho học tập nghiên cứu nhiều hơn là đưa vào triển khai thực tế. Các bạn gặp rất trường hợp dùng mô hình TCP/IP, ngay trên mạng máy tính của bạn cũng đang dùng TCP/IPv4 hoặc TCP/IPv6. Mô hình TCP/IP còn được gọi với tên khác là : mô hình DoD ( mô hình của bộ quốc phòng Mỹ)



Hình 1.3: Mô hình bộ giao thức TCP/IP

**Tầng 1 : Network Access Layer**(tầng truy cập) có thể coi tầng truy cập là một tầng riêng biệt hoặc cũng có thể tách thành 2 tầng vật lý và tầng liên kết dữ liệu như trong mô hình OSI, tầng truy cập được sử dụng để truyền gói tin từ tầng mạng đến các host trong mạng. Thành phần tầng truy cập bao gồm cả các thiết bị vật lý ( hun, switch, cáp mạng, card mạng HBA-Host Bus Adapter và các đặc tả mức thấp như tín hiệu điện.

**Tầng 2 : Internet Layer**(tầng mạng) Nhiệm vụ của tầng mạng trên mô hình TCP/IP là giải quyết vấn đề dẫn các gói tin đi qua các mạng để đến đúng đích mong muốn.

**Tầng 3 : Transport Layer**(tầng vận chuyển) cũng giống với tầng vận chuyển của mô hình OSI, tầng vận chuyển làm nhiệm vụ phân nhỏ các gói tin có kích thước lớn khi gửi và tập hợp lại khi nhận, đảm bảo tính toàn vẹn cho dữ liệu (không lỗi,không mất, không lặp, đúng thứ tự).

**Tầng 4 : Application Layer**(tầng ứng dụng) là nơi các chương trình mạng như Web Browser, Mail User Agent làm việc để liên lạc giữa các node mạng. Do mô hình TCP/IP không có tầng nào nằm giữa tầng ứng dụng và tầng vận chuyển , nên tầng ứng dụng của mô hình TCP/IP bao gồm cả các giao thức hoạt động như tầng trình diễn và phiên trong mô hình OSI. Việc này thường do người lập trình viên thực hiện.

Các giao thức tương ứng với các tầng trong bộ giao thức TCP/IP được thể hiện dưới đây:

|  |  |  |
| --- | --- | --- |
| 4 | Tầng ứng dụng | [DNS](http://vi.wikipedia.org/wiki/Domain_Name_System), [TFTP](http://vi.wikipedia.org/w/index.php?title=Trivial_File_Transfer_Protocol&action=edit), [TLS/SSL](http://vi.wikipedia.org/w/index.php?title=Transport_Layer_Security&action=edit), [FTP](http://vi.wikipedia.org/wiki/File_Transfer_Protocol), [HTTP](http://vi.wikipedia.org/w/index.php?title=HyperText_Transfer_Protocol&action=edit), [IMAP](http://vi.wikipedia.org/w/index.php?title=Internet_Message_Access_Protocol&action=edit), [IRC](http://vi.wikipedia.org/wiki/Internet_Relay_Chat), [NNTP](http://vi.wikipedia.org/w/index.php?title=Network_News_Transfer_Protocol&action=edit), [POP3](http://vi.wikipedia.org/w/index.php?title=Post_Office_Protocol&action=edit), [SIP](http://vi.wikipedia.org/w/index.php?title=Session_Initiation_Protocol&action=edit), [SMTP](http://vi.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol), [SNMP](http://vi.wikipedia.org/w/index.php?title=Simple_Network_Management_Protocol&action=edit), [SSH](http://vi.wikipedia.org/wiki/Secure_Shell), [TELNET](http://vi.wikipedia.org/wiki/Telnet), [ECHO](http://vi.wikipedia.org/w/index.php?title=ECHO_protocol&action=edit), [BitTorrent](http://vi.wikipedia.org/wiki/BitTorrent), [RTP](http://vi.wikipedia.org/w/index.php?title=Real-time_Transport_Protocol&action=edit), [PNRP](http://vi.wikipedia.org/w/index.php?title=Peer_Name_Resolution_Protocol&action=edit), [rlogin](http://vi.wikipedia.org/w/index.php?title=Rlogin&action=edit), [ENRP](http://vi.wikipedia.org/w/index.php?title=Endpoint_Handlespace_Redundancy_Protocol&action=edit), … |
| Các giao thức định tuyến như [BGP](http://vi.wikipedia.org/wiki/BGP) và [RIP](http://vi.wikipedia.org/wiki/RIP), chạy trên TCP và UDP - theo thứ tự từng cặp: BGP dùng TCP, RIP dùng UDP - còn có thể được coi là một phần của [tầng ứng dụng](http://vi.wikipedia.org/wiki/T%E1%BA%A7ng_%E1%BB%A9ng_d%E1%BB%A5ng) hoặc [tầng mạng](http://vi.wikipedia.org/wiki/T%E1%BA%A7ng_m%E1%BA%A1ng). |
| 3 | Tầng giao vận | [TCP](http://vi.wikipedia.org/wiki/Transmission_Control_Protocol), [UDP](http://vi.wikipedia.org/wiki/User_Datagram_Protocol), [DCCP](http://vi.wikipedia.org/w/index.php?title=Datagram_Congestion_Control_Protocol&action=edit), [SCTP](http://vi.wikipedia.org/w/index.php?title=Stream_Control_Transmission_Protocol&action=edit), [IL](http://vi.wikipedia.org/w/index.php?title=IL_Protocol&action=edit), [RUDP](http://vi.wikipedia.org/w/index.php?title=Reliable_User_Datagram_Protocol&action=edit), … |
| Các giao thức định tuyến như [OSPF](http://vi.wikipedia.org/w/index.php?title=OSPF&action=edit) (tuyến ngắn nhất được chọn đầu tiên), chạy trên IP, cũng có thể được coi là một phần của [tầng giao vận](http://vi.wikipedia.org/wiki/T%E1%BA%A7ng_giao_v%E1%BA%ADn), hoặc [tầng mạng](http://vi.wikipedia.org/wiki/T%E1%BA%A7ng_m%E1%BA%A1ng). [ICMP](http://vi.wikipedia.org/w/index.php?title=ICMP&action=edit) (Internet control message protocol| - tạm dịch là Giao thức điều khiển thông điệp Internet) và [IGMP](http://vi.wikipedia.org/w/index.php?title=IGMP&action=edit) (Internet group management protocol - tạm dịch là Giao thức quản lý nhóm Internet) chạy trên IP, có thể được coi là một phần của [tầng mạng](http://vi.wikipedia.org/wiki/T%E1%BA%A7ng_m%E1%BA%A1ng). |
| 2 | Tầng mạng | [IP](http://vi.wikipedia.org/w/index.php?title=Internet_Protocol&action=edit) ([IPv4](http://vi.wikipedia.org/w/index.php?title=IPv4&action=edit), [IPv6](http://vi.wikipedia.org/w/index.php?title=IPv6&action=edit)) |
| [ARP](http://vi.wikipedia.org/w/index.php?title=ARP&action=edit) (Address Resolution Protocol - Giao thức phân giải địa chỉ chuyển từ địa chỉ IP – địa chỉ MAC của cạc mạng) và [RARP](http://vi.wikipedia.org/w/index.php?title=RARP&action=edit) (Reverse Address Resolution Protocol - Giao thức phân giải ngược địa chỉ đổi từ địa chỉ MAC sang địa chỉ IP) hoạt động ở bên dưới IP và trên [tầng liên kết](http://vi.wikipedia.org/w/index.php?title=T%E1%BA%A7ng_li%C3%AAn_k%E1%BA%BFt&action=edit) (link layer). Có thể nói chúng nằm ở khoảng trung gian giữa hai tầng. |
| 1 | Tầng liên kết | [Ethernet](http://vi.wikipedia.org/w/index.php?title=Ethernet&action=edit), [Wi-Fi](http://vi.wikipedia.org/w/index.php?title=Wi-Fi&action=edit), [Token ring](http://vi.wikipedia.org/w/index.php?title=Token_ring&action=edit), [PPP](http://vi.wikipedia.org/wiki/Point-to-Point_Protocol), [SLIP](http://vi.wikipedia.org/w/index.php?title=Serial_Line_Internet_Protocol&action=edit), [FDDI](http://vi.wikipedia.org/w/index.php?title=Fiber_distributed_data_interface&action=edit), [ATM](http://vi.wikipedia.org/w/index.php?title=Asynchronous_Transfer_Mode&action=edit), [Frame Relay](http://vi.wikipedia.org/w/index.php?title=Frame_Relay&action=edit), [SMDS](http://vi.wikipedia.org/w/index.php?title=SMDS&action=edit), … |

### 1.3.4. Intranet và Extranet

Khi Internet trở nên phổ biến toàn cầu và chứng tỏ được các ưu điểm của nó (như tính mềm dẻo của kết nối và các công cụ trao đổi thông tin dễ dàng tiện lợi như Web/Email, …) thì xuất hiện ý tưởng tổ chức các mạng nội bộ của một tổ chức theo kiểu một mạng Internet nhỏ, từ đó ra đời thuật ngữ “Intranet” để chỉ các mạng như vậy. Trong quá trình phát triển của thương mại điện tử, nhất là trong các ứng dụng Doanh nghiệp-đến-Doanh nghiệp (B2B) một tổ chức có thể mở một phần mạng của mình phục vụ mục đích để các đối tác bên ngoài truy cập vào một cách thuận tiện (trong nhiều trường hợp sử dụng các giao thức và dịch vụ Internet), khi đó phần mạng đó được gọi là “Extranet”.

## Các vấn đề chung về rủi ro trên Internet

### Đánh cắp định danh.

Khái niệm **Đánh cắp định danh** trong một số luật hình sự là một loại hình tội phạm trong đó người phạm tội thu nhận được các yếu tố thông tin chính yếu của một cá nhân như là số liệu chứng minh thư, đăng ký xe, định danh số,…. nhằm mục tiêu giả danh cá nhân đó để kiếm lời.

Như vậy đánh cắp định danh trong hệ thống máy tính chỉ là một trường hợp riêng của loại hình này, liên quan đến đánh cắp định danh số. Trong phạm vi giáo trình này chúng ta không đề cập đến tính chất và mục tiêu tội phạm của vấn đề đánh cắp định danh số mà hiểu vấn đề này chỉ theo khía cạnh kỹ thuật thực hiện. Có thể có những trường hợp sử dụng các kỹ thuật lấy lén định danh số mà chưa phải là phạm tội.

**Định danh số (Digital Indentity)** là sự thể hiện của một người trong hệ thống thông tin, nó được dùng trong các tương tác giữa người và máy tính hệ thống cũng như giữa người đó với những người khác trong hệ thống. Định danh số sinh ra để làm cho các giao dịch qua hệ thống thông tin được dễ dàng và an toàn, tương tự như các giao dịch thông thường. Tuỳ theo bản chất và nhu cầu của mỗi giao dịch mà định danh số có thể phức tạp hay đơn giản. Tuy nhiên tổng quát mà nói thì định danh số bao gồm 2 phần

* Danh tính của người đó
* Các yếu tố đặc trưng của người đó (còn gọi là thuộc tính của danh tính).

Trong trường hợp phổ biến và đơn giản nhất thì định danh số bao gồm tên người dùng và một bí mật nào đó dùng để xác thực (ví dụ như mật khẩu).

Tổ chức Liberty Alliance phân loại 3 trường hợp tội phạm đánh cắp định danh.

* Sử dụng định danh ăn cắp được để mở một tài khoản mới để kiếm lợi.
* Sử dụng định danh ăn cắp được để lạm dụng tài khoản hiện có của người chủ thật.
* Ăn cắp định danh tội phạm: khi tội phạm đánh cắp định danh của 1 người khác và đưa định danh đó cho bộ phận luật pháp thay thế cho định danh của mình.

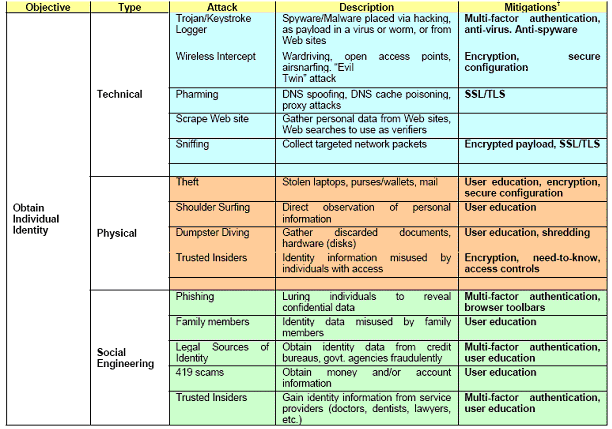
Về lý thuyết kẻ ăn cắp định danh có thể tìm cách xâm nhập vào cơ sở dữ liệu để lấy các thông tin cá nhân, tuy nhiên thông thường thì nó sử dụng các phương pháp cổ điển như lục tìm trong các giấy tờ thải trong thùng rác (Dumpster Diving) hay là nhìn trộm qua vai (Shoulder Surfing). Trong môi trường mạng Internet thì định danh số còn là mục tiêu của các kỹ thuật đánh cắp mà bản chất của nó là: hoặc xâm nhập để trộm các thông tin thuộc tính nếu nó được lưu trữ hay truyền trong mạng, hoặc là thực hiện lừa đảo để người chủ định danh số tự khai và thuộc tính đó.

Ví dụ minh hoạ: tham khảo Identity Theft Resource Center (ITRC) http://idtheftcenter.org/facts.shtml

Thống kê, chiều hướng phát triển: Đánh cắp định danh số là vấn đề lớn khi thực hiện các giao dịch điện tử trên internet. Báo cáo của tổ chức FTC (Mỹ) cho biết chỉ trong 2004 những thiệt hại của các tổ chức kinh doanh và tài chính do đánh cắp đinh doah số gây ra là 47,6 tỷ đô la Mỹ.

*Các phương pháp đánh cắp định danh:*

Các phương pháp đánh cắp định danh rất đa dạng và phong phú, nhưng có thể chia làm 3 loại: sử dụng kỹ thuật cao, hoặc đánh cắp mang tính vật lý thông thường hoặc sử dụng các biện pháp mánh khoé lừa đảo xã hội (xem bảng dưới đây)



Hình 1.4: Các loại hình đánh cắp định danh

### Khai thác lỗ hổng.

Các tấn công nhằm vào các lỗ hổng kỹ thuật của hệ thống công nghệ thông tin nhằm mục tiêu xâm nhập hay phá hoại hệ thống. Hàng năm có đến hàng ngàn các lỗ hổng mới được phát hiện trong các phần mềm và phần cứng của các Hãng được sử dụng rộng rãi trên thế giới như Microsoft, Cisco, Oracle, … Bản chất của các lỗ hổng kỹ thuật là một lỗi phần mềm của thiết bị hay ứng dụng mà tin tặc có thể lợi dụng để gây hại.

Trước kia ai tìm được lỗ hổng mới thường tự do thông báo rộng rãi cho công chúng, qua đó các tin tặc có thể viết ra các phần mềm tấn công vào lỗ hổng đó trước khi hãng sản xuất kịp làm ra các bản vá nâng cấp để bịt lỗ hổng. Sau đó, người ta đã có thoả thuận lỗ hổng tìm ra chỉ được công bố cho hãng sản xuất để họ bí mật nghiên cứu và làm ra bản vá rồi mới công bố rộng rãi. Tuy nhiên ngay cả trong trường hợp đó các lỗ hổng vẫn bị khai thác trên thực tế vì sau khi công bố lỗ hổng và bản vá thì đại đa số các máy trên internet vần cần một khoảng thời gian khá dài để áp dụng bản vá. Tấn công SQL Slammer nổi tiếng được bắt đầu thực hiện khoảng vài tháng sau khi bản vá tương ứng đã được công bố nhưng hầu hết các máy tính vẫn được vá.

Ngoài ra, có trường hợp tin tặc có khả năng thực hiện tấn công ngay trong ngày đầu tiên khi lỗ hổng được công bố, hay thậm chí chính tin tặc là người tìm ra lỗ hổng. Trường hợp này được gọi là “zero-day exploit” và đươc coi là hiểm hoạ lớn với Internet.

*Ví dụ minh hoạ:* tấn công Blaster. Blaster là tên của một sâu máy tính lan truyền trên các máy Windows vào tháng 8 năm 2003. Sâu này tạo ra một tấn công SYN flood ngày 15 tháng 8 vào cổng 80 của tên miền của Microsoft là Windowsupdate.com, bằng cách đó nó tạo ra một tấn công từ chối dịch vụ phân tán nhằm làm tê liệt trang chủ này. Microsoft không bị thiệt hại nhiều vì tấn công nhằm vào windowupdate.com chứ không đánh vào trang đã được chuyển hướng là windowsupdate.microsoft.com. Tuy nhiên Microsoft cũng đã phải tạm tắt trang chủ để ngăn chặn tác hại. Sâu Blaster phát tán là do việc lợi dụng lỗ hổng tràn bộ đệm trong dịch vụ DCOM RPC trên hệ điều hành, lỗ hổng này đã có bản vá một tháng trước đó trong các thông báo của Microsoft ngày 16 tháng 7 năm 2003. Mặc dù vậy, chính máy chủ của Microsoft cũng được vá. Ngày 29 tháng 8 người ta đã bắt được chủ nhân 18 tuổi ở Minnesote của phiên bản B của sâu Blaster và xử tù 18 tháng.

Người ta nhận thấy chiều hướng ngày càng rút ngắn thời gian từ lúc lỗ hổng được công bố cho đến lúc có tấn công được đưa ra. Ngoài ra cũng có những lỗ hổng được công bố mà hàng vẫn chưa kịp đưa ra bàn vá, đôi khi là do rò rỉ thông tin. Việc các tấn công được đưa ra hầu như cùng lúc (zero – day) với công bố lỗ hổng cùng cho thấy một khả năng có những kênh tội phạm ngầm qua đó tin tặc có thể có những thông tin nội bộ về lỗ hổng trước khi được công bố rộng rãi.

### Khai thác lỗi vận hành.

*Định nghĩa*

Một hệ thống Internet có thể không có các điểm yếu hay lỗ hổng trong các thiết bị phần cứng và phần mềm nhưng có thể bị tấn công khai thác các điểm yếu trong khi nó được vận hành.

*Phân loại*

Một trong những nguyên nhân chính gây ra nhiều lỗi vận hành là do sự tham gia và gây lỗi của con người trong quá trình vận hành. Ngoài ra, bản thân hệ thống khi vận hành cũng có thể bộc lộ các điểm yếu không được phát hiện khi nó ở trong trạng thái tĩnh.

*Ví dụ minh hoạ*

*Tấn công “lừa đảo xã hội” social-engineering:* các kĩ thuật người lừa đảo tham gia vận hành hệ thống để lấy các thông tin bí mật cần thiết. Từ này được dùng nhiều sau khi tin tặc nổi tiếng là Kelvin Mitnick chỉ ra rằng lừa một người để lấy mật khẩu của họ thì dễ hơn nhiều là tìm cách xâm nhập bẻ khóa vào hệ thống.

*Tấn công “câu cá” (phishing):* là một hình thức của lừa đảo xã hội. Tấn công này thông thường thực hiện thông qua việc gửi thư điện tử đến người dùng đề nghị họ khai báo mật khảu vì một lý do nào đó như bảo trì, nâng cấp hệ thống.

*Tấn công “lục lọi thùng rác” (dumpster diving):* khai thác lỗi vận hành hệ thống tin nếu các thông tin in trên giấy không được chú ý hủy trước khi vứt vào thùng rác. Vấn đề tương tự xảy ra khi ổ cứng máy tính được đem đi sửa hoặc bỏ đi mà không trải qua một thủ tục an ninh dữ liệu nào (ví dụ: sao lưu rồi xóa “chết” dữ liệu trong ổ cứng).

*Tấn công “lừa đảo xã hội ngược”:* tin tặc giả danh là người có trách nhiệm hoặc được ủy quyền để những người dùng hệ thống tự tìm đến để hỏi thông tin thay vì tin tặc phải tìm đến người dùng. Một trường hợp điển hình là một kiểu tấn công vào các tổ chức không có các quy tắc an toàn vận hành cần thiết khi phải thuê dịch vụ từ bên ngoài. Tin tặc đầu tiên tạo ra một vấn đề trong hệ thống mạng, sau đó thông qua quảng cáo được thuê đến sửa và trong quá trình đó tin tặc yêu cầu cung cấp một số thông tin cần thiết.

*Một số kiểu nguy cơ được nhắc đến trong các chuẩn vê an toàn thông tin như ISO 27001:*

*Không chia sẻ trách nhiệm*: trách nhiệm và quyền hạn với hệ thống cần được xem xét chia sẻ ở mức độ cần thiết để tạo ra trường hợp “người dùng quyền lực” (poweruser) có quá nhiều quyền và có thể vô tình hay có ý sử dụng quyền đó để gây hại cho hệ thống.

*Thiếu sự phân tách rành rọt giữa bộ phận phát triển, thử nghiệm và vận hành:* có thể gây rủi ro, dễ dàng bị tin tặc lợi dụng xâm nhập vào bộ phận phát triển thử nghiệm rồi qua đó xâm nhập và hệ thống vận hành thật.

*Không có sự quản lý an ninh chặt chẽ với bên cung cấp dịch vụ từ bên ngoài* (đã được nêu ở ví dụ trên).

*Quản lý và xử lý các vật mang tin an toàn: một trường hợp bị tấn công* đã được nêu ở ví dụ trên.

*Lỗi vận hành khi thông tin được luân chuyển trong hệ thống:* quá trình trao đổi thông tin và phần mềm bên trong cũng như giữa bên trong với bên ngoài hệ thống có thể tạo ra rất nhiều lỗ hổng an ninh

### Tấn công từ chối dịch vụ

DoS là tấn công thường thực hiện qua mạng vào một máy làm cho máy đó mất khả năng thực hiện dịch vụ mà nó cần phải thựchiện.

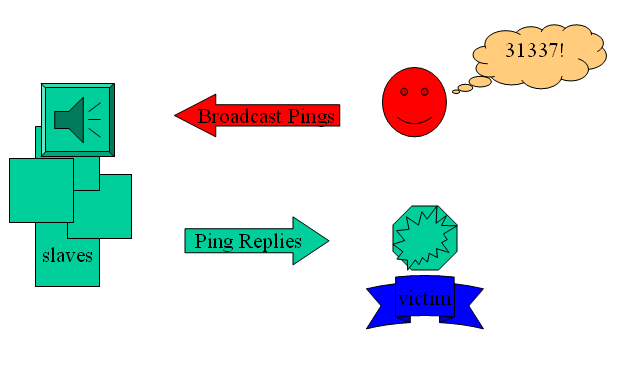
Tấn công DoS đầu tiên nhằm vào máy tính là phá hoại máy tính bằng cách dùng búa đập. Tấn công DoS ngày nay được hiểu là các tấn công qua mạng, làm hỏng một dịch vụ mạng nào đó. Tấn công DoS có thể đơn giảm là rút dây mạng ra khỏi ổ cắm. Mô hình tấn công DoS qua mạng có thể là sử dụng 1 máy tính để gửi các dữ liệu tấn công đến 1 máy khác bằng cách nào đó để máy đó không thể xử lý được và do đó ngừng cung cấp dịch vụ cần thiết mà nó đang cung cấp. Để cho có hiệu quả, tin tặc ngày nay thường sử dụng nhiều máy tính để tấn công một máy tính đích, tấn công này được gọi là tấn công từ chối dịch vụ phân tán (Distributed DoS- DDoS). Bằng các này, không hiệu quả tấn công tăng lên mà nguồn gốc tấn công cũng rất khó bị phát hiện.

Tấn công DDoS là hiểm hoạ lớn đối với Internet và TMĐT, vì về nguyên tắc, tạo ra một tấn công DDoSS là dễ dàng hơn việc xâm nhập vào hệ thống đích. Do đó, ngày nay DDoSS hay được những tin tặc xấu sử dụng để tống tiền, phá hoại kinh doanh trực tuyến của đối thủ,…

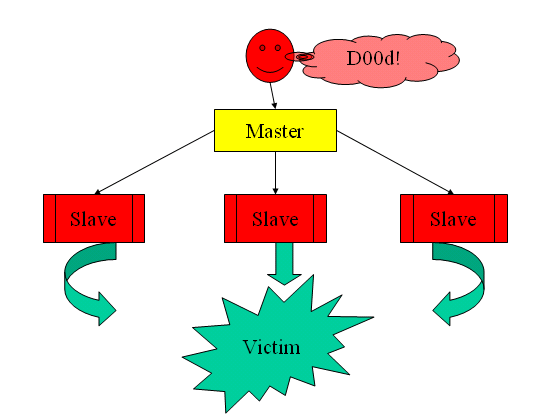
*Sự tiến triển của các loại hình tấn công DoS:*

- *Các công cụ cổ điển có từ năm 1990 – 1997:* Sử dụng một máy tính mạnh hơn để “chèn ép” máy yếu hơn ra khỏi kênh kết nối modem hay irc. Sử dụng Ping fload, SYN Flood và UDP flood.

- Tiếp theo sau đó là *tấn công Smurf* – kiểu tấn công 2 lớp đầu tiên: Máy tính của tin tặc đóng giả máy bị tấn công, lừa cho tất cả các máy khác gửi dữ liệu tràn ngập đến máy tính bị tấn công, sử dụng kỹ thuật Ping Flood.



Hình 1.4: Mô hình tấn công Smurf (2 lớp)



Hình 1.5: Tấn công 3 lớp thời nay

*Các công cụ tấn công DDoS:* Các công cụ tấn công DDoS thời nay thường áp dụng kỹ thuật tấn công 3 lớp, sử dụng 5 phương pháp cơ bản sau:

*- Smurf*: Yêu cầu Ping bằng ICMP đến địa chỉ đã bị chuyển hướng. Địa chỉ nguồn đã bị giả mạo chính là địa chỉ của máy đích bị tấn công. Những máy nhận được yêu cầu PING sẽ phải hồi và làm tràn ngập máy đích bị tấn công.

*- Tràn ngập UDP*: Gửi số lượng lớn các gói tin UDB đến hệ thống đích, làm cho các tài nguyên mạng bị thắt cổ chai.

- *Tràn ngập TCP SYN:* Gửi số lượng lớn các yêu cầu mở kết nối TCP đến đích. Hệ thống đích luôn phải xử lý các yêu cầu này do đó bị bấn.

Có 3 họ công cụ cổ điển tấn công DDoS là:

- *Trinoo:* Công cụ DDoS được công bố đầu tiên năm 1997. Máy tấn công, máy Master và Slave liên hệ với nhau thông qua giao thức UDB được mã hoá. Phương pháp tấn công là tràn ngập UDP. Chạy trên Solaris và Linux. Dễ bị phát hiện các luồng thông tin và mật khẩu.

- *TFN (Tribe Flood Network):* Từ năm 1998, máy tấn công liên lạc với Master thông qua các giao thức TCP, UDB, SSH, ICMP, Telnet mã hoá. Không cần mật khẩu để thực hiện lệnh. Các lệnh được gửi đi dưới dạng các số 16 bits. Master liên lạc với Slave bằng ICMP. Các tấn công có thể là: ICMP, SYN, UDP, Smurf chạy trên Linux và Solaris. Phiên bản mới là TFN2K có từ năm 1999 dựa trên FTN. Sử dụng các gói tin “mồ côi” (Decoy packet) và các biện pháp khác để làm cho luồng dữ liệu khó bị phát hiện và lọc. Làm giả địa chỉ nguồn thông tin. Có loại hình tấn công mới như tràn ngập các gói tin hỏng, gây ra sự tàn pháp lớn hơn mà chỉ cần ít gói tin hơn có trên UNIX và Windows NT.

- *Stachedraht:* Cũng có nhiều lựa chọn tấn công như TFNm bao gồm UDB, ICMP, TCP SYN và tràn ngập phát tán PING.

Tấn công DDoS điển hình nhất trong lịch sử vẫn là cuộc tấn công DDoS ồ ạt vào năm 2000 nhằm vào một loạt các trang Web thương mại điện tử lớn như Amazon.com, CNN.com, eBay và E-trade. Ngày 7/11/2000 các website này đã phải ngừng cung cấp dịch vụ trong vòng vài giờ do bị tràn ngập luồng dữ liệu. Các máy tính Slave được sử dụng là các máy của trường Đại học California. Các công cụ được sử dụng bao gồm Trinoo, TFN, TFN2K và Stachedraht.

### Virus và các mã độc hại trên Internet

**Virus**

Virus là các đoạn mã có khả năng tự nhân bản. Virus có thể chứa hoặc không chứa các chương trình tấn công hay các cổng hậu. Virus là đoạn mã được cài trên máy tính và chạy ngoài ý muốn của người sử dụng.

**Sâu máy tính (Worm)**

Sâu máy tính (Worm): một chương trình độc lập có khả năng tự tạo ra chính bản thân mình và lây nhiễm từ máy tính này qua máy tính khác qua mạng. Khác với virus, sâu thường không sửa đổi các chương trình khác trong máy tính.Lịch sử sâu máy tính bắt đầu bởi sâu Morris năm 1988, được viết bới sinh viên tốt nghiệp trường đại học Cornell và được thả lên mạng ARPA net (tiêu đề của mạng Internet) để thử nghiệm các hậu quả của nó trên các hệ thống UNIX. Sâu nhân bản và vượt ra khỏi tầm kiểm soát và nhiễm vào khoảng 6000 máy tính nối mạng bao gồm cả các máy chính phủ cũng như của các trường đại học. Morris bị đuổi khỏi trường đại học Cornell, bị phạt 3 năm quản thúc và 10.000 $. Sâu Morris dựa trên việc khai thác lỗ hổng được biết từ trước trong các chương trình sendmail, finger, rsh/rexec của UNIX và khai thác các mật khẩu yếu.

