ĐẠI HỌC QUỐC GIA HÀ NỘI
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ

NGUYỄN THỊ HẰNG

NGHIÊN CỨU BÀI TOÁN AN TOÀN THÔNG TIN CHO DOANH NGHIỆP VỪA VÀ NHỎ

LUẬN VĂN THẠC SĨ CÔNG NGHỆ THÔNG TIN

Hà Nội - 2017

ĐẠI HỌC QUỐC GIA HÀ NỘI
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ

NGUYỄN THỊ HẰNG

NGHIÊN CỨU BÀI TOÁN AN TOÀN THÔNG TIN CHO DOANH NGHIỆP VỪA VÀ NHỎ

Ngành: Công nghệ thông tin
Chuyên ngành: Quản lý Hệ thống thông tin
Mã số: Chuyên ngành đào tạo thí điểm

LUẬN VĂN THẠC SĨ CÔNG NGHỆ THÔNG TIN

NGƯỜI HƯỚNG DẪN KHOA HỌC: TS. LÊ PHÊ ĐÔ
TS. PHÙNG VĂN ỔN

Hà Nội - 2017

LỜI CÁM ƠN

Đầu tiên, tôi xin được bày tỏ lòng biết ơn sâu sắc tới hai thầy hướng dẫn Tiến sĩ Lê Phê Đô và Tiến sĩ Phùng Văn Ổn đã tận tâm, tận lực hướng dẫn, định hướng phương pháp nghiên cứu khoa học cho tôi; đồng thời cũng đã cung cấp nhiều tài liệu và tạo điều kiện thuận lợi trong suốt quá trình học tập, nghiên cứu để tôi có thể hoàn thành luận văn này.

Tôi xin chân thành cảm ơn các thầy cô giáo trong Bộ môn Hệ thống thông tin và Khoa Công nghệ thông tin, trường Đại học Công nghệ - Đại học Quốc gia Hà Nội đã nhiệt tình giảng dạy, truyền đạt những kiến thức, kinh nghiệm quý báu trong suốt thời gian tôi học tập tại trường.

Cuối cùng, tôi xin gửi lời cảm ơn tới gia đình, bạn bè và đồng nghiệp đã luôn quan tâm, ủng hộ và động viên, giúp tôi có nghị lực phấn đấu để hoàn thành tốt luận văn.

Hà Nội, tháng 7 năm 2017
Học viên thực hiện luận văn

Nguyễn Thị Hằng

LỜI CAM ĐOAN

Luận văn thạc sĩ đánh dấu cho những thành quả, kiến thức tôi đã tiếp thu được trong suốt quá trình rèn luyện, học tập tại trường. Tôi xin cam đoan luận văn này được hoàn thành bằng quá trình học tập và nghiên cứu của tôi dưới sự hướng dẫn khoa học của hai thầy giáo, TS. Lê Phê Đô và TS. Phùng Văn Ổn.

Nội dung trình bày trong luận văn là của cá nhân tôi hoặc là được tổng hợp từ nhiều nguồn tài liệu tham khảo khác đều có xuất xứ rõ ràng và được trích dẫn hợp pháp.

Tôi xin hoàn toàn chịu trách nhiệm và chịu mọi hình thức kỷ luật theo quy định cho lời cam đoan của mình.

Hà Nội, tháng 7 năm 2017
Người cam đoan

Nguyễn Thị Hằng

MỤC LỤC

DANH SÁCH CÁC KÝ HIỆU VÀ CHỮ VIẾT TẮT

TT	VIẾT TẮT	TIẾNG ANH	TIẾNG VIỆT
1.	AES	Advanced Encryption Standard	Chuẩn mã hoá tiên tiến
2.	ATTT	Information Security	An toàn thông tin
3.	CA	Certification Authority	Tổ chức chứng nhận
4.	CIA	Confidentiality, Integrity, Availability	Bộ ba tính bí mật, toàn vẹn, sẵn sàng
5.	CNTT	Information Technology	Công nghệ thông tin
6.	DES	Data Encryption Standard	Chuẩn mã hoá dữ liệu
7.	DNVVN	Small and Medium Enterprise	Doanh nghiệp vừa và nhỏ
8.	HTTT	Information System	Hệ thống thông tin
9.	RA	Registration Authority	Tổ chức đăng ký
10.	RSA	Rivest, Shamir, & Adleman	Thuật toán mật mã khoá công khai
11.	IP	Internet Protocol Address	Địa chỉ IP của máy tính
12.	IPS	Intrusion Prevention Systems	Hệ thống ngăn ngừa xâm nhập
13.	ISMS	Information Security Management System	Hệ thống quản lý an toàn thông tin
14.	TMĐT	E-commerce	Thương mại điện tử

DANH MỤC CÁC HÌNH VẼ

DANH MỤC CÁC BẢNG

MỞ ĐẦU

1. Tính cấp thiết của đề tài

Trong nền kinh tế tri thức, thông tin đã trở thành một vấn đề sống còn đối với mọi lĩnh vực của đời sống kinh tế - xã hội đặc biệt là trong quản lý kinh tế, nó quyết định sự thành bại của các doanh nghiệp trên thương trường nếu họ biết sử dụng sao cho đạt hiệu quả nhất. Ứng dụng CNTT giúp các doanh nghiệp nắm bắt thông tin một cách chính xác kịp thời, đầy đủ, góp phần nâng cao hiệu quả kinh doanh, sức cạnh tranh với thị trường trong và ngoài nước.

Tuy nhiên, cùng với sự phát triển nhanh chóng của các lĩnh vực công nghệ thì nguy cơ mất an toàn thông tin cũng là một vấn đề bức thiết đối với các doanh nghiệp khi gần đây xảy ra rất nhiều cuộc tấn công mạng, tấn công bởi các hacker với mức độ và hậu quả nghiêm trọng.

Theo số liệu của phòng Công nghiệp và Thương mại Việt Nam, lực lượng doanh nghiệp vừa và nhỏ Việt Nam hiện chiếm gần 98% tổng số doanh nghiệp trên cả nước, phát triển đa dạng các ngành nghề, lĩnh vực. Mỗi ngành nghề, lĩnh vực đòi hỏi thông tin trong đó cần phải được bảo mật, xác thực và toàn vẹn. Bảo đảm an toàn thông tin vừa giúp doanh nghiệp phát triển, vừa giúp doanh nghiệp có được hình ảnh uy tín, được các bên đối tác đánh giá và tin tưởng khi hợp tác.

Xuất phát từ thực tế đó, học viên đã chọn đề tài **"Nghiên cứu bài toán an toàn thông tin cho doanh nghiệp vừa và nhỏ"** làm luận văn thạc sĩ của mình nhằm góp phần giúp các DNVVN có thêm một số giải pháp quản lý, bảo vệ thông tin an toàn, hiệu quả.

2. Mục tiêu nghiên cứu

Trên cơ sở làm rõ những vấn đề lý luận và thực tiễn về **an toàn thông tin số**; sau khi phân tích đặc điểm hệ thống thông tin của các DNVVN, thực trạng an toàn thông tin trên thế giới và tại Việt Nam, học viên tìm hiểu một số hệ mật mã đảm bảo an toàn thông tin hiện đang được sử dụng phổ biến, đề xuất một số giải pháp giúp các DNVVN đảm bảo an toàn thông tin; đáp ứng yêu cầu doanh nghiệp Việt Nam hội nhập ngày càng sâu rộng và thành công vào nền kinh tế khu vực và thế giới.

3. Nội dung nghiên cứu

Ngoài phần mở đầu và kết luận, nội dung luận văn bao gồm:

Chương 1: Bài toán an toàn thông tin cho DNVVN.

Chương 2: Các hệ mật mã đảm bảo an toàn thông tin được dùng phổ biến hiện nay.

Chương 3: Một số giải pháp đảm bảo an toàn thông tin cho DNVVN.

Chương 4: Cài đặt và thử nghiệm chữ ký số đảm bảo ATTT trong việc ký kết hợp đồng điện tử cho DNVVN.

CHƯƠNG 1: BÀI TOÁN AN TOÀN THÔNG TIN CHO DNVVN

1.1. Cơ sở lý luận về an toàn thông tin

1.1.1. An toàn thông tin

Từ khi ra đời đến nay, mạng máy tính đã đem lại hiệu quả to lớn trong các lĩnh vực của đời sống kinh tế, chính trị, xã hội. Bên cạnh đó, người sử dụng mạng phải đối mặt với các mối đe doạ an toàn thông tin. An toàn thông tin trên mạng máy tính là một lĩnh vực đang được đặc biệt quan tâm đồng thời cũng là một công việc hết sức khó khăn, phức tạp.

Theo Luật Giao dịch điện tử ban hành ngày 29 tháng 11 năm 2005, an toàn thông tin số được định nghĩa như sau:

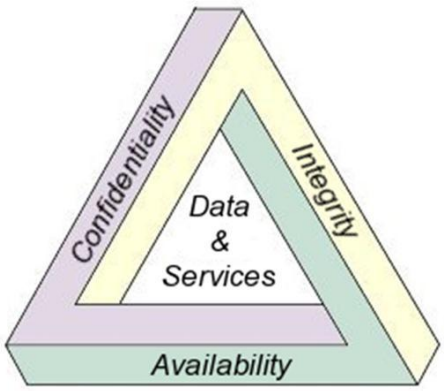
"An toàn thông tin số là thuật ngữ dùng để chỉ việc bảo vệ thông tin số và các hệ thống thông tin chống lại các nguy cơ tự nhiên, các hành động truy cập, sử dụng, phát tán, phá hoại, sửa đổi và phá huỷ bất hợp pháp nhằm bảo đảm cho các hệ thống thông tin thực hiện đúng chức năng, phục vụ đúng đối tượng một cách sẵn sàng, chính xác và tin cậy (sau đây gọi chung là an toàn thông tin)".

Nội dung của an toàn thông tin số bao gồm bảo vệ an toàn mạng và hạ tầng thông tin, an toàn máy tính, dữ liệu và ứng dụng công nghệ thông tin [2].

1.1.1.1. Các yếu tố đảm bảo an toàn thông tin [9]

An toàn thông tin bao gồm các hoạt động quản lý, nghiệp vụ và kỹ thuật đối với hệ thống thông tin nhằm bảo vệ, khôi phục các hệ thống, các dịch vụ và nội dung thông tin đối với nguy cơ tự nhiên hoặc do con người gây ra. Việc bảo vệ thông tin, tài sản và con người trong hệ thống thông tin nhằm bảo đảm cho các hệ thống thực hiện đúng chức năng, phục vụ đúng đối tượng một cách sẵn sàng, chính xác và tin cậy. An toàn thông tin bao hàm các nội dung bảo vệ và bảo mật thông tin, an toàn dữ liệu, an toàn máy tính và an toàn mạng.

An toàn thông tin mang nhiều đặc tính, những đặc tính cơ bản của an toàn thông tin bao gồm: Tính bảo mật (Confidentiality), tính toàn vẹn (Integrity) và tính sẵn sàng (Availability). Ba đặc tính này còn được gọi là tam giác bảo mật CIA. Các đặc tính này cũng đúng với mọi tổ chức, không lệ thuộc vào việc chúng chia sẻ thông tin như thế nào.



Hình 1. 1. Đặc tính cơ bản của an toàn thông tin

Tính bảo mật: Là tâm điểm chính của mọi giải pháp an toàn cho sản phẩm/hệ thống CNTT. Giải pháp an toàn là tập hợp các quy tắc xác định quyền được truy cập đến thông tin, với một số lượng người sử dụng thông tin nhất định cùng số lượng thông tin 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 dữ liệu nào và đảm bảo rằng các kiểm soát truy cập có hiệu lực, loại bỏ những truy cập trái phép vào các khu vực là độc quyền của cá nhân, tổ chức. Tính bảo mật rất cần thiết (nhưng chưa đủ) để duy trì sự riêng tư của người có thông tin được hệ thống lưu giữ.

Tính toàn vẹn: Không bị sửa đổi là đặc tính phức hợp nhất và dễ bị hiểu lầm của thông tin. 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 cần một loạt các biện pháp đồng bộ nhằm hỗ trợ và đảm bảo sự kịp thời và đầy đủ, cũng như sự bảo mật hợp lý cho thông tin.

Tính sẵn sàng: Đảm bảo độ sẵn sàng của thông tin, tức là thông tin có thể được truy xuất bởi những người được phép vào bất cứ khi nào họ muốn. Ví dụ, nếu một server bị ngừng hoạt động hay ngừng cung cấp dịch vụ trong vòng 5 phút trên một năm thì độ sẵn sàng của nó là 99.9999%. Đây là một đặc tính quan trọng, nó là khía cạnh sống còn của ATTT, 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 là thước đo, phạm vi giới hạn của một hệ thông tin.

Các tổ chức, doanh nghiệp muốn đảm bảo an toàn thông tin thì luôn cần phải duy trì được sự cân bằng của ba yếu tố trên, ngoài ra các thuộc tính khác như tính xác thực, trách nhiệm giải trình, tính thừa nhận và tính tin cậy cũng có thể liên quan.

1.1.1.2. Các nguy cơ mất an toàn thông tin

Các mối đe doạ được hiểu là những sự kiện, những tác động hoặc hiện tượng tiềm năng có thể, mà khi xảy ra sẽ mang lại những thiệt hại.

Các mối đe doạ an toàn mạng được hiểu là những khả năng tác động lên hệ thống mạng máy tính, khi xảy ra sẽ dẫn tới sự sao chép, biến dạng, huỷ hoại dữ liệu; là khả năng tác động tới các thành phần của hệ thống dẫn tới sự mất mát, sự phá huỷ hoặc sự ngừng trệ hoạt động của hệ thống mạng…

Như đã nêu ở mục 1.1.1.1, hệ thống mạng được gọi là an toàn phải thoả mãn bộ ba CIA. Tương ứng, các mối đe doạ an toàn mạng cũng được phân thành ba loại:

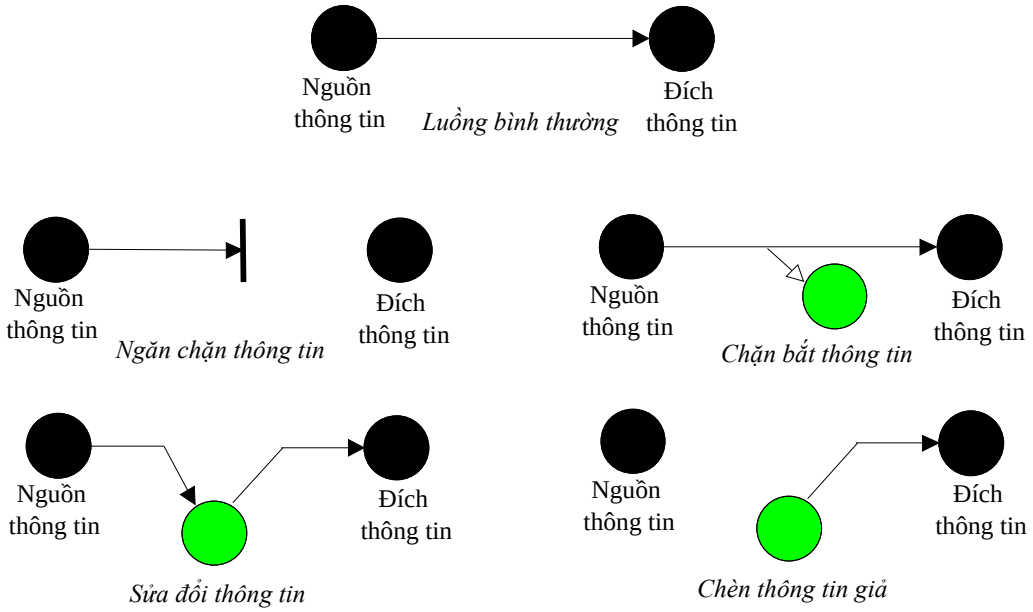
- ***Mối đe doạ phá vỡ tính bí mật*** là nguy cơ việc thông tin trong quá trình xử lý bị xem trộm, dữ liệu trao đổi trên đường truyền bị lộ, bị khai thác trái phép…

- ***Mối đe doạ phá vỡ tính toàn vẹn*** là dữ liệu khi truyền đi từ nơi này đến nơi khác, hay đang lưu trữ có nguy cơ bị thay đổi, sửa chữa làm sai lệch nội dung thông tin.

- ***Mối đe doạ phá vỡ tính sẵn sàng*** là hệ thống mạng có nguy cơ rơi vào trạng thái từ chối phục vụ, khi mà hành động cố ý của kẻ xấu làm ngăn cản tiếp nhận tới tài nguyên của hệ thống; sự ngăn cản tiếp nhận này có thể là vĩnh viễn hoặc có thể kéo dài trong một khoảng thời gian nhất định

1.1.2. Tấn công luồng thông tin trên mạng

Luồng thông tin được truyền từ nơi gửi (nguồn) đến nơi nhận (đích). Trên đường truyền công khai, thông tin bị tấn công bởi những người không được uỷ quyền nhận tin (gọi là kẻ tấn công).



Hình 1. 2. Mô hình tấn công luồng thông tin [9]

Các tấn công luồng thông tin trên mạng bao gồm:

Tấn công ngăn chặn thông tin

Tấn công ngăn chặn thông tin (interruption) là tấn công làm cho tài nguyên thông tin bị phá huỷ, không sẵn sàng phục vụ hoặc không sử dụng được. Đây là hình thức tấn công làm mất khả năng sẵn sàng phục vụ của thông tin.

Ví dụ: Những ví dụ về kiểu tấn công này là phá huỷ đĩa cứng, cắt đứt đường truyền tin, vô hiệu hoá hệ thống quản lý tệp.

Tấn công chặn bắt thông tin

Tấn công chặn bắt thông tin (interception) là tấn công mà kẻ tấn công có thể truy cập tới tài nguyên thông tin. Đây là hình thức tấn công vào tính bí mật của thông tin.

Trong một số tình huống kẻ tấn công được thay thế bởi một chương trình hoặc một máy tính.

Ví dụ: Việc chặn bắt thông tin có thể là nghe trộm để thu tin trên mạng (trộm mật khẩu) và sao chép bất hợp pháp các tệp tin hoặc các chương trình.

Tấn công sửa đổi thông tin

Tấn công sửa đổi thông tin (modification) là tấn công mà kẻ tấn công truy nhập, chỉnh sửa thông tin trên mạng. Đây là hình thức tấn công vào tính toàn vẹn của thông tin. Nó có thể thay đổi giá trị trong tệp dữ liệu, sửa đổi chương trình và sửa đổi nội dung các thông điệp truyền trên mạng.

Ví dụ: Kẻ tấn công sử dụng các đoạn mã nguy hiểm, virus…

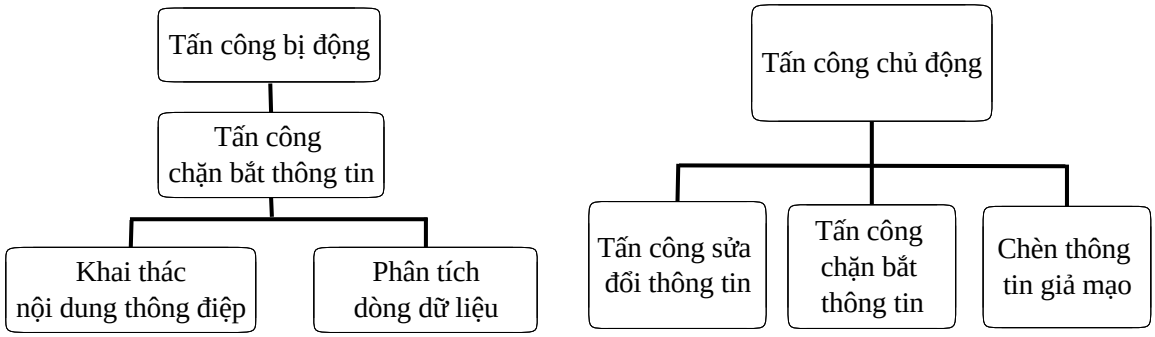
Chèn thông tin giả mạo

Kẻ tấn công chèn các thông tin và dữ liệu giả vào hệ thống. Đây là hình thức tấn công vào tính xác thực của thông tin. Nó có thể là việc chèn các thông báo giả mạo vào mạng hay thêm các bản ghi vào tệp.

Ví dụ: Tấn công giả mạo địa chỉ IP.

1.1.3. Phân loại các kiểu tấn công luồng thông tin trên mạng

Các kiểu tấn công luồng thông tin trên được phân chia thành hai lớp cơ bản là tấn công bị động (passive attacks) và chủ động (active attacks)



Hình 1. 3. Phân loại các kiểu tấn công luồng thông tin trên mạng [9]

Tấn công bị động

Là kiểu tấn công chặn bắt thông tin như nghe trộm và quan sát truyền tin. Mục đích của kẻ tấn công là biết được thông tin truyền trên mạng.

Có hai kiểu tấn công bị động là khai thác nội dung thông điệp và phân tích dòng dữ liệu.

Việc khai thác nội dung thông điệp có thể được thực hiện bằng cách nghe trộm các đoạn hội thoại, đọc trộm thư điện tử hoặc xem trộm nội dung tập tin.

Trong kiểu phân tích dòng dữ liệu, kẻ tấn công thu các thông điệp được truyền trên mạng và tìm cách khai thác thông tin. Nếu nội dung các thông điệp bị mã hoá thì đối phương có thể quan sát mẫu thông điệp để xác định vị trí, định danh của máy tính liên lạc và có thể quan sát tần số và độ dài thông điệp được trao đổi từ đó đoán ra bản chất của các cuộc liên lạc.

Tấn công bị động rất khó bị phát hiện vì nó không làm thay đổi dữ liệu và không để lại dấu vết rõ ràng. Biện pháp hữu hiệu để chống lại kiểu tấn công này là ngăn chặn (đối với kiểu tấn công này, ngăn chặn tốt hơn là phát hiện).

Tấn công chủ động

Là kiểu tấn công sửa đổi dòng dữ liệu hay tạo ra dòng dữ liệu giả. Tấn công chủ động được chia thành các loại nhỏ sau:

- Giả mạo (Masquerade): một thực thể (người dùng, máy tính, chương trình…) đóng giả thực thể khác.
- Dùng lại (Replay): chặn bắt các thông điệp và sau đó truyền lại nó nhằm đặt được mục đích bất hợp pháp.
- Sửa thông điệp (Modification of messages): một bộ phận của thông điệp bị sửa đổi hoặc các thông điệp bị làm trễ và thay đổi trật tự để đạt được mục đích bất hợp pháp.

Như vậy, hai kiểu tấn công: tấn công bị động và tấn công chủ động có những đặc trưng khác nhau. Kiểu tấn công bị động khó phát hiện nhưng có biện pháp để ngăn chặn thành công. Kiểu tấn công chủ động dễ phát hiện nhưng lại rất khó ngăn chặn, nó cũng đòi hỏi việc bảo vệ vật lý tất cả các phương tiện truyền thông ở mọi lúc, mọi nơi. Giải pháp để chống lại các kiểu tấn công này là phát hiện chúng và khôi phục mạng khi bị phá vỡ hoặc khi thông tin bị trễ.