Sâu máy tính gây ra tác hại lớn cuối thế kỷ 20 và những năm đầu thế kỷ 21 do khả năng phát tán nhanh và rộng trên toàn cầu của nó

**Trojan và các loại mã độc hại khác**

Chương trình “con ngựa thành Troa” (Trojan horse) là một chương trình độc hại được lây nhiễm hoặc ẩn chứa bên trong một phần mềm hợp lệ. Từ này xuất phát từ câu chuyện cổ Hy Lạp tương ứng. Sau này người ta gọi rút gọn là Trojan mặc dù theo truyền thuyết thì người Hy Lạp chứ không phải người Troa tạo ra con ngựa này. Trojan không thể hoạt động độc lập, điều này khác với virus và sâu. Trojan phụ thuộc vào hành động của người dùng, ngay cả nếu Trojan có tự nhân bản hoặc thậm chí tự phân phối chính nó, mỗi một máy bị hại mới phải chạy chương trình chứa Trojan. Trojan thường phục vụ một mục tiêu thực hiện một tấn công nào khác, nó không phụ thuộc vào các lỗ hổng an ninh trong hệ thống.

Một số Trojan cổ điển bao gồm : Back Orifice, Back Orifice 2000, NetBus, Subseven, Downloader – EV, Pest Trap... Trong đó Back Orifice được một nhóm tin tặc “Cult of the Dead Cow” công bố vào năm 1998. Khi cài lên máy trạm Windows nó cho phép truy cập từ xa trái phép vào máy.

**Mã độc hại khác**

Mã độc hại bao hàm mọi loại chương trình (bao gồm cả macro và script) được lập trình chủ định để nhằm tạo ra các sự kiện không được mong đợi (thong thường là có hại) trên máy tính bị hại. Mã độc hại khác với các phần mềm lỗi, là các phần mềm có mục tiêu tốt nhưng chứa các lỗi trầm trọng có thể gây ra hại. Các loại mã độc hại khác bao gồm :

**- Spyware:** các phần mềm có mục đích thương mại tạo ra để thu thập thông tin về người sử dụng máy tính, tạo ra các cửa sổ pop-up để quảng cáo, hoặc thay đổi hành vi của web-browser với mục đích thương mại cho tác giả của spyware.

**- Botnet:** các máy tính bị nhiễm phần mềm malbot này có thể được điều khiển thông qua các kênh irc hoặc một hệ thống chat khác. Mạng botnet có đến hang ngàn máy dễ dàng được sử dụng để tấn công DDoS đến một số trang thương mại điện tử.

**- Rootkit:** Bộ công cụ phần mềm được dùng với mục đích giấu diếm các tiến trình đang chạy, các tệp hoặc dữ liệu hệ thống khỏi hệ điều hành. Rootkit có thể được sử dụng bởi các phần mềm độc hại, cho phép kẻ xâm nhập duy trì truy cập hệ thống mà không bị phát hiện. Rootkit có trong HĐH Linux, Solaris và một vài phiên bản Windows. Rootkit thường sửa lại một phần của HĐH hoặc cài đặt bản thân nó như một trình điều khiển (driver) hay một module của nhân (kernel). Từ “rootkit” xuất phát từ vụ việc nổi tiếng năm 2005 khi hãng Sony cho cài đặt Rootkit vào máy tính chạy Windows khi CD của hãng này đang chạy trên máy tính đó với mục tiêu bảo vệ bản quyền chống sao chép đĩa CD.

### Các mối đe doạ khác

**Các mối đe doạ đặc thù với kỹ thuật Mobile**

Điện thoại di động sẽ bị tấn công nhiều hơn cùng với xu hướng hội tụ công nghệ:

* Điện thoại thông minh tăng khả năng kết hợp với thiết bị khác
* có nhiều ứng dụng như của PC: IM, audio, video, web
* được tăng cường thêm nhiều loại kết nối: bluetooth, WiFi, 3G, GPRS, 2G, SMS

Nhiều loại tấn công:

* phishing SMS
* Trojan làm tốn tiền người dùng (gửi SMS tới số dịch vụ đắt tiền, hoặc tăng băng thông bằng dữ liệu thừa)
* Phần mềm gián điệp: trộm call-log, SMS gửi về máy di động khác, kích hoạt camera

**Wireless**

Việc sử dụng các giao thức mạng không dây ngày càng trở nên phổ biến trên Internet làm xuất hiện các mối nguy hiểm mới, do việc môi trường truyền dẫn mở là không trung làm cho khả năng xâm nhập trái phép của tin tặc dễ dàng hơn nhiều so với việc xâm nhập mạng có dây. Các giao thức mạng LAN không dây, các giao thức không dây dùng cho các thiết bị cầm tay,…đều có thể bị khai thác lợi dụng.

Một số các điểm yếu đặc thù của mạng không dây và các thiết bị cầm tay bao gồm:

* Trước hết, mọi điểm yếu tồn tại trong mạng có dây thông thường đều áp dụng cho mạng không dây
* Tin tặc có thể tạo được truy cập vào mạng máy tính thông qua một kết nối không dây, vượt qua mọi bảo vệ của tường lửa thông thường.
* Các thông tin nhạy cảm không mã hoá hoặc mã hoá không đủ mạnh truyền giữa 2 thiết bị không dây dễ dạng bị nghe trộm ở giữa.
* Các tấn công từ chối dịch vụ có thể nhằm vào các thiết bị hay kết nối không dây
* Tin tặc có thể phạm tính riêng tư của người dùng không dây và có thể theo dõi sự di chuyển vị trí của họ.
* Tin tặc có thể tạo các thiết bị trái phép ( như thiết bị client hay điểm truy cập giả) để thu nhập trái phép các thông tin bí mật.
* Các thiết bị cầm tay dễ dàng bị đánh cắp và dễ bị lộ các thông tin nhạy cảm trong nó.
* Một thiết bị trong mạng không dây không được cấu hình đúng sẽ dễ dàng bị truy xuất dữ liệu
* Virus và mã độc hại có thể làm hỏng dữ liệu trên các thiết bị không dây và sau đó lây nhiễm vào mạng có dây
* Tin tặc có thể thông qua các kết nối không dây để nối đến các tổ chức khác để tiếp tục tấn công hoặc che giấu các hành vi của mình
* Tin tặc có thể sử dụng các dịch vụ mạng không dây không tin cậy của một dịch vụ khác để có thể truy cập vào các tài nguyên mạng của tổ chức
* Tấn công bên trong mạng có thể dễ dàng thực hiện thông qua các kết nối không dây ngẫu nhiên

**Spam và Spam ảnh**

Spam nói chung là việc gửi thông tin “rác” – các thông tin mà người nhận không mong muốn và chờ đợi nhận). Khi Internet kết nối rộng rãi người dùng thì vấn nạn này mạng lại thiệt hại lớn cho người dùng và các bên tham gia vào Internet khác. Spam đặc biệt phổ biến dưới dạng thư điện tử (email). Để chống lại Spam người ta có thể dùng kỹ thuật lọc theo các từ khoá. Chính vì vậy mới gần đây những kẻ tạo spam đang bắt đầu chuyển sang việc sử dụng ảnh trong email để tránh bị lọc theo từ khoá.

Năm 2005: spam ảnh mới chiếm 10%, nhưng đến tháng 11/2006 spam ảnh đã chiếm tới 40% số lượng thư rác. Spam ảnh lớn dung lượng bằng 3 lần spam văn bản thông thường do đó chiếm băng thông lớn hơn nhiều so với spam bằng văn bản thông thường. Nội dung thường gặp là rao bán, quảng cáo: Cổ phiếu rẻ, Thuốc, Bằng cấp,…

**P2P**

Mạng P2P (Peer to Peer) là tập hợp các máy tính ( còn gọi là các nút – node) đồng thời vừa là các máy khách vừa là máy chủ thực hiện một dịch vụ chung nào đó. Các nút có thể trao đổi dữ liệu, chia sẻ tài nguyên, cung cấp dịch vụ thư mục, hỗ trợ thông tin và cũng cung cấp công cụ hợp tác thời gian thực.

Mạng P2P có những kiến trúc thông tin và điều khiển khác nhau. Một số máy chủ cung cấp dịch vụ đánh chỉ số tập trung (index) có thể cung cấp các dịch vụ thư mục cho dữ liệu và dịch vụ. Trong mạng số hoá và thư mục này, hoàn toàn bình đẳng với các nút khác. Trong các kiến trúc lai ghép thì hai kiểu tổ chức như trên kết hợp với nhau theo các mức độ khác nhau và một nhóm các nút có thể bầu ra một số các nút lên làm máy chủ chỉ số và dịch vụ khu vực.

Có nhiều ứng dụng chính thống cũng sử dụng P2P,. Các hãng phần mềm công cụ như Microsoft hay Sun cũng cung cấp các công cụ và khuyến khích lập trình các ứng dụng P2P. Tuy nhiên, các ứng dụng P2P có thể bị sử dụng sai mục đích hoặc bị khai thác để chia sẻ bất hợp pháp các tài liệu có bản quyền, thu thập các thông tin bí mật, phân phối các mã độc hại, các thông tin xấu, sử dụng làm kênh diều khiển mạng botnet,…

Đa số các chương trình P2P sử dụng một tập các cổng định trước, nhưng nó có thể tự động hoặc làm tay lựa chọn các cổng khác nhau nếu cần thiết để lọt qua sự phát hiện, tường lửa hay các bộ lọc khác. Xu hướng hiện nay là tăng cường sử dụng các vỏ bọc (Wrapper) http và dùng mã hoá để qua mặt các ngăn chặn của tổ chức

**MPEG:**

Phim trực tuyến ngày càng phổ biến, trở thành mục tiêu hấp dẫn cho hacker

Người dùng thường ít đề phòng khi mở phim trực tuyến như file đính kèm

Định dạng phim dễ sử dụng, redirect khi xem phim, là công cụ tuyệt vời để gài phần mềm nguy hiểm

VD: sâu W32/Realor nằm trong file MPEG, tự động bật trang web nguy hiểm không cần người dùng kích hoạt.

Trang web nguy hiểm có thể chứa phần mềm ăn cắp mật khẩu hoặc cài chương trình bot vào máy người dùng.

**VoIP**

Các hình thức thoại qua giao thức IP dẫn đến các nguy cơ mới. Các cuộc gọi thoại trở thành mục tiêu của Spam. Tin tặc có thể áp dụng kỹ thuật tấn công từ chối dịch vụ đối với các hệ thống thoại, địa chỉ IP của điện thoại có thể bị đánh cắp để thực hiện các cuộc gọi mà người chủ điện thoại phải trả tiền, các kỹ thuật IP có thể sử dụng để nghe lén và bắt các cuộc gọi IP.

Chưa có các cuộc tấn công thoại IP nào lớn gây tiếng vang rộng rãi trên thế giới, nhưng việc sử dụng thoại IP ngày càng trở lên rộng rãi sẽ không tránh khỏi những rủi ro và các tấn công vào thoại IP sẽ ngày càng nhiều với quy mô lớn hơn nữa.

Hiện nay các hệ thống VoIP thường sử dụng các giao thức riêng, nhưng ngày càng tăng chuẩn hoá sử dụng giao thức SIP ( Session Initiation Protocol). Sự chuẩn hoá này sẽ dẫn đến các tấn công có thể gia tăng. Ngoài ra, hiện nay có thể tải miễn phí phần mềm tổng đài IP PBX ( Private Branch Exchange) của công ty Asterisk. Phần mềm miễn phí càng làm cho công nghệ VoIP dễ dàng được các tin tặc tiếp cận và thử nghiệm SIP để phát triển các tấn công hiệu quả hơn.

Mạng truyền gói tin bao gồm nhiều thành phần như các địa chỉ IP và MAC của các thiết bị thoại, địa chỉ của các bộ định tuyến và tường lửa, các phần mềm VoIP như phần mềm xử lý cuộc gọi, các phần mềm định tuyến cuộc gọi. Nhiều các thông số mạng này được thiết lập động mỗi khi các thành phần mạng khởi động lại, hoặc khi điện thoại VoIP khởi động lại hoặc mới được thêm vào mạng. Vì có nhiều vị trí trong mạng có các thông số động như vâyn, tin tặc có nhiều sự lựa chọn các điểm yếu tiềm năng để tấn công mạng VoIP.

## Các thuộc tính và nguyên tắc cơ bản của an toàn thông tin

### Các thuộc tính cơ bản

An toàn thông tin yêu cầu nhằm đảm bảo 3 đặc điểm quan trọng nhất của thông tin, đó là: tính bí mật, tính toàn vẹn và tính sẵn sàng. Các đặc điểm này bao trùm toàn bộ phạm trù an toàn các hệ thông thông tin. Các đặc điểm này cũng đúng với mọi tổ chức, không lệ thuộc vào việc chúng chia sẻ thông tin như thế nào.

**Tính bí mật**

Tính bí mật là tâm điểm chính của mọi giải pháp an toàn cho một sản phẩm/hệ thống CNTT. Một giải pháp an toàn là tập hợp các quy tắc xác định quyền được truy cập đến với thông tin đang tìm kiếm, đối với một số lượng người sử dụng thông tin nhất định và một số lượng thông tin là tài sản nhất định. Trong trường hợp kiểm soát truy cập cục bộ, nhóm người truy cập sẽ được kiểm soát xem là họ đã truy cập những số liệu nào. Tính bí mật là sự đảm bảo rằng các chức năng kiểm soát truy cập có hiệu lực. Đảm bảo tính bí mật là nhằm loại bỏ những sự truy cập không đựợc phép vào các khu vực là độc quyền của các cá nhân, tổ chức.

**Tính toàn vẹn**

Tính toàn vẹn, không bị sửa đổi là đặc tính phức hợp nhất và dễ bị hiểu lầm của thông tin. Một định nghĩa khái quát hơn được sử dung ở trong tài liệu này là vấn đề cấp độ là chất lượng của số liệu (thông tin), chứ không phải là con người được/ hoặc không được phép truy cập. Đặc tính toàn vẹn được hiểu là chất lượng của thông tin được xác định căn cứ vào độ xác thực khi phản ánh thực tế. Số liệu càng gần với thực tế bao nhiêu thì chất lượng thông tin càng chuẩn bấy nhiêu.

Để đảm bảo tính toàn vẹn của thông tin là môt loạt các các biện pháp đồng bộ nhằm hỗ trợ và đảm bảo tính thời sự kịp thời và sự đầy đủ trọn vẹn, cũng như sự bảo mật hợp lý cho thông tin.

**Tính sẵn sàng**

Tính sẵn sàng của thông tin cũng là một đặc tính quan trọng, không khác gì các đặc tính đã đề cập đến ở. Đó là khía cạnh sống còn của an toàn thông tin, đảm bảo cho thông tin đến đúng địa chỉ (người được phép sử dụng) khi có nhu cầu, hoặc được yêu cầu.

Tính sẵn sàng đảm bảo độ ổn định đáng tin cậy của thông tin, cũng như đảm nhiệm chức năng là thước đo, xác định phạm vi tới hạn của an toàn một hệ thống thông tin.

### Các nguyên tắc trong an toàn thông tin

ATTT các hệ thống dựa trên các đòi hỏi của pháp luật hiện hành, các tiêu chuẩn, các tài liệu phương pháp chuẩn, được bảo đảm bằng tổ hợp các thiết bị kỹ thuật – chương trình và các biện pháp tổ chức trợ giúp chúng ở tất cả các giai đoạn công nghệ của xử lý TT và trong tất cả các chế độ hoạt động của các thiết bị kể cả khi sửa chữa và niêm cất.

Các thiết bị kỹ thuật – chương trình của bảo vệ không được gây ảnh hưởng xấu tới các đặc trưng hoạt động cơ bản của hệ thống (độ tin cậy, tính linh hoạt, khả năng thay đổi cấu hình…). Một trong những phần không thể bỏ qua của công việc về ATTT là việc đánh giá hiệu quả của các thiết bị bảo vệ, được tiến hành theo phương pháp có tính tới toàn bộ các đặc trưng kỹ thuật của đối tượng được đánh giá kể cả các giải pháp kỹ thuật và sự thực hiện trên thực tế các thiết bị bảo vệ. Việc bảo vệ hệ thống phải đi kèm sự kiểm soát hiệu quả các thiết bị bảo vệ được đề xuất định kỳ bởi người dùng hoặc bởi cơ quan kiểm tra.

Những đòi hỏi nêu trên có thể thực hiện nhờ 7 nguyên tắc sau đây:

1. Nguyên tắc tính hệ thống.

Tiếp cận hệ thống trong ATTT coi rằng: cần phải kiểm kê tất cả các yếu tố, các điều kiện và các nhân tố có quan hệ với nhau, có tương tác với nhau và có biến đổi theo thời gian:

* + Trong tất cả các dạng hoạt động TT và thể hiện TT.
  + Với tất cả các thành tố của HT.
  + Trong tất cả các chế độ hoạt động.
  + Ở tất cả các giai đoạn của chu kỳ sống.
  + Trong sự tương tác của đối tượng bảo vệ với môi trường bên ngoài.

Khi thực hiện ATTT hệ thống cần phải tính tới tất cả các chỗ xung yếu, các vị trí dễ tổn thương của hệ thống xử lý TT, và cả đặc trưng, các đối tượng tiềm năng, các hướng của các tấn công và hệ thống từ phía những kẻ phá hoại (đặc biệt kẻ ác ý có trình độ chuyên môn cao), các con đường xâm nhập vào các hệ thống phân tán và các kênh tiếp cận trái phép (TCTP) tới thông tin. Hệ thống bảo vệ phải được thiết lập với việc tính tới không chỉ tất cả các kênh xâm nhập đã biết, mà còn cả khả năng xuất hiện các kênh hoàn toàn mới của các nguy cơ an toàn.

* + 1. Nguyên tắc tổng thể.

Trong tay các chuyên gia an toàn máy tính có rất nhiều biện pháp, phương pháp và thiết bị bảo vệ hệ thống máy tính. Các thiết bị tính toán hiện đại, các hệ điều hành, các thiết bị chương trình ứng dụng và chỉ dẫn đều có cài đặt các yếu tố bảo vệ khác nhau. Sử dụng tổng thể đồng bộ các yếu tố này yêu cầu sự tương thích đồng bộ của các thiết bị khác loại khi xây dựng hệ thống toàn vẹn để bịt kín tất cả các kênh xâm nhập của các hiểm hoạ và không chứa các vị trí xung yếu ở nơi tiếp giáp của các thành tố của hệ.

* + - 1. Nguyên tắc bảo vệ liên tục.

Bảo vệ TT - đó không phải là biện pháp một vài lần và thậm chí đó không phải là tập hợp cụ thể của các biện pháp đã thực hiện và các thiết bị đã cài đặt, mà đó là một quá trình liên tục hướng tới mục tiêu, yêu cầu phải đưa ra các giải pháp phù hợp ở tất cả các giai đoạn của chu kỳ sống của hệ thống (bắt đầu ngay từ lúc thiết kế chứ không phải chỉ trong khi khai thác hệ thống). Thiết kế hệ thống bảo vệ phải được tiến hành song song với thiết lập chính hệ thống được bảo vệ.

Phần lớn các thiết bị bảo vệ kỹ thuật và vật lý cần có sự trợ giúp thường xuyên của các biện pháp tổ chức (hành chính) để thực hiện có hiệu quả các chức năng của chúng. (Ví dụ như sự thay đổi kịp thời bảo quản chặt chẽ và ứng dụng linh hoạt các tên, mật khẩu, các khoá mã, sự phân quyền v.v…). Sự gián đoạn (hoặc ngừng tạm thời) trong công việc của các thiết bị bảo vệ có thể bị bọn ác ý lợi dụng để phân tích các phương pháp và các thiết bị được áp dụng để chúng đưa vào các chương trình đặc biệt, các thiết bị cài bẫy và các phương tiện khác để qua mặt hệ thống bảo vệ khi hệ thống làm việc trở lại.

* + - 1. Nguyên tắc đầy đủ hợp lý.

Thiết lập một hệ bảo vệ tuyệt đối không chọc thủng được là một điều không tưởng vì rằng với đầy đủ điều kiện và phương tiện có thể vượt qua mọi hệ bảo vệ bất kỳ. Ví dụ, các phương tiện bảo vệ mật mã trong phần lớn các trường hợp không bảo đảm độ bền vững tuyệt đối, mà chúng chỉ bảo đảm sự bí mật TT trong điều kiện bị tấn công mã thám liên tục bằng các máy tính hiện đại, trong một khoảng thời gian phù hợp với yêu cầu bảo vệ mà thôi. Do đó cần nói về một độ bảo vệ vừa đủ nào đó. Một HT bảo vệ hiệu quả có giá khá đắt. Nó sử dụng công suất đáng kể của máy tính và các tài nguyên đi kèm và do đó nó có thể gây thêm cho người dùng hệ thống một sự bất tiện và rắc rối đáng kể. Điều quan trọng là phải lựa chọn đúng mức độ bảo vệ cần thiết, mà trong đó các chi phí, độ mạo hiểm và phạm vi các thiệt hại có thể là chấp nhận được (Bài toán phân tích độ mạo hiểm).

* + - 1. Nguyên tắc mềm dẻo hệ thống.

Thông thường phải thiết lập hệ bảo vệ trong các điều kiện bất định khá lớn. Cho nên các biện pháp thực hiện và các thiết bị lắp đặt cho bảo vệ, nhất là ở giai đoạn đầu đi vào hoạt động, có thể bảo đảm hoặc là một độ bảo vệ quá mức hoặc là quá thấp. Do vậy để có thể điều chỉnh độ bảo vệ, các thiết bị như vậy phải có sự mềm dẻo nhất định. Đặc biệt quan trọng điều này, khi mà hệ bảo vệ được đưa vào một HT đang làm việc mà không được phép phá vỡ quá trình hoạt động bình thường của nó. Ngoài ra, điều kiện bên ngoài, các yêu cầu bảo vệ theo thời gian cũng có thay đổi. Trong những tình huống như vậy, tính chất mềm dẻo HT bảo vệ sẽ giúp cho việc nâng cấp HT dễ dàng mà không phải thay thế mới toàn bộ máy móc thiết bị của HT.

* + - 1. Nguyên tắc công khai của thuật toán và cơ chế bảo vệ.

Bản chất của nguyên tắc này là ở chỗ, sự bảo vệ không được chỉ dựa vào bị mật cơ cấu tổ chức và các thuật toán hoạt động của các tiểu hệ (bộ phận). Dù có biết thuật toán làm việc của HT bảo vệ thì cũng không thể qua mặt được nó (thậm chí cả tác giả của HT bảo vệ cũng vậy).

* + - 1. Nguyên tắc đơn giản trong sử dụng.

Các cơ chế bảo vệ phải dễ hiểu và đơn giản trong sử dụng. Việc áp dụng các thiết bị bảo vệ không được buộc phải biết các ngôn ngữ đặc biệt hoặc buộc phải thực hiện các động tác đòi hỏi lao động khó khăn đối với người dùng hợp pháp, kể cả việc thực hiện các thao tác khó hiểu rắc rối.

## Tình hình an toàn thông tin tại Việt Nam và trên thế giới

**Tình hình an toàn thông tin tại Việt Nam**

Tình trạng vi phạm an toàn thông tin tại Việt Nam ngày một nghiêm trọng. Việt Nam đang là nước bị tin tặc lộng hành khá phổ biến tuy lĩnh vực Internet của Việt Nam chưa được xem là phát triển cao trong khu vực. Có rất nhiều các Website quan trọng liên quan đến tài chính, chứng khoán mặc dù đã được các tổ chức về an toàn cảnh báo nhiều lần nhưng tình trạng an toàn vẫn không được cải thiện. Thực tế đó phản ánh sự lơ là trong công tác an toàn thông tin, gián tiếp gây thiệt hại lớn về kinh tế: hệ thống máy tính bị đánh cắp, dữ liệu bị đánh cắp, gây thiệt hại cho doanh nghiệp và khách hàng. Chuyện mua bán trên mạng bằng thẻ tín dụng đánh cắp, thẻ tín dụng giả đã không còn là chuyện hiếm từ vài năm trở lại đây. Tình hình an toàn mạng thông tin Việt Nam hiện nay còn rất nhiều thách thức, đặc biệt là nguồn nhân lực có trình độ còn thiếu trầm trọng, và sự đầu tư cho lĩnh vực này mới chỉ nhỏ giọt, ít được sự quan tâm và chưa đúng tầm. Về môi trường pháp lý, sự chưa hoàn thiện và thiếu đồng bộ dẫn tới tình trạng không có chế tài đủ mạnh để răn đe các Hacker có hành vi phát tán Virus trên diện rộng và tấn công vào những hệ thống máy tính doanh nghiệp để trục lợi. Trong khi đó, khả năng công nghệ bị đánh giá là thiếu và yếu. Một hạ tầng mạng không đủ mạnh sẽ không thể đương đầu với những thách thức và đe dọa an toàn có mức độ tinh vi và chuyên nghiệp ngày càng cao. Bên cạnh đó, mức đầu tư cho công nghệ thông tin tại Việt Nam vẫn còn ở mức thấp. Trung bình các nước trên thế giới có mức đầu tư cho công nghệ là 8-10%. Còn tại Việt Nam, con số này thấp hơn nhiều. Do mức đầu tư hạn hẹp nên rất ít doanh nghiệp, tổ chức có một bộ phận IT riêng, chủ yếu những công việc này chỉ do một số ít người kiêm nhiệm. Từ đó dẫn tới tình trạng an ninh, an toàn thông tin lỏng lẻo, có nhiều kẽ hở để kẻ xấu lợi dụng. Các vụ tấn công hiện nay được tổ chức bài bản hơn, quy mô hơn, kín đáo hơn và mức độ thiệt hại cũng lớn hơn. Hiện nay tại Việt nam có một số các tổ chức chịu trách nhiệm xử lí sự cố an toàn thông tin như: Trung tâm ứng cứu khẩn cấp máy tính Việt Nam VNCERT (Vietnam Computer Emergency Response Team – VNCERT), Hiệp hội an toàn thông tin Việt Nam VNISA (Vietnam Information Security Association), cơ quan E15- Bộ công an…. Nhiệm vụ chính của các tổ chức trên là hướng dẫn cho tổ chức và cá nhân triển khai biện pháp an toàn thông tin, đồng thời đưa ra những cảnh báo về các mối đe dọa an toàn thông tin trong nước cũng như trên thế giới. Ngoài ra còn có một số công ty như Misoft chuyên cung cấp dịch vụ tư vấn, đào tạo về an toàn thông tin, phân phối sản phẩm (phần cứng và phần mềm) an ninh mạng, triển khai và bảo trợ, hỗ trợ kỹ thuật các hệ thống an toàn an ninh mạng. Nhiệm vụ chính của của các Công ty kinh doanh sản phẩm an toàn mạng là mang đến cho khách hàng các dịch vụ và giải pháp an toàn an ninh hệ thống thông tin tốt nhất nhằm luôn đảm bảo tính bí mật, tính toàn vẹn, tính sẵn sàng của hệ thống thông tin, phục vụ hiệu quả công việc sản xuất, kinh

**Tình hình an toàn thông tin trên Thế Giới**

Cùng với sự phát triển nhanh chóng của mạng thông tin các phương thức tấn công mạng ngày càng trở nên tinh vi và nguy hiểm. Hiện nay một số điểm mới trong các mối đe dọa càng trở nên khó tưởng tượng: các sự kiện và tấn công có mưu kế, thay đổi đáng kể trong các bối cảnh đe dọa, các vụ bắt giữ phạm tội có tổ chức, các phương pháp thông minh phù hợp với các thiết bị mới thông minh. Một số các thay đổi đáng kể là có liên quan đến mạng máy tính ma (botnets) và các mối đe dọa đối với bản tin và thiết bị di động. Xét trên phạm vi chung thì gần đây spam và các mạng máy tính ma giảm đi đáng kể do chúng hoạt động offline, tuy nhiên các khảo sát cho thấy phần nhiều chúng đang chuẩn bị tiếp tục phát triển theo các cách khác. Android đã trở thành nền tảng mục tiêu thứ ba trong di động xét trên các khía cạnh lịch sử. Các mối đe dọa phần mềm độc hại đối với nền tảng di động vẫn tiếp tục phát triển trên cả về tri thức lẫn tính năng với tốc độ có thể che lấp cả các phần mềm độc hại trong thế giới PC. Cuộc chiến chống mạng tội phạm vẫn tiếp tục, trong khia các tấn công đang trong chu kì thay đổi. Các hoạt động tội phạm hiện nay tiếp tục tập trung vào các bối cảnh công nghệ và an toàn thông tin. Đầu năm 2011 , phần mềm độc hại xuất hiện nhiều nhất trong lịch sử. Các phần mềm chống vius giả tăng lên và Trojan đánh cắp mật khẩu vẫn thể hiện mức độ hoạt động ổn định. Đồng thời, phần mềm độc hại Autorun và Koobface, đang được phổ biến toàn cầu, và nằm trong Top 5 trong xu hướng các đe dọa. Các con số thống kê hàng ngày cho thấy 49% các tấn công là các website phần mềm độc hại. Các số liệu dưới đây cho thấy xu hướng của các đối tượng viết phần mềm độc hại, lừa đảo, mạng tội phạm, đang tiếp tục sử dụng các sự kiện hàng ngày, tin, thể thao, và các sự kiện lễ hội như mồi nhử cho các kế hoạch của chúng. Xu hướng tấn công triển khai từ phía khách hàng tiếp tục giảm và trang đầu cho các tấn công dùng SQL thay đổi liên tục. Các xu hướng mới gần đây là sự tăng nhanh các website lừa đảo và các website phần mềm mã độc nói

# Quản lý nhà nước trong lĩnh vực an toàn thông tin

## An toàn thông tin quốc gia

An toàn thông tin quốc gia được hiểu là trạng thái được bảo vệ của các quyền lợi dân tộc của nhà nước ta trong lĩnh vực thông tin. Đó là tập hợp cân bằng và hài hoà các quyền lợi của cá nhân, của xã hội và của Nhà nước về thông tin.