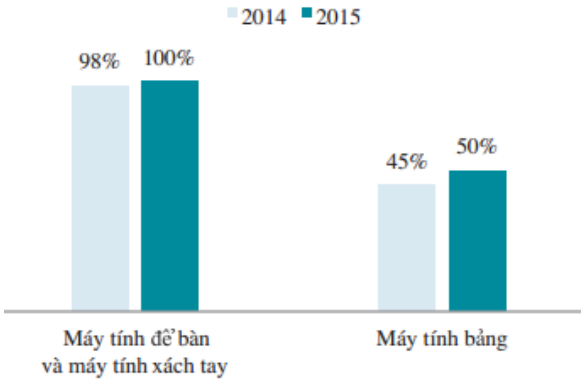
1.2. Thực trạng ATTT đối với các DNVVN

1.2.1. Đặc điểm hệ thống thông tin của các DNVVN

Do nhận thức được hiệu quả của ứng dụng công nghệ thông tin, các doanh nghiệp nói chung và DNVVN nói riêng đã có ứng dụng CNTT trực tiếp trong sản xuất kinh doanh, hầu hết các doanh nghiệp có ứng dụng CNTT trong quản lý, điều hành, …

Về hạ tầng kỹ thuật

Hạ tầng kỹ thuật bao gồm các thiết bị CNTT như máy tính, máy in, các thiết bị trực tiếp xử lý thông tin và mạng máy tính. Thiết bị CNTT là điều kiện cơ sở để doanh nghiệp triển khai thực hiện ứng dụng CNTT. Theo "Báo cáo Thương mại điện tử năm 2015 (BCTMĐT 2015), Cục Thương mại điện tử và Công nghệ thông tin, Bộ Công Thương", báo cáo dựa trên kết quả phân tích 4.751 phiếu khảo sát thu về từ các doanh nghiệp thuộc nhiều loại hình, lĩnh vực và quy mô, trong đó có 88% là các DNVVN. Kết quả khảo sát cho thấy, số lượng DNVVN có trang bị máy tính để bàn và máy tính xách tay 100%. Tỷ lệ doanh nghiệp trang bị máy tính bảng có xu hướng tăng từ 45% năm 2014 lên 50% năm 2015.



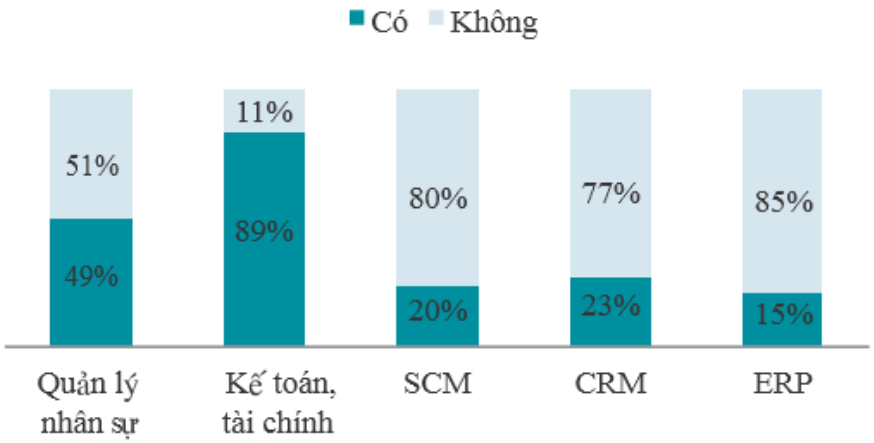
Hình 1. 4. Tỷ lệ máy tính trong doanh nghiệp [3]

Mạng và kết nối Internet là điều kiện kỹ thuật cơ sở để doanh nghiệp ứng dụng CNTT trên toàn bộ doanh nghiệp và tham gia thị trường thương mại điện tử, hiện đã có 98% số doanh nghiệp tham gia khảo sát đã kết nối Internet. Tỉ lệ doanh nghiệp truy cập Internet cao nhất tập trung ở hai thành phố lớn là Hà Nội và thành phố Hồ Chí Minh.

Theo số liệu khảo sát, hiện nay các doanh nghiệp đang sử dụng Internet với các mục đích chính như tìm kiếm thông tin, trao đổi thông tin , quản lý đơn hàng qua email, quảng cáo, tiếp thị sản phẩm và dịch vụ, mua hàng qua mạng,… Trong đó, hầu hết các nghiệp cho rằng mục đích sử dụng Internet là tìm kiếm và trao đổi thông tin.

Về ứng dụng CNTT trong hoạt động quản lý điều hành [3]

Hầu hết các DNVVN mới chỉ sử dụng các phần mềm phục vụ tác nghiệp đơn giản như thư điện tử, phần mềm văn phòng, ngoài ra còn có hai phần mềm được sử dụng phổ biến là phần mềm kế toán, tài chính (89%) và quản lý nhân sự (49%). Bên cạnh đó, một số phần mềm khác được doanh nghiệp sử dụng như: phần mềm quan hệ khách hàng (Customer Relationship Management – CRM) với 23% doanh nghiệp sử dụng, phần mềm quản lý hệ thống cung ứng (Supply Chain Management – SCM) với 20% doanh nghiệp sử dụng và phần mềm lập kế hoạch nguồn lực (Enterprise Resource Planning – ERP) với tỷ lệ 15% doanh nghiệp sử dụng.

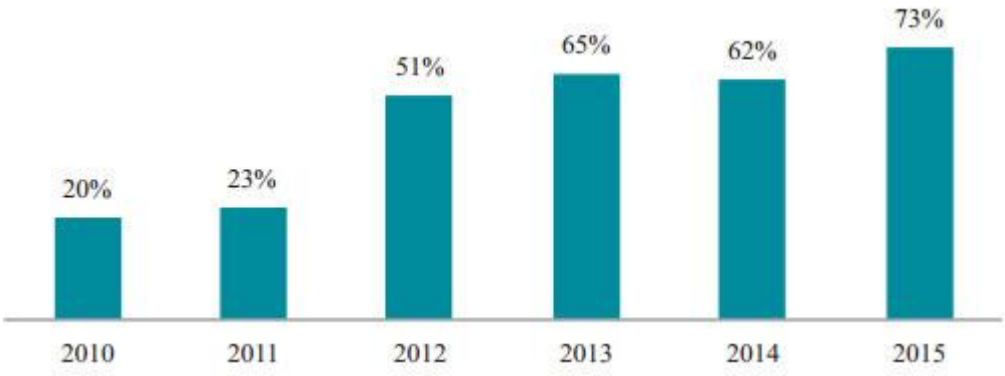


Hình 1. 5. Tỷ lệ ứng dụng phần mềm trong DNVVN [3]

Bên cạnh việc ứng dụng các phần mềm phục vụ tác nghiệp kể trên, các DNVVN cũng đã thiết lập website vào trong hoạt động sản xuất kinh doanh phổ biến hơn. Cụ thể, trong năm 2015 số doanh nghiệp có website là 45%, 8% doanh nghiệp cho biết sẽ xây dựng website trong năm tiếp theo. Ba nhóm doanh nghiệp sở hữu website cao nhất theo lĩnh vực kinh doanh là công nghệ thông tin và truyền thông (72%), y tế - giáo dục - đào tạo (66%), du lịch - ăn uống (62%)[3].

Về nguồn nhân lực phụ trách CNTT

Tỷ lệ doanh nghiệp có cán bộ chuyên trách về CNTT và TMĐT tăng qua các năm, từ 20% năm 2010 lên 73% năm 2015.

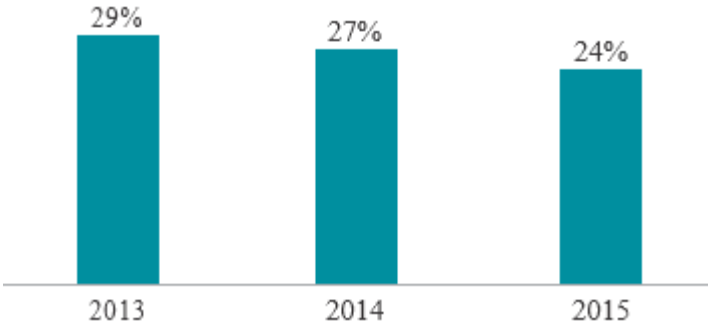


Hình 1. 6. Tỷ lệ DNVVN có cán bộ chuyên trách về CNTT qua các năm [3]

Trong đó, ba lĩnh vực hoạt động của doanh nghiệp có tỷ lệ cán bộ chuyên trách CNTT và TMĐT cao nhất công nghệ thông tin và truyền thông (94%), giải trí (90%) tài chính và bất động sản (85%).

Hình 1. 7. Tỷ lệ doanh nghiệp có cán bộ chuyên trách về CNTT và TMĐT theo lĩnh vực kinh doanh

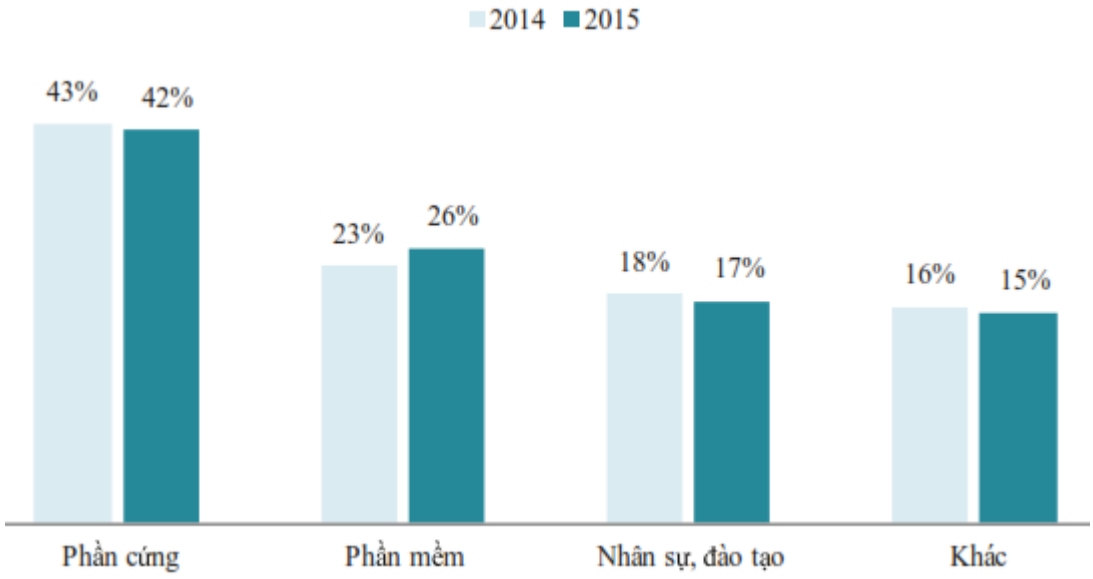
Tuy nhiên việc tuyển dụng ***nhân sự có kỹ năng về CNTT thì lại gặp khó khăn***, kết quả khảo sát trong 3 năm gần đây cho thấy tỷ lệ này có chiều hướng giảm, từ 29% năm 2013 xuống còn 24% năm 2015.



Hình 1. 8. Khó khăn trong việc tuyển dụng nhân sự có kỹ năng CNTT và TMĐT [3]

Về cơ cấu chi phí cho hạ tầng CNTT trong doanh nghiệp

Chi phí cho hạ tầng công nghệ thông tin trong doanh nghiệp tương tự nhau qua các năm. Năm 2015, phần cứng vẫn chiếm tỷ trọng đầu tư cao nhất (42%), tiếp đến là phần mềm (26%), nhân sự và đào tạo (17%). Việc mua sắm phần cứng, phần mềm cũng là vấn đề lớn đối với doanh nghiệp, ***nhiều doanh nghiệp dễ dàng quyết định mua phần cứng, nhưng lại rất khó khăn khi mua phần mềm***.