* Quyền lợi của các cá nhân trong lĩnh vực thông tin: Đó là sự thực hiện các quyền con người và quyền công dân (được ghi trong hiến pháp) trong tiếp cận các thông tin, trong sử dụng thông tin với mục đích tiến hành các hoạt động không bị cấm bởi pháp luật, vì sự phát triển thể chất, tâm hồn và trí tuệ của cá nhân, cũng như trong việc bảo vệ các thông tin liên quan tới an toàn bản thân.
* Quyền lợi xã hội trong lĩnh vực thông tin: Đó chính là việc đảm bảo các quyền lợi của cá nhân nêu trên; củng cố nền dân chủ XHCN; xây dựng nhà nước pháp quyền của dân, do dân, vì dân; đạt được và duy trì sự ổn định chính trị – xã hội; phát huy bản sắc dân tộc đi đôi với đổi mới đất nước về mặt văn hoá, tinh thần; tăng cường sự lãnh đạo của Đảng CSVN, đẩy mạnh CNH – HĐH; hướng tới một Việt Nam dân giàu nước mạnh, xã hội công bằng, dân chủ, văn minh.
* Quyền lợi của nhà nước trong lĩnh vực thông tin: Đó là xây dung các điều kiện để phát triển hài hoà hạ tầng cơ sở TT của đất nước; thực hiện các quyền hiến pháp về tự do con người và cá nhân trong việc thu nhận thông tin và sử dụng chúng với mục đích bảo đảm tính liên tục của thể chế XHCN, toàn quyền và chủ quyền lãnh thổ của nước ta; bảo đảm sự ổn định chính trị, kinh tế và xã hội; phát triển sự hợp tác quốc tế bình đẳng và cùng có lợi.

Trên cơ sở quyền lợi dân tộc của Việt Nam trong lĩnh vực thông tin, sẽ hình thành các nhiệm vụ chiến lược và nhiệm vụ trước mắt của chính sách (đối nội và đối ngoại) của Nhà nước trong lĩnh vực bảo đảm ATTT.

Từ góc độ bảo đảm ATTT, trong các quyền lợi dân tộc về TT có thể chia ra 4 thành phần cơ bản như sau:

* Một là, tuân thủ các quyền hiến pháp về tự do con người và công dân trong lĩnh vực thu nhận thông tin và sử dụng thông tin; bảo đảm sự nghiệp đổi mới, CNH – HĐH đất nước; gìn giữ và củng cố các giá trị đạo đức của xã hội, bản sắc văn hoá dân tộc, các tiềm lực văn hoá và khoa học của đất nước.
* Hai là, bảo đảm TT về các chủ trương, đường lối, chính sách của Đảng và Nhà nước Việt Nam. Điều này liên quan tới việc cung cấp cho dư luận xã hội nước ta và dư luận quốc tế các TT chính xác về các chủ trương, đường lối, chính sách của Đảng và Nhà nước Việt Nam; quan điểm chính thức của Đảng, Nhà nước về các sự kiện có ý nghĩa xã hội quan trọng của Việt Nam và thế giới; liên quan tới việc bảo đảm sự tiếp cận của các công dân tới các nguồn TT quốc gia công khai.
* Ba là, phát triển các công nghệ thông tin (CNTT) hiện đại; phát triển nên CNTT trong nước, trong đó có công nghiệp sản xuất các thiết bị tin học hoá, các thiết bị liên lạc viễn thông; bảo đảm các sản phẩm này cho thị trường trong nước và xuất khẩu, cũng như bảo đảm cho việc tích trữ, bảo vệ và sử dụng có hiệu quả các tài nguyên TT trong nước. Ngày nay, chỉ có trên cơ sở như vậy mới giải quyết được vấn đề xây dựng công nghệ cao, tái trang bị nền sản xuất công nghiệp, phát huy hiệu quả các thành tựu khoa học công nghệ trong nước. Việt Nam cần phải có vị trí xứng đáng trong khu vực và trên thế giới về CNTT và công nghiệp vi điện tử.
* Bốn là, bảo vệ các tài nguyên TT khỏi các tiếp cận trái phép; bảo đảm an toàn cho các hệ thống TT và các hệ thống liên lạc - viễn thông đã được triển khai cũng như đang được thiết lập trên lãnh thổ nước ta.

## Văn bản pháp lý của một số quốc gia và Việt Nam

### Văn bản pháp lý của một số quốc gia

Luật về gian lận và lạm dụng máy tính (Computer Fraud and Abuse Act).

Đây là luật gốc liên bang, Điều 18 Hiến pháp Hoa kỳ, mục 1030, đưa vào năm 1984, từ đó được bổ sung vài lần. (Luật này nghiêm cấm xâm nhập, làm hỏng và truy nhập trái phép). (Để vắn tắt ta viết như sau: 18 U.S.C.Đ 1030, 1984, CFAA).

* + Cố gắng định vị tội phạm máy tính trong một đạo luật hoàn chỉnh.
  + Luật này đưa ra khái niệm “máy tính được bảo hộ” có định nghĩa là một máy tính:

“(A) chỉ dùng riêng cho cơ quan tài chính hoặc Chính phủ Mỹ, hoặc, trong trường hợp nó không được dành riêng cho sử dụng như vậy, được dùng bởi hoặc cho cơ quan tài chính hoặc Chính phủ Mỹ và trong việc xem xét các tác động vi phạm hiến pháp được dùng bởi hoặc cho cơ quan tài chính hoặc Chính phủ Mỹ;

hoặc

(B) dược sử dụng trong thương mại hoặc liên lạc toàn Liên bang hoặc ngoại thương, kể cả máy tính để ở ngoài nước Mỹ mà được sử dụng theo cách ảnh hưởng đến thương mại hoặc liên lạc toàn Liên bang hoặc liên lạc của nước Mỹ”.

* Bao gồm 7 loại hành vi bị cấm:
  1. Truy nhập trái phép tới máy tính đang chứa các dữ liệu về quốc phòng, quan hệ quốc tế hoặc các dữ liệu hạn chế của Chính phủ liên bang.
  2. Truy nhập trái phép tới máy tính chứa các thông tin nhất định về tài chính và ngân hàng.
  3. Truy nhập trái phép, sử dụng, xuyên tạc (thay đổi), thay đổi cấu trúc, hoặc làm lộ về máy tính hoặc thông tin trong máy tính làm việc nhân danh và vì lợi ích của Chính phủ Mỹ.
  4. Sự truy nhập không có cho phép một “máy tính được bảo hộ”, mà toà án hiện đang chỉ định đối với bất kỳ máy tính nào đó được kết nối với Internet.
  5. Các gian lận máy tính.
  6. Lan truyền các mã gây hại các hệ thống máy tính hoặc các mạng.
  7. Buôn bán các mật khẩu máy tính.
     + Các hình phạt bao gồm từ 5.000 đến 100.000 USD, hoặc hai lần giá trị thu được bởi hành vi phạm pháp, đôi khi còn cao hơn, hoặc phạt tù từ 1 năm đến 20 năm, hoặc cả hai.

Luật bảo vệ các liên lạc điện tử (Electronic Communications Privacy Act – ECPA).

18 U.S.C.Đ2510 – 2221, 1986, ECPA. (Luật này nghiêm cấm các can thiệp bất hợp pháp và sự tiết lộ các liên lạc điện tử được truyền tải hoặc lưu cất trong các mạng).

* + - * + Bổ xung mở rộng các điều luật liên bang về chống nghe trộm các liên lạc “miệng” và “giấy” bằng các truyền tải thông thường.

Mở rộng sự bảo vệ tới “các liên lạc điện tử” – Khái niệm quan trọng này được định nghĩa như là “bất kỳ sự truyền tải nào của các ký hiệu, các tín hiệu, chữ viết, hình ảnh, âm thanh, dữ liệu, hoặc kiến thức của bất kỳ ai khác được truyền toàn bộ hoặc từng phần bằng hệ thống vô tuyến, hữu tuyến, điện tử, điện quang hay quang học, mà tác động tới thương mại toàn liên bang hoặc ngoại thương”, - loại trừ “các liên lạc giấy và miệng”, “sự ghi nhận chỉ âm sắc”, “thiết bị ghi dấu vết”, và “thông tin chuyển tiền điện tử” được lưu giữ và được bảo vệ bằng luật khác.

Bảo vệ chống can thiệp trong khi truyền tải.

Đưa ra các hình phạt và các quyền bảo vệ chống các hành vi làm hại, các bồi thường thoả đáng, các phí thuê luật sư và các giá cả theo kiện.

Định ra các thủ tục cho truy nhập hợp pháp của các cơ quan thực thi pháp luật. Về vấn đề này có mấy lưu ý quan trọng. Thứ nhất, các nhân viên thực thi pháp luật luôn luôn được cho phép lấy lệnh của Toà án để truy nhập vào các liên lạc hoặc các bản ghi của chúng. Một bổ xung vào luật này yêu cầu các nhà cung cấp dịch vụ Internet (ISP) cài đặt thiết bị cần thiết cho phép các cuộc nghe ngầm theo lệnh của Toà án. Thứ hai, luật này cho phép các nhà ISP đọc nội dung các liên lạc nhằm để duy trì dịch vụ hoặc để bảo vệ chính mình khỏi bị hại. Chẳng hạn, ví dụ, nhà cung cấp dịch vụ có thể ghi đọc luồng để loại trừ các virut.

Luật thống nhất và tăng cường nước Mỹ, cung cấp các công cụ cần thiết để ngăn chặn và đối phó với chủ nghĩa khủng bố (gọi tắt là đạo luật yêu nước của Hoa Kỳ) ( The Uniting and Strengthening America by Providing Appropriate Tools to Intercept and Obstruct Terrorism Act – USA Patriot Act).

Luật này được thông qua năm 2001 khi mà những tấn công khủng bố liên tục xảy ra trên lãnh thổ Mỹ. Luật yêu nước Hoa Kỹ được bổ sung và mở rộng vào tháng 3 năm 2006. Luật bao gồm một loạt điều khoản hỗ trợ tiếp cận buộc thực thi luật đối với các liên lạc điện tử. Theo luật này, cơ quan thực thi pháp luật chỉ cần thuyết phục Toà án rằng đích ở đây là một nhân viên của một tổ chức nước ngoài thì sẽ nhận được lệnh cho phép nghe ngầm ngay. Điều khoản an toàn máy tính cơ bản của Luật yêu nước là sự điều chỉnh, mở rộng của luật chống gian lận và lạm dụng máy tính:

• Cố ý tạo ra sự lan truyền một mã gây hại cho một “ máy tính được bảo hộ ” là một trọng tội (tội nghiêm trọng).

• Do sai sót gây ra thiệt hại cho một hệ thống máy tính tương tự như là hậu quả của truy nhập bất hợp pháp cũng bị coi là một trọng tội.

• Gây ra thiệt hại ( dù là không cố ý ) như là truy nhập bất hợp pháp tới một máy tính được bảo vệ cũng coi là một tội ác ( nhẹ hơn ).

• Sửa đổi vài luật đang tồn tại để cung cấp cho chính phủ các công cụ bổ sung để ghi dấu vết, ngăn chặn và tiêu diệt chủ nghĩa khủng bố.

• Tạo điều kiện chia sẻ các thông tin về an ninh quốc gia và thực thi luật này.

• Cho phép các tiếp cận bổ xung của chính phủ tới các thông tin cần thiết, gồm cả các thông tin điện tử.

Luật hiện đại hóa công nghệ ngân hàng 1999. ( Financial Industries Modernization Act of 1999 – Gramm-Leach-Bliley )

*15 U.S.C.Đ Đ6801 – 6810 ( chống tiết lộ thông tin tài chính riêng )*

*15 U.S.C.Đ Đ6821 – 6827 ( chống tiếp cận gian lận )*

Luật này còn có tên thường gọi là luật Gramm – Leach – Bliley, 1999; bao gồm an toàn dữ liệu cho các khách hàng của các thiết chế tài chính. Mỗi thiết chế ( cơ quan ) tài chính phải có chính sách an toàn của mình để thông báo cho các khách hàng. Và các khách hàng phải được cung cấp cơ hội để khước từ mọi việc dùng dữ liệu không đúng mục đích kinh doanh cần thiết mà các dữ liệu được thu thập cho nó. Luật Gramm-Leach-Bliley và các quy định áp dụng nó cũng đòi hỏi các thiết chế ngân hàng phải được đánh giá an toàn – rủi ro chi tiết định kỳ. Dựa trên cơ sở các kết quả của sự đánh giá này, cơ quan tài chính phải thông qua “ một chương trình an toàn thông tin ” tăng cường nhằm bảo vệ chống truy nhập trái phép hoặc việc dùng các thông tin riêng không công bố của các khách hàng.

Luật chuyển tiền điện tử của Mỹ.( US Electronic Funds TransferAct)

Luật này nghiêm cấm việc sử dụng, vận chuyển, bán, nhận hay cung cấp các vật dụng hay món nợ thu được một cách gian lận hoặc do thất bại, sửa đổi, ăn cắp, hoặc giả mạo trong thương mại toàn liên bang hay ngoại thương.

Luật năm 1998 về ngăn chặn sự giả mạo và ăn cắp định danh.

Đây là sự điều chỉnh bổ sung của 18 U.S.C.Đ1028 ( khởi tố hình sự việc chuyển giao cố ý hay sử dụng định danh của một người khác cho các mục đích phi pháp ). Trộm cắp định danh cũng có thể vi phạm các luật hình sự liên bang khác như 18 U.S.C.Đ1029: gian lận thẻ tín dụng, 18 U.S.C.Đ1030: gian lận máy tính, 18 U.S.C.Đ1341: gian lận thư tín, 18 U.S.C.Đ1343: gian lận điện tín, và 18 U.S.C.Đ1344: gian lận thiết chế tài chính.

Luật 2004 về tăng cường các hình phạt ăn cắp định danh

Các điều chỉnh bổ xung vào các điều luật đã có, luật này xác lập hai loại “ trộm cắp định danh trầm trọng ”:

* + Trộm cắp danh tính liên quan tới chủ nghĩa khủng bố
  + Trộm cắp danh tính liên quan với các trọng tội khác.

Luật này tăng các hình phạt và hợp pháp hoá khoản tiền phụ phí theo kiện một vụ ăn cắp địn danh.

Luật năm 2003 về các giao dịch tiền tệ chính xác và công bằng.

Đây là các điều chỉnh và tái khẳng định đối với Luật về báo cáo tiền tệ công bằng năm 1970 ( Fair Credit Reporting Act of 1970 ), mà luật 1970 là bổ xung cho 15 U.S.C.Đ Đ1681-1681(u).

Luật 2003 này bao gồm các điều khoản nhằm hạn chế sự ăn cắp định danh và trợ giúp các bị hại trong ăn cắp định danh tái bảo vệ ( lấy lại định danh hoặc được bồi thường thiệt hại).

Luật này còn có một số chứng thư ( Titles ). Chứng thư I ( Titles I ) quy định về việc ngăn chặn ăn cắp định danh và việc truy hồi nguồn gốc tiền tệ. Chứng thư VII quy định về mối quan hệ tới các luật của bang.

Liên quan tới Luật giao dịch tiền tệ ( 2003 ) và Luật báo cáo tài chính (1970), uỷ ban thương mại liên bang của Hoa Kỳ ( FTC – Federal Trade Commision ) đưa ra một số văn bản hướng dẫn quan trọng.

Vào tháng 2/2005, FTC công bố Các chỉ dẫn về phương hướng lưu giữ hợp thức các thông tin của khách hàng. Các chỉ dẫn này có hiệu lực từ tháng 7/2005, và quy định về sự sắp xếp các báo cáo của khách hàng và các thông tin thu được từ các báo cáo này.

Vào tháng 7/2006, FTC và Hiệp hội các ngân hàng liên bang Hoa Kỳ công bố để lấy ý kiến Các chỉ dẫn cho việc đặt “ cờ đỏ ” (phạt tiền) trộm cắp định danh và mâu thuẫn địa chỉ. Khi được thông qua, các chỉ dẫn này sẽ đòi hỏi các cơ quan tài chính và các báo cáo đầu tư phải phát triển và ứng dụng các chương trình ngăn chặn trộm cắp định danh.

Thoả thuận của Uỷ ban Châu Âu về tội phạm điều khiển. ( Council of Europe Agreement on Cybercrime – ECAC).

Tháng 11 năm 2001, Mỹ, Canada, Nhật bản và 22 nước Châu Âu đã ký Thoả thuận của EC về tội phạm điều khiển (ECAC) để thống nhất xác định các hoạt động tội phạm trong không gian điều khiển (cyberspace) và hỗ trợ việc truy nã và xét xử chúng vượt qua biên giới quốc gia. Ý nghĩa của thoả thuận này không chỉ quan trọng ở chỗ coi các hoạt động tội phạm này là phi pháp, mà còn ở chỗ việc cả 25 nước này đều công nhận chúng là các tội ác xuyên quốc gia mình sẽ giúp cho các cơ quan thực thi pháp luật dễ dàng hơn trong việc hợp tác với nhau, trong việc dẫn độ các tội phạm đã thực hiện tội ác chống một nước này từ lãnh thổ một nước khác. Tuy nhiên để thực tế hỗ trợ được cho sự truy nã, xét xử và trừng phạt các tội phạm máy tính, cần phải vào cuộc không chỉ 25 nước này mà nhiều hơn nhiều vì như ta đã nói về bản chất toàn cầu của các tội phạm máy tính. Cho nên thoả thuận EC cũng kêu gọi các nước khác ( ngoài 25 nước đã ký ) tham gia vào. Bản thoả thuận cũng yêu cầu các nước thông qua nó, tiến hành ban bố các đạo luật hình sự giống nhau về tin tặc ( hacking ), về gian lận và làm giả trong lĩnh vực điện toán, truy nhập bất hợp pháp, các vi phạm bản quyền, quấy rối trên mạng và khiêu dâm trẻ em. Bản Thoả thuận này cũng bao gồm các điều khoản về các hiệu lực truy nã và các thủ tục cần thiết như là săn lùng trên các mạng và chặn bắt các liên lạc và các yêu cầu về hợp tác thực thi luật qua biên giới trong truy lùng, bắt giữ và dẫn độ. Văn bản gốc của Thoả thuận đã được bổ sung bằng một phụ lục coi là một tội hình sự bất kỳ hình thức tuyên truyền nào thông qua các mạng máy tính về phân biệt chủng tộc và bài ngoại.

Luật về bảo vệ dữ liệu của Cộng đồng châu Âu ( EU ). ( Europe Union Data Protection Act ).

Luật về bảo vệ dữ liệu EU, dựa trên Bản chỉ dẫn về an ninh châu Âu, là mô hình pháp lý cho tất cả các nước trong EU. Nó xác lập các quyền riêng tư và trách nhiệm bảo hộ đối với mọi công dân của các nước thành viên. Luật này quy định về sự thu thập và lưu trữ các dữ liệu riêng về các cá nhân, như họ tên, địa chỉ và các số đặc chỉ ( nhận dạng, thông hành ...). Luật đòi hỏi mục đích kinh doanh của việc thu thập dữ liệu và giám sát chống tiết lộ. Thông qua vào năm 1994, đây là một trong số các luật sớm nhất xác lập các yêu cầu bảo hộ đối với việc an toàn các dữ liệu cá nhân. Điều quan trọng hơn cả ở đây là: Luật yêu cầu sự bảo hộ tương tự ở cả bên ngoài các nước EU trong trường hợp các tổ chức trong EU đưa các dữ liệu được bảo hộ ra khỏi lãnh thổ EU.

### Một số văn bản pháp luật về ATTT ban hành tại Việt Nam.

Pháp lệnh bảo vệ bí mật nhà nước (BMNN).

Để nâng cao trách nhiệm của cơ quan nhà nước, các tổ chức xã hội, các công dân trong nhiệm vụ bảo vệ bí mật nhà nước ngày 11-1-2001 Chủ tịch nước đã công bố Pháp lệnh bảo vệ bí mật nhà nước (do Uỷ ban thường vụ quốc hội thông qua).

* Định nghĩa bí mật nhà nước (là loại thông tin đặc biệt về chính trị, kinh tế, quốc phòng, an ninh.... mà nhà nước không công bố hoặc chưa công bố và nếu bị tiết lộ thì sẽ gây nguy hại cho Nhà nước CHXHCN Việt Nam.
* Nghiêm cấm mọi hành vi xâm phạm BMNN (như thu thập, làm lộ, làm mất, chiếm đoạt, mua bán, tiêu huỷ trái phép) và quy định việc tiếp xúc, bảo quản và xử lý BMNN.
* Lần đầu đưa ra các độ mật: Tuyệt mật, Tối mật và Mật của các thông tin BMNN (mà được áp dụng vào các dạng TT khác sau này).
* Nói rõ tại điều 5: Mật mã quốc gia thuộc độ Tuyệt mật và tại điều 15: Nội dung BMNN nếu truyền đưa bằng phương tiện viễn thông và máy tính thì phải được mã hoá theo quy định của pháp luật về cơ yếu.
* Quy định nội dung quản lý nhà nước về BMNN (Chính phủ thống nhất quản lý nhà nước về bảo vệ BMNN, Bộ công an chịu trách nhiệm trước Chính phủ về bảo vệ BMNN).
* Ngày 28-3-2002 Chính phủ có Nghị định số 33/2002/NĐ-CP quy định chi tiết thi hành pháp lệnh này. Tại điều 15 của Nghị định số 33 nói rõ: Nghiêm cấm các cơ quan, tổ chức và cá nhân tự nghiên cứu, sản xuất, cung cấp, quản lý, sử dụng mật mã để tiến hành các hoạt động xâm phạm an ninh quốc gia.

Đây là văn bản luật đầu tiên có một số quy định về mật mã và sử dụng mật mã ở Việt Nam.

Luật Giao dịch điện tử (GDĐT).

Luật Giao dịch điện tử có hiệu lực từ ngày 1/3/2006. Luật GDĐT ra đời là một đòi hỏi bức thiết của việc ứng dụng CNTT trong nước cũng như hội nhập quốc tế. Trong nhiều năm qua, đầu tư cho CNTT của nước ta tuy chưa lớn bằng một số nước nhưng cũng chiếm tỷ lệ cao trong ngân sách. CNTT đã góp phần nâng cao hiệu quả của nhiều hoạt động kinh tế xã hội, song chúng ta chưa có một văn bản pháp luật nào công nhận giá trị pháp lý của các ứng dụng này. Do vậy, bên cạnh hệ thống quản lý hành chính, giao dịch được tin học hoá hoạt động khá hiệu quả, chúng ta vẫn phải duy trì các hệ thống thủ công truyền thống theo quy định của pháp luật. Luật GDĐT ra đời cũng tạo ra cơ sở pháp lý bảo đảm an ninh, an toàn cho GDĐT, bảo vệ quyền lợi hợp pháp của các bên tham gia GDĐT. Tinh thần cơ bản của Luật GDĐT là công nhận giá trị pháp lý của thông điệp dữ liệu – một hình thức thể hiện mới của giao dịch bên cạnh hình thức *văn bản và lời nói* như quy định của bộ Luật Dân sự.

Luật công nghệ thông tin (Luật CNTT).

Luật CNTT được chủ tịch nước công bố ngày 12/7/2006. Luật quy định về hoạt động ứng dụng và phát triển CNTT, quyền và nghĩa vụ của cơ quan, tổ chức, cá nhân tham gia hoạt động ứng dụng và phát triển CNTT.

Về các hành vi phạm pháp liên quan đến an toàn, an ninh thông tin trên mạng, luật bao gồm các nhóm hành vi:

* Nhóm hành vi vi phạm pháp luật có tính chất chống lại con người. Khoản 2, Điều 12 Luật CNTT quy định nghiêm cấm hành vi cung cấp, trao đổi, truyền đưa, lưu trữ, sử dụng thông tin số nhằm mục đích kích động bạo lực, tuyên truyền chiến tranh xâm lược, gây hận thù giữa các dân tộc và nhân dân các nước, kích động dâm ô, đồi truỵ, tội ác, tệ nạn xã hội, mê tín dị đoan, phá hoại thuần phong mỹ tục của dân tộc, xuyên tạc, vu khống, xúc phạm uy tín của tổ chức, danh dự, nhân phẩm, uy tín của công dân; quảng cáo, tuyên truyền hàng hoá, dịch vụ thuộc danh mục cấm đã được pháp luật quy định.
* Về nhóm hành vi xâm phạm tài sản của tổ chức, cá nhân. Khoản 1, Điều 12 nghiêm cấm hành vi cản trở bất hợp pháp hoạt động của hệ thống máy chủ, tên miền quốc gia, phá hoại cơ sở hạ tầng thông tin, phá hoại thông tin trên môi trường mạng.

Khoản 3, Điều 12 nghiêm cấm hành vi xâm phạm quyền sở hữu trí tuệ trong hoạt động công nghệ thông tin, sản xuất, lưu hành sản phẩm công nghệ thông tin trái pháp luật; giả mạo trang thông tin điện tử của tổ chức, cá nhân khác; tạo đường dẫn trái phép đối với tên miền của tổ chức, cá nhân sử dụng hợp pháp tên miền đó.

Khoản 1, Điều 21 quy định tổ chức, cá nhân thu thập, xử lý và sử dụng thông tin cá nhân của người khác trên môi trường mạng phải được người đó đồng ý, trừ trường hợp pháp luật có quy định khác.

Điều 71 quy định tổ chức, cá nhân không được tạo ra, cài đặt, phát tán virus máy tính, phần mềm gây hại vào thiết bị số của người khác để thực hiện một trong những hành vi bao gồm: thay đổi các tham số cài đặt của thiết bị số; thu thập thông tin của người khác; xoá bỏ, làm mất tác dụng của các phần mềm bảo đảm an toàn, an ninh thông tin được cài đặt trên bị số; ngăn chặn khả năng của người sử dụng xoá bỏ hoặc hạn chế sử dụng những phần mềm không cần thiết; chiếm đoạt quyền điều khiển thiết bị số; thay đổi, xoá bỏ thông tin lưu trữ trên thiết bị số....

Khoản 2, Điều 72 quy định tổ chức cá nhân không được thực hiện một trong những hành vi bao gồm: xâm nhập, sửa đổi, xoá bỏ nội dung thông tin của tổ chức, cá nhân khác trên môi trường mạng; cản trở hoạt động cung cấp dịch vụ của hệ thống thông tin; ngăn chặn việc truy nhập đến thông tin của tổ chức, cá nhân khác trên môi trường mạng, phá khoá mã, trộm cắp, sử dụng mật khẩu, khoá mật mã và thông tin của tổ chức, cá nhân khác trên môi trường mạng.

* Về nhóm hành vi vi phạm pháp luật có tính chất chống lại Chính phủ. Khoản 2, Điều 12 nghiêm cấm hành vi cung cấp, trao đổi, truyền đưa, lưu trữ, sử dụng thông tin số nhằm mục đích chống Nhà nước Cộng hoà xã hội chủ nghĩa Việt Nam, phá hoại khối đoàn kết toàn dân; tiết lộ bí mật Nhà nước, bí mật quân sự, an ninh, kinh tế, đối ngoại và những bí mật khác đã được pháp luật quy định.

Khoản 2, Điều 68 quy định tên miền quốc gia Việt Nam “.vn” dành cho tổ chức Đảng, cơ quan Nhà nước phải được bảo vệ và không được xâm phạm.

Ở Việt Nam, Luật CNTT được ban hành kết hợp với các văn bản quy phạm pháp luật hiện có đã tạo lập hành lang pháp lý tương đối phù hợp nhằm ngăn ngừa các hành vi vi phạm pháp luật liên quan đến máy tính và môi trường mạng, góp phần bảo đảm an toàn, an ninh thông tin trên mạng.

## Giới thiệu các cơ quan, tổ chức, đầu mối đảm bảo an toàn thông tin trong nước

**Trung tâm ứng cứu khẩn cấp máy tính Việt Nam – VNCERT**

Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT) là đơn vị trực thuộc Bộ Thông tin và Truyền thông, thực hiện chức năng điều phối các hoạt động ứng cứu sự cố máy tính trong toàn quốc; cảnh báo kịp thời các vấn đề về an toàn mạng máy tính; xây dựng, phối hợp xây dựng các tiêu chuẩn kỹ thuật về an toàn mạng máy tính; thúc đẩy hình thành hệ thống các trung tâm ứng cứu khẩn cấp máy tính (CERT) trong các cơ quan, tổ chức, doanh nghiệp; là đầu mối thực hiện hợp tác với các tổ chức CERT nước ngoài.

**Công ty cổ phần an ninh an toàn thông tin CMC**

Công ty cổ phần an ninh an toàn thông tin CMC là một thành viên của tập đoàn CMC, là một trong những đơn vị làm về an toàn thông tin, cung cấp các giải pháp bảo mật cho hệ thống và người dùng cuối chống lại các phần mềm mã độc, cung cấp các dịch vụ đánh giá an toàn thông tin, tư vấn bảo mật và xử lý sự cố an toàn thông tin cho các tổ chức đơn vị khi có yêu cầu.

**Công ty an ninh mạng BKAV**

Công ty cổ phần an ninh BKAV là một là một trong những công ty đi tiên phong về bảo mật tại Việt Nam, BKAV cung cấp các giải pháp diệt virus, giải pháp an ninh mạng, điều tra phân tích tấn công và đánh giá, kiểm định hệ thống an toàn thông tin.