Hình 1. 9. Cơ cấu chi phí cho hạ tầng công nghệ thông tin [3]

Số liệu tổng hợp cho thấy, do quy mô về nguồn nhân lực và vốn, **hệ thống thông tin của các DNVVN so với các doanh nghiệp lớn còn nhiều hạn chế**:

Các DNVVN không thể đầu tư có chiều sâu vào các ứng dụng CNTT cũng như hệ thống mạng đắt tiền. Các phần mềm mang tính đồng bộ, an toàn, hiệu quả như ERP là "bài toán khó" đối với các doanh nghiệp.

Về mặt nhân sự CNTT, các DNVVN chưa đầu tư một cách lâu dài, chưa có các cán bộ chuyên trách đảm nhiệm vai trò an toàn thông tin, việc đào tạo ý thức ATTT cho toàn bộ người dùng của các DNVVN gần như chưa được triển khai.

Bên cạnh đó, nhiều doanh nghiệp không biết cách thiết lập một quy trình chuẩn và các biện pháp bảo vệ hệ thống của mình.

Do đó, việc nghiên cứu các giải pháp đảm bảo ATTT cho các doanh nghiệp vừa và nhỏ là vấn đề cấp thiết

1.2.2. Thực trạng ATTT thế giới

Trong những năm gần đây, an toàn thông tin ngày càng trở nên quan trọng đối với các quốc gia trên thế giới. Nó không chỉ ảnh hưởng đến các vấn đề về an ninh, quốc phòng mà còn tác động trực tiếp đến nền kinh tế của các quốc gia nói chung và của doanh nghiệp, cá nhân mỗi người nói riêng.

Năm 2016 tình hình tấn công mạng trên thế giới gia tăng đáng kể, có diễn biến rất phức tạp và khó đoán trước, hàng loạt công ty bị đánh cắp tài khoản người dùng, trong đó nổi bật là vụ đánh cắp thông tin tài khoản người dùng tại Yahoo tháng 12/2016. Công ty là nạn nhân của một vụ tấn công từ tháng 8/2013 - kết quả của việc tin tặc chiếm được mã hóa riêng của công ty. Tin tặc đã lấy đi dữ liệu từ hơn 1 tỉ tài khoản người dùng, bao gồm tên, địa chỉ email, số điện thoại, ngày sinh, mật khẩu dạng "hàm băm"…. Đây là vụ rò rỉ thông tin tài khoản lớn chưa từng có. Trước đó, tháng 9/2016, công ty Yahoo tuyên bố, tin tặc "do chính phủ tài trợ" cũng đã đánh cắp dữ liệu từ 500 triệu người dùng.

Hay tháng 5/2016, hàng trăm triệu tài khoản LinkedIn và Myspace đã bị tin tặc tấn công và chiếm quyền điều khiển. Tháng 6/2016, 32 triệu tài khoản Twitter bị hack bởi một tin tặc Nga có tên Tessa88....

Năm 2016 cũng là năm mã độc tống tiền - Ransomware trở thành vấn nạn

Theo số liệu của Kaspersky Lab (khảo sát từ tháng 4/2014 đến tháng 3/2016), năm 2016, cứ 40 giây lại xuất hiện một cuộc tấn công vào doanh nghiệp, số lượng các cuộc tấn công từ mã độc tống tiền nhắm vào doanh nghiệp đã tăng lên gấp 3 lần. Cụ thể, các cuộc tấn công sử dụng mã độc tống tiền đã tăng từ 131.111 vụ trong giai đoạn 2014 - 2015, lên 718.536 vụ trong giai đoạn 2015-2016.

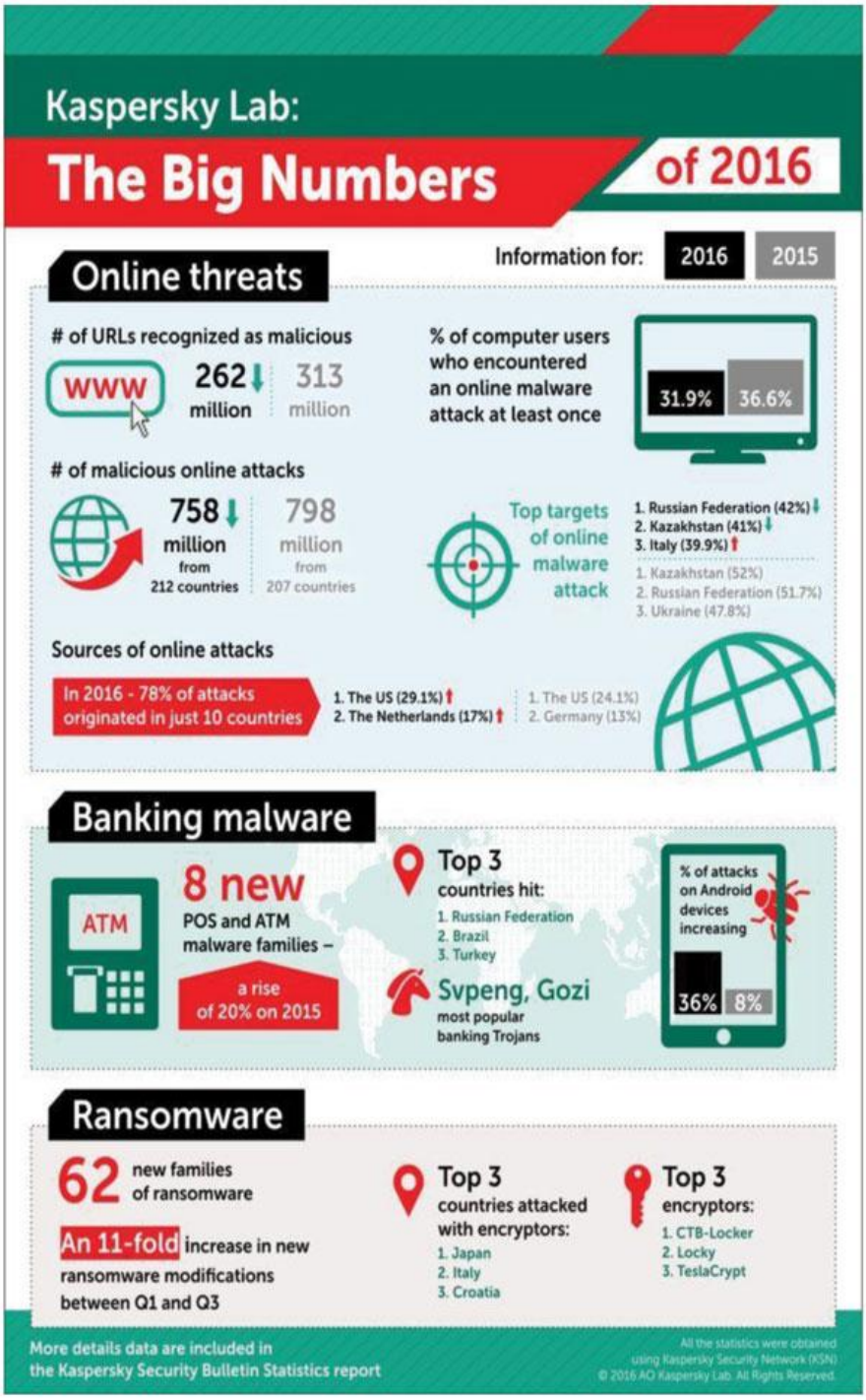
Gần đây nhất là vụ tấn công mạng bằng mã độc WannaCry diễn ra vào ngày 12/5/2017 - vụ tấn công mạng chưa từng có trong lịch sử khiến 300.000 máy tính tại 150 quốc gia nhiễm mã độc tống tiền WannaCry [30], gây ảnh hưởng nghiêm trọng đến các bệnh viện, khiến các nhà máy phải đóng cửa và làm cho Microsoft cũng như các nhà nghiên cứu an ninh đau đầu.

Ngoài ra tấn công mạng bằng mã độc lây nhiễm trên thiết bị IoT cũng xảy ra tràn lan:

Tháng 10/2016, một mạng botnet cỡ lớn đã tấn công DDoS vào Dyn, nhà cung cấp hệ thống tên miền lớn của thế giới, khiến gần như một nửa nước Mỹ bị mất kết nối Internet. Đợt tấn công DDoS nhắm vào Dyn đã khiến hàng loạt trang web lớn như Twitter, GitHub và Netflix bị đánh sập trong một ngày. Theo các nhà nghiên cứu, một

mã độc với tên gọi Mirai đã lợi dụng những lỗ hổng và sử dụng những thiết bị bị nhiễm để tung ra những cuộc tấn công từ chối dịch vụ quy mô lớn.

Tháng 11/2016 hơn 900.000 thiết bị định tuyến băng thông rộng (broadband routers) của nhà cung cấp dịch vụ viễn thông Deutsche Telekom, Đức đã bị ngưng trệ hoạt động sau một cuộc tấn công gây ảnh hưởng đến hệ thống điện thoại, truyền hình và dịch vụ Internet của nước này, do các thiết bị bị lây nhiễm Mirai [32].

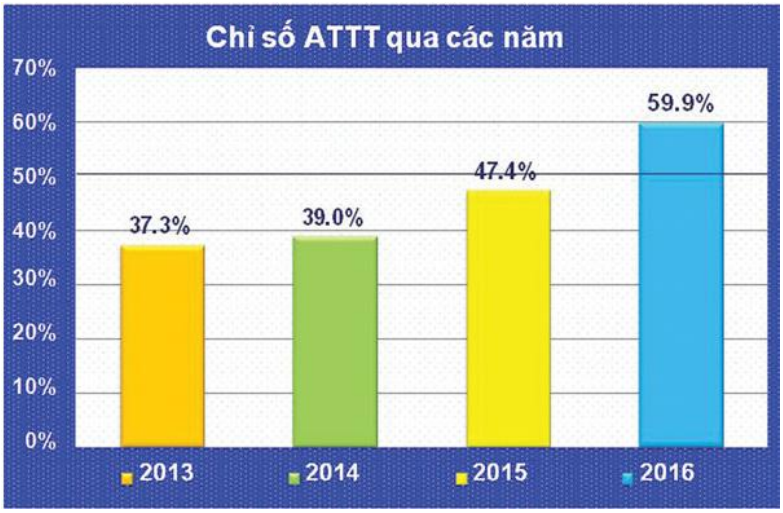


Hình 1. 10. Tình hình tấn công mạng trên thế giới năm 2016 (nguồn Kaspersky Lab)

Tháng 4/2016, dữ liệu của công ty luật Mossack Fonseca tại Panama bị rò rỉ, bao gồm 2,6 TB dữ liệu, gấp 100 lần so với vụ rò rỉ dữ liệu Wikileaks từng gây chấn động toàn cầu vào năm 2010. Đây là các thông tin trong khoảng thời gian từ năm 1977 đến tháng 12/2015 của công ty luật Mossack Fonseca, trong đó có 11,5 triệu tài liệu, bao gồm cả email và hợp đồng kinh doanh. Tin tặc tiết lộ hơn 214.000 công ty "vỏ bọc" được thành lập trên 200 quốc gia và vùng lãnh thổ. Các công ty này thường được dùng vào các mục đích chuyển giá và trốn thuế. Nguyên nhân được xác định là lỗ hổng trên trang web của hãng Moscack Fonseca, đã tạo cơ hội giúp "John Doe" có thể sở hữu được lượng lớn các dữ liệu bị rò rỉ.