## Nhận dạng tội phạm mạng và vấn đề hình sự trong an toàn thông tin.

### Đánh cắp định danh

Đánh cắp định danh là quá trình thu thập thông tin cá nhân để thủ phạm giả danh người khác. Điều này thường được thực hiện để có được thẻ tín dụng của nạn nhân, để lại cho nạn nhân những khoản nợ mà không hề hay biết. Mỹ xác định hành vi trộm cắp danh tính như sau: “Tội phạm trộm cắp và lừa đảo danh tính là thuật ngữ dùng để chỉ các loại tội phạm ăn cắp, gian lận, lừa dối và sử dụng trái phép dữ liệu cá nhân của người khác” .

Sử dụng dữ liệu cá nhân của người khác để thực hiện bất kỳ loại hành vi gian lận hoặc lừa dối là đánh cắp định danh. Tội phạm loại này thường thực hiện vì lợi ích kinh tế hay động cơ tài chính . Tội phạm cũng có thể sử dụng dữ liệu cá nhân để mạo danh người khác, hủy hoại danh tiếng … Ví dụ thủ phạm có thể đặt mua tài liệu khiêu dâm sử dụng danh tính người khác. Tuy nhiên hầu hết các sự cố đánh cắp định danh liên quan đến động cơ kinh tế. Ủy ban thương mại liên bang thống kê rằng trong năm 2005, 8,3 triệu người Mỹ là nạn nhân của tội phạm trộm cắp định danh. Đa số các sự cố nhận dạng hành vi trộm cắp là về vấn đề tài chính, với 3,2 triệu vụ liên quan đến lạm dụng tài khoản tín dụng và 1.800.000 liên quan đến sử dụng thông tin của nạn nhân để mở tài khoản mới. Thiệt hại lên đến hàng tỷ đô la mỗi năm do hành vi trộm cắp định danh. Rõ ràng đây là một vấn đề rất quan trọng .

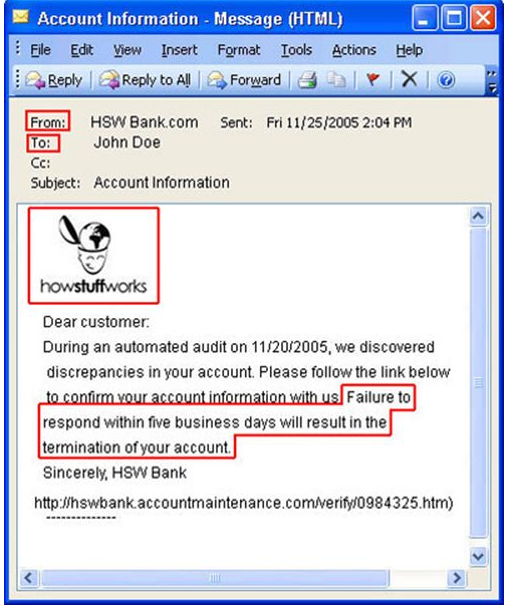
Trộm cắp định danh làm mất danh tiếng nạn nhân thường là một vấn đề dân sự, không phải tội phạm. Đánh cắp định danh không có động cơ kinh tế là một lỗi nhỏ do đó thường xử lý thông qua tố tụng dân sự chứ không phải là truy tố hình sự. Điều quan trọng là phải xem xét các phương tiện mà hành vi trộm cắp định danh sử dụng. Đầu tiên và hầu hết các bước quan trọng để phạm tội là đạt được quyền truy cập vào dữ liệu cá nhân để có thể trộm danh tính. Có bốn cách có thể truy cập vào thông tin cá nhân:

* Giả mạo.
* Tấn công hoặc sử dụng phần mềm gián điệp.
* Truy cập trái phép dữ liệu.
* Dựa vào thông tin rác.

#### Giả mạo

Giả mạo là quá trình ăn cắp những dữ liệu cá nhân từ các nạn nhân mục tiêu. Hành vi này thường được thực hiện thông qua e-mail. Thủ phạm có thể thiết lập một trang web ảo được thiết kế giống như trang web của một tổ chức tài chính hợp pháp (ngân hàng, thẻ tín dụng vv..). Sau đó thủ phạm sẽ gửi email cho càng nhiều người càng tốt, thông báo rằng tài khoản của họ cần xác minh và cung cấp cho họ một liên kết họ có thể bấm vào đăng nhập và xác minh tài khoản của họ. Khi ai đó nhấn vào liên kết, họ được đưa đến trang web giả mạo, nạn nhân nhập thông tin đăng nhập của mình để xác minh tài khoản, cung cấp cho thủ phạm với tên đăng nhập và mật khẩu . Sau đó thủ phạm có thể giả mạo đăng nhập vào tài khoản thực của nạn nhân và ăn cắp tiền.

Thủ thuật này ngày càng trở nên phổ biến. Email như hình 1.1 là một ví dụ khá điển hình của lừa đảo trực tuyến. Không như những email bình thường, đây là lá thư yêu cầu nạn nhân reply ngay lập tức, nếu không, tài khoản của sẽ bị khóa. Nếu nạn nhân ấn nút reply, không những dữ liệu cá nhân bị đánh cắp, tay trộm còn có thể thông qua đó phát tán virus và tiếp tục lây nhiễm sang những người dùng khác. Tệ hại hơn thế, nạn nhân ấy có thể đang vô thức tham gia vào quá trình rửa tiền giúp những tay tin tặc này.



Hình 2.1. Lừa đảo trực tuyến qua Email

Và cách thường gặp và cũng đơn giản nhất đó là sử dụng các phần mềm tạo email cho phép người dùng điền thông tin vào 2 phần “From” và ”Reply-to”. Những phần mềm này rất tiện dụng với những người sử dụng nhiều địa chỉ email, nhưng mặt khác nó giúp cho công việc của bọn lừa đảo dễ dàng hơn. Chỉ cần điền thông tin (trông có vẻ đáng tin cậy) vào mục “From”, ta đã có thể tạo ra một message trông hoàn toàn hợp pháp.

Một số máy chủ email cho phép các máy tính được phép kết nối trực tiếp đến cổng giao thức chuyển mail đơn giản (SMTP) mà không cần sử dụng password. Điều này cho phép tay lừa đảo có thể trực tiếp kết nối tới server và thông qua đó gửi tin nhắn đến hàng loạt cá nhân.

Tội phạm giả mạo có thể khó điều tra với một số lý do. Đầu tiên, nạn nhân thường không biết bị mắc lừa cho đến lâu sau khi nó đã xảy ra. Thứ hai là chúng sử dụng ngay và có kỹ năng ẩn dấu vết. Chúng chỉ tiến hành hoạt động lừa đảo chỉ trong một thời gian hạn chế sau đó dừng lại. Có nghĩa là khi bị tiến hành điều tra hoạt động lừa đảo có sự sẵn sàng dừng lại một thời gian. Thứ ba là các trang web giả mạo thường được thiết lập trên máy chủ công cộng, đôi khi là trên một máy chủ thứ ba bất đắc dĩ. Sau đó, các trang web thường được tháo dỡ ngay sau khi thủ phạm đã có đủ lượng dữ liệu cá nhân. Những yếu tố này có nghĩa là loại tội phạm này phải điều tra càng sớm càng tốt ngay sau khi xảy ra.

#### Tấn công hoặc sử dụng phần mềm gián điệp

Với một số chuyên gia bảo mật, có thể kì lạ khi phân loại tội phạm sử dụng tấn công và phần mềm gián điệp với nhau, nhưng khi nói đến việc đánh cắp định danh, thì cả tấn công lẫn sử dụng phần mềm gián điệp đều có cùng một mục tiêu: Đạt quyền truy cập vào hệ thốngmáy tính để có được dữ liệu cần thiết.

* **Tấn công**: Là một hoặc một chuỗi các hành động cố gắng vượt qua sự an toàn của hệ thốngđể truy cập vào dữ liệu không có chủ quyền. Có nhiều cách để thực hiện tấn công, bao gồm cả việc tìm kiếm một số lỗ hổng trong hệ điều hành khai thác, tấn công từ xa hợp pháp để truy cập được vào hệ thốngmục tiêu, liên quan đến hầu hết các kiến thức cơ bản của mạng và hoạt động của hệ thống. Bất cứ phương pháp nào được sử dụng, nếu hệ thốngmục tiêu có dữ liệu cá nhân mà thủ phạm muốn, chúng có thể nhận được toàn bộ dữ liệu từ hệ thốngmáy tính. Khi nói đến tấn công, có một thuật ngữ mà người ta thường nhắc đến, đó là Hacker.

Thuật ngữ hacker được sử dụng trên hầu hết các phương tiện truyền thông biểu thị kẻ xâm nhập bất hợp pháp vào hệ thống. Trong hai thập kỷ qua, những thuật ngữ đã trở nên phổ biến đó là Hacker mũ trắng, Hacker mũ đen và Hacker mũ xám.

* Hacker mũ trắng là những người sử dụng các kỹ năng của mình để bảo vệ hệ thống. Hacker mũ trắng chỉ thực hiện xâm nhập vào hệ thốngkhi được cho phép bởi người quản trị hệ thống. Đó thường là thực hiện các thử nghiệm nhằm tìm ra các điểm yếu trên hệ thốngđể người quản trị có thể vá các điểm yếu trước khi bị kẻ xấu lợi dụng tấn công.
* Trái ngược với hacker mũ trắng là hacker mũ đen. Hacker mũ đen tiến hành các hoạt động bất hợp pháp, gắn liền với tội phạm máy tính. Thuật ngữ này đồng nghĩa với cracker. Thông thường khi các phương tiện truyền thông thảo luận về hacking, họ đề cập đến hacker mũ đen.
* Hacker mũ xám là thuật ngữ để chỉ về các hacker vừa mang tính chất hacker mũ trắng vừa mang tính chất hacker mũ đen. Họ có thể vi phạm pháp luật, nhưng thường là không có mục đích xấu.

Ví dụ một người tiến hành kiểm tra thâm nhập cho các công ty là một hacker mũ trắng. Hacker mũ xám là hacker đứng giữa, mặc dù thường xuyên bên ngoài pháp luật. Một hacker mũ xám có thể cố gắng tìm ra điểm yếu trong hệ thốngmà không cần sự cho phép của chủ sở hữu hệ thống, nhưng là tìm vị trí chứ không phải là khai thác chúng, các hacker mũ xám sẽ thông báo cho chủ sở hữu của hệ thống. Không dễ dàng để hiểu được hacking. Mặc dù nhiều phim cho thấy có thể truy cập vào hệ thốngbảo mật cao trong vài phút, điều này hẳn là không đúng sự thật. Hacking giống như một vụ trộm cần có mục tiêu, kỹ năng và thời gian để xâm nhập. Và cũng như các vụ trộm, xâm nhập vào hệ thốngan toàn đòi hỏi phải có kỹ năng và kiến thức chuyên sâu. Một hacker có tay nghề cần hiểu biết rõ về hệ điều hành mạng và các biện pháp an ninh. Hacker giỏi rất hiếm.

* **Phần mềm gián điệp**: Phần mềm gián điệp cũng có mục tiêu thu thập dữ liệu cá nhân từ máy tính mục tiêu. Không giống như hacking tuy nhiên mục tiêu duy nhất của phần mềm gián điệp là để có được dữ liệu. Nó thường liên quan đến một số phần mềm được tải về của máy tính mục tiêu. Phần mềm có thể ghi lại tên, mật khẩu người dùng, các tổ hợp phím, các trang web truy cập hoặc các dữ liệu khác. Thậm chí có những sản phẩm phần mềm gián điệp có thể chụp ảnh màn hình định kỳ, ghi lại mọi hoạt động trên màn hình. Trong một số trường hợp, điều này có thể được thực hiện bằng các phần mềm gián điệp theo định kỳ hoặc tải dữ liệu đến một địa chỉ Internet cụ thể, từ dó thủ phạm có thể truy cập bất hợp pháp đến dữ liệu. Nếu thủ phạm đặc biệt có tay nghề, địa chỉ này sẽ là một máy chủ bên thứ ba hoàn toàn không liên quan đến tội phạm. Phần mềm gián điệp rất phổ biến vì 2 lý do. Đầu tiên, nó khá dễ dàng có được. Đó là bởi vì nhiều sản phẩm với mục đích hợp pháp có thể sử dụng như phần mềm gián điệp. Ví dụ sản phẩm được thiết kế để giám sát truy cập web cho trẻ em, năng suất lao động, hoặc cho mục đích hợp pháp khác cũng có thể được sử dụng như phần mềm gián điệp. Thứ hai thật là dễ dàng để cung cấp. Thường thì phần mềm gián điệp được gửi qua một con Trojan có nghĩa là phần mềm có mục đích hữu ích mà còn cung cấp một số tin nguy hiểm. Ví dụ khi tải về một trò chơi miễn phí hoặc mã chứng khoán từ Internet, người dùng cũng vô tình tải về phần mềm gián điệp.

Cả tấn công và phần mềm gián điệp có thể dễ dàng điều tra hơn là tội phạm giả mạo. Vì phần mềm gián điệp để lại dấu vết rõ ràng, dữ liệu thu được phải truyền đi một nơi nào đó. Vấn đề thực sự với cả phần mềm gián điệp và tấn công đó là mức độ kỹ năng của thủ phạm.

#### Truy cập trái phép dữ liệu

Truy cập trái phép dữ liệu là hành vi truy cập đến dữ liệu mà không được phép. Hành vi phổ biến là khi một người có quyền hợp pháp một số nguồn dữ liệu cụ thể hoặc là để truy cập dữ liệu không được phép hoặc sử dụng các dữ liệu một cách khác hơn so với cách họ được ủy quyền. Một ví dụ là nhân viên bệnh viện truy cập hồ sơ bệnh nhân sử dụng các dữ liệu để ăn cắp thông tin của bệnh nhân. Hoặc một người không có quyền truy cập vào tất cả những hồ sơ ấy. Ví dụ này sẽ là một hacker đột nhập vào hệ thốngđể ăn cắp dữ liệu.

Phương pháp phổ biến nhất của loại tội phạm này là đăng nhập với tài khoản của người khác. Điều đó cho phép thủ phạm có thể truy cập đến các tài nguyên hoặc dữ liệu mà người có mật khẩu đã được truy cập và sử dụng bởi nhiều người đặt mật khẩu yếu, tệ hơn là viết mật khẩu của họ ra bàn cho dễ nhớ hoặc chia sẻ mật khẩu với người khác. Ví dụ, một người quản lý bị bệnh nhưng cần kiểm tra xem khách hàng có gửi email hay không nên đã gọi cho trợ lý đăng nhập email của mình. Như vậy, trợ lý có thể sử dụng tài khoản đó hoặc tiết lộ cho người khác (vô tình hay cố ý), có nghĩa là bây giờ có một cơ hội lớn cho những người khác sử dụng đăng nhập vào mà người quản lý truy cập dữ liệu không cho phép. Có nhiều lý do đằng sau những truy cập trái phép này. Có thể là tò mò đơn giản, muốn biết những gì không biết như lương hay thông tin cá nhân của các nhân viên khác. Tuy nhiên cũng có những lý do nghiêm trọng hơn như: đánh cắp danh tính, lấy danh sách khách hàng trước khi rời khỏi công ty với mục đích ăn cắp khách hàng hay bán nghiên cứu nhạy cảm của công ty cho một đối thủ cạnh tranh,… Đây là lý do tại sao kiểm soát truy cập trái phép dữ liệu phải được thực hiện nghiêm túc bởi các chuyên gia an ninh mạng và pháp luật.

#### Dựa vào thông tin rác

Các cá nhân cũng như tổ chức thường xuyên loại bỏ dữ liệu cũ cũng là một cách tiếp cận cho bọn tội phạm. Có thể là bất cứ dữ liệu nào từ các hóa đơn cũ ném vào thùng rác để loại bỏ các sao lưu. Từ đó thủ phạm có thể có được các phương tiện truyền dữ liệu (giấy, đĩa mềm, ổ đĩa…) từ thùng rác và sau đó lấy dữ liệu cá nhân. Trong năm 2004, một cơ quan tuyển dụng quân đội Mỹ ở khu vực Dallas đã tìm thấy hồ sơ bị loại bỏ của một tân binh mới trong thùng rác. May mắn là các dữ liệu được phát hiện bởi một phóng viên mà không phải một tên trộm danh tính. Từ góc độ Pháp luật, điều tra loại tội phạm này cũng khó khăn. Xác định nguồn gốc của dữ liệu khi bị bỏ đi là đơn giản, nhưng việc xác định thủ phạm thực tế có thể rất khó khăn.

### Rình rập, quấy rối

Tội phạm loại này là tương đối mới và ngày càng phát triển. Hành vi của tội phạm này đó là bạo lực, trong đó có tấn công tình dục và giết người. Hầu hết các quốc gia đã từ lâu thông qua nhiều luật chống rình rập, những hành vi này gần đây đã mở rộng trên không gian mạng. Thủ phạm sử dụng Internet để sách nhiễu, đe dọa người khác. Hoặc như Bộ tư pháp Mỹ đưa ra:

“ Không có định nghĩa cụ thể về tội phạm rình rập trên mạng, đó có thể là việc sử dụng internet, thư điện tử, hoặc các thiết bị thông tin liên lạc điện tử khác để theo dõi người khác. Tội phạm rình rập nhìn chung là hành vi quấy rối hoặc đe dọa một cá nhân ví dụ như theo dõi một người, xuất hiện ở nhà của một người hoặc địa điểm kinh doanh, thực hiện cuộc gọi quấy rối, để lại lời nhắn bằng văn bản hoặc là phá hoại tài sản. Hầu hết các luật liên quan đến tội phạm rình rập là mối đe dọa đối với nạn nhân, gia đình nạn nhân. Trong một số hành vi liên quan đến hành vi gây phiền nhiễu hay đe dọa có thể là rình rập bất hợp pháp, hành vi như vậy có thể là mở màn cho bạo lực và cần trừng trị nghiêm túc. ”

Điều đó có nghĩa là nếu một người sử dụng Internet theo dõi nhằm mục đích quấy rối, đe dọa người khác thì đó là tội phạm rình rập trên mạng. Một ví dụ điển hình về rình rập trên mạng là việc gửi email đe dọa. Nhưng định nghĩa về quấy rối, đe dọa hiện nay rất mơ hồ. Rõ ràng, nếu một người gửi email cho một người đe dọa giết người và cung cấp hình ảnh của người nhận để chứng minh rằng người gửi quen thuộc với sự xuất hiện của mục tiêu, đó chính là rình rập trên mạng. Cũng có những email có một đe dọa mơ hồ, chẳng hạn như “ Mày sẽ nhận được những gì xứng đáng” liệu có phải là rình rập? Đây không phải là một câu hỏi dễ trả lời, và không có câu trả lời duy nhất cho tất cả tình huống. Thế nào là đe dọa, quấy rối khác nhau rất nhiều từ thẩm quyền, nhưng hướng dẫn chung là nếu các email (hoặc tin nhắn) nội dung bất thường sẽ được coi là đe dọa trong lời nói bình thường, sau đó sẽ có thể được coi là mối đe dọa nếu được gửi bằng điện tử. Vậy để tìm ra mối đe dọa thì điều quan trọng là tìm ra bốn yếu tố sau:

* **Độ tin cậy**: Điều này dễ dàng xác định. Đối với mối đe dọa cho là đáng tin cậy, phải có dấu hiện hợp lý rằng nó có thể được thực hiện. Ví dụ một phụ nữ ở Nebraska đang thảo luận trên Internet và nhận được mối đe dọa chung từ một người dùng sống tại Bangkok trong một quá trình tranh luận. Trong tình huống này, người gửi rất có thể không biết nơi sống của người nhận. Trên thực tế có người sử dụng tên ảo trên Internet, người gửi có thể thậm chí không biết tên, giới tính, tuổi tác của người nhận thực tế. Có nghĩa là mối đe dọa này có độ tin cậy thấp. Tuy nhiên nếu người phụ nữ ở Nebraska nhận được mối đe dọa từ người sử dụng tại Bangkok đi kèm với thông tin cá nhân như địa chỉ, nơi làm việc, hoặc một bức ảnh đó là mối đe dọa tin cậy.
* **Tần suất**: Đưa ra nhận xét thiếu khôn ngoan trên Internet, một lời nhận xét thù địch chỉ là phản ứng gay gắt, quá nhanh trên Internet. Loại hình này đã bình luận trong một phòng chat hoặc trên một thông báo. Thường xuyên quấy rầy ý kiến và đe dọa theo thời gian, dần dần xây dựng để chỉ nơi họ sẽ hành động. Trong khi đó chắc chắn có thể là trường hợp mối đe dọa điều tra đảm bảo duy nhất, như một quy luật chung, các mối đe dọa cô lập là mối quan tâm ít hơn một mô hình của quấy rối và đe dọa.
* **Đặc trưng**: Đề cập đến thủ phạm liên quan đến bản chất của các mối đe dọa, các mục tiêu của các mối đe dọa, và các phương tiện thực hiện các mối đe dọa. Tất nhiên, nó rất quan trọng với cán bộ thực thi pháp luật để nhận ra rằng mối đe dọa thực tế đôi khi có thể mơ hồ. Nói cách khác, mối đe dọa thực sự sẽ không luôn luôn cụ thể. Nhưng mối đe dọa thường có thật. Ví dụ một người nào đó nhận được một email nói rằng “*Mày phải trả giá cho điều đó*” ít quan tâm hơn một email có chứa một mối đe dọa cụ thể của bạo lực, chẳng hạn như “*Tao sẽ chờ mày sau khi làm việc và bắn vào đầu mày*” cùng với một bức ảnh để lại nơi làm việc của người nhận. (Hình ảnh này cũng làm cho nó rất đáng tin cậy). Mối đe dọa này rất cụ thể và cần được quan tâm hơn trong khi thực thi pháp luật.
* **Cường độ**: Vấn đề này đề cập đến những giai điệu chung của truyền thông, bản chất của ngôn ngữ và cường độ của các mối đe dọa. Mối đe dọa bạo lực phải luôn đc thực hiên nghiêm túc thực thi pháp luật. Thông thường, khi một người nào đó chỉ đơn giản là thông báo hoặc phản ứng thái độ có thể lập báo cáo coi là đe dọa, nhưng trong trường hợp này hầu hết mọi người lập báo cáo cường độ thấp, chẳng hạn như đe dọa để đánh bại một người nào đó. Các mối đe dọa như này ít quan tâm hơn đó là mối đe dọa chia cắt một ai đó. Điều này là do bình thường những người bất bạo động, có thể mất bình tĩnh. Nhưng bình thường, những người bất bạo động không thường mất bình tĩnh và muốn cắt một người nào đó thành miếng bằng cưa máy. Bất cứ lúc nào có mối đe dọa lớn lên đến mức độ vượt quá những gì một người bình thường có thể nói, ngay cả trong một tình huống thù địch, các mối đe dọa sẽ trở thành mối quan tâm lớn hơn.

Hiện nay thì tất cả bốn tiêu chí trên cần phải xem xét để xác định một mối đe dọa là khả thi. Cán bộ thực thi pháp luật phải luôn dựa vào tình huống và phải luôn luôn nghi vấn về phía cảnh báo.

### Truy cập bất hợp pháp tới hệ thốngmáy tính và các dữ liệu nhạy cảm

Truy cập trái phép vào hệ thốngmáy tính hoặc dữ liệu có thể được cho là mục đích khác hơn so với tội phạm đánh cắp định danh. Ví dụ, thủ phạm có thể muốn ăn cắp dữ liệu bí mật của công ty, tài liệu tài chính nhạy cảm hoặc các dữ liệu khác. Thông tin này có thể được sử dụng để thu hút khách hàng từ đối thủ cạnh tranh, phát hành để làm hỏng cổ phiếu của công ty, hoặc sử dụng để tống tiền. Trong mọi trường hợp, các yếu tố phổ biến là thủ phạm hoặc là không được cho phép truy cập dữ liệu hoặc không được phép sử dụng dữ liệu vậy mà cố tình sử dụng nó. Các phương pháp tương tự như bất kể mục đích của các truy cập trái phép. Nó có thể được thực hiện thông qua hacking hoặc phần mềm gián điệp, các nhân viên truy cập dữ liệu hoặc thông qua phương tiện truyền thông dữ liệu bị loại bỏ. Đặc biệt, hành vi trộm cắp dữ liệu là một vấn đề quan trọng, lý do chính là khó khăn để ngăn chặn nhân viên được phép truy cập đến dữ liệu. Đôi khi cũng rất khó để phân biệt giữa các truy cập trái phép và được phép.

### Lừa đảo trực tuyến

Tội phạm lừa đảo khá phổ biến. Một trong số các hành vi lừa đảo trực tuyến trên Internet bao gồm:

* Lừa đảo đầu tư.
* Lừa đảo giao dịch.
* Nhận/ lừa đảo tiền đặt hàng.
* Vi phạm bản quyền dữ liệu.

#### Lừa đảo đầu tư

Là phần tư vấn, môi giới đầu tư không hợp pháp, đây không phải là một trào lưu mới mà cũng không hẳn là một hoạt động phạm tội. Thậm chí một số môi giới chứng khoán hợp pháp chứng tỏ sự sinh tồn của họ đơn giản chỉ là kêu gọi mọi người đầu tư vào một cổ phiếu cụ thể. Mặc dù thực tế điều này đôi khi được sử dụng bởi các nhà môi giới chứng khoán hợp pháp, nhưng đây lại là một phương pháp khá phổ biến với những tội phạm lừa đảo. Khái niệm này thường được gọi là “*bơm và rút tiền*”: Tội phạm mua một số lượng đáng kể cổ phiếu có giá trị thấp. Sau đó, chúng sử dụng những chiêu để làm tăng nhu cầu đối với cổ phiếu và từ đó giá cổ phiếu được đẩy lên. Chúng cũng có thể đưa ra những lời khuyên giả, cho thấy các công ty để đảm bảo một hợp đồng lớn của chính phủ hoặc một bằng sáng chế, hoặc để phát hành một sản phẩm đột phá mới. Khi các cổ phiếu đã được đẩy lên mức cao, thủ phạm sẽ bán cổ phiếu khi đó các công ty sản xuất không được lợi, giá cổ phiếu sau đó trở về mức ban đầu của nó và có khi còn thấp hơn. Đây mới chỉ là một ví dụ về lừa đảo đầu tư.

Máy tính và Internet không làm thay đổi quá trình cơ bản của các chương trình lừa đảo, chúng chỉ làm cho tội phạm dễ dàng thâm nhập hơn. Chìa khóa của lừa đảo kiểu này đó là thay vì kêu gọi thông qua điện thoại, chúng gửi một bức thư điện tử hấp dẫn đến càng nhiều người càng tốt. Tất nhiên, thủ phạm nhận ra rằng hầu hết mọi người sẽ không đáp trả những email hấp dẫn ấy, nhưng nếu 1/10% làm theo, thủ phạm gửi lên đến một triệu email, vẫn có thể đẩy lên một số tiền đáng kể. Đây là một lý do tại sao thư rác lại là một vấn đề: phần lớn các thư rác nhận được thực sự là một phần của một số hành vi lừa đảo.

Có rất nhiều biến thể lừa đảo trên mạng. Một ví dụ phổ biến là gửi cho các nạn nhân một email dường như là từ một người nổi tiếng ở nước ngoài. Người đó cần sự giúp đỡ của người nhận trong việc chuyển giao một khoản tiền lớn từ đất nước của mình tới một ngân hàng ở Hoa Kỳ. Trong một số tình huống, người gửi yêu cầu thông tin tài khoản ngân hàng của người nhận để chuyển tiền vào tài khoản đó. Tất nhiên cuối cùng là chuyển tiền ra khỏi tài khoản của nạn nhân. Một cách tiếp cận phổ biến hơn là nói các nạn nhân phải nhận một khoản phí nhỏ để xử lý chuyển giao. Thủ phạm thu phí và không bao giờ thấy xuất hiện nữa.

Những tội phạm loại này cũng khó khăn để điều tra. Phải truy tìm lại email nhưng đôi khi chúng lại không hữu ích. Các email thường được gửi từ những tài khoản vô danh mà khó có thể theo dõi được. Để theo dõi thì phải kiểm tra các tài liệu thực tế và kiểm tra đường truyền tới một địa chỉ mail thực tế. Thông thường, địa chỉ này là một hộp bưu điện, không phải là văn phòng hoặc một nơi cư trú nào đó.

#### Lừa đảo giao dịch trực tuyến

Hiện nay giao dịch đấu giá trực tuyến khá phổ biến. Người dùng hợp pháp có thể khó khăn xác định một mức giá tốt, hoặc loại bỏ các mặt hàng không còn nhu cầu. Cũng như nhiều địa điểm kinh doanh hợp pháp, tuy nhiên, bọn tội phạm nỗ lực thao tác lừa đảo để ăn cắp từ các nạn nhân. Ủy ban thương mại Liên bang Mỹ (FTC) liệt kê bốn phạm trù sau của lừa đảo giao dịch trực tuyến:

* Không giao hàng hóa.
* Giao hàng có giá trị thấp hơn so với quảng cáo.
* Cung cấp hàng hóa không đúng thời hạn.
* Không tiết lộ các thông tin liên quan về một sản phẩm hoặc các điều khoản của người bán.