1.2.3. Thực trạng ATTT đối với các doanh nghiệp Việt Nam

Theo khảo sát của Hiệp hội An toàn thông tin Việt Nam, chỉ số ATTT của Việt Nam trong năm 2016 là 59,9%. Đây là bước tiến đáng kể trong những năm qua, bởi năm 2015, con số này là 47,4%. Tuy lần đầu chỉ số ATTT của Việt Nam vượt ngưỡng trung bình, nhưng theo các chuyên gia, với mức độ tấn công ngày càng mạnh, kỹ thuật tấn công ngày càng tinh vi của tin tặc, các tổ chức, doanh nghiệp cần phải nâng cao cảnh giác hơn nữa với tội phạm mạng.



Hình 1. 11. Chỉ số ATTT qua các năm (nguồn VNISA)

Báo cáo của Trung tâm ứng cứu khẩn cấp máy tính Việt Nam (VNCERT) thống kê, năm 2016 có tổng số 134.375 sự cố tấn công mạng của cả 3 loại hình Phishing (lừa đảo), Malware (mã độc) và Deface (thay đổi giao diện). So với năm 2015, số lượng vụ tấn công mạng năm 2016 nhiều gấp hơn 4,2 lần (năm 2015 là 31.585), trong đó, loại hình tấn công Phishing là 10.057 sự cố (gấp hơn 1,7 lần so với năm 2015), Malware là 46.664 sự cố (gấp gần 2,8 lần năm 2015) và Deface là 77.654 sự cố (gấp hơn 8,7 lần năm 2015)

Con số này lớn hơn khá nhiều so với các sự cố của Việt Nam được ghi nhận trong những năm trước đó. Cụ thể; 2011 là 757 sự cố; 2012 là 2179 sự cố; 2013 là 4.810 sự cố; 2014 là 28.186 sự cố và 2015 là 31.585 sự cố. Tình hình an toàn, an ninh thông tin

ở Việt Nam vẫn diễn ra khá phức tạp với các loại hình tấn công mã độc, tấn công có chủ đích APT, lừa đảo qua mạng, qua tin nhắn rác, các mã độc phát tán qua email rác…

Năm 2016 nổi lên tình trạng lừa đảo thông tin qua mạng xã hội. Kẻ xấu luôn luôn tìm cách đưa ra những hình thức, thủ đoạn mới để lừa những người sử dụng nhằm thực hiện hành vi đánh cắp thông tin, thu lợi bất chính, xuất hiện hình thức biến đổi lừa đảo mới khi hacker tạo ra những website giả mạo có giao diện rất giống những website chính thống. Khi người sử dụng thực hiện theo chỉ dẫn trong website để có thể nhân giá trị thẻ cào lên, mã thẻ cào được nhập vào website giả mạo này sẽ bị đánh cắp.

Tổng hợp các số liệu cho thấy, các vụ tấn công mạng vào nước ta không còn lẻ tẻ và quy mô nhỏ nữa mà được xác định là tấn công có chủ đích, có tổ chức và kế hoạch rõ ràng, đáng kể đến là vụ tấn công vào sân bay Nội Bài, Tân Sơn Nhất chiều 29/7/2016. Hàng loạt màn hình hiển thị thông tin chuyến bay cùng hệ thống phát thanh của sân bay Nội Bài, Tân Sơn Nhất bất ngờ bị tấn công, trên các màn hình hiển thị nội dung kích động, xuyên tạc về Biển Đông. Hệ thống phát thanh của sân bay cũng phát đi những thông điệp tương tự. Cùng thời điểm, trên website của hãng hàng không quốc gia Việt Nam (vietnamairlines.com) cũng bị thay đổi nội dung, đồng thời đăng tải thông tin của hơn 400.000 thành viên Golden Lotus. Vụ tấn công sau đó được Vietnamairlines và các cơ quan chức năng trong lĩnh vực ATTT phối hợp xử lý tốt. Nhưng đây là vụ tấn công mạng nghiêm trọng vào hệ thống hạ tầng CNTT quan trọng của quốc gia và để lại nhiều hệ lụy xấu.

Năm 2016, tấn công mạng cũng diễn ra mạnh, tập trung vào lĩnh vực tài chính

Điển hình cho các vụ tấn công vào lĩnh vực tài chính là Ngân hàng TMCP Ngoại thương Việt Nam (Vietcombank). Tháng 8/2016, một khách hàng của Vietcombank đã bị mất số tiền 500 triệu đồng qua giao dịch Internet Banking. Nguyên nhân được xác định là do khách hàng đã truy cập vào một trang web giả mạo qua điện thoại di động, khiến thông tin và mật khẩu của khách hàng đã bị đánh cắp, sau đó tin tặc lợi dụng lấy cắp tiền trong tài khoản.

Trước đó, Ngân hàng BIDV và HSBC cũng được nhắc đến trong vụ việc liên quan chiếm thông tin tài khoản thẻ tín dụng, sử dụng để quảng cáo cho Fanpage lạ trên Facebook, đặt phòng qua Agoda, mua Game, sử dụng dịch vụ facebook với số tiền lên đến hàng chục triệu đồng….

Trước thực trạng tấn công mạng ngày càng gia tăng và lan tràn, thì ý thức về an toàn thông tin của doanh nghiệp, nhất là DNVVN, lại có chiều hướng đi xuống, các doanh nghiệp chưa quan tâm nhiều đến an toàn thông tin. Kết quả khảo sát về hiện trạng an toàn thông tin tại DNVVN năm 2016 của Hiệp hội An toàn thông tin (VNISA) cho thấy, chỉ có 34% doanh nghiệp có người phụ trách về ATTT. Tỷ lệ các đơn vị có phê duyệt và ban hành chính sách ATTT cũng giảm sút so với năm 2014 (23,7% trong năm 2016 so với 30% của năm 2015). Số lượng các doanh nghiệp có quy định bảo mật thông tin

cá nhân cũng giảm sút và có rất ít doanh nghiệp áp dụng các tiêu chuẩn bảo mật thông dụng như ISO 27001 hoặc PCI.

Do đặc điểm quy mô và tài chính còn hạn hẹp, nên việc đầu tư hệ thống bảo mật thông tin đối với nhiều các DNVVN được xem là hoạt động lãng phí. Bên cạnh đó, việc đào tạo đội ngũ quản trị viên các hệ thống thông tin cũng chưa được đầu tư, kiến thức, kỹ năng bảo đảm an toàn mạng, nhất là kỹ năng xử lý các tình huống xâm phạm gần như không có.

1.3. Bài toán an toàn thông tin cho DNVVN

1.3.1. Các nguy cơ mất ATTT đối với DNVVN

Nguy cơ mất an toàn thông tin về khía cạnh vật lý

Nguy cơ mất an toàn thông tin về khía cạnh vật lý là nguy cơ do mất điện, nhiệt độ, độ ẩm không đảm bảo, hỏa hoạn, thiên tai, thiết bị phần cứng bị hư hỏng, các phần tử phá hoại như nhân viên xấu bên trong và kẻ trộm bên ngoài.

Nguy cơ bị mất, hỏng, sửa đổi nội dung thông tin:

Người dùng có thể vô tình để lộ mật khẩu hoặc không thao tác đúng quy trình tạo cơ hội cho kẻ xấu lợi dụng để lấy cắp hoặc làm hỏng thông tin.

Kẻ xấu có thể sử dụng công cụ hoặc kỹ thuật của mình để thay đổi nội dung thông tin (các file) nhằm sai lệnh thông tin của chủ sở hữu hợp pháp.

Nguy cơ bị tấn công bởi các phần mềm độc hại

Các phần mềm độc hại tấn công bằng nhiều phương pháp khác nhau để xâm nhập vào hệ thống với các mục đích khác nhau như: virus, sâu máy tính (Worm), phần mềm gián điệp (Spyware),...

Nguy cơ xâm nhập từ lỗ hổng bảo mật

Lỗ hổng bảo mật thường là do lỗi lập trình, lỗi hoặc sự cố phần mềm, nằm trong một hoặc nhiều thành phần tạo nên hệ điều hành hoặc trong chương trình cài đặt trên máy tính.

Hiện, nay các lỗ hổng bảo mật được phát hiện ngày càng nhiều trong các hệ điều hành, các web server hay các phần mềm khác, ... Và các hãng sản xuất luôn cập nhật các lỗ hổng và đưa ra các phiên bản mới sau khi đã vá lại các lỗ hổng của các phiên bản trước.

Nguy cơ xâm nhập do bị tấn công bằng cách phá mật khẩu

Quá trình truy cập vào một hệ điều hành có thể được bảo vệ bằng một khoản mục người dùng và một mật khẩu. Đôi khi người dùng khoản mục lại làm mất đi mục đích bảo vệ của nó bằng cách chia sẻ mật khẩu với những người khác, ghi mật khẩu ra và để nó công khai hoặc để ở một nơi nào đó cho dễ tìm trong khu vực làm việc của mình.

Kẻ tấn công sử dụng một phần mềm dò thử các mật khẩu khác nhau có thể. Phần mềm này sẽ tạo ra các mật khẩu bằng cách kết hợp các tên, các từ trong từ điển và các số. Ta có thể dễ dàng tìm kiếm một số ví dụ về các chương trình đoán mật khẩu trên mạng Internet như: Xavior, Authforce và Hypnopaedia. Các chương trình dạng này làm việc tương đối nhanh và luôn có trong tay những kẻ tấn công.

Nguy cơ mất ATTT do sử dụng e-mail

Tấn công có chủ đích bằng thư điện tử là tấn công bằng email giả mạo giống như email được gửi từ người quen, có thể gắn tập tin đính kèm nhằm làm cho thiết bị bị nhiễm virus. Cách thức tấn công này thường nhằm vào một cá nhân hay một tổ chức cụ thể. Thư điện tử đính kèm tập tin chứa virus được gửi từ kẻ mạo danh là một đồng nghiệp hoặc một đối tác nào đó. Người dùng bị tấn công bằng thư điện tử có thể bị đánh cắp mật khẩu hoặc bị lây nhiễm virus.

Nguy cơ mất ATTT với website

Về mặt kỹ thuật, các website của các DNVVN thường được xây dựng thông qua một bên thứ ba, nhưng hầu hết các công ty xây dựng website ở Việt Nam chưa có tiêu chuẩn hoặc có quy trình kiểm soát các vấn đề về bảo mật trong quá trình xây dựng. Vì thế, rất nhiều website tồn tại những lỗ hổng nghiêm trọng cho phép xâm nhập và chiếm quyền điều khiển. Các lỗ hổng thường gặp như: SQL Injection, Cross-site Scripting, Upload....

Hầu hết các website của DNVVN khi bị tấn công thì gần như bị tê liệt, bị xóa dữ liệu, thời gian khôi phục rất dài và tỉ lệ thiệt hại lớn. Nguy hiểm hơn, hacker sẽ tiến hành khai thác một cách âm thầm và lấy cắp các thông tin nhạy cảm như: danh sách khách hàng, danh sách nhân viên, tài liệu dự án,....

Nguy cơ mất ATTT do kỹ nghệ xã hội

Khi các thiết bị và phương tiện bảo vệ thông tin tin cậy ngày càng nhiều thì giới đạo chích, một mặt tiếp tục khai thác các điểm yếu của hệ thống kỹ thuật, mặt khác lại hướng sự chú ý vào khâu yếu nhất của hệ thống, đó là con người.

Chúng có thể sử dụng các chiêu lừa đảo khác nhau và tận dụng các điểm yếu về tâm lý như tính nhẹ dạ cả tin, hám lợi... của con người, các chiêu tấn công phi kỹ thuật đó được gọi chung là kỹ nghệ xã hội (social engineering). Thực tế đã cho thấy rằng khả năng thành công của phương thức tấn công này cao gấp nhiều lần tấn công trực diện vào hệ thống kỹ thuật.