Đầu tiên là không giao hàng hóa. Đây là một hành động rõ ràng. Nạn nhân gửi tiền và người bán không giao hàng. Loại tội phạm này dễ dàng điều tra, truy tố. Loại thứ hai, giao hàng có giá trị thấp hơn, có nhiều khó khăn hơn để điều tra và truy tố loại này. Người bán luôn có thể nói người mua hiểu lầm về thông báo đấu giá được diễn đạt một cách mơ hồ. Hai loại cuối thì thường không có bị cáo để thực thi pháp luật và trong nhiều trường hợp cũng không cấu thành tội để điều tra. Nếu không cung cấp kịp thời vật chứng thì rõ ràng không phải là một tội phạm, nhưng trong hoàn cảnh khác có thể đặt vấn đề là một vu kiện dân sự. Việc không tiết lộ những thông tin liên quan tương tự như là giao cái gì đó nhỏ hơn giá trị và có thể khó điều tra hoặc truy tố.

#### Lừa đảo nhận/ chuyển tiền

Một loạt các trò gian lận trên Internet có liên quan đến việc trao đổi một lệnh chuyển tiền giả hoặc ký séc tiền thật. Các chương trình gian lận khá phổ biến trên các trang web Craigslist. Nạn nhân có một số mặt hàng bán trên Craigslist chẳng hạn như một chiếc đồng hồ đẹp. Tội phạm liên lạc với nạn nhân và đồng ý mua hàng. Tuy nhiên, thủ phạm tuyên bố sống bên ngoài khu vực và phải có một người đến nhận hàng. Sau đó đến lấy hàng và ký séc giả mạo không có giá trị gì.

#### Vi phạm bản quyền dữ liệu

Vi phạm bản quyền là các hành vi trộm cắp tài sản trí tuệ. Trong nhiều năm qua, vấn đề vi phạm bản quyền liên tục được nhắc đến. Có thể đó là bản quyền phần mềm, bài hát, đoạn phim,… được trao đổi, mua bán mà chưa có sự đồng ý từ tác giả. Và dù cho người đó có được người sở hữu cho sử dụng thì đưa nó cho bạn bè, hoặc bán nó vẫn là hành vi phạm tội. Thông thường thì các trường hợp đó là vấn đề dân sự. Vụ kiện sẽ ngăn chặn cả thủ phạm và giải quyết thiệt hai bằng tiền một cách đáng kể. Mặc dù hầu hết mọi người đã quen thuộc với các khái niệm phần mềm lậu và tải nhạc bất hợp pháp, có một nhóm vi phạm bản quyền dữ liệu có liên quan đến hành vi trộm cắp danh tính. Trong một số trường hợp, cá nhân ăn cắp danh tính, không sử dụng mà mang bán chúng. Người mua có thể là người nước ngoài bất hợp pháp muốn tài liệu hướng dẫn về việc làm hoặc một kẻ chạy trốn muốn có một danh tính khác. Ngày nay có cả một thị trường chợ đen ngày càng phổ biến về dữ liệu bị đánh cắp.

### Phát tán tin rác, mã độc hại

Một dạng tội phạm nữa rất phổ biến hiện nay là tội phạm chuyên thực hiện các hành vi phát tán tin rác, mã độc hại. Phát tán tin rác là hành vi gửi các tin nhắn hoặc các email chứa nội dung quảng cáo, marketing và được gửi một cách vô tội vạ gây phiền toái cho người nhận. Đôi khi, nó dẫn dụ người nhẹ dạ, tìm cách đọc số thẻ tín dụng và các tin tức cá nhân của họ. Theo thống kê từ hãng bảo mật Kaspersky Lab tháng 6-2013, tỉ lệ thư rác chiếm trung bình đến 71,1% lượng thư điện tử toàn cầu. Trong đó hơn một nửa số thư rác có nguồn gốc từ Trung Quốc (23,9%) và Mỹ (17,2%) - hai quốc gia hàng đầu về phát tán thư rác. Việt Nam xếp vị trí thứ sáu với tỉ lệ phần trăm thư rác chiếm khoảng 3,3%.

Viết mã độc - Phát tán mã độc là một trong những hình thức tấn công mới trên mạng. Kẻ tấn công sử dụng các chương trình mã độc để lây nhiễm vào các hệ thống, phần mềm nhằm mục đích phá hoại hệ thốnghoặc đánh cắp các thông tin trái phép. Để thực hiện phát tán mã độc, kẻ tấn công thường gửi một email có chứa mã độc tới nạn nhân hoặc đính kèm trong một phần mềm phổ dụng; người dùng chỉ cần kích hoạt chương trình là mã độc sẽ tự động lây nhiễm vào hệ thống. Như vậy, kẻ tấn công có thể theo dõi toàn bộ hoạt động trên hệ thốngbị lây nhiễm hoặc sử dụng hệ thốngbị lây nhiễm như một công cụ thực hiện tấn công tới các đối tượng khác.

## Phân biệt hacker mũ trắng, hacker mũ đen và vấn đề đạo đức trong an toàn thông tin

**Hacker mũ trắng** là những người thích tìm kiếm những lỗ hổng bảo mật trong một hệ thốngmáy tính với mục đích “vá” những lỗ hổng đó hơn là khai thác chúng với ý đồ xấu. Nhiều hacker mũ trắng tập hợp lại thành những nhóm kiểm tra bảo mật, được các công ty thuê để xâm nhập vào hệ thốngmạng nội bộ hay các ứng dụng Web nhằm kiểm tra khả năng phòng thủ, tính bảo mật hệ thống. Một số hacker mũ trắng hoạt động vì sở thích, hay là “người theo chủ nghĩa thuần tuý”. Những người này sử dụng thời gian rảnh rỗi để kiểm tra khả năng bảo mật của những phần mềm họ đang sử dụng. Nếu phát hiện có lỗi, họ sẽ gửi thông tin đến những nhà sản xuất. Hành vi chuẩn của những hacker mũ trắng là không nói chuyện đến tiền bạc và cung cấp toàn bộ thông tin về lỗi bảo mật cho người sở hữu hệ thốnghay hãng sản xuất phần mềm với mục đích giúp đỡ.

**Hacker mũ đen** là những người xâm nhập vào một hệ thốngvới ý định ban đầu là phá hoại hệ thốngmạng hay làm giàu cho bản thân. Cách thức hoạt động của hacker mũ đen khá đa dạng. Trong những năm gần đây, họ xâm nhập vào các địa chỉ có cơ sở dữ liệu cao như eBay, Amazon.com, MSNBC… Sử dụng các máy tính botnet để tấn công từ chối dịch vụ phân tán bất kỳ hệ thốngnào họ muốn. Hành vi nghiêm trọng nhất của hacker mũ đen là ăn cắp hay tống tiền. Ngoài ra, hacker mũ đen còn có thể ăn cắp hồ sơ thẻ tín dụng của khách hàng một công ty để đòi tiền chuộc. tính không còn đòi hỏi phải có kiến thức máy tính chuyên sâu. Do trên mạng luôn có sẵn các công cụ xâm nhập, bất kỳ hacker nào có lòng hận thù hay ác tâm đều có thể đội lên đầu chiếc mũ đen.

**Đạo đức nghề nghiệp trong an toàn thông tin**

Đạo đức nghề nghiệp không phải là một loại đạo đức đặc biệt dành cho một nghề nghiệp nào đó, mà đạo đức nghề nghiệp là hình chiếu của các quy tắc đạo đức chung lên những tình huống đặc trưng đối với một nghề nghiệp nhất định. Trong An toàn thông tin có Năm quy tắc đạo đức cơ bản:

1. Giúp đỡ những người có tinh thần học hỏi Người làm ATTT không được phép từ chối chia sẻ với người khác những kiến thức trong lĩnh vực CNTT và bảo vệ thông tin. Những kiến thức này phải được truyền đạt một cách không vụ lợi cho tất cả những ai có mong muốn học hỏi.

2. Tránh những điều có hại Trong công việc của mình, người làm ATTT cần phải tránh việc gây hại cho đối tượng được bảo vệ (thiệt hại từ tác dụng phụ), trừ trường hợp việc gây hại là cần thiết để ngăn chặn một thiệt hại lớn hơn. Cần tránh gây hại cho những bên không liên quan, cho dù việc gây hại đó giúp tránh được thiệt hại cho đối tượng được bảo vệ.

3. Không phát tán những thông tin nguy hiểm Người làm ATTT không được cung cấp cho bất kỳ ai thông tin về các điểm yếu mà có thể bị khai thác (ngoại trừ việc cung cấp thông tin cho chủ sở hữu hoặc nhà phát triển hệ thốngchứa điểm yếu nhằm mục đích loại trừ điểm yếu đó). Không được cung cấp cho bất kỳ ai những chương trình độc hại hoặc chương trình đa mục đích, nếu như có căn cứ để cho rằng người được cung cấp sẽ sử dụng chương trình một cách ác ý.

4. Sử dụng có chừng mực Khi có được quyền truy cập tới hệ thốnghoặc thông tin về hệ thống, người làm ATTT chỉ được sử dụng quyền truy cập/thông tin đó để thực hiện việc bảo vệ, ngăn chặn các mối nguy hại và tăng cường mức an toàn, mà không được sử dụng quyền truy cập/thông tin đó cho bất kỳ mục đích nào khác, kể cả mục đích vô hại. Khi thực hiện xong nhiệm vụ, quyền truy cập cần được đóng lại, còn thông tin thì cần phải được xóa bỏ.

5. Giữ bí mật Người làm ATTT cần phải giữ bí mật mọi thông tin được tiếp cận trong quá trình cung cấp dịch vụ bảo vệ, nếu thông tin đó là bí mật thương mại, bí mật đời tư, bí mật nghề nghiệp hay bất kỳ dạng thông tin mật nào khác, dù cho có hay không có thỏa thuận về việc giữ bí mật các thông tin. Những quy tắc đạo đức trên đây không chỉ là nỗ lực ban đầu trong việc văn bản hóa chuẩn mực đạo đức nghề nghiệp cho những người làm trong lĩnh vực bảo vệ thông tin, mà chúng cần được quy định chính thức cho các tổ chức ứng cứu sự cố máy tính, giám sát an toàn mạng, cung cấp dịch vụ ATTT. Đó là một trong những yếu tố đảm bảo rằng thành viên của đội sẽ thực hiện chức năng của mình một cách vô tư, công bằng.

# Hệ thốngtiêu chuẩn an toàn thông tin

## Giới thiệu hệ thốngtiêu chuẩn ISO/IEC 27000 về quản lý an toàn thông tin

Một trong các biện pháp phòng ngừa được nhắc đến trong thời gian qua chính là triển khai áp dụng Hệ thốngQuản lý An toàn Thông tin (ISMS: Information Security Management System) theo các nguyên tắc của bộ tiêu chuẩn quốc tế ISO 27000. Có thể nói rằng, ISO 27000 là một phần của hệ thông quản lý chung trong tổ chức, được thực hiện dựa trên nguyên tắc tiếp cận các rủi ro trong hoạt động, để thiết lập, áp dụng, thực hiện, theo dõi, xem xét, duy trì và cải tiến đảm bảo an toàn thông tin của tổ chức.

Cho tới nay, việc áp dụng hệ thốngquản lý an toàn thông tin phù hợp ISO 27000 đã được triển khai rộng khắp ở hầu hết các quốc gia trên thế giới đặc biệt là trong lĩnh vực tài chính ngân hàng. Tại Việt Nam, một số ngân hàng cũng đang triển khai áp dụng hệ thốngnày và bước đầu đã có được những kết quả nhất định.

Xét về lịch sự hình thành của bộ tiêu chuẩn, ISO 27000 cũng có nguồn gốc từ Anh quốc. Bắt đầu vào năm 1992, Phòng Thương mại và Công nghiệp Anh (UK Department Trade and Industrial) ban hành ra qui phạm thực hành về hệ thốngan toàn thông tin dựa trên các hệ thốngđảm bảo an toàn thông tin nội bộ của các công ty dầu khí. Tài liệu này sau đó được Viện tiêu chuẩn hoá Anh chính thức ban hành thành tiêu chuẩn quốc gia với mã hiệu BS 7799-1 vào năm 1995. Năm 2000, tiêu chuẩn này được Tổ chức Tiêu chuẩn hoá Quốc tế (ISO) chính thức chấp nhận và ban hành với mã hiệu ISO/IEC 17799:2000 - tiền thân của bộ tiêu chuẩn ISO 27000 ngày nay.

Bộ tiêu chuẩn ISO 27000 đã và sẽ bao gồm những tiêu chuẩn cụ thể sau:

- ISO 27000 quy định các vấn đề về từ vựng và định nghĩa (thuật ngữ)

- ISO 27001:2005 xác định các yêu cầu đối với hệ thốngquản lý an toàn thông tin

- ISO 27002:2007 đưa ra qui phạm thực hành mô tả mục tiêu kiểm soát an toàn thông tin một các toàn diện và bảng lựa chọn kiểm soát thực hành an toàn tốt nhất

- ISO 27003:2007 đưa ra các hướng dẫn áp dụng

- ISO 27004:2007 đưa ra các tiêu chuẩn về đo lường và định lượng hệ thốngquản lý an toàn thông tin để giúp cho việc đo lường hiệu lực của việc áp dụng ISMS

- ISO 27005 tiêu chuẩn về quản lý rủi ro an toàn thông tin

- ISO 27006 tiêu chuẩn về hướng dẫn cho dịch vụ khôi phục thông tin sau thảm hoạ của công nghệ thông tin và viễn thông

Trong các tiêu chuẩn trên, ISO/IEC 27001: 2005 chính là những yêu cầu bắt buộc đối với Tổ chức khi xây dựng, vận hành và duy trì ISMS, và cũng là cơ sở để các tổ chức tư vấn, đánh giá quản lý chất lượng thực hiện công việc chuyên môn của mình. Các tiêu chuẩn khác trong bộ ISO/IEC 27000 được coi như những công cụ hỗ trợ phục vụ cho tiêu chuẩn ISO/IEC 27001:20005. Trong tương lai gần, sẽ có thêm nhiều tiêu chuẩn hướng dẫn áp dụng Hệ thốngquản lý an ninh thông tin cho một số ngành có mức độ rủi ro cao như viễn thông, y tế....

Về cấu trúc, tiêu chuẩn ISO/IEC 27001:2005 bao gồm các yêu cầu được sắp xếp theo trật tự các điều khoản như: 4. Hệ thốngquản lý an ninh thông tin; 5. Trách nhiệm lãnh đạo; 6. Đánh giá nội bộ ISMS; 7. Xem xét lãnh đạo ISMS; 8. Cải tiến ISMS.

Yêu cầu áp dụng 11 mục tiêu kiểm soát (được cụ thể hóa ở các mục của phụ lục A) của Tiêu chuẩn bao gồm: A.5 Chính sách An ninh; A.6 An ninh thông tin của Tổ chức; A.7 Quản lý tài sản; A.8 An ninh nhân lực; A.9 An ninh vật lý và môi trường; A.10 Quản lý các tác nghiệp và truyền thông; A.11 Kiểm soát truy cập; A.12 Duy trì và phát triển các hệ thống; A.13 Quản lý sự cố An ninh thông tin; A.14 Quản lý tính liên tục trong kinh doanh; A.15 Sự tuân thủ.

Về nội dung, trọng tâm của ISMS yêu cầu quản lý rủi ro đối với toàn bộ tài sản của Tổ chức nhằm đảm bảo quá trình kinh doanh liên tục và tuân thủ các chế định và pháp định quốc gia, quốc tế. Trong đó, 3 nhóm tài sản được kiểm soát ở mức độ cao nhất là tài sản thông tin, tài sản con người, tài sản vật lý. Việc kiểm soát các tài sản của Tổ chức phải được thực hiện theo yêu cầu 11 mục tiêu kiểm soát và phải được Tổ chức cam kết qua Bản công bố áp dụng.

ISO/IEC 27001:2005 yêu cầu áp dụng mô hình PDCA để kiến trúc nên mọi quá trình kiểm soát trong ISMS đáp ứng những mong đợi của Tổ chức và các bên quan tâm tới hoạt động sản xuất – kinh doanh của Tổ chức

Cam kết xây dựng Hệ thống ISMS. Đại diện lãnh đạo An ninh thông tin (Giám đốc An ninh thông tin) là lãnh đạo cao nhất của Tổ chức. Đây là yếu tố quyết định sự thành công của ISMS và là một bằng chứng cho khách hàng và các bên quan tâm biết về việc thực hiện những cam kết của Tổ chức thiết lập, duy trì, xem xét và cải tiến ISMS.

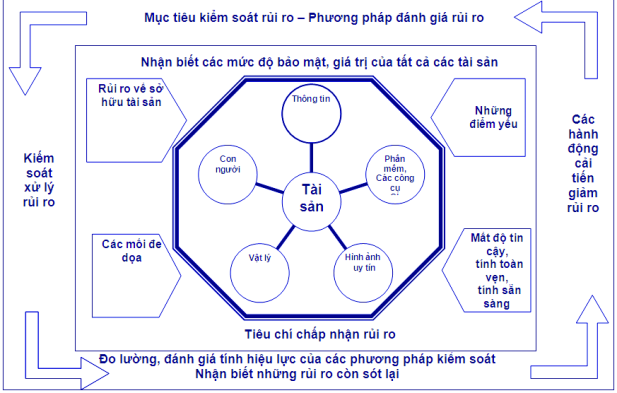
Xác định phạm vi, giới hạn áp dụng ISMS: Đây là công việc đầu tiên quá trình xây dựng ISMS. Tùy thuộc vào quy mô và sự phức tạp của hoạt động sản xuất, kinh doanh và cung cấp dịch vụ mà Tổ chức xác định phạm vi áp dụng, số lượng địa điểm áp dụng cũng như lộ trình triển khai áp dụng ISMS phải đảm bảo những yêu cầu cơ bản sau:

- Phù hợp với yêu cầu chế định và pháp định, yêu cầu của khách hàng về kiểm soát an ninh thông tin.

- Phù hợp với đặc điểm nguồn nhân lực và tiềm lực tài chính.

- Thực hiện được những cam kết của Tổ chức với các bên quan tâm.

Xây dựng chính sách ISMS. Chính sách an ninh thông tin là văn bản công bố những cam kết lâu dài trong việc thực hiện và duy trì ISMS của Tổ chức tới các bên quan tâm. Chính sách ANTT được từng bước thực hiện thông qua việc thực hiện các mục tiêu kiểm soát và các hoạt động kiểm soát ISMS của Tổ chức.



*Hình 3.1. Thiết lập, thực hiện vận hành ISMS*

Xác định tài sản và giá trị tài sản, nhận biết rủi ro, phân tích – lượng hóa rủi ro, đánh giá rủi ro và lựa chọn các phương án xử lý rủi ro đối với tài sản của Tổ chức: Liệt kê tất cả các tài sản, xác định giá trị, những rủi ro xuất hiện (rủi ro về sở hữu tài sản, những điểm yếu, các mối đe đọa, mất độ tin cậy, tính toàn vẹn, tính sẵn sàng), xây dựng các biện pháp kiểm soát, đo lường, đánh giá tính hiệu lực của các phương pháp kiểm soát, nhận biết những rủi ro còn sót lại theo yêu cẩu ISO/IEC 27001:2005 là

những hạng mục công việc quan trọng nhất nhưng cũng khó khăn và phức tạp nhất trong toàn bộ quá trình xây dựng ISMS. Tùy thuộc vào phạm vi áp dụng, vào đặc điểm ngành sản xuất, kinh doanh, cung cấp dịch vụ mà các mức độ rủi ro đối với các nhóm tài sản thông tin, con người và vật lý ở mỗi Tổ chức là khác nhau. Kinh nghiệm của những đơn vị áp dụng hiệu quả ISMS cho thấy:

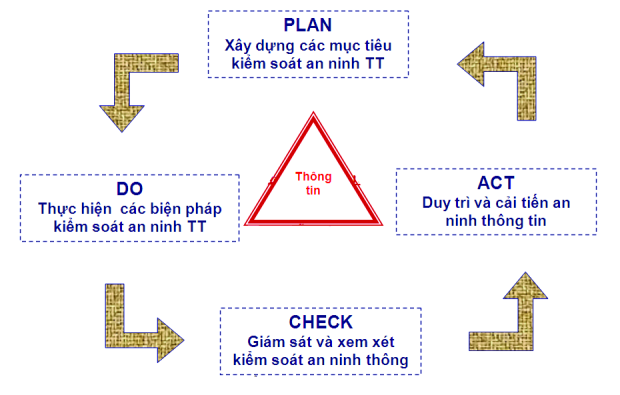
- Mọi quy trình kiểm soát trong ISMS tuân thủ mô hình PDCA. Hình 2 minh họa cho quy trình kiểm soát tài sản thông tin đảm bảo tính bảo mật, tính toàn vẹn và tính sẵn sàng theo mô hình PDCA.

- Sử dụng các công cụ trong bộ tiêu chuẩn ISO/IEC 27000 có hiệu quả như áp dụng tiêu chuẩn ISO/IEC 27005: 2007 để quản lý rủi ro, tiêu chuẩn ISO/IEC 27004: 2007 để đo lường ISMS.

- Tập trung đầu tư hạ tầng kỹ thuật, công nghệ để giảm rủi ro từ những mối đe dọa. Ví dụ: xây dựng các vành đai an ninh vật lý – môi trường, các giải pháp công nghệ bảo vệ cơ sở dữ liệu (các biện pháp kiểm soát quyền truy cập – các phần mềm ngăn chặn quyền truy cập trái phép, chống truy cập từ bên ngoài, các phần mềm mã hóa cơ sở dữ liệu, xác thực người dùng, chữ ký điện tử hoặc chứng thực điện tử, kiểm soát các thiết bị ngoại vi...).

- Thực hiện có hiệu quả những cam kết những chính sách an ninh thông tin.

Xây dựng 11 mục tiêu kiểm soát và các kiểm soát theo yêu cầu phụ lục A của tiêu chuẩn để thực hiện chính sách an ninh thông tin và những cam kết của lãnh đạo đơn vị. Thiết lập hệ thốngcác quy trình, hướng dẫn công việc, lưu hồ sơ theo yêu cầu tiêu chuẩn. Đào tạo nguồn nhân lực để thực hiện, vận hành, giám sát, xem xét, duy trì và cải tiến ISMS. Đây là giai đoạn tốn nhiều thời gian, công sức của các đơn vị, nó thể hiện trí tuệ của cả một Tổ chức.



*Hình 3.2. Quy trình thiết lập và vận hành hệ thống ISMS*

Đạt được giấy chứng nhận ISO/EC 2700/:2005 là giai đoạn xác định mức độ thành công đối với hệ thốngquản lý ANTT theo yêu cầu ISO/IEC 27001:2005

## Vấn đề kiểm định và đánh giá mức độ an toàn thông tin.

### Khái niệm đánh giá an toàn hệ thốngthông tin

Hầu như trong bất kỳ hệ thốngmạng nào cũng đều có điểm yếu mà kẻ tấn công có thể lợi dụng để thực hiện tấn công chiếm quyền điều khiển hệ thống, đánh cắp dữ liệu hoặc cài cắm các chương trình có hại. Các điểm yếu này xuất phát từ các phiên bản hệ điều hành, ứng dụng khi phát triển, người quản trị cấu hình chưa chặt chẽ hoặc do người sử dụng không tuân thủ đúng theo các chính sách an ninh. Chính vì thế, kịp thời phát hiện ra các sơ hở tồn tại trong hệ thốnglà rất quan trọng bởi vì nhờ thế mà người quản trị có thể có thể kịp thời đưa ra các giải pháp sơ hở trước khi bị hacker lợi dụng tấn công. Để làm được việc này, chúng ta cần phải thực hiện đánh giá an toàn cho hệ thống(gọi khác đi là kiểm thử an toàn cho hệ thống)

Theo NIST, đánh giá an toàn hệ thốngthông tin (Information Security Assessment) là quy trình xác định các đối tượng (ví dụ: máy tính, hệ thống, mạng, quy trình vận hành, con người) có đáp ứng các yêu cầu bảo mật hay không. Quy trình này tập trung vào 3 phương pháp là: thử nghiệm, kiểm tra và phỏng vấn. Thử nghiệm là quá trình thực hiện giám định một hoặc nhiều đối tượng theo điều kiện quy định để so sánh kết quả thực tế với dự kiến​​. Kiểm tra là quá trình xem xét, quan sát, kiểm tra hoặc phân tích để làm rõ, khẳng định và lấy bằng chứng. Phỏng vấn là quá trình tiến hành các cuộc thảo luận với các cá nhân hoặc các nhóm trong một tổ chức để tìm hiểu, xác định vị trí của các đối tượng liên quan tới an toàn thông tin.

Để có thể xác định điểm yếu trong hệ thống, người đánh giá cần tiến hành các kiểm tra an ninh tới hệ thống. Có 2 phương pháp thường sử dụng để thực hiện kiểm tra an ninh là quét lỗ hổng (Vulnerability Scanner) và thực hiện xâm nhập. Quét lỗ hổng là quá trình tìm những điểm yếu, lỗ hổng an ninh trong mạng. Ý tưởng cơ bản của phương pháp này là quét toàn bộ nút mạng và cổng có trên từng nút mạng, sau đó với thông tin nhận được sẽ phân tích và đánh giá hệ thốngan toàn như thế nào. Thuật ngữ “đánh giá lỗ hổng” được sử dụng trong trường hợp quét lỗ hổng có nghĩa là quá trình tìm kiếm những dấu hiệu đã biết của lỗ hổng bên trong hoặc bên ngoài một mạng. Quá trình này sẽ xác định lỗ hổng để có thể loại bỏ trước khi nó bị chương trình độc hại hoặc tin tặc khai thác. Trong hầu hết trường hợp, các lỗ hổng đều được biết và do đó có thể được tìm thấy. Các lỗ hổng tạo thành mối đe dọa trong mạng bao gồm lỗi phần mềm, dịch vụ không cần thiết, cấu hình sai hoặc tài khoản người dùng không an toàn, … Có một thực tế là những lỗ hổng đơn lẻ có nguy cơ về an ninh không cao nhưng khi tồn tại chung trong một hệ thốngcó thể trở thành lỗ hổng lớn, gây ra những nguy cơ về rủi ro an ninh rất cao. Thực hiện xâm nhập đi xa hơn so với quét lỗ hổng, nó tập trung vào quá trình khai thác, lợi dụng các lỗ hổng, điểm yếu nhằm thử xâm nhập, leo thang đặc quyền, duy trì truy cập vào hệ thốngmục tiêu, hoặc tìm ra sự tồn tại tương hỗ của các lỗ hổng trên một hoặc nhiều hệ thốngđể tạo ra sự truy cập vào hệ thốngmà thường khó đạt được khi khai thác những lỗ hổng đơn lẻ.

### Khái niệm kiểm định an toàn hệ thốngthông tin

Đánh giá an toàn hệ thốngthông tin là một phần trong quá trình đảm bảo an toàn cho hệ thốngthông tin. Kết quả của quá trình đánh giá an toàn thông tin là đưa ra một danh sách các kết quả về các lỗ hổng tồn tại trong hệ thốngvà hướng khắc phục để từ đó người quản trị có thể biết được hiện trạng hệ thốngmạng và sửa chữa lỗ hổng. Tuy nhiên để có thể chứng minh hệ thốngđã đảm bảo an toàn theo các tiêu chí đề ra thì cần thực hiện kiểm định, nhằm khẳng định các biện pháp đảm bảo an toàn là đầy đủ và chính xác.

Kiểm định an toàn hệ thốngthông tin (Information Security Audit) là quá trình kiểm toán về mức độ an ninh thông tin trong một tổ chức để đảm bảo các đối tượng trong hệ thốngđược áp dụng đầy đủ, chính xác và cập nhật các giải pháp an toàn. Việc kiểm toán này dựa trên một tiêu chuẩn nhất định, tiêu chuẩn đó vừa phù hợp với tiêu chí đặt ra của tổ chức vừa là căn cứ để kiểm tra đánh giá. Nếu tổ chức đạt được các yêu cầu theo quy định, tổ chức sẽ được cấp chứng nhận về kiểm định và chứng nhận này có giá trị trong phạm vi cả nước.

Hiện nay trên thế giới, tiêu chuẩn được áp dụng rộng rãi trên thế giới để kiểm định an toàn hệ thốngthông tin là bộ tiêu chuẩn ISO 27001:2005. Tại Việt Nam, tiêu chuẩn này đã được dịch ra áp dụng làm tiêu chuẩn quản lý an toàn thông tin, tuy nhiên đến thời điểm hiện tại vẫn chưa có phiên bản chính thức.

### Phân biệt đánh giá và kiểm định an toàn hệ thốngthông tin

Từ các khái niệm ở trên, chúng ta cũng có thể thấy rõ sự khác nhau giữa “Đánh giá” và “Kiểm định” an toàn hệ thốngthông tin. Đánh giá là quá trình kiểm tra xác định các lỗ hổng, điểm yếu với mục đích tìm ra lỗi để kịp thời sửa chữa, giúp cho hệ thốngan toàn hơn. Kiểm định cũng thực hiện các hành động kiểm tra, tuy nhiên để đánh giá kết quả đạt được so với mục tiêu đặt ra ban đầu. Ngoài ra, việc đánh giá được thực hiện bởi một cá nhân, một nhóm hoặc một tổ chức và chỉ cần thống nhất giữa các bên liên quan; còn việc kiểm định phải do một cơ quan có thẩm quyền, được nhà nước cho phép mới có thể thực hiện.

Hiện tại ở Việt Nam có rất nhiều các cơ quan tổ chức có thể thực hiện đánh giá an toàn thông tin, tuy nhiên mới chỉ có QUACERT – Trung tâm chứng nhận phù hợp – trực thuộc Tổng cục Tiêu chuẩn Đo lường Chất lượng là có thể thực hiện kiểm định an toàn thông tin và cấp chứng nhận theo tiêu chuẩn ISO 27001.