Các nghiên cứu trong lĩnh vực kỹ nghệ xã hội đã chỉ ra rất nhiều điểm yếu của con người mà giới đạo chích có thể tận dụng để thực hiện các hành vi lừa đảo. Nhưng ngay cả những phẩm chất tốt như lòng nhân ái, sự hào hiệp, sự chân thực cũng là kẽ hở để đạo chích lợi dụng. Vì vậy, ngoài việc nắm kiến thức chung về phẩm chất của con người, giới kỹ sư xã hội rất chú trọng phân biệt đặc tính của từng kiểu người được hình thành

do nghề nghiệp. Ví dụ, người làm lãnh đạo thường thể hiện nhẫn nại khi lắng nghe cấp dưới nhưng cũng có kiểu nói áp đặt, mệnh lệnh khi giao nhiệm vụ; thư ký thường có giọng nói dịu dàng, dễ chịu và lễ độ khi đầu dây bên kia là người lãnh đạo của mình; nhân viên dịch vụ kỹ thuật thường có thái độ thân thiện, nhẫn nại, sẵn sàng đáp ứng yêu cầu của khách hàng. Nắm được những đặc điểm của từng kiểu người sẽ giúp đạo chích có cơ hội thực hiện thành công những mánh lới giả mạo.

1.3.2. Những tổn thất của DNVVN trước những nguy cơ mất ATTT

Có rất nhiều tổn thất có thể xảy ra, có thể được phân thành các loại sau [10]:

1. DNVVN có thể bị phá sản;
2. Doanh nghiệp có thể bị ngừng kinh doanh;
3. Tổn thất về tài chính;
4. Trách nhiệm pháp lý;
5. Mất khách hàng;
6. Thiệt hại về danh tiếng;
7. Thiệt hại về thông tin;
8. Rò rỉ thông tin;
9. Mất chi phí để khôi phục;
10. Mất năng suất.

Hầu hết các DNVVVN đều bị mất mát về tài chính trong thời gian dài, mất mát về danh tiếng cũng như mất niềm tin đối với khách hàng do mất ATTT.

Theo nghiên cứu do Kaspersky Lab và B2B International thực hiện, tổn thất về tài chính của doanh nghiệp vừa và nhỏ (DNVVN) do các cuộc tấn công mạng gây ra tiếp tục tăng lên. Năm 2015, trung bình thiệt hại sau mỗi vụ là 38.000 USD. Con số này bao gồm chi phí thuê chuyên gia xử lí hậu quả, mất cơ hội kinh doanh và tổn thất do trì hoãn công việc.

Thông thường, việc xâm nhập thị trường và ổn định tài chính là ưu tiên hàng đầu đối với những người chủ doanh nghiệp nhỏ - người rất ít hoặc không chú ý đến vấn đề bảo mật thông tin. Và kết quả là hệ thống CNTT của họ trở thành mục tiêu đầu tiên cho tội phạm mạng.

Nghiên cứu cho thấy, trong năm 2016, 1/3 số DNVVN được khảo sát phải trì hoãn công việc và mất đi cơ hội kinh doanh, 88% số đó phải nhờ vào sự giúp đỡ từ chuyên gia bên thứ ba, trung bình chiếm khoảng 11.000 USD trong các khoản phí tổn của công ty. Tổn thất về lợi nhuận khoảng 16.000 USD, trong khi tổn hại về danh tiếng, nghĩa là tổn hại về hình ảnh công ty, được ước tính hơn 8.000 USD.

1.3.3. Danh mục các tài sản thông tin của DNVVN cần được bảo vệ [10]

Tài sản thông tin của doanh nghiệp là những thứ mà doanh nghiệp cần bảo vệ về mặt ATTT bao gồm 02 dạng tài sản dữ liệu và tài sản dịch vụ.

Tài sản dữ liệu

Dưới đây là danh sách các tài sản dữ liệu phổ biến tại các DNVVN:

• *Tài sản dữ liệu chung:*

- Hồ sơ nhân sự;
- Hồ sơ kế toán và dữ liệu tài chính;
- Hợp đồng và thoả thuận;
- Giấy phép phần mềm và bảo hành phần cứng;
- Hồ sơ thuế, hồ sơ đăng ký kinh doanh;
- Cơ sở dữ liệu liên lạc của khách hàng.

• *Tài sản dữ liệu liên quan đến lĩnh vực hoạt động cụ thể, ví dụ:*

- Lĩnh vực phần mềm: mã chương trình và tài liệu;
- Lĩnh vực sản xuất: mác thiết kế sản phẩm;
- Cơ quan du lịch: tài liệu du lịch;
- Kho: kiểm kê và lập kế hoạch;
- Nhà phát triển dự án: dữ liệu trạng thái xây dựng dự án;
- Nhà cung cấp dịch vụ: sản phẩm mới hoặc dịch vụ dữ liệu và kế hoạch tiếp thị.

Lưu ý: Danh tiếng của một doanh nghiệp chính là tài sản của doanh nghiệp đó, nó có thể bị hư hỏng do lạm dụng tài sản thông tin hoặc hệ thống máy tính, ví dụ như: việc lạm dụng các trang web, thư rác, gửi thư điện tử bị nhiễm virus cho khách hàng hoặc sự chậm trễ quá mức trong việc đáp ứng các yêu cầu qua email.

Tài sản dịch vụ

Tài sản dịch vụ bao gồm các dịch vụ cung cấp trực tiếp cho khách hàng:

- Lương;
- Theo dõi và sắp xếp lại mức độ tồn kho;
- Cơ sở đồ họa cho những người thiết kế;
- Lập kế hoạch bảo trì;
- Dự toán chi phí;
- Chuyển tiền điện tử;
- Dịch vụ mạng trung tâm dữ liệu.

Tài sản dữ liệu và tài sản dịch vụ có mối liên hệ chặt chẽ với nhau, ví dụ như dịch vụ **lương** phụ thuộc vào dữ liệu **hồ sơ nhân sự, mức lương, thời gian làm việc**, vv.

Làm thế nào để xác định tài sản thông tin của doanh nghiệp?

Cách thứ nhất: Liệt kê tài sản thông tin theo danh mục. Tài sản thông tin có thể được phân thành 02 loại: tài sản thông tin nội bộ và thông tin bên ngoài.

- Tài sản thông tin nội bộ: tài sản thuộc về doanh nghiệp gồm:

+ Thiết bị máy tính và mạng;

+ Tài sản thông tin lưu trữ, xử lý hoặc được truyền tải bởi thiết bị.

- Tài sản thông tin bên ngoài bao gồm:

+ Tài sản do doanh nghiệp quản lý nhưng có thể chia sẻ ra ngoài như thông tin sản phẩm, tên miền (đối với ISP lưu trữ tên miền);

+ Tài sản thuộc sở hữu của bên ngoài nhưng được sử dụng bởi doanh nghiệp như: Đường truyền thông, máy chủ,…

Cách thứ hai: Xác định các loại thông tin quan trọng theo 3 đặc tính: Bảo mật, toàn vẹn và sẵn sàng. Nói cách khác, doanh nghiệp nên xây dựng bảng phân tích mức độ quan trọng của tài sản thông tin, ví dụ như sau:

Bảng 1. 1. Phân loại tài sản thông tin quan trọng dựa trên các đặc tính

Danh mục tài sản của công ty TNHH X	**Tài sản thông tin cần được bảo vệ**		
	Tính bảo mật	**Tính toàn vẹn**	**Tính sẵn sàng**
Dữ liệu kế toán		x	
Dữ liệu khách hàng	x		
Kế hoạch chiến lược của công ty	x		
Đường truyền IPS			x
Dịch vụ TMĐT	x	x	x

CHƯƠNG 2: CÁC HỆ MẬT MÃ ĐẢM BẢO ATTT ĐƯỢC DÙNG PHỔ BIẾN HIỆN NAY

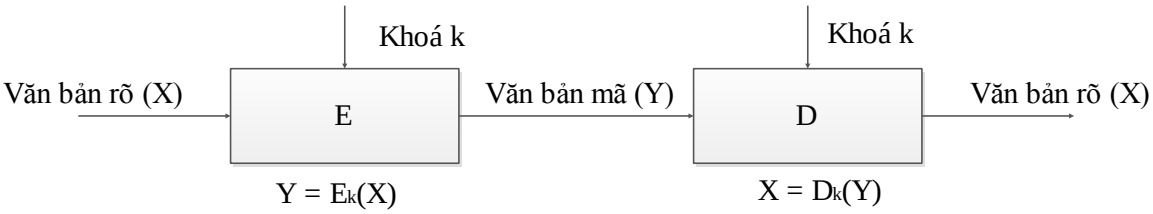
2.1. Tổng quan về hệ mật mã

2.1.1. Định nghĩa

Hệ mật mã [7] được định nghĩa bởi bộ năm (P, C, K, E, D), trong đó:

P: là tập hữu hạn các bản rõ có thể
C: là tập hữu hạn các bản mã có thể
K: là tập hữu hạn các khoá có thể
E: là tập hữu hạn các hàm lập mã
D: là tập các hàm giải mã.

Với mỗi k ∈ K có một hàm lập mã $e_k \in E, e_k$: P → C và một hàm giải mã $d_k \in D, d_k: C \rightarrow P$ sao cho $d_k(e_k(x)) = x$ với $\forall x \in P$



Hình 2. 1. Quá trình mã hoá và giải mã

2.1.2. Phân loại các hệ mật mã

Hệ mật mã có nhiều loại nhưng chia làm hai loại chính: Hệ mật mã khoá đối xứng và Hệ mật mã khoá công khai.

Hệ mật mã khoá đối xứng [9]: là hệ mật mã sử dụng khoá lập mã và khoá giải mã giống nhau. Cứ mỗi lần truyền tin bảo mật cả người gửi A và người nhận B sẽ thoả thuận với nhau một khoá chung k, sau đó người gửi dùng e_k để mã hóa thông báo gửi đi và người nhận sẽ dùng d_k để giải mã thông điệp được nhận từ người gửi A. Một số thuật toán nổi tiếng trong mã hoá đối xứng là: DES, Triple DES(3DES), RC4, AES…

Hệ mật mã khoá công khai [9]: Khoá mã hoá hay còn gọi là khoá công khai (public key) dùng để mã hoá dữ liệu. Khoá giải mã hay còn được gọi là khoá bí mật (private key) dùng để giải mã dữ liệu. Trong hệ mật này, khoá mã hoá và khoá giải mã là khác nhau. Về mặt toán học, khi biết khoá công khai ta có thể tính được khoá bí mật. Khoá bí mật được giữ bí mật trong khi khoá công khai được công khai. Người gửi thông điệp A sẽ dùng khoá công khai của B để mã hoá dữ liệu muốn gửi tới người B và người B sẽ dùng khoá bí mật của mình để giải mã thông điệp nhận được.

Có nhiều hệ mật mã sử dụng khóa công khai được triển khai rộng rãi như hệ mật RSA, hệ mật Elgamal sử dụng giao thức khoá Diffie-Hellman và nổi lên trong nhưng năm gần đây là hệ mật dựa trên giao thức đường cong Eliptic. Trong những hệ mật mã trên, thì hệ mật mã RSA được sử dụng nhiều nhất.