# Nhận biết các nguy cơ mất an toàn thông tin

## Khái niệm các hiểm họa an toàn thông tin

Hiểm hoạ ATTT của hệ thốngcông nghệ thông tin là những khả năng tác động lên thông tin được xử lý trong hệ thốngvà dẫn tới sự biến dạng, huỷ diệt, sao chép, sự ngăn chặn tiếp cận tới thông tin; là khả năng tác động tới các thành phần của hệ thốngdẫn tới sự mất mát, sự phá huỷ hoặc sự ngừng trệ hoạt động của vật mang thông tin, các thiết bị tương tác với vật mang hoặc các thiết bị điều khiển chúng.

## Các hiểm họa điển hình gây mất an toàn thông tin

Như trên đã phân tích, khi xuất hiện một hệ thốngnào đó, trong môi trường địa lý tự nhiên và môi trường xã hội có rất nhiều các yếu tố tác động vào hệ thống và các thông tin được xử lý trong hệt hống đó. Đặc biệt trong xã hội hiện đại, có rất nhiều người quan tâm tới các thông tin chứa trong hệ thống đó. Nghĩa là tồn tại rất nhiều các hiểm hoạ ATTT đối với mỗi hệ thống bất kỳ.

Ngày nay người ta đã khảo sát được rất nhiều loại hiểm hoạ ATTT đối với hệ thống, danh mục các hiểm hoạ như vậy có tới hàng trăm. Các hiểm hoạ hay xảy ra và thường gặp điển hình là:

* + Sao chép (copy) bất hợp pháp các vật mang thông tin.
  + Thao tác không thận trọng dẫn đến giải mật các thông mật hoặc là làm lộ các thông mật.
  + Bỏ qua (không tuân thủ) các quy tắc tổ chức (đã được xác lập) khi làm việc với thông tin của hệ thống

Để vạch ra được các yêu cầu ATTT đối với việc bảo vệ hệ thống, trước hết phải tiến hành phân tích hiểm hoạ của hệ thống . Phải liệt kê được danh mục các hiểm hoạ; đánh giá được xác suất thực hiện của chúng; cần xác định được mô hình kẻ phá hoại. Đó chính là nội dung cơ bản của phân tích hiểm hoạ hệ thống. Ngoài việc làm rõ các hiểm hoạ có thể, cần phải tiến hành phân tích chúng trên cơ sở phân loại theo các dấu hiệu, mà mỗi dấu hiệu sau đó sẽ phản ánh một trong những yêu cầu tổng quát đối với hệ bảo vệ thông tin. Các hiểm hoạ cùng loại (cùng tương ứng với một dấu hiệu) sẽ cho phép chi tiết hoá yêu cầu tổng quát nói trên đối với mỗi dấu hiệu phân loại.

**Phân loại các hiểm hoạ.**

Sự cần thiết phải phân loại các hiểm hoạ ATTT đối với một hệ thống là do những điều kiện khách quan sau đây: Kiến trúc của các thiết bị xử lý thông tin hiện đại, thiết kế về tổ chức, về cấu tạo, về chức năng hoạt động của các trung tâm máy tính và các mạng; công nghệ và điều kiện xử lý tự động các thông tin hiện nay ở trong trạng thái mà thông tin, tích luỹ, lưu giữ và xử lý trong đó phải chịu các ảnh hưởng ngẫu nhiên của cực kỳ nhiều các yếu tố, đến mức không thể nào đặt ra được bài toán miêu tả toàn bộ tập hợp các hiểm hoạ đối với mỗi hệ thống. Cho nên, đối với hệ bảo vệ, người ta thực hiện việc xác định không phải danh mục đầy đủ các hiểm hoạ, mà chỉ là danh mục các lớp hiểm hoạ mà thôi.

Phân loại các hiểm hoạ ATTT của một hệ thống có thể thực hiện theo loạt các dấu hiệu cơ bản sau đây:

1. Theo bản chất xuất hiện.
   * Các hiểm hoạ tự nhiên: Đó là các hiểm hoạ do sự tác động lên hệ thống và các thành phần, của các quá trình vật lý khách quan hoặc các hiện tượng thiên tai ngẫu nhiên, không phụ thuộc vào con người.
   * Các hiểm hoạ nhân tạo: Đó là các hiểm hoạ ATTT đối với hệ thống gây ra bởi hoạt động của con người.
     1. Theo mức độ định trước.
   * Hiểm hoạ của hành động ngẫu nhiên và/hoặc hiểm hoạ sinh ra do các lỗi hoặc sự bất cẩn của nhân viên.
   * Hiểm hoạ từ các hành động cố ý định trước (kẻ xấu đánh cắp thông tin).
     + - 1. Theo nguồn trực tiếp sinh ra.
   * Nguồn sinh trực tiếp là môi trường tự nhiên: như thiên tai, bão tố, phóng xạ….
   * Nguồn sinh trực tiếp là con người: cài cắm nội gián, mua chuộc, sao chụp trộm…
   * Nguồn sinh là các phần mềm hợp pháp: Khi chạy chương trình làm việc mà gây nên treo máy hoặc gây ra các biến đổi trong cấu trúc dữ liệu.
   * Nguồn sinh là các phần mềm bất hợp pháp: như virus, ngựa Troa, bom logic…

Theo vị trí của nguồn sinh ra.

* + Nguồn sinh nằm ngoài lãnh thổ kiểm soát nơi đặt hệ thống như : thu trộm các bức xạ thấp như điện từ âm thanh từ các thiết bị và đường dây hoặc thu và khuyếch đại các bức xạ tích cực từ các thiết bị phụ trợ không trực tiếp tham gia quá trình xử lý thông tin (đường điện thoại, đường điện nuôi, lò sưởi…).
  + Nguồn sinh nằm ngay trong lãnh thổ kiểm soát (toà nhà đặt máy) như: ăn cắp rác thải công nghệ (giấy viết, giấy nháp có chứa thông tin), các thiết bị nghe trộm, cháy nổ…
  + Nguồn sinh có tiếp cận tới thiết bị đầu cuối.
  + Nguồn sinh đặt ngay trong hệ thống: ví dụ, thiết kế cài đặt các thiết bị, các chương trình lấy cắp, phá hoại… Sử dụng không đúng các tài nguyên.

Theo mức độ phụ thuộc vào hoạt động của hệ thống thông tin.

* + Không phụ thuộc vào hoạt động của hệ thống: ví dụ công phá mật mã bảo vệ, ăn cắp các vật mang tin (đĩa từ, bộ nhớ, băng từ…).
  + Chỉ xuất hiện trong quá trình tự động xử lý thông tin: như hoàn thành và tán phát các chương trình vi rút…
  1. Theo mức độ tác động lên hệ thống.
  + Hiểm hoạ thụ động không làm thay đổi gì về cấu trúc và nội dung hệ thống: ví dụ sao chụp các dữ liệu mật.
  + Hiểm hoạ tích cực gây ra những thay đổi nhất định trong cấu trúc và nội dung của hệ thống: ví dụ các bẫy, các vi rút, ngựa Troa, bọ, rệp… làm biến dạng thông tin …
    - 1. Theo các giai đoạn tiếp cận của người dùng hoặc các chương trình tới các tài nguyên hệ thống.
  + Thể hiện khi thực hiện tiếp cận tài nguyên hệ thống: ví dụ tiếp cận trái phép tới hệ thống.
  + Thể hiện sau khi được phép tiếp cận tới hệ thống: ví dụ sử dụng trái phép hoặc sai tài nguyên hệ thống…

Theo phương pháp tiếp cận tới các tài nguyên hệ thống.

* + Sử dụng con đường chuẩn thông thường tiếp cận tài nguyên: ví dụ lợi dụng mật khẩu, giả danh người dùng…
  + Sử dụng các phương tiện ngầm (không chuẩn): qua mặt các thiết bị kiểm soát, chọc thủng hệ điều hành hệ thống….

Theo nơi cư trú hiện tại của thông tin được lưu giữ và xử lý trong hệ thống.

* + Tiếp cận thông tin tại các bộ nhớ ngoài (sao chép trộm từ ổ đĩa cứng).
  + Tiếp cận thông tin tại vùng nhớ hoạt động (ROM, RAM): ví dụ đọc thông tin từ vùng nhớ dành cho hệ điều hành hoặc thiết bị bảo vệ…
  + Tiếp cận thông tin đang đi lại trên các đường liên lạc: ví dụ trích đường liên lạc để biến đổi thông tin, ăn trộm danh tính người dùng để mạo nhận, đánh lừa xác thực, chiếm đoạt thông tin đường truyền…
  + Tiếp cận thông tin phản xạ từ terminal, hoặc trên máy in: ví dụ ghi các thông tin phản xạ vào một camera mật…

## Kỹ thuật tấn công Social engineering

### Tấn công lừa đảo dựa vào các kỹ thuật về con người (Human-based)

Kiểu tấn công lừa đảo dựa vào các kỹ thuật về con người (Human-based) là kiểu tấn công thực hiện các kỹ thuật thu thập thông tin nhạy cảm bằng cách tấn công tương tác trực tiếp với nạn nhân, khai thác các yếu tố về lòng tin, sự sợ hãi và nhu cầu giúp đỡ người khác một cách tự nhiên của con người. Ví dụ như một kẻ tấn công lừa những nhân viên mới đến làm việc hoặc trong giai đoạn thử việc rằng hắn ta là cấp trên, lãnh đạo và yêu cầu nhân viên mới này để hắn truy cập vào hệ thống. Hoặc là gọi điện thoại giả là một khách hàng bị quên mất mật khẩu, yêu cầu được giúp đỡ để lấy lại mật khẩu...

Sau đây là các kỹ thuật tấn công lừa đảo dựa vào các kỹ thuật về con người.

**Mạo danh làm 1 người dùng cuối hợp lệ:** Mạo danh là nhân viên hoặc người dùng hợp lệ. Trong kỹ thuật này, kẻ tấn công sẽ giả dạng thành nhân viên công ty hoặc người dùng hợp lệ của hệ thống. Kẻ tấn công mạo danh mình là người gác cổng, nhân viên, đối tác, để đột nhập công ty. Một khi đã vào được bên trong, chúng tiến hành thu thập các thông tin từ thùng rác, máy tính để bàn, hoặc các hệ thống máy tính, hoặc là hỏi thăm những người đồng nghiệp.

Ví dụ: "Xin chào! tôi là John, từ chi nhánh X. Tôi quên mất mật khẩu của mình. Tôi có thể nhận lại nó được ko ?”

**Mạo danh làm 1 người dùng quan trọng:** Đóng giả làm một người quan trọng của một công ty khách, khách hàng tiềm năng... Kẻ tấn công sẽ giả mạo là một người trong vai trò của một người sử dụng quan trọng như người quản lý cấp cao, trưởng phòng, hoặc những người cần trợ giúp ngay lập tức, kẻ tấn công có thể dụ dỗ người dùng cung cấp cho chúng mật khẩu truy cập vào hệ thống.

Ví dụ: "Xin chào! tôi là Kevin, Thư ký của giám đốc điều hành. Tôi đang làm việc ở một dự án cực kỳ cấp bách và tôi bị mất mật khẩu trong hệ thống. Bạn có thể giúp tôi ko?”

**Mạo danh làm một nhân viên hỗ trợ kỹ thuật:** Trong kỹ thuật này, kẻ tấn công mạo danh thành 1 nhân viên hỗ trợ kỹ thuật của tổ chức để tiếp xúc với khách hàng và cố gắng yêu cầu khách hàng cung cấp các thông tin nhạy cảm. Đa số nạn nhân sẽ dễ dàng cung cấp các thông tin nhạy cảm vì nghĩ rằng đây là một trong những quy trình làm việc của tổ chức và tổ chức này chẳng có lý do gì để sử dụng các thông tin của mình vào các công việc gây hại cả. Đây là một trong những tâm lý thiếu an toàn rất phổ biến hiện nay, nhất là ở Việt Nam thì mức độ hiểu biết và vận dụng quyền cá nhân của người dân vẫn còn chưa tốt.

Ví dụ: "Thưa ông, tôi là Mathew, hỗ trợ kỹ thuật của công ty X. Tối qua chúng tôi có một sự cố hệ thống ở đây, và chúng tôi đang kiểm tra những dữ liệu cuối cùng. Ông có thể gửi tôi ID và Password của ông không?”

**Mạo danh làm người thứ ba được ủy quyền bởi một người hay tổ chức nào đó:** Lấy danh nghĩa được sự cho phép hoặc ủy quyền của một người nào đó để truy cập vào hệ thống. Thông thường thì kẻ tấn công giả mạo là một người được ủy quyền bởi một người quan trọng, có địa vị cao và có sức ảnh hướng lớn tới nạn nhân, như thế sẽ gây được áp lực và nhận được sự nể trọng, nhún nhường của nạn nhân, thậm chí nạn nhân có thể sẽ bỏ qua các thủ tục và chính sách thông thường của tổ chức để thực hiện yêu cầu của người này.

Ví dụ: Xin chào! tôi là John Brown. Tôi với các kiểm toán viên bên ngoài của Arthur Sanderson. Chúng tôi được mời tới tổ chức bạn để thanh tra đột xuất về thủ tục khôi phục thảm họa của tổ chức bạn. Chi nhánh của bạn có 10 phút để chỉ cho tôi cách làm sao để các bạn khôi phục một trang web bị hỏng. Chúng ta hãy bắt đầu ngay bây giờ.

**Nghe trộm:** Trong kỹ thuật này, kẻ tấn công sẽ nghe trộm, nghe lén các cuộc hội thoại hoặc lén đọc các tin nhắn của nạn nhân, chặn bắt bất cứ dạng thông tin nào như Audio, Video hoặc là các bản viết tay…Hơn nữa, kẻ tấn công có thể sử dụng các kênh giao tiếp như là đường dây điện thoại, thư điện tử, các tin nhắn nhanh... để thu thập thông tin cần thiết cho mục đích của chúng.

**Nhìn trộm:** Nhìn trộm hay nôm na là nhìn qua vai là tên nói về một hành động của một kẻ trộm sử dụng để tìm hiểu mật khẩu, số định danh , số tài khoản của cá nhân nào đó. Kẻ trộm sẽ nhìn qua vai hoặc quan sát ở khoảng cách với một chiếc ống nhóm, thực hiện điều này nhằm lấy được các mẩu thông tin của nạn nhân như mật khẩu, mã PIN, các bản thiết kế…

**Bới rác:** Bới rác là hành động nhằm thu thập thông tin bằng cách cố gắng moi móc thùng rác của một người hay một tổ chức để thu được các thông tin cần thiết thông qua những vật liệu mang tin bị vứt bỏ trong thùng rác như giấy in, ảnh, hồ sơ, hóa đơn, chìa khóa, các vật lưu lại dấu vân tay, các vật lưu lại ADN như tóc, nước bọt, máu, da… , các thiết bị lưu trữ thông tin như đĩa mềm, đĩa CD/DVD, ổ cứng… , sau đó kẻ tấn công có thể sử dụng các kỹ thuật tái tạo, dán ghép các mảnh tài liệu bị hủy để trích xuất thông tin chứa trong đó.

Các thông tin có thể thu thập được bao gồm:

*- Hóa đơn điện thoại*

*- Thông tin liên lạc*

*- Thông tin tài chính*

*- Chiến lược kinh doanh*

*- Thông tin hoạt động của tổ chức*

*- Các văn bản, hợp đồng, con dấu...*

*- Thư từ, công văn, chữ ký…*

**Theo đuôi:** Một người dùng bất hợp pháp đeo một cái bảng định danh giả, đi vào một vùng được đảm bảo an ninh chặt chẽ bằng cách theo sau một người hoặc nhóm người có thảm quyền hợp lệ thông qua những cánh cửa mà nó yêu cầu khóa truy cập.

Ví dụ: Kẻ tấn công đeo một chiếc thẻ giả đi theo sau một người dùng hợp lệ đi đến một cánh cổng kiểm tra quyền ra vào bằng cách quẹt thẻ. Khi người dùng hợp lệ kia quẹt thẻ và được chấp nhận đi vào thì cánh cổng được mở ra để cho người dùng hợp lệ đi vào, kẻ tấn công sẽ đi ngay sau và cũng giả vờ quẹt thẻ vào thiết bị, tuy không hợp lệ nhưng kẻ tấn công cùng một lúc đi vào với người dùng hợp lệ kia mà cánh cửa chưa kịp đóng lại. Bằng cách đó kẻ tấn công đã đi vào được trong hệ thống trông giống như là một người dùng hợp lệ, cả người quan sát camera theo dõi cũng khó mà phát hiện ra được.

**Giúp đỡ kẻ ngốc (PiggyBacking):** Một người được ủy quyền cung cấp quyền truy cập tới một người không có thẩm quyền bằng cách mở cửa an ninh giúp anh ta.

Ví dụ: "Tôi bỏ quên thẻ ra vào của tôi ở nhà rồi, anh giúp tôi nhé”

**Tấn công lừa đảo ngược:**Trong kỹ thuật này, kẻ tấn công sẽ ngầm phá hoại một phần nào đó trong cơ sở vật chất của tổ chức, sau đó hắn ta sẽ mạo danhmột người xuất hiện trong vị trí của một nhân viên sửa chữa, hỗ trợ kỹ thuật để khắc phục hư hỏng mà hắn vừa phá hoại để được trao quyền đi vào trong và truy cập tài nguyên của tổ chức.

Tấn công lừa đảo ngược bao gồm các bước:

*- Bước 1: Ngầm phá hoại một phần nào đó trong cơ sở vật chất của tổ chức.*

*- Bước 2: Tiếp thị các giải pháp sửa chữa, khắc phục hư hỏng mà hắn vừa phá hoại.*

*- Bước 3: Mạo danh hỗ trợ kỹ thuật giúp sửa chữa hư hỏng hắn tạo ra và lấy được quyền đi vào trong hệ thống.*

Ví dụ: Tấn công, cài virus vào máy tính nạn nhân rồi tiếp thị phần mềm diệt virus, tiện thể cài trojan vào và đánh cắp thông tin.

### Tấn công lừa đảo dựa vào các kỹ thuật máy tính (Computer-based)

Kiểu tấn công lừa đảo dựa vào các kỹ thuật máy tính (Computer-based) là kiểu tấn công thực hiện các kỹ thuật thu thập thông tin nhạy cảm bằng cách sủ dụng sự giúp đỡ của các chương trình máy tính, mạng máy tính, mạng điện thoại…Ví dụ như sử dụng lỗi XSS trên máy chủ và gửi cho người dùng một đường dẫn siêu liên kết đến trang của ngân hàng nhưng lại chuyển hướng sang hiển thị trang web của kẻ tấn công giống hệt ngân hàng để thu thập tài khoản và mật khẩu...

Sau đây là các kỹ thuật tấn công lừa đảo dựa vào các kỹ thuật máy tính.

**Cửa sổ nhảy (Pop-up):**

Các cửa sổ đột nhiên xuất hiện khi lướt web trên mạng internet và yêu cầu thông tin của người dùng để đăng nhập. Pop-ups đánh lừa các người dùng nhấn vào các siêu liên kết mà chuyển hướng họ sang một trang web giả mạo yêu cầu thông tin cá nhân, hoặc tải về các chương trình độc hại như là Keyloggers, Trojans, Spyware…

**Thư lừa đảo cảnh báo (Hoax Letters):** Thư lừa đảo là các thư điện tử gửi cảnh báo cho người dùng về các loại virus, Trojan, worm mới mà nó có thể gây hại cho máy của người dùng. Trong trường hợp này nạn nhân được thuyết phục tải về và cài đặt các chương trình hay ứng dụng hữu ích như cải thiện hiệu suất của CPU, RAM, hoặc các tiện ích hệ thống hoặc như một crack để sử dụng các phần mềm có bản quyền. Và một Spyware hay Malware ( chẳng hạn như Keylogger) sẽ được cài đặt thông qua một chương trình độc hại ngụy trang dưới một chương trình hợp pháp.

**Thư lừa đảo theo hệ thống hoặc Even (Chain Letters):** Chain Letters là các email mà biếu tặng các món quà miễn phí như là tiền và phần mềm và điều kiện đưa ra là người dùng phải chuyển tiếp thư này đến một số lượng người nhất định.

**Tin nhắn chat nhanh (Instant Chat Messenger):** Thu thập thông tin cá nhân bằng cách tán gẫu với người dùng trực tuyến đã được chọn để lấy thông tin như ngày sinh và tên thật

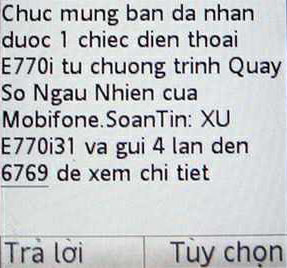
**Thư điện tử rác (Spam Email):** Các thư điện tử không liên quan, không mong muốn và không được yêu cầu được gửi đi để thu thập thông tin tài chính, số an sinh xã hội và các thông tin về mạng

**Phishing:** Thuật ngữ này áp dụng cho một thư điện tử xuất hiện đến từ một công ty kinh doanh, ngân hàng hoặc thẻ tín dụng yêu cầu chứng thực thông tin và cảnh báo sẽ xảy ra hậu quả nghiêm trọng nếu việc này không được làm. Bức thư điện tử thường chứa một đường dẫn đến một trang web giả mạo trông hợp pháp với logo của công ty và nội dung có chứa form để yêu cầu tài khoản, mật khẩu, số thẻ tín dụng hoặc số PIN.

**Vishing:** Thuật ngữ là sự kết hợp của “voice” (gọi điện) và phishing. Đây cũng là một dạng phising, nhưng kẻ tấn công sẽ trực tiếp gọi điện cho nạn nhân thay vì gởi email. Người sử dụng sẽ nhận được một thông điệp tự động với nội dung cảnh báo vấn đề liên quan đến tài khoản ngân hàng. Thông điệp này hướng dẫn họ gọi đến một số điện thoại để khắc phục vấn đề. Sau khi gọi, số điện thoại này sẽ kết nối người được gọi tới một hệ thống hỗ trợ giả, yêu cầu họ phải nhập mã thẻ tín dụng. Và VoIP tiếp tay đắc lực thêm cho dạng tấn công mới này vì giá rẻ và khó giám sát một cuộc gọi bằng Voip.

**Tin nhắn điện thoại (SMS):** Kẻ tấn công sử dụng tín nhắn điện thoại làm công cụ chuyển thông tin lừa đảo tới nạn nhân, trong nội dung kẻ tấn công gửi đi yêu cầu nạn nhân gửi đi thông tin nhạy cảm hoặc thực hiện các thao tác dẫn đến bị lộ thông tin cá nhân. Ngoài ra kẻ tấn công lừa đảo còn dùng biện pháp này để dụ dỗ nạn nhân nhắn tin dịch vụ để chuyển tiền từ tài khoản điện thoại sang cho hắn.

Ví dụ: Tin nhắn SMS lừa đảo tiền trong tài khoản của nạn nhân. Trong những năm gần đây, ở Việt Nam đã nở rộ kiểu lừa đảo thông qua tin nhắn, kẻ lừa đảo gửi các tin nhắn dụ nạn nhân rằng họ may mắn trở thành người được nhận khuyến mại đặc biệt với các món quà giá trị cao. Nạn nhân mắc lừa sẽ làm theo hướng dẫn lừa đảo trong tin nhắn và sẽ mất tiền trong tài khoản điện thoại của họ.



Hình 4.1: Tin nhắn lừa đảo phổ biến xuất hiện trên các

mạng điện thoại ở Việt Nam

## Đánh giá rủi ro internet

An toàn Internet nhằm làm giảm nhẹ các rủi ro do Internet sinh ra. Chuẩn quốc tế ISO 17799 (nay là ISO27001) nhắm đến quản lý các rủi ro đó, được thi hành bằng việc phát triển một chiến lược quản lý và giảm thiểu rủi ro, trong đó bao gồm việc định nghĩa tài sản, nguy cơ, điểm yếu và đo lường rủi ro. Kiểm soát được chọn lựa nhằm phòng tránh, chuyển giao và giảm thiểu rủi ro đến mức độ chấp nhận được. Đánh giá rủi ro an ninh thường bao gồm các bước sau:

**Nhận dạng tài sản thông tin** trong khu vực cần bảo mật: Tài sản có thể là những vật hữu hình, như là phần cứng, hoặc vô hình, như là cơ sở dữ liệu của tổ chức. Theo định nghĩa, tài sản có giá trị đối với tổ chức, vì vậy đòi hỏi sự bảo vệ. Tài sản cần được xác định, và chủ sở hữu phải được định nghĩa. Một giá trị định lượng tương đối cần được xác định cho mỗi tài sản để mức độ quan trọng của tài sản được thiết lập khi rủi ro được định lượng.

**Xác định mối nguy cơ đe dọa đến tài sản** – nguy cơ đe dọa được tạo ra do sự lợi dụng những điểm yếu của tài sản và tạo nên rủi ro. Những mối nguy cơ đe dọa đến mỗi tài sản cần được nhận dạng. Có thể có rất nhiều mối nguy cơ đe dọa đến tài sản, tuy nhiên chỉ nên xem xét đến những mối nguy cơ có tính hiện thực cao. Chỉ có những mối nguy cơ đe dọa có khả năng xảy ra cao, hoặc dẫn đến thiệt hại lớn cần được xem xét. Ví dụ, một mối nguy cơ đến cơ sở dữ liệu của tổ chức chính là việc mất cắp hoặc sửa đổi dữ liệu.

**Xác định mức độ tổn thương của tài sản** – Mức độ tổn thương là những điểm yếu của tài sản có thể được lợi dụng bởi các mối nguy cơ đe dọa và tạo ra rủi ro. Một tài sản có thể có nhiều tổn thương. Ví dụ, mức độ tổn thương đến cơ sở dữ liệu của một tổ chức có thể là do sự yếu kém về kiểm soát truy cập hoặc thiếu sự backup.

**Xác định xác xuất xảy ra** – Xác xuất xảy ra cho mỗi phối hợp: mối đe dọa rủi ro/sự tổn thương cần được xác định, sự phối hợp với khả năng xảy ra quá thấp có thể được bỏ qua.

**Tính toán thiệt hại** – Thiệt hại cần được định lượng với con số giá trị cụ thể nhằm xác định rõ giá trị mất mát do mỗi sự cố tấn công thành công. Giá trị này thiết lập được sự nghiêm trọng của mỗi rủi ro và không tính đến xác xuất khả năng xảy ra.

**Tính toán rủi ro** - Đánh giá và giảm thiểu rủi ro là mục tiêu của hệ thống quản lý an toàn thông tin ISO27001. Nói một cách toán học, rủi ro có thể được tính theo công thức: (xác xuất xảy ra) X mức độ thiệt hại = Rủi Ro. Công thức này dẫn đến việc đo lường và so sánh mức độ nghiêm trọng của các rủi ro, cho phép việc tập trung nguồn lực vào giải quyết những mối rủi ro lớn nhất.

Sự hiệu quả của quy trình ISO27001 dựa trên sự chính xác và trọn vẹn của việc đánh giá rủi ro an ninh. Rủi ro không thể được giảm nhẹ khi chưa được xác định rõ ràng! Các kiểm soát được tạo ra để giảm nhẹ rủi ro được xác định trong bước đánh giá rủi ro. Sự chọn lựa của các kiểm soát được xem xét dựa trên sự cân bằng giữa khả năng của ban lãnh đạo chấp nhận rủi ro và việc áp dụng kiểm soát.

## Nguy cơ mất an toàn thông tin do các yếu tố vật lý

An ninh vật lý mô tả các biện pháp được thiết kế để từ chối (ngăn chặn) truy cập trái phép về vật lý (bao gồm những kẻ tấn công, thậm chí những người xâm nhập tình cờ) vào một tòa nhà, phòng, tài nguyên, hoặc nơi lưu trữ thông tin; và hướng dẫn làm thế nào để thiết kế các cấu trúc để chống lại các hành vi phá hoại tiềm ẩn. An ninh vật lý có thể đơn giản như là khóa một cánh cửa hoặc là phức tạp hơn như nhiều lớp hàng rào bảo vệ an ninh. Tương ứng như vậy, các nguy cơ gây mất an toàn thông tin do yếu tố vậy lý gây ra có thể quy về 3 loại sau đây:

**Nguy cơ phá vỡ tính bí mật (hay là hiểm hoạ lộ tin).**

Khi mà thông tin đến với người mà người đó không có quyền tiếp cận tới nó thông tin ta nói hiểm hoạ lộ tin đã xảy ra. Cứ mỗi lần có một tiếp cận tới một thông tin mật nào đó đang được lưu trữ, chuyển tải hoặc xử lý trong hệ thống thông tin đều có nguy cơ lộ tin diễn ra. Người ta còn gọi là sự rò rỉ thông tin mật. Khi kẻ tấn công cố gắng xâm nhập vào một hệ thống máy tính, mà các biện pháp kỹ thuật thất bại, thì tấn công vào môi trường vật lý và tấn công vào con người là những lựa chọn đem lại khả năng thành công cao. Trong an toàn thông tin một khi đã tiếp cận được với hệ thống ở mức vật lý, thì dữ liệu mà kẻ tấn công có được mang giá trị cao khi đã toàn quyền kiểm soát hệ thống ở mức thấp nhất.

**Nguy cơ phá vỡ tính toàn vẹn thông tin.**

Bất kỳ sự thông tinay đổi cố ý nào tới thông tin đang tham gia vào quá trình xử lý đều làm phá vỡ sự toàn vẹn của nó. Sự thay đổi hợp pháp thông tin là sự thay đổi thông tin được thực hiện bởi chủ thể được uỷ quyền với mục đích rõ ràng (ví dụ cập nhật thông tineo chu kỳ các CSDL). Trong các thay đổi thông tin hợp pháp nếu xảy ra các lỗi ngẫu nhiên về bảo đảm chương trình hoặc bảo đảm thiết bị cũng sẽ dẫn tới phá vỡ sự toàn vẹn thông tin.

**Nguy cơ phá vỡ tính sẵn sàng.**

Khi mà hành động cố ý của kẻ xấu hoặc của một người dùng nào đó, làm ngăn cản tiếp cận tới một tài nguyên nhất định của hệ thống thì ta nói một hiểm hoạ từ chối dịch vụ đã xảy ra. Sự ngăn cản tiếp cận này có thể là vĩnh viễn hoặc có thể trong một thời gian nhất định. Trường hợp này chúng ta thường nghĩ đến nguyên nhân như cháy nổ, hỏa hoạn, lũ lụt… Làm cho hệ thống công nghệ thông tin ngừng hoạt động.

# Quản lý và xử lý sự cố mất an toàn thông tin

## Tổng quan về sự cố an toàn thông tin

## Sự cố an ninh là gì ?

Một sự có về an ninh hay nói cách khác là sự cố về an toàn thông tin được hiểu là những vi phạm một cách rõ ràng về các chính sách an toàn thông tin, là những hành vi nhằm cố gắng đạt được những quyền truy cập trái phép, là những hành vi làm ảnh hưởng đến tính sẵn sang của hệ thống và những hành vi sửa đổi tài nguyên mà không được sự đồng ý của chủ sở hữu.

Sự cố về an ninh, an toàn thông tin có thể xảy ra theo nhiều cách khác nhau. Các sự cố về an ninh, an toàn thông tin được phân loại dựa trên vector tấn công. Các vector tấn công thông thường :

* **External/Removable Media**: Là một cuộc tấn công được thực hiện từ các thiết bị lưu trữ di động và các thiết bị ngoại vi.
* **Attrition**: Một cuộc tấn công sử dụng phương pháp vét cạn (Brute force) để thỏa hiệp, làm suy giảm hay phá hủy các hệ thống, mạng lưới hay dịch vụ
* **Web**: Một cuộc tấn công được thực hiện từ một trang web hoặc các ứng dụng trên nền web
* **Email**: Một cuộc tấn công được thực hiện thông qua một email hoặc các tệp tin đích kèm email
* **Sử dụng không đúng cách**: Các sự cố xảy ra do vi phạm các chính sách của một sổ chức (trừ các loại trên)
* **Mất thiết bị**: Sự cố xảy ra cho mất trộm mất cắp thiết bị chẳng hạn như USB, điện thoại thông minh, máy tính xách tay…
* **Khác**: Các cuộc tấn công không thuộc các loại trên

### Ứng phó sự số là gì ?

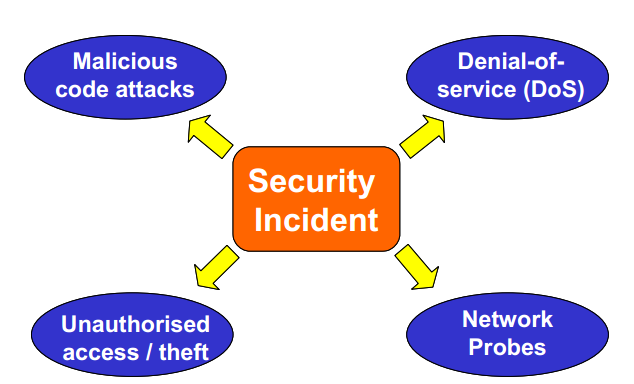
Ứng phó sự cố là các hành động được thực hiện nhằm giám sát, phát hiện và thực hiện đối phó với các sự cố an ninh, an toàn thông tin gây ảnh hưởng đến tính toàn vẹn, tính bí mật và tính sẵn sang của thông tin và hệ thống thông tin. Việc ứng phó sự cố đòi hỏi một quy trình cụ thể cùng với một nhóm chuyên gia có đầy đủ kinh nghiệm và năng lực thực hiện quy trình đó.

Quy trình ứng phó sự cố bao gồm 7 bước:

* Chuẩn bị
* Phát hiện
* Phân tích
* Ngăn chặn
* Loại bỏ
* Phục hồi
* Hoạt động sau sự cố

### Phân loại sự cố

Các sự cố về bảo mật có thể được phân loại như sau:



*Hình 5.1. Phân loại sự cố an toàn thông tin*

* **Tấn công bằng mã độc hại**: Mã độc hại có thể là các chương trình như virus, worm, trojan…Các kẻ tấn công thường sử dụng các mã độc hại để đạt được quyền truy cập, chiếm mật khẩu, chụp hoặc ghi lại các thông tin nhạy cảm khác. Các cuộc tấn công bằng mã độc thường khó phát hiện. Một số ví dụ về tấn công mã độc hại được biết đến như:
  + Worm hay virus lây lan nhanh chóng qua email (I Love You, Melissa)
  + Spy (Virus Caligula, Marker Virus, Groov Virus)
  + Các mã khai thác nhằm chiếm quyền điều khiển từ xa (Back Office, NetBus..)
* **Tấn công từ chối dịch vụ**: Các cuộc tấn công từ chối dịch vụ được các kẻ tấn công thực hiện nhằm mục đích làm ngưng trệ hoạt động của hệ thống. Một số ví dụ về tấn công DoS:
  + DoS liên quan đến Email: ví dụ như Spam, Bom mail…
  + DoS các dịch vụ mạng: ví dụ như Slammer Worm, Chargen ĐoS
  + DoS hệ thống mạng: Ví dụ như SYN Flood, Ping of Death, Smurf ….
* **Truy cập trái phép**: Là những hành động cố gắng truy cập vào những tài nguyên hệ thống một cách trái phép. Nó có thể được thực hiện bằng cách cài thêm một chường trình lên hệ thống máy tính, chặn bắt các thông tin đăng nhập vào hệ thống hay leo thang đặc quyền… Một số ví dụ về truy cập trái phép:
  + Nhân viên ăn cắp các thông tin bí mật
  + Truy cập vào hệ thống bằng tài khoản của cựu nhân viên
  + Truy cập trái phép vào tài khoản của người quản trị hệ thống
  + Truy cập vào hệ thống trái phép bằng cách khai thác các lỗ hổng trong hệ thống.
* **Dò quét mạng**: Mục tiêu của hoạt động này là thu thập các thông tin về cơ sở hạ tầng, mạng lưới của một công ty hay tổ chức nào đó. Các cuộc dò quét mạng cho phép phát hiện các thông tin về hệ thống như địa chỉ IP, các cổng đang mở trên máy chủ, các dịch vụ đang hoạt động trên máy chủ, phiên bản hệ điều hành đang dùng…. Một cuộc tấn công dò quét mạng có thể không dẫn đến một sự thỏa hiệp đối với hệ thống nhưng nó báo hiệu rằng sẽ có một cuộc tấn công trong tương lai. Các hình thức dò quét mạng phổ biến:
  + Host discovery (ping sweep, SYN-FIN scan…)
  + Service discovery (TCP Scan, UDP scan…)

### Phân loại mức nghiêm trọng của sự cố

Sau khi phân loại các sự cố, mức độ nghiêm trọng của sự cố có thể được xác định. Mức độ nghiêm trọng của sự cố sẽ ảnh hưởng đến quá trình và các hành động cần thực hiện để ứng phó với sự cố đó. Có 5 mức độ nghiêm trọng có thể được gán cho các sự cố về bảo mật:

* **Nghiêm trọng**: Những sự cố có thể ảnh hưởng đến cuộc sống con người, gây ra mất mát về tài nguyên mà không thể khôi phục
* **Cao**: Những sự cố này có thể ảnh hưởng đến tính toàn vẹn hoặc bảo mật của dữ liệu, nó có thể gây thiệt hại về kinh doanh, danh tiếng cho một công ty hay tổ chức
* **Trung bình**: Những sự cố này ảnh hưởng đến sự sắn sang của thông tin, ảnh hưởng đến sự sẵn sẵng sàng của hệ thống mà không ảnh hưởng đến tính toàn vẹn hay bảo mật dữ liệu
* **Thấp**: Những sự cố này có thể ảnh hưởng đến tính bảo mật, toàn vẹn hoặc sẵn sàng của dữ liệu tuy nhiên không có thiệt hại gì xảy ra.
* **Không quan trọng**: Những sự cố này gây ra những nguy cơ hoặc thiệt hại không đáng kể cho công ty hay tổ chức

## Chính sách, kế hoạch và thủ tục xử lý sự cố an toàn thông tin

### Chính sách

Chính sách về quản lý và ứng phó sự cố của từng các nhân hay tổ chức là khác nhau. Tuy nhiên, hầy hết các chính sách đều bao gồm các yếu tố sau:

* Cam kết quản lý
* Mục đích và mục tiêu của chính sách
* Phạm vi của chính sách
* Định nghĩa về sự cố bảo mật và các vấn đề liên quan
* Cơ cấu tổ chức, định nghĩa về vai trò, mức độ và quyền hạn
* Xếp hạng mức độ ưu tiên hoặc mức độ nghiêm trọng của sự cố
* Performance Measures
* Báo cáo và mẫu phương thức liên lạc

### Kế hoạch

Cá nhân hay tổ chúc cần có một kế hoạch chính thức, tập trung và phối hợp các bên liên quan để giải quyết các sự cố về bảo mật. Một kế hoạch ứng phó với sự cố sẽ cung cấp một lộ trình thực hiện các biện pháp nhằm giải quyết sự cố. Kế hoạch về ứng phó sự cố thường bao gồm các yếu tố sau:

* Nhiệm vụ
* Mục tiêu và chiến lược
* Sự phê chuẩn các yêu cầu quản lý cấp cao
* Phương pháp của tổ chức để ứng phó với sự cố
* Cách thức để đội ứng phó sự cố liên lạc với các thành phần khác trong một tổ chức hoặc là liên lạc với một tổ chức khác
* Đánh giá khả năng ứng phó vơi sự cố và tính hiệu quả của nó
* Làm cách nào đẻ kế hoạch có thể được áp dụng một cách tổng thể cho toàn bộ tổ chức

### Thủ tục

Các thử tục về ứng phó cự cố cần phải được xây dựng dựa trên chính sách và kế hoạch ứng phó sự cố. Thủ tục hoạt động tiêu chuẩn (Standard operating procedures - SOPs) là một sự phân chia cụ thể về mặt quy trình kỹ thuật nó bao gồm kỹ thuật, checklist, các biểu mẫu đước sử dụng bởi đội ứng phó sự cố. Việc chuẩn hóa các thủ tục sẽ làm giảm đi đáng kể sự thiếu sót, sai sót trong quá trình xử lý sự cố đặc biệt là đối với những tình huống nhạy cảm, căng thẳng. SOPs phải được kiểm tra để đảm bảo tính chính xác và tính hữu dụng của nó. SOPs nên bao gồm những yếu tố sau:

* **Chia sẻ thông tin với bên ngoài:**

Trong quá trình ứng phó sự cố, đội ứng phó sự cố cần phải được chia sẻ thông tin ra bên ngoài trong một số trường hợp. Chẳng hạn như để thực thi pháp luật, trả lời các đơn vị truyền thông, hoặc tìm kiếm các chuyên gia bên ngoài giúp đỡ xử lý sự cố.

Các tổ chức cũng có thể chủng động chia sẻ thông tin về sự cố với các đồng nghiệm khác nhằm phát hiện và phân tích các sự cố giúp cho việc giải quyết sự cố nhanh chóng hơn. Các thủ tục về vấn đề chia sẻ thông tin ra bên ngoài cầm phải được thiết lập nhằm đảm bảo các thông tin nhạy cảm không bị lộ ra bên ngoài một cách trái phép có thể dẫn đến những tổn thất về kinh tế cũng như danh tiếng cho tổ chức. Đội ứng phó sự cố phải lưu lại tất cả các thông tin, địa chỉ liên lạc với phía bên ngoài công ty, tổ chức để có thể quản lý về mặt trách nhiệm trong trường hợp thất thoát thông tin xảy ra



*Hình 5.2. Các đối tượng chia sẻ thông tin của đội ứng phó sự cố*

* **Phương tiện**

Đội ứng phó sự cố nên thiết lập các thủ tục cho việc công bố thông tin qua các phương tiện truyền thông tuân theo chính sách của tổ chức. Ví dụ như một người trong đội ứng phó sự cố, sẽ tham gia cùng với các thành viên của phòng quan hệ công chúng trước các phương tiện truyền thông:

* + Tổ chức các buổi tập huấn về tương tác với các phương tiện truyền thông liên quan khi có sự cố xảy ra, trong đó phải đảm bao việc không tiết lộ các thông tin nhạy cảm chẳng hạn như các chi tiết kỹ thuật của các biện pháp đối phó.
  + Thiết lập một thủ tục ngắn gọn để các phương tiện truyền thông liên lạc liên quan đến các thông tin nhạy cảm của một sự việc cụ thể trước khi thảo luận chính thức với các phương tiện truyền thông.
  + Duy trì các thông tin về tình trạng hiện tại của sự cố và liên tục cập nhật thông tin
  + Nhắc nhở toàn bộ nhân viên về các thủ tục chung khi xử lý yêu cầu của các phương tiện truyền thông.
  + Tập huấn các cuộc phỏng vấn giả và các cuộc họp báo khi có sự cố xảy ra. Một cố câu hỏi thường được các phương tiện truyền thông yêu cầu như:
    - Ai là kẻ tấn công ? Tại sao ?
    - Cuộc tấn công xảy ra khi nào ? Chuyện gì đã xảy ra ? Điều này xảy ra do bảo mật kém hay do nguyên nhân nào khác ?
    - Cách thức là sự cố này có thể lan rộng ra ? Bạn đã xác định sự cố như thế nào và nên làm gì để sự cố này không xảy ra trong tương lai ?
    - Tác động của sự cố này như thế nào ? Mức độ nghiêm trọng như thế nào ? Tác động của sự cố này đến các thông tin cá nhân (PII) ? Thiệt hại ước tính của sự cố này là bao nhiêu ?
* **Thi hành luật**

Các đội phản ứng sự cố cần được làm quen và thảo luận với các đại diện của cơ quan thực thi pháp luật trước khi sự cố xảy ra về các điều kiện để thực thi pháp luật trong trường hợp cần thiết như báo cáo, cách thức thực hiện báo cáo, những bằng chứng cần thu thập và làm thế nào để thu thập các bằng chứng đó.

Các cơ quan pháp luật ở các nước khác cũng có thể tham gia trong trường hợp kẻ tấn công nằm bên ngoài phạm vi của quốc gia.

Các nhân đại diện thực thi pháp luật phải được chỉ định một cách phù hợp với yêu cầu của pháp luật và thủ tục của tổ chức. Nhiều tổ chức muốn bổ nhiệm một thành viên trong đội ứng phó sự cố làm đại diện trong việc thực thi pháp luật. Người này nên làm quen với các thủ tục, báo cáo của tất cả các cơ quan pháp lý có liên quan. Một lưu ý rằng công ty hay tổ chức thường chỉ nên liên lạc với một cơ quan pháp lý để tránh việc xung đột trong vấn đề phán quyết.

* **Một số thành phần bên ngoài**

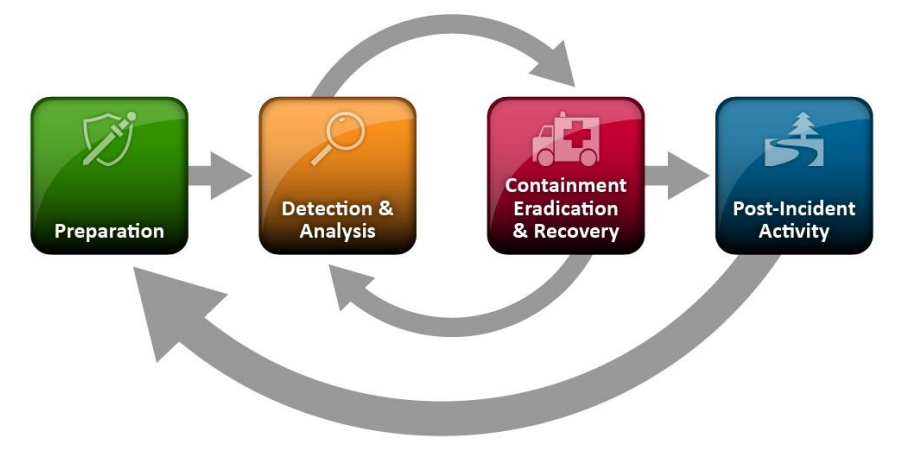
Công ty hay tổ chức trong quán trình ứng phó sự cố có thể muốn thảo luận và trao đổi về sự cố với các nhóm bên ngoài:

* + ISP: Quá trình ứng phó sự cố có thể cần sự hỗ trợ của các ISP trong việc ngăn chặn một cuộc tấn công mạng lớn hoặc truy tìm nguồn gốc của cuộc tấn công đó.
  + Chủ sở hữu của địa chỉ tấn công: Nếu một cuộc tấn công có nguồn gốc xuất phát từ một tổ chức bên ngoài, việc xử lý sự cố có thể được thực hiện bằng cách nói chuyện, trao đổi với tổ chức bên ngoài đó nhằm mục đích thu thập chứng cư hay ngăn chặn cuộc tấn công.
  + Các nhà cung cấp phần mềm: Đội ứng phó sự cố có thể muốn trao đổi với các nhà cung cấp phần mềm về các hoạt động đáng ngờ của phần mềm. Sự trao đổi này có thể chỉ ra được các cuộc tấn công chiếm quyền điều khiển máy chủ thông qua một phần mền dễ bị tổn thương. Các nhà cung cấp phần mềm cũng có thể cung cấp các thông tin về các mỗi đe dọa, các lỗ hổng chưa được vá ở các phiên bản cũ để giúp đội ứng phó xử lý sự cố.
  + Các đội ứng phó sự cố khác:

Một số đội ứng phó sự cố khác có thể cũng gặp các sự cố tương tự nên việc chủ động chia sẻ thông tin sẽ tăng hiệu quả trong quá trình xử lý sự cố (ví dụ như cảnh báo sớm, tăng khả năng chuẩn bị ứng phó sự cố)

## Quy trình xử lý sự cố mất an toàn thông tin.

Quy trình ứng phó sự cố bao gồm nhiều gian đoạn. Giai đoạn đầu tiên là việc thành lập và đào tạo một đội phản ứng sự cố và lựa chọn các công cụ cũng như nguồn lực cần thiết. Trong thời gian chuẩn bị, tổ chức cũng phải hạn chế số lượng các sự cố xảy ra. Việc phát hiện các lỗ hổng bảo mật là cần thiết để cảnh báo cho các tổ chức bất kể khi nào xảy ra sự cố. Sauk hi sự cố được xử lý đầy đủ, tổ chức cần phải phát hành một báo cáo chi tiết về nguyên nhân và chi phí của vụ việc, các bước để tổ chức ngăn chặn trong tương lai.



*Hình 5.3. Quy trình ứng phó sự cố*

### Chuẩn bị

Các phương pháp ứng phó sự cố thường nhấn mạng việc chuẩn bị. Nó không chỉ thiết lập khả năng để tổ chức ứng phó với sự cố mà còn ngăn ngừa sự cố bằng cách đảm bảo rằng hệ thống mạng và các ứng dụng đủ an toàn để vận hành. Mặc dù đội ứng phó sự cố thường không chịu trách nhiệm trong việc phòng ngừa sự cố xảy ra tuy nhiên bước này cung cấp các thông tin, lời khuyên cơ bản để chuẩn bị ứng phó và phòng ngừa sự cố xảy ra.

#### Chuẩn bị ứng phó sự cố

Danh sách các mục dưới đây cung cấp các ví dụ về các công vụ và nguồn lực trong quá trình xử lý sự cố. Những mục này là những điểm bắt đầu cho việc thảo luận các công cụ sử dụng cũng như nguồn lực xử lý sự cố của một tổ chức.

Chuẩn bị về liên lạc và truyền thông:

* Thông báo cho các thành viên và những người liên quan bên trong và bên ngoài tổ chức ví dụ như các đội phản ứng xử lý sự cố khác hoặc cơ quan thực thi pháp luật. Thông tin có thể bao gồm số điện thoại, địa chỉ email, các khóa công khai và hướng dẫn cho việc xác minh danh tính.
* Lây thông tin ngay lập tức từ các đội khác bên trong tổ chức bao gồm cả vấn đề leo thang thông tin
* Cơ chế cảnh báo sự cố. Ví dụ như số điện thoại, địa chỉ email, hệ thống tin nhắn… Nên có một kênh riêng cho việc báo cáo sự cố nặc danh
* Phát hành hệ thống cho phép theo dõi các thông tin và trạng thái của sự cố.
* Phần mềm mã hóa được sử dụng để liên lạc giữa các thành viên trong nhóm, giữa nhóm với các tổ chức bên ngoài.
* Các cơ chế bảo mật lưu trữ để đảm bảo an toàn cho bằng chứng cũng như các tài liệu nhạy cảm khác.

Chuẩn bị về phân tích sự cố phần cứng và phần mềm

* Các biện pháp và thiết bị sao lưu để tạo ảnh đĩa, bảo quản file log và lưu trữ các dữ liệu sự cố liên quan.
* Máy tính xách tay phục vụ cho hoạt động phân tích dữ liệu, chặn bắt gói tin, viết báo cáo.
* Máy trạm, máy chủ, thiết bị mạng để phục vụ cho việc mô phỏng sự lây lan của phần mềm độc hại hoặc khôi phục lại các bản sao lưu dữ liệu.
* Máy in di động để tạo các bản sao lưu tệp tin log và các bằng chứng trong trường hợp hệ thống không có kết nối mạng.
* Hệ thống chặn bắt và phân tích lưu lượng mạng.
* Ổ cứng hoặc thiết bị lưu trữ di động chứa các chương trình tin cậy để thu thập thông tin, bằng chứng từ hệ thống.
* Các thiết bị thu thập chứng cứ như máy ảnh kỹ thuật số, máy ghi âm, túi bảo quản bằng chứng…

Phân tích tài nguyên sự cố

* Danh sách các port thường được sử dụng, các port lạ, các port Trojan sử dụng
* Tài liệu về hệ điều hành, các ứng dụng, các giao thức, các sản phần antivirus và các sản phẩm phát hiện xâm nhập
* Sơ đồ mạng và danh mục các tài nguyên quan trọng.
* Baseline của hệ thống mạng hiện tại và các ứng dụng

#### Ngăn ngừa sự cố

Giữ số lượng các sự cố ở mức thấp là rất quan trọng trong việc bảo vệ các quá trình kinh doanh của tổ chức. Nếu các kiểm soát về an ninh là không đủ thì số lượng các sự cố quá lớn có thể dẫn đến việc đội ứng phó sự cố không thể xử lý kịp. Điều này dễ dẫn đến việc sự cố được đáp ứng chậm dẫn đến những thiệt hại không thể lường trước được.

Mặc dù đội ứng phó sự cố nói chung không chịu trách nhiệm bảo vệ tài nguyên nhưng họ có thể xác định và đánh giá những rủi ro không thể nhận thức được. Đội ứng phó sự cố có thể xác định được những khoảng trống của các chính sách tạo điều kiện cho các cuộc tấn công tiền năng. Các kiến nghị sau giúp nâng cao vấn đề bảo mật trong các hệ thống mạng và ứng dụng:

* **Đánh giá rủi ro**: Đánh gia rủi ro định kỳ cho hệ thống và ứng dụng là việc làm nhằm xác định những rủi ro có thể gây ra bởi sự kết hợp giữa các mối đe dọa và lỗ hổng bảo mật. Việc đánh giá rủi ro định kỳ cung cấp cho tổ chức các mỗi rủi ro tiền năng qua đó đưa ra được các biện pháp đối phó phù hợp. Việc đánh giá rủi ro định kỳ cũng cho phép các thành viên nhấn mạnh các hoạt động giám sát và phản ứng đối với tài nguyên hệ thống.
* **Tổ chức an ninh**: Tất cả các tổ chức nên kiểm tra các cấu hình tiêu chuẩn của hệ thống . Ngoài việc liên tục cập nhật các bản vá, việc cấu hình nên được thực hiện theo nguyên tắc đặc quyền tối thiểu. Người sử dụng chỉ được cấp những quyền tối thiểu tương ứng với vai trò của người dùng đó trong hệ thống.
* **An toàn hệ thống mạng**: Các vành đai mạng nên được cấu hình để từ chối tất cả các hoạt động không cho phép một cách rõ ràng.
* **Phòng chống mã độc hại**: phần mền phát hiện và phòng chống mã độc phải được triển khai trên toàn bộ tổ chức. Các phần mềm phòng chống mã độc nên hoạt động cả các cấp bảo vệ mức hệ điều hành và mức ứng dụng.
* **Nâng cao nhận thức của toàn bộ nhân viên**: Triển khai đào tạo nâng cao nhận thức về an toàn thông tin cho toàn bộ nhân viên trong tổ chức. Bài học kinh nghiệm rút ra được từ các sự cố trước đây cần được chia sẻ cho các nhân viên để giảm tần số xuất hiện của sự cố.

### Phát hiện và phân tích

#### Dấu hiệu của sự cố

Đối với nhiều tổ chức, công đoạn khó khăn nhất trong quá trình ứng phó sự cố là phát hiện chính xác và đánh giá sự cố xem sự cố đã xảy ra hay chưa, loại hình, mức độ nghiêm trọng của sự cố. Điều này được thực hiện bằng cách kết hợp ba yếu tố sau:

* Sự cố có thể được phát hiện thông qua nhiều phương tiện khác nhau, các mức độ và tính trung thực cũng khác nhau. Khả năng phát hiện tự động bao gồm việc dựa trên các sự kiện của hệ thống phát hiện xâm nhập IDS, phần mềm chống mã độc hại và phân tích quá trình đăng nhập. Sự cố có thể được phát hiện thông qua những báo cáo của người dùng.
* Số lượng các sự cố tiền ẩn thưởng rất cao. Ví dụ như nó không phổ biến cho một tổ chức cụ thể hoặc hệ thống phát hiện thông báo quá nhiều sự kiện trong một khoảng thời gian.
* Việc phát hiện sự cố phụ thuộc vào kiến thức kỹ thuật, kinh nghiệm trong việc phân tích các dữ liệu liên quan đến sự cố của đội ứng phó sự cố

Dấu hiệu về sự cố có thể rơi vào 2 loại. Một là những dấu hiệu tiền thân, nó là những dấu hiệu cho thấy sự cố có thể xảy ra trong tương lai. Hai là dấu hiệu chỉ thị, nó là những dấu hiệu cho thấy sự cố đã xảy ra hoặc có thể xảy ra ngay lập tức. Nếu một dấu hiệu tiền thân được phát hiện, tổ chức có thể thực hiện ngăn chặn sự cố này trước khi sự cố xảy ra. Một số dấy hiệu tiền thân như là:

* Log của máy chủ web ghi nhận được các bản ghi của các công cụ dò quét lỗ hổng bảo mật
* Mối đe dọa từ các nhóm hacker sẽ tấn công tổ chức
* Một lời tuyên bố tấn công nhằm vào các máy chủ hay ứng dụng của tổ chức

Trong khi các dấu hiệu tiền thân là khá ít thì các dấu hiệu chỉ thị lại rất phổ biến:

* Các thiết bị phát hiện xâm nhập cảnh báo kẻ tấn công đang khai thác lỗi tràn bộ đệm.
* Phần mềm chống mã độc hại cảnh báo một máy chủ bị nhiễm phần mềm độc hại.
* Một quản trị viên nhìn thấy một tệp tin khác thường trên máy chủ.
* Máy chủ ghi lại tự thay đổi cấu hình kiểm toán của mình.
* Tệp tin log ghi lại rất nhiều lần đăng nhập sai đến một hệ thống
* Một quản trị viên thấy lưu lượng bất thường bên trong hệ thống mạng

#### Nguồn thông tin

Các dấu hiệu của sự cố được xác định từ nhiều nguồn thông tin khác nhau, phổ biến là từ các phần mềm phòng chống mã độc hại, các bản ghi nhật ký, hệ thống phát hiện xâm nhập, con người…

* IDPS:
* SIEMs:
* Antivirus:
* File integrity checking
* Monitoring services
* System, application, security logs
* Network device logs
* Netflows
* Thông tin về các lỗ hổng bảo mật mới
* Người bên ngoài và bên trong tổ chức

#### Phân tích sự cố

Việc phân tích sự cố sẽ dễ dàng hơn nếu các dấu hiệu được đảm bảo là chính xác. Tuy nhiên các dấu hiệu không phải lúc nào cũng đúng. Ví dụ như các hệ thống phát hiện xâm nhập có thể đưa ra những cảnh báo sai. Hoặc tệ hơn, hệ thống phát hiện xâm nhập đưa ra quá nhiều cảnh báo, nó làm cho việc phân tích trở nên vô cùng khó khăn.

Thậm chí là nếu một số dấu hiệu là chính xác, nó cũng không đảm bảo được là sự cố đã xảy ra. Một số sự cố dễ dàng được phát hiện ví dụ như nội dung của trang web đã bị thay đổi. Tuy nhiên không nhiều những sự cố dễ dàng phát hiện được như vậy. Biện pháp khắc phục tốt nhất là xây dựng một đội ngũ giàu kinh nghiệm và thành thạo có thể phân tích, xác định chính xác các dấu hiệu và đưa ra những hành động thích hợp. Nếu không có một đội ngũ nhân viên có khả năng phát hiện và phân tích sự việc thì việc ứng phó sự cố sẽ không hiệu quả và những sai lầm, tốn kém có thể xảy ra.

Đội phản ứng sự cố nên phân tích một cách nhanh chóng và xác định xem sự cố đã thật sự xảy ra hay chưa. Khi đã xác định một sự cố đã thật sự xảy ra, nhóm nghiên cứu bắt đầu thực hiện các bước phân tích ban đầu đề xác định phạm vi của sự việc ví dụ như mạng, máy chủ, hệ thống bị ảnh hưởng, cái gì có thể là nguồn gốc của vụ việc, làm thế nào để sự việc xảy ra. Những phân tích ban đầu sẽ cung cấp thông tin cho các hoạt động phân tích sâu tiếp theo.