2.1.3. Một số khái niệm cơ bản về sử dụng mật mã [6].

1. **Bản rõ** X được gọi là là bản tin gốc. Bản rõ có thể được chia nhỏ có kích thước phù hợp.
2. **Bản mã** Y là bản tin gốc đã được mã hoá. Ở đây ta thường xét phương pháp mã hóa mà không làm thay đổi kích thước của bản rõ, tức là chúng có cùng độ dài.
3. **Khoá** K là thông tin tham số dùng để mã hoá, chỉ có người gửi và người nhận biết. Khóa là độc lập với bản rõ và có độ dài phù hợp với yêu cầu bảo mật.
4. **Mã hoá** là quá trình chuyển bản rõ thành bản mã, thông thường bao gồm việc áp dụng thuật toán mã hóa và một số quá trình xử lý thông tin kèm theo.
5. **Giải mã** chuyển bản mã thành bản rõ, đây là quá trình ngược lại của mã hóa.
6. **Mật mã** là chuyên ngành khoa học của Khoa học máy tính nghiên cứu về các nguyên lý và phương pháp mã hoá. Hiện nay người ta đưa ra nhiều chuẩn an toàn cho các lĩnh vực khác nhau của công nghệ thông tin.
7. **Thám mã** nghiên cứu các nguyên lý và phương pháp giải mã mà không biết khoá. Thông thường khi đưa các mã mạnh ra làm chuẩn dùng chung giữa các người sử dụng, các mã đó được các kẻ thám mã cũng như những người phát triển mã tìm hiểu nghiên cứu các phương pháp giải một phần bản mã với các thông tin không đầy đủ.
8. **Lý thuyết mã** bao gồm cả mật mã và thám mã. Nó là một thể thống nhất, để đánh giá một mã mạnh hay không, đều phải xét từ cả hai khía cạnh đó. Các nhà khoa học mong muốn tìm ra các mô hình mã hóa khái quát cao đáp ứng nhiều chính sách an toàn khác nhau.

2.2. Hệ mật AES [9]

2.2.1. Giới thiệu

AES (Advanced Encryption Standard - Tiêu chuẩn mã hóa nâng cao) được thiết kế bởi Joan Daemen và Vincent Rijmen, hai nhà khoa học người Bỉ. Thuật toán được đặt tên là Rijmen khi tham gia cuộc thi thiết kế AES do Viện chuẩn quốc gia Hoa kỳ US NIST ra lời kêu gọi tìm kiếm chuẩn mã mới vào năm 1997. Sau đó có 15 đề cử được chấp nhận vào tháng 6 năm 1998 và được rút gọn còn 5 ứng cử viên vào tháng 6 năm 1999. Đến tháng 10 năm 2000, mã Rijndael được chọn làm chuẩn mã nâng cao - AES và được xuất bản là chuẩn FIPS PUB 197 VÀO 11/2001.

2.2.2. Thuật toán

2.2.2.1 Cơ sở toán học của AES

Trong AES các phép toán cộng và nhân được thực hiện trên các byte trong trường hữu hạn $GF(2^8)$

Phép cộng:

$A = (a_1\ a_2\ a_3\ a_4\ a_5\ a_6\ a_7\ a_8)$; $B = (b_1\ b_2\ b_3\ b_4\ b_5\ b_6\ b_7\ b_8)$;

C = A + B = (c_1 c_2 c_3 c_4 c_5 c_6 c_7 c_8), trong đó: $c_i = a_i + b_i$

Ví dụ 1:

A = 56_H; B = $3D_H$

Dạng cơ số Hecxa: $56_H + 3D_H = 93$

Dạng nhị phân: 01010110 + 00111101 = 10010011

Dạng đa thức: $(x^6 + x^4 + x^2 + x) + (x^5 + x^4 + x^3 + x^2 + 1) = (x^7 + x^4 + x + 1)$

Phép nhân:

A = (a_1 a_2 a_3 a_4 a_5 a_6 a_7 a_8); B = (b_1 b_2 b_3 b_4 b_5 b_6 b_7 b_8);

C = A.B = (c_1 c_2 c_3 c_4 c_5 c_6 c_7 c_8)

Ví dụ 2:

A = $C3_H$; B = 85_H

Dạng cơ số Hecxa: $(C3_H).(85_H) = AE_H$

Dạng nhị phân: (11000011).(10000101) = 10101110

Dạng đa thức: $(x^7 + x^6 + x + 1).(x^7 + x^2 + 1) = (x^7 + x^5 + x^3 + x^2 + 1)$

2.2.2.2. Mở rộng khóa

AES thực hiện việc mở rộng khóa dựa trên khóa gốc K, tạo thành chu trình tạo khóa để sinh ra 10, 12 hoặc 14 khóa con, tương ứng với 10, 12 hoặc 14 chu kỳ lặp của giải thuật AES.

Việc mở rộng khóa chính tạo thành bảng khóa mở rộng. Bảng khóa mở rộng là mảng 1 chiều chứa các từ, mỗi từ có độ dài 4 byte, được ký hiệu *W[Nb*(Nr+1)]* (với Nb = 4). Việc phát sinh bảng khóa mở rộng phụ thuộc vào độ dài Nk của khóa chính.

Chu trình tạo khóa con AES sử dụng hai hàm:

SubWord() thực thiện việc thay thế từng byte thành phần của từ 4 byte được đưa vào và trả về kết quả là một từ 4 byte đã được thay thế. Việc thay thế này sử dụng bảng thay thế S-box.

RotWord() thực hiện việc dịch chuyển xoay vòng 4 byte thành phần (a, b, c,d) của từ được đưa vào. Kết quả trả về của hàm RotWord là một từ 4 byte đã được dịch chuyển (b, c, d, a).

Các hằng số chu kỳ Rcon[i] được xác định:

Rcon[i] = [x^{i-1}, {00}, {00}, {00}]

Trong đó: $x^{i-1} \Leftrightarrow \{02\}^{i-1}$ trong trường GF(2^8)

Như vậy ta có bảng hằng số mở rộng với trường hợp Nr = 10 như sau:

Bảng 2. 1. Bảng hằng số mở rộng Rcon của AES – 128

01	02	04	08	10	20	40	80	1B	36
00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00

Khóa của chu kỳ thứ *i* bao gồm các từ 4 byte có chỉ số từ *Nb*i* đến *Nb*(i+1) – 1* (với Nb = 4) của bảng mã khóa mở rộng. Như vậy mã khóa của chu kỳ thứ *i* bao gồm các phần tử từ *W[Nb*i], W[Nb*i + 1],…W[Nb*(i+1) – 1]*.

Bảng 2. 2. Bảng khóa mở rộng AES – 128

W_0	W_1	W_2	W_3	W_4	W_5	W_6	W_7	W_8	W_9	W_{10}	W_{11}	…

Khóa con chu kỳ 0	Khóa con chu kỳ 1	Khóa con chu kỳ 2	…

Giải thuật AES bao gồm nhiều bước biến đổi được thực hiện tuần tự, kết quả đầu ra của bước biến đổi này sẽ là đầu vào của bước biến đổi kia. Kết quả trung gian giữa các bước biến đổi được gọi là trạng thái (State). Độ dài của khối đầu vào, khối đầu ra cũng như độ dài của khối trung gian State là 128 bit. Được biểu diễn bằng một ma trận gồm 4 dòng và 4 cột.

Độ dài của khóa K trong giải thuật AES có thể là 128, 192 hoặc 256 bit. Khóa được biểu diễn bằng một ma trận gồm 4 dòng và Nk cột (Nk = 4, 6 hoặc 8; Nk được tính bằng độ dài của khóa chia 32). Số lượng chu kỳ tính toán trong giải thuật AES được ký hiệu là Nr, độ lớn của Nr phụ thuộc vào độ dài của khóa. Nr được xác định theo công thức:

$$Nr = \max\{Nb, Nk\} + 6$$

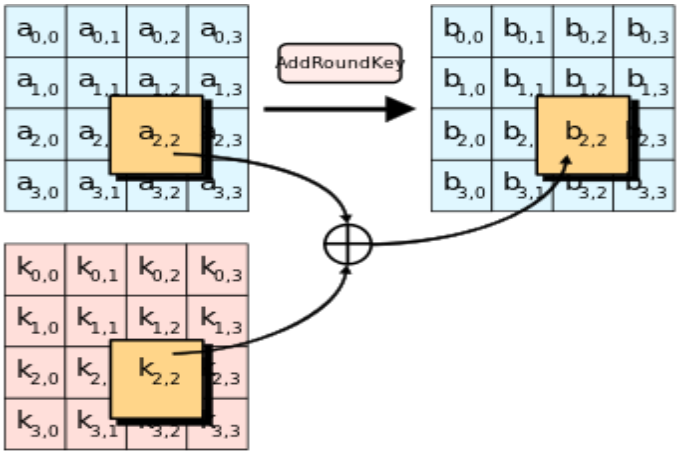
Bảng 2. 3. Mối liên hệ giữa Nk, Nb và Nr

	Độ dài khóa (Nk words)	**Kích thước khối (Nb words)**	**Số chu kỳ (Nr)**
AES – 128	4	4	10
AES – 192	6	4	12
AES – 256	8	4	14

2.2.2.3. Quá trình mã hóa

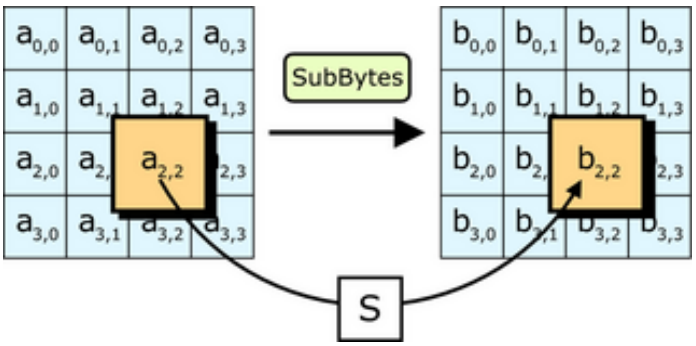
Quá trình mã hóa của giải thuật AES trải qua 10, 12 hoặc 14 chu kỳ, tương ứng với độ dài của khóa là 128, 192 hoặc 256 bit. Mỗi chu kỳ bao gồm 4 bước được thự hiện tuần tự:

Bước 1: AddRoundKey - mỗi byte của khối trạng thái được kết hợp với khóa con. Các khóa con này được tạo ra từ quá trình tạo khóa con (xem Hình 2.2).



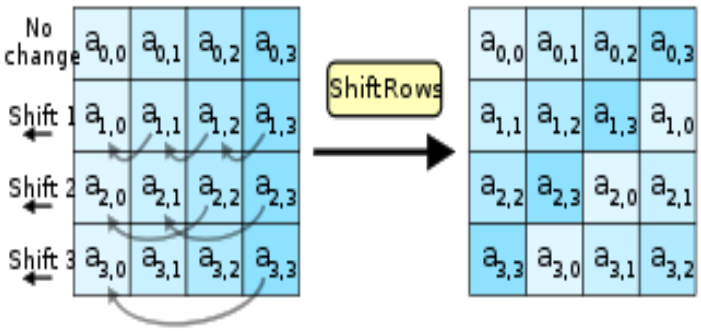
Hình 2. 2. AddRoundKey

Bước 2: SubBytes - mỗi byte trong khối trạng thái được thay thế bằng một byte khác trong bảng tra S-box (xem Hình 2.3).



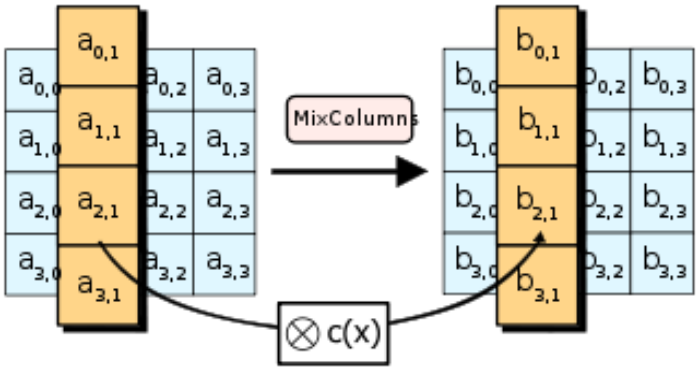
Hình 2. 3. SubBytes

Bước 3: ShiftRows - Các hàng trong khối được dịch vòng, số lượng vòng dịch phụ thuộc vào thứ tự của hàng (xem Hình 2.4).



Hình 2. 4. ShiftRows

Bước 4: MixColumns - các cột trong khối được trộn theo một phép biến đổi tuyến tính (xem Hình 2.5).



Hình 2. 5. MixColumns

Các bước của quá trình mã hóa được thực hiện trên trạng thái hiện hành S. Kết quả S' của mỗi bước sẽ trở thành đầu vào của bước tiếp theo.

Ví dụ:

Sơ đồ ở dạng thập lục phân cho mã hóa AES mảng State. Đầu vào Nb=4 và khóa Nk=4.

Input = 3243f6a8885a308d313198a2e0370734

Key = 2b7e 151628aed2a6abf7158809cf4f3c

Round number	Start of Round	After SubBytes	After ShiftRows	After MixColums		Round Key Value	
Input	32 88 31 e0 43 5a 31 37 f 6 30 98 07 a8 8d a2 34				⊕	2b 28 ab 09 7e ae f7 cf 15 d2 15 4f 16 a6 88 3c	=
1	19 a0 9a e9 3d f4 c6 F8 e3 e2 8d 48 be 2b 2a 08	d4 e0 b8 1e 27 bf b4 41 11 98 5d 52 Ae f1 e5 30	d4 e0 b8 1e bf b4 41 27 5d 52 11 98 30 ae f1 e5	04 e0 48 28 66 cb f8 06 81 19 d3 26 e5 9a 7a 4c	⊕	a0 88 23 2a fa 54 a3 6c fe 2c 39 76 17 b1 39 05	=
2	a4 68 6b 02 9c 9f 5b 6a 7f 35 ea 50 f2 2b 43 49	49 45 7f 77 de db 39 02 d2 96 87 53 89 f1 1a 3b	49 45 7f 77 de db 39 02 d2 96 87 53 89 f1 1a 3b	58 1b db 1b 4d 4b e7 6b ca 5a ca b0 f1 ac a8 e5	⊕	f2 7a 59 73 c2 96 35 59 95 b9 80 f6 f2 43 7a 7f	=
3	aa 61 82 68 8f dd d2 32 5f e3 4a 46 03 ef d2 9a	ac ef 13 45 73 c1 b5 23 cf 11 d6 5a 7b df b5 b8	ac ef 13 45 23 c1 b5 73 d6 11 cf 5a d8 7b df 7b	75 20 53 bb ec 0b c0 25 09 63 cf d0 93 33 7c dc	⊕	3d 47 1e 6d 80 16 23 7a 47 fe 7e 89 7d 3e 44 3b	=
4	48 67 4d d6 6c 1d e3 5f 4e 9d b1 b8 a8 c0 50 01	52 85 e3 f6 50 a4 11 cf 2f 5e c8 6c 28 d7 07 94	52 85 e3 f6 a4 11 cf 50 c8 6a 2f 5e 94 28 d7 07	0f 60 6f 5e d6 31 c0 b3 da 38 10 13 a9 Bf 6b 01	⊕	af a8 b6 db 44 52 71 0b a5 5b 25 ad 41 7f 3b 00	=
5	e0 c8 d9 85 92 63 b1 B8 7f 63 35 be a8 c0 50 01	e1 e8 35 97 4f fb c8 6c d2 fb 96 ae 9b ba 53 7c	e1 e8 35 97 fb c8 6c 4f 96 ae d2 fb 7c 9b ba 53	25 bd b6 4c d1 11 3a 4c a9 d1 33 c0 ad 68 8a b0	⊕	d4 7c ca 11 88 0b f9 00 a3 3e 86 93 7a fd 41 fd	=
6	f1 cl 7c 5d 00 92 c8 b5 6f 4c 8b d5 55 ef 32 0c	a1 78 10 4c 63 4f e8 d5 a8 29 3d 03 fc df 23 fe	a1 78 10 4c 4f e8 d5 63 3d 03 a8 29 fe fc df 23	4b 2c 33 37 86 4a 9d d2 8d 89 f4 18 6d 80 e8 d8	⊕	6d 11 db ca 88 4a 9d d2 a3 3e 86 93 7a fd 41 fd	=
7	26 3d e8 Fd 0e 41 64 d2 2e b7 72 8b 17 7d a9 25	f1 27 9b 54 ab 83 43 b5 31 a9 40 3d f0 ff d3 3f	f7 27 9b 54 83 43 b5 ab 40 3d 31 a9 3f f0 ff d3	14 46 27 34 15 16 46 2a b5 15 56 d8 bf ec d7 43	⊕	4e 5f 84 4e 54 5f a6 a6 f7 c9 4f de 0e f3 b2 4f	=
8	5a 15 a3 7a 41 49 e0 8c 42 dc 19 04 b1 1f 65 0a	be d4 0a da 83 3b el 64 2c 86 d4 f2 c8 c0 4d fe	be d4 0a da 3b e1 64 83 d4 f2 2c 86 fe c8 c0 4d	00 b1 54 fa 51 c8 76 1b 2f 89 6d 99 dl ff cd ea	⊕	ea b5 31 7f d2 8d 2b 8d 73 ba f5 29 21 d2 60 2f	=
9	ea 04 65 b5 83 45 5d 96 5c 33 98 b0 f0 2d ad c5	87 f2 4d 97 ec 6e 4c 90 4a c3 46 a7 8c d8 95 a6	87 f2 4d 97 6e 4c 90 ec 46 e7 4a c3 a6 8c d8 95	47 40 a3 4c 37 d4 70 9f 94 e4 3a 42 ed a5 a6 bc	⊕	ac 19 28 57 77 fe d1 5c 66 dc 29 00 f3 21 41 6e	=
10	ab 59 8b lb 40 2e a1 c3 f2 38 13 42 1e 84 e7 d2	e9 cb 3d af 31 32 2e 09 7d 2c 89 07 72 5f 94 b5	e9 cb 3d af 31 32 2e 09 7d 2c 89 07 b5 72 5f 94		⊕	d0 c9 e1 b6 14 ee 3f 63 f9 25 0c 0c a8 89 c8 a6	=
Output	39 02 dc 19 25 dc 11 6a 84 09 85 0b 1d fb 97 32						

Kết quả bản mã: 3925841d02dc09fbdc118597196a0b32

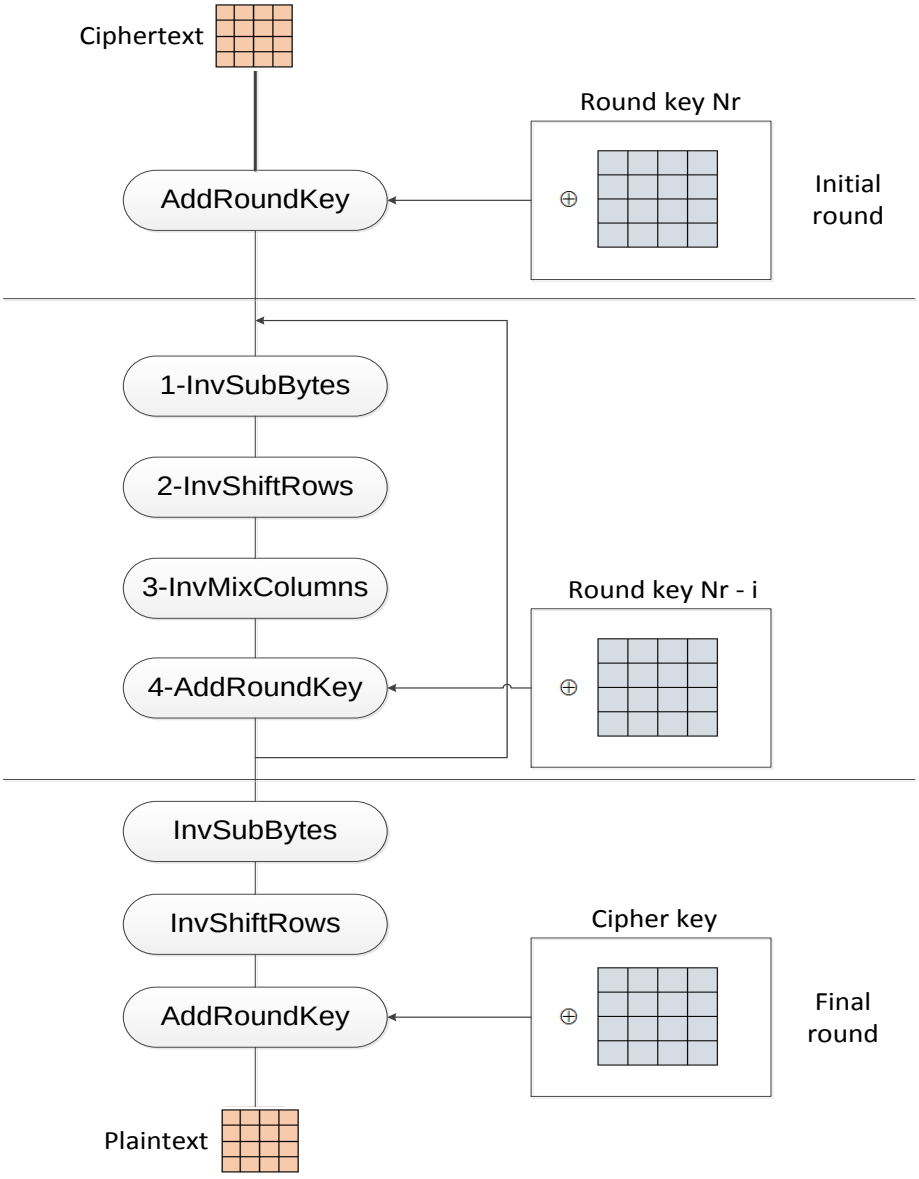
2.2.2.4. Quá trình giải mã

Là quá trình ngược của quá trình mã hóa AES. Quá trình giải mã cũng trải qua 10, 12 hoặc 14 chu kỳ tương ứng với số chu kỳ của quá trình mã hóa. Mỗi chu kỳ gồm 4 bước được thực hiện tuần tự với nhau gồm InvSubBytes, InvShiftRows, InvMixColumns (là các phép biến đổi ngược với SubBytes, ShiftRows, MixColumns) và bước AddRoundKey.

Quá trình giải mã được thể hiện như lưu đồ dưới đây (xem Hình 2.6)

- Khối dữ liệu đầu vào là Ciphertext được sao chép vào mảng trạng thái S.
- Thực hiện thao tác AddRoundKey đầu tiên trước khi thực hiện các chu kỳ mã hóa. Sử dụng khóa ở chu kỳ thứ Nr của chu trình mã hóa.
- Mảng trạng thái sau đó sẽ trải qua Nr = 10, 12 hay 14 chu kỳ biến đổi (tương ứng với 10, 12 hay 14 chu kỳ mã hóa).

+ Nr – 1 chu kỳ đầu tiên: mỗi chu kỳ gồm 4 bước biến đổi liên tiếp nhau.
+ Chu kỳ thứ Nr, thao tác InvMixColumns được thay thế bằng thao tác AddRoundkey.



Hình 2. 6. Quy trình giải mã AES

2.2.3. Đánh giá

Kể