Các khuyến nghị sau đây giúp việc phân tích sự cố dễ dàng và hiệu quả hơn:

* **Hồ sơ về hệ thống mạng**: Lập hồ sơ các vị trí thay đổi để dễ dàng xác định và khoanh vùng sự cố hơn.
* **Hiểu về các hành vi bình thường**: Các thành viên trong đội ứng phó sự cố cần hiểu về các hành vi bình thường để có thể xác định được các hành vi bất bình thường bên trong hệ thống. Cách để có được điều này là rà soát các thông tin trong nhật ký và các cảnh báo bảo mật. Tiến hành đánh gia thường xuyên các bản ghi log sẽ cho chung ta một cái nhìn tổng quan về sự bình thường và bất bình thường của hệ thống.
* **Tạo chính sách về lưu trữ các bản ghi log**: Thông tin liên quan đến sự cố có thể được lưu trữ tại một số nơi trên hệ thống chẳng hạn như tường lửa, các bản ghi log của ứng dụng… Việc phân tích các bản ghi log cũ có thể cho ra các dấu hiệu của các cuộc tìm kiếm thông tin, dò quét tạo tiền đề cho sự cố xảy ra hoặc có thể xác định được các sự cố đã xảy ra mà chưa được phát hiện.
* **Giữ cho tất cả các thiết bị được đồng bộ về thời gian**: Giao thức NTP có thể giúp cho hệ thống đồng bộ về mặt thời gian. Thời gian chuẩn của hệ thống có thể cung cấp chính xác thời gian sự cố xảy ra, các cuộc tấn công xảy ra chính xác vào thời gian nào…
* **Chạy các công cụ chặn bắt dữ liệu mạng để cho thêm các thông tin bổ sung**. Đôi khi dữ liệu từ các bản ghi là không đủ cho quá trình phân tích. Các dữ liệu về lưu lượng mạng cho phép ta biết chính xác những gì đang xảy ra bên trong hệ thống mạng của tổ chức.

#### Đánh giá mức độ ưu tiên cho sự cố

Xác định mức độ ưu tiên cho các sự kiện cũng là một vấn đề quant rọng. Các sự cố không nên được xử lý theo thứ tự thời gian phát hiện. Thay vào đó, việc xử lý các sự cố cần được ưu tiên dựa vào các yếu tố sau:

* **Tác động về mặt chức năng của sự cố**: Sự cố nhắm đến mục tiêu là các hệ thống công nghệ thông tin thường ảnh hưởng đến hoạt động kinh doanh. Việc xử lý sự cố nên được xem xét đến việc làm ảnh hưởng đến hoạt động của hệ thống.Nên xem xét cả những tác động về mặt chức năng trong tương lai có thể xảy ra.
* **Tác động về mặt thông tin của sự cố**: Sự cố có thể ảnh hưởng đến tính bảo mật, tính toàn vẹn và tính sẵn sàng của hệ thống.Việc xử lý sự cố cần được xem xét sự ảnh hưởng về mặt thông tin đến hoạt động bình thường của tổ chức. Nó cũng có thể liên quan đến các tỏ chức khác nếu như sự cố ảnh hưởng đến các dữ liệu gắn liền với tổ chức đố.
* **Phục hồi sự cố**: Mức độ của sự cố ảnh hưởng đến chi phí khôi phục, thời gian và nguồn lực của tổ chức trong đó chưa kể đến một số trường hợp các sự cố xảy ra không thể phục hồi.

Một số phân loại của tác động về mặt chức năng như sau:

|  |  |
| --- | --- |
| **Loại** | **Định nghĩa** |
| Không | Là các sự cố không ảnh hưởng gì tới khả năng cung cấp dịch vụ đến tất cả các người dùng |
| Thấp | Ảnh hưởng tối thiểu, hệ thống của tổ chức có thể cung cấp dịch vụ cho người dùng nhưng tính hiệu quả bị ảnh hưởng |
| Trung Bình | Tổ chức mất khả năng cung cấp một dịch vụ quan trọng với một phần người dùng hệ thống |
| Cao | Tổ chức không còn có thể cung cấp một số dịch vụ quan trọng cho bất kỳ người dùng nào. |

Các mức độ tác động về mặt thông tin có thể được phân loại như sau:

|  |  |
| --- | --- |
| **Loại** | **Định nghĩa** |
| Không | Thông tin không bị thay đổi, sửa, xóa hay bị tổn hạn gì cả |
| Vi phạm bảo mật | Các thông tin cá nhân (PII) bị truy cập trái phép |
| Vi phạm sở hữu | Các thông tin độc quyền của tổ chức bị truy cập trái phép |
| Mất tính toàn vẹn | Các thông tin nhạy cảm hoặc độc quyền bị thay đổi hoặc xóa |

Phân loại khẳ năng phục hồi:

|  |  |
| --- | --- |
| **Loại** | **Định nghĩa** |
| Bình thường | Thời gian để phục hồi có thể dự đoán được với nguồn lực hiện tại |
| Bổ sung | Thời gian phục hồi có thể dự đoán được với nguồn lực bổ sung |
| Gia tăng | Thời gian phục hồi không thể dự đoán trước được, cần thêm nguồn lực và sự giúp đỡ từ bên ngoài |
| Không thể phục hồi | Không thẻ phục hồi |

### Ngăn chặn, Loại bỏ và Phục hồi

#### Lựa chọn chiến lực ngăn chặn

Chiến lược ngăn chặn khác nhau dựa trên các loại sự cố khác nhau. Ví dụ chiến lược ngăn chặn đối với sự cố lây nhiễm phần mềm độc hại khác so với chiến lược ngăn chặn sự cố tấn côn dừ chối dịch vụ DDoS. Các tổ chức nên tạo ra các chiến lược ngắn hạn riêng biệt cho từng loại sự cố lớn, có các tài liệu chuẩn nội dung chiến lược rõ ràng để tạo điều kiện thuận lợi chi việc đưa ra quyết định. Các tiêu chí xác định các chiến lược thích hợp bao gồm:

* Các thiệt hại tiền năng
* Mất cắp tài nguyên phần cứng
* Cần bảo vệ bằng chứng
* Tính sẵn sàng của dịch vụ
* Thời gian và nguồn lực cần thiết để thực hiện chiến lược
* Tính hiệu quả của chiến lược
* Thời gian của giải pháp

Trong một số trường hợp, các tổ chức chuyển hướng tấn công sang một sanbox hay sang hệ thống honeynet để theo dõi hoạt động tấn công của hệ thống, thường là để thu thập thêm bằng chứng. Đội ứng phó sự cố nên thảo luận chiến lược này với bộ phẩn quản lý để xác minh tính khả khi. Các chiến lược theo dõi hoạt động của kẻ tấn công ngoài sử dụng sanbox là không nên sử dụng. Nếu một tổ chức quyết định theo dõi kẻ tán công trên hệ thống thật của mình, nó có thể tồn tại những rủi ro lớn. Các chiến lực ngăn chặn chậm chạm là rất nguy hiểm vì kẻ tấn công có thể leo thang và truy cập trái phép vào các hệ thống khác từ hệ thống đã bị thỏa hiệp.

#### Thu thập và xử lý bằng chứng

Lý do chính trong việc thu thập bằng chứng là để phục vụ cho các thủ tục tố tụng pháp lý. Bằng chứng cần được thu thập theo thủ tục nhất định, đáp ứng tất cả các luật và quy định. Việc này có thể được tìm hiểu bằng cách trao đổi và thảo luận với luật sư hoặc các nhân viên pháp lý. Bằng chứng cần phải được hạch toàn mọi lúc. Bát cứ một hành động chuyển giao bằng chứng nào đều cần được ghi chép và có chữ ký. Một bản ghi chi tiết đi kèm với các bằng chứng bao gồm những điều sau:

* Xác định thông tin: ví dụ như số serial, tên thiết bị, địa chỉ MAC, địa chỉ IP…
* Tên, chức danh, số điện thoại của cá nhân thu thập hoặc xử lý bằng chứng trong quá trình điều tra.
* Thời gian và ngày tháng
* Địa điểm nơi lưu trữ bằng chứng.

#### Xác định nguồn gốc tấn công

Trong thời gian xử lý sự cố, đội ứng phó sự cố đôi khi muốn xác định máy chủ hoặc cá nhân đang thực hiện tấn công vào hệ thống. Mặc dù thông tin này khá quan trong nhưng việc xử lý sự cố lại chỉ tập trung vào vấn đề ngăn chặn, xóa và phục hồi. Những điều dưới đây là hoạt động phổ biến nhất để xác định nguồn gốc của cuộc tấn công:

* **Địa chỉ IP tấn công**: Địa chỉ IP có thể cho biết nguồn gốc của một cuộc tấn công. Tuy nhiên nó có thể bị giả mạo. Các nhân viên trong đội ứng phó nên xác định lại tính chính xác của danh sách các địa chỉ IP tấn công bằng các biện pháp kỹ thuật cần thiết.
* **Nghiên cứu kẻ tấn công qua các công cụ tìm kiếm**: thực hiện tìm kiếm thông tin vè kẻ tấn công bằng cách sử dụng các công cụ tìm kiếm. Ví dụ như là tìm hiểu người đăng ký sử dụng địa chỉ IP, thông tin về tên hay nhóm hay nickname…
* **Sử dụng cơ sở dữ liệu về sự cố**
* **Giám sát các kênh truyền thông của hacker**: Một số hacker tấn công các hệ thống với mục đích thể hiện bản thân. Họ thường khoe những cuộc tấn công đã thực hiện được lên mạng xã hội, các kênh IRC, zone-h…

#### Xóa và phục hồi

Sau khi sự cố đã được ngăn chặn. việc loại bỏ các thành phần của sự cố ra khỏi hệ thống là cần thiết ví dụ như sự cố về lây lan mã độc hại. Trong quá trình xóa, điều quan trọng là xác định tất cả các ảnh hưởng đối với tổ chức để có kế hoạch xử lý. Đối với một số sự cố, quá trình xóa là không cần thiết hoặc được thực hiện trong quá trình phục hồi.

Trong quá trình phục hồi, các quản trị viên hệ thống khôi phục lại hoạt động bình thường của hệ thống và xác nhận rằng hệ thống đang hoạt động bình thường. Quá trình phục hồi có liên quan đến các hành động như khôi phục lại từ các bản sao lưu hệ thống sạch, xây dựng lại hệ thống từ đầu, thay thế tệp tin bị thỏa hiệp bằng các bản sạch, cài đặt các bản vá lỗi, thay đổi mật khẩu, thắt chặt các hính sách an ninh mạng.

Xóa và phục hồi nên được thực hiện theo từng giai đoạn để bước khắc phục sự cố được ưu tiên. Đối với các sự cố có quy mô lớn, việc phục hồi có thể mất rất nhiều thời gian, vì vậy việc chia giai đoạn đảm bảo trong giai đoạn đầu tiên, các cơ chế an ninh tổng thể được tăng cường để ngăn chặn các sự cố tương tự trong tương lai. Giai đoạn sau nên tập trung vào những thay đổi dài hạn (ví dụ như những thay đổi về có sở hạ tầng...).

### Hoạt động sau sự cố

#### Bài học kinh nghiệm

Một phần quan trọng trong quá trình xử lý sự cố là việc rút ra các bài học kinh nghiệm về cuộc ứng phó sự cố. Tổ chức nên thực hiện các cuộc họp bữa các bên liên quan và rút ra các bài học kinh nghiệm cần thiết để đảm bảo sự cố tương tự sẽ không xảy ra. Cuộc họp cũng sẽ chỉ ra được cách thức phối hợp giữa các bên liên quan khi có sự cố xảy ra. Một số câu hỏi nên được giải đáp là:

* Chính xác điều gì đã xảy ra ? vào thời gian nào ?
* Nhân viên và các quản lý thực hiện giải quyết vụ việc có tốt không ?
* Những điều gi mà nhân viên và các quản lý nên làm khi có sự cố xảy ra ?
* Làm thế nào để chia sẻ thông tin với các tổ chức khác ?
* Các hành động để ngăn chặn sự cố tương tự trong tương lai là gì ?
* Các dấu hiệu về sự cố tương tự là gì ?
* Những công cụ hay nguồn lực nào cần thiết để giải quyết nhanh sự cố trong tương lai ?

#### Lưu trữ bằng chứng

Tổ chức cần thiết lập chính sách cho việc lưu trữ các bằng chứng trong thời gian dài. Hầu hết các tổ chức lưu giữ bằng chứng trong nhiều tháng hoặc nhiều năm sau khi vụ việc kết thúc. Một số yếu tố sau cần được xem xét trong quá trình tạo chính sách:

* **Truy tố**: Nếu những kẻ tấn công bị truy tố, những bằng chứng cần phải được giữa lại khi các hoạt động về mặt pháp lý được hoàn thành. Trong một số trường hợp, điều này có thể mất rất nhiều thời gian, có thể lên đến vài năm.
* **Lưu giữ dữ liệu**: Hầu hết các tổ chức có chính sách về thời gian sống cho các dữ liệu. Ví dụ các thư điện tử sẽ được giữ lại 180 ngày. Sau 180 ngày các thư điện tử sẽ bị xóa hoàn toàn.
* **Chi phí**: Chi phí cho các thiết bị phần chứng thực hiện lưu trữ bằng chứng cần dược xem xét. Chi phí có thể là đáng kể nếu như bằng chứng được lưu giữ trong thời gian dài.

## Tổ chức nhóm CSIRT.

Một đội ứng phó sự cố nên ở trạng thái sẵn sàng trước những phát hiện hoặc nghi ngờ rằng có một sự cố về bảo mật đã xảy ra. Một hoặc nhiều thành viên trong nhóm tùy thuộc vào độ lớn của đội xử lý sự cố sẽ thực hiện xử lý sự cố. Việc xử lý sự cố bao gồm việc phân tích các dữ liệu, xác định tác động của vụ việc, các hành đồng để hạn chế thiệt hại và khôi phục lại sự hoạt động bình thường của dịch vụ.

### Mô hình

Các mô hình chính cho một đội ứng phó sự cố:

* **Đội ứng phó sự cố tâp trung**: Đội ứng phó sự cố này là đội duy nhất xử lý sự cố cho tổ chức của bạn. Đây là mô hình có hiệu quả trong các tổ chức nhỏ và nhỏ.
* **Đội ứng phó sự cố phân tán**: Có nhiều đội ứng phó sự cố cùng xử lý sự cố cho tổ chức. Mỗi đội có thể đảm nhiệm một trong các công đoạn trong quy trình ứng phó sự cố hoặc có thể mỗi đội ở một vị trí địa lý khác nhau của tổ chức. Đây là một mô hình có hiệu quả đối với các tổ chức lớn, có tài nguyên phân bổ ở nhiều vị trí địa lý khác nhau. Tuy nhiên, các đội phải có một thành phần duy nhất quản lý chung để tạo sự nhất quán trong quá trình xử lý cũng như chia sẻ thông tin.
* **Đội điều phối**: là một đội tư vấn cho các đội khác mà không có thẩm quyền với các đội đấy. Ví dụ như một đội nghiên cứu có thể tham gia hỗ trợ các đội ứng phó sự cố riêng biệt.

Nhân sự cho đội ứng phó sự cố có thể áp dụng 3 hình thức sau:

* **Toàn bộ là nhân viên của tổ chức**: Toàn bộ thành viên trong đội ứng phó sự cố đều là nhân viên của tổ chức. Hình thức này sẽ gây hạn chế trong việc yêu cầu sự hỗ trợ từ các nhà thầu hay các nhà cung cấp.
* **Một phần là thuê bên ngoài**: Tổ chức sẽ thuê ngoài một phần trong quy trình ứng phó sự cố. Phổ biến nhất là tổ chức thuê ngoài việc giám sát phát hiện xâm nhập, tưởng lửa và các thiết bị an ninh, phân tích các dấu hiệu đáng ngờ và báo cáo từng sự việc với đội ứng phó sự cố của tổ chức. Một số tổ chức thực hiện các quy trình cơ bản trong ứng phó sự cố và kêu gọi sự giúp đỡ của các nhà thầy hoặc các nhà cung cấp dịch vụ.
* **Thuê toàn bộ bên ngoài**: Hình thức này thường được sử dụng khi đội ứng phó sự cố của tổ chức không sẵn sàng thực hiện hoạt động ứng phó sự cố ( có thể đang xử lý các sự cố khác) hoặc nhân viện trong tổ chức không có đủ trình độ để thực hiện xử lý sự cố. Tổ chức sẽ phải có một nhân viên thực hiện công việc giám sát các công việc của những người được thuê làm công tác ứng phó sự cố.

### Lựa chọn mô hình phù hợp

Khi lựa chọn mô hình là hình thức nhân sự cho một đội ứng phó sự cố, các tổ chức cần xem xét những yếu tố sau:

* **Sự cần thiết của tính sẵn sàng 24/7 của đội ứng phó sự cố**: Hầu hết các tổ chức cần các thành viên đội ứng phó sự cố trực 24/7 nhằm ứng phó với các sự cố một cách nhanh nhất có thể. Việc trực 24/7 là rất cần thiết cho những sự cố tiền năng hay những sự cố kéo dài. Trong một số trường hợp, việc trực 24/7 của đội ứng phố sự cố là không cần thiết ví dụ như mục đích là truy tìm nguồn gốc của một cuộc tấn công đã xảy ra.
* **Kết hợp giữa thành viên full-time và part-time**: Nếu tổ chức có kinh phí và nhân sự hạn hẹp nên tính toán đến vấn đề này. Đội tứng phó sự cố có thể không nhất thiết phải thường trực mà chỉ hoạt động khi có sự cố thật sự xảy ra. Một nhóm các nhân viên hỗ trợ IT có thể thực hiện tiếp nhận và thực hiện các thủ tục đơn giản như tiếp nhận thông bao sự cố, thu thập dữ liệu sau đó thông báo trực tiếp cho đội ứng phó sự cố nếu có vẻ như là một sự cố nghiêm trọng đang xảy ra.
* **Tinh thần của nhân viên**: Việc ứng phó sự cố là rất căng thẳng. Nhiều tổ chức sẵn sàng tìm ra những người giàu kinh nghiệm, có tay nghề, và đặc biệt là có thể hỗ trợ 24/7.
* **Chi phí**: Chi phí là một yếu tố quan trọng, đặc biệt là nếu nhân yêu cầu phải có văn phòng hoạt động 24/7. Các chi phí cho việc ứng phó sự cố thường được bỏ qua và không được nằm trong ngân sách. Tuy nhiên nó rất quan trọng trong hoạt động úng phó sự cố như chi phí cho các công cụ hỗ trự ứng phó sự cố, các công cụ điều tra số, các chi phí bảo vệ cho khu vực làm việc hay các đối tác truyền thông.
* **Nhân viên thẩm định**: Việc xử lý sự cố đòi hỏi những kiến thức chuyên môn và kinh nghiệm cao trong lĩnh vực kỹ thuật và không phải tổ chức nào cũng có những nhân viên đảm bảo được việc đó. Việc thuê các đội ứng phó cự cố bên ngoài thực hiện ứng phó sự cố cho tổ chức là cần thiết. Tuy nhiên, những nhân viên của tổ chức thường có những kiên thức tốt hơn về môi trường của tổ chức. Vì thế, nhân viên thẩm định là rất quan trọng trong việc xác định các báo động sau liên quan đến các hành vi cụ thể trong quá trình ứng phó sự cố.

Khi xem xét sử dụng nhân sự bên ngoài để thực hiện ứng phó sự cố, các tổ chức cần chú ý những điểm sau:

* **Chất lượng hiện tại và trong tương lai**: Các tổ chức nên xem xét không chỉ chất lượng hiện tại của việc ứng phó sự cố mà nên xem xét các hành động đảm bảo chất lượng của việc xử lý sự cố trong tương lai.
* **Phân chia trách nhiệm**: Các tổ chức thường bác bỏ các yêu cầu từ đội ứng phó sự cố bên ngoài liên quan đến môi trường hoạt động của hệ thống bên trong tổ chức ( Ví dụ như ngắt kết nối một máy chủ web). Điều quan trọng là phải xác định được hành động nào là thích hợp tại thời điểm quyết định. Các đội liên quan đến vấn đề sự cố bên trong tổ chức cũng nên hỗ trợ đội ứng phó sự cố bên ngoài khi cần thiết.
* **Tiết lộ những thông tin nhạy cảm**: Xác định các thông tin cần thiết có thể cung cấp cho bên thứ 3 là gì. Các thông tin nhảy cảm nên được giới hạn hết mức có thể. Ví dụ các đội ứng phó sự cố bên ngoài tổ chức có thể biết những hoạt động của người dùng có ID là 1234 những không được phép biết họ là ai hay họ có vai trò gì. Sauk hi tiếp nhận cuộc điều tra về sự cố, hai bên nên có các thỏa thuật không tiết lộ thông tin trong đó có các điều khoản cấm tiết lộ thông tin và các hình thức xử phạt nếu vi phạm.
* **Thiếu sự tương quan**: Sự tương quan giữa nhiều nguồn dữ liệu là rất quan trọng. Trong một ví dụ thực tế, nếu hệ thống phát hiện xâm nhập ghi lại được một cuộc tấn công vào máy chủ web, nhung không có việc truy xuất vào các bản ghi dữ liệu của máy chủ, điều này có thể không xác định là hành động tấn công đó có thành công hay không. Để có hiệu của, đội ứng phó sự cố ngoài sẽ yêu cầu được truy cập vào các hệ thống quan trọng. Điều này làm tăng chi phí quản lý cũng như nguy cơ tiết lộ những thông tin nhạy cảm.
* **Xử lý sự cố trên nhiều vị trí địa lý khác nhau**: Để việc xử lý sự cố có hiệu quả, các đội ứng phó sự cố thường yêu cầu được đến trực hiện vị trí của hệ thống để thực hiện điều tra. Việc này có thể dẫn đến việc phát sinh các chi phí về cơ sở vật chất cho đội ứng phó sự cố ngoài cũng như các vấn đề liên quan đến an toàn vật lý.
* **Duy trì các kỹ năng ứng phó sự cố tại tổ chức**: các tổ chức thuê ngoài hoàn toàn các đội ứng phó sự cố nên cố gắng duy trì các kỹ năng ứng phó sự cố cơ bản đối với một nhóm nhân viên bên trong tổ chức. Các tình huống có thể phát sinh trong khi các đội ứng phó sự cố ngoài không có mặt ở đó và cần được thực hiện gấp. Những kỹ thuật viên của tổ chức nên học được khẳ năng hiểu dược ý nghĩa, các thuật ngữ và các khuyến nghị của đội ứng phó sự cố.

### Thành viên trong đội ứng phó sự cố

Một nhân viên duy nhất nên được chỉ định để phụ trách việc ứng phó sự cố.

Trong mô hình thuê ngoài hoàn toàn, người này sẽ thực hiện giám sát, đánh giá và thẩm định hoạt động ứng phó sự cố. Người này có nhiệm vụ thực hiện các liên lạc với các bên liên quan (ví dụ như các cấp trên, các phòng ban liên quan, các đội ứng phó khác hay các tổ chức khác trong trường hợp cần thiết, tiếp xúc trực tiếp với các đơn vị truyền thông…) Người quản lý cần phải thành thạo kỹ thuật, có kỹ năng giao tiếp tốt đặc biệt là giao tiếp và nói trước nhiều người. Người quản lý cũng đảm bảo hoạt động ứng phó sự cố được thực hiện đúng cách, đúng quy trình.

Ngoài người quản lý, trong đội cầm có một người quản lý về mặt kỹ thuật. Người này phải có kiến thức về kỹ thuật sâu rộng, rất có kinh nghiệm trong việc xử lý sự cố, giám sát hệ thống và điều tra số. Đây là người chịu trách nhiệm về chất lượng công việc kỹ thuật của đội.

Thành viên của đội xử lý sự cố cần phải có kỹ thuật vững vàng về các mảng như quản trị hệ thống mạng, lập kỹ, phát hiện xâm nhập, điều tra số, phân tích mã động. Mỗi thành viên trong nhóm cần phải có kỹ năng giải quyết vấn đề và tư duy tốt.

Các gợi ý sau đây sẽ giúp ích cho việc xây dựng và duy trì đội kỹ thuật:

* Đảm bảo đầy đủ ngân sách cho việc tăng cường và mở rộng tầm hiểu biết về các lĩnh vực kỹ thuật cũng như các vấn đề về mặt pháp lý. Điều này bao gồm việc gửi nhân viên đến các hội thảo, hội nghị về kỹ thuật, đầu tư tài liệu, phòng lab cũng như có kế hoạch đào tạo các nhân viên kỹ thuật để nâng cao trình độ.
* Cho các thành viên trong đội được thực hiện các nhiệm vụ khác nhau.
* Tạo một chương trình đào tạo để hỗ trợ các nhân viên mới học hỏi kinh nghiệm trong việc xử lý sự cố.
* Xây dựng các kịch bản về sự cố và cùng nhau thảo luận về cách xử lý chúng ra sao.

Các thành viên trong đội ứng phó sự cố cần phải có những kỹ năng khác ngoài kỹ năng chuyên môn. Kỹ năng làm việc theo nhóm là rất quan trọng vì bản chất của sự ứng phó sự cố là sự hợp tác và phối hợp. Kỹ năng nói cũng là một kỹ năng quan trọng bởi vì các thành viên trong đội phải tương tác với nhau. Bên cạnh đó, kỹ năng viết giúp cho các thành viên có thể chuẩn bị cho mình các thủ tục và báo cáo cần thiết.

### Sự phụ thuộc bên trong tổ chức

Một điều rất quan trọng là xác định các nhóm hay các thành phần khác bên trong tổ chức có cần phải tham gia vào quá trình xử lý sự cố hay không để có được sự hợp tác của họ khi cần thiết.

* **Người quản lý**: Những người quản lý thực hiện xây dựng chính sách ứng phó sự cố, chi ngân sách và vấn đề về nhân sự. Những người quản lý cũng chịu trách nhiệm về việc phối hợp giữa các bên trong vấn đề giải quyết sự cố.
* **Đảm bảo thông tin**: Các nhân viên an ninh có thể cần thiết trong một số giai đoạn của sử lý sự cố (Phòng ngừa, ngăn chặn, xóa, phục hồi). Ví dụ như thay đổi các chính sách kiểm soát an ninh mạng.
* **Nhân viên hỗ trợ IT**: Các kỹ thuật viện công nghệ thông tin không chỉ có các kỹ năng về hỗ trợ người dùng cuối mà họ cũng có những hiểu biết tốt về công nghệ hay cơ sở hạ tầng mà họ quản lý. Sự hiểu biết này có thể đảm bảo các hành động thích hợp được thực hiện trong trường hợp hệ thống bị ảnh hưởng bởi sự cố.
* **Bộ phận pháp lý**: Các chuyên gia pháp lý nên xem xét các kế hoạch ứng phó sự cố, chính sách và thủ tục để đảm bảo tính phù hợp về mặt pháp luật.
* **Bộ phận truyền thông**: Tùy theo tính chất và tác động của một sự cố mà có thể tồn tại nhu cầu thông báo đến các đơn vị truyền về sự cố và kết quả của việc ứng phó sự cố.
* **Bộ phận nhân sự**: nếu một nhân viên bị nghi ngờ gây ra sự cố, bộ phận nhân sự có thể giam gia ví dụ như trong các trường hợp hỗ trợ hoàn thành thủ tục tố tụng pháp luật
* **Bộ phận kinh doanh**: Tổ chức cần đảm bảo việc các chính sách, thủ tục và các kế hoạch kinh doanh cần phải được đồng bộ. Các sự cố về an ninh máy tính có thể làm suy yếu sự phục hồi kinh doanh của một tổ chức. các chuyên gia về kinh doanh cần được biết về sự cố và mức độ ảnh hưởng để có thể đánh giá tác động đến hoạt động kinh doanh , đánh giá rủi ro nhằm đưa ra những kế hoạch phù hợp.
* **Bộ phân an ninh**: Một số sự cố an ninh máy tính xảy ra thông qua các vi phạm về vấn đề an ninh vật lý. Các đội phải ứng sự cố cần đến trực tiếp các cớ sở để xử lý sự cố.

### Các dịch vụ của đội ứng phó sự cố

Trọng tâm của một đội ứng phó sự cố là xử lý sự cố, nhưng nó khá là hiếm đội ứng phó sự cố nào mà chỉ hoạt động xử lý sự cố đơn thuần. Sau đây là một số dịch vụ ngoài mà đội ứng phó sự cố có thể cung cấp:

* Phát hiện xâm nhập: Điều này rất quan trọng đối với một đội ứng phó sự cố. Phát hiện xâm nhập là bước đầu tiên, nó có thể chỉ ra những sự kiện là tiềm năng cho một cuộc tấn công. Việc phát hiện sớm ảnh hưởng trực tiếp đến sự hiệu quả của hoạt động ứng phó sự cố.
* Tư vấn: Đội ứng phó sự cố có thể khuyến cáo tổ chức trong các vấn đề liên quan đến các lỗ hổng mới tiềm năng, các lỗ hổng về chính sách có thể dẫn đến tiền năng cho các cuộc tấn công.
* Đào tạo: Đội ứng phó sự cố có thể thực hiện đào tạo nâng cao nhận thức về an toàn thông tin cho các nhân viên cũng như đào tạo nâng cao tình độ chuyên môn cho các kỹ thuật viên trong tổ chức
* Chia sẻ thông tin: Các đội xử lý sự cố thường xuyên chia sẻ thông tin với nhau nhằn nâng cao khả năng phản ứng và xử lý sự cố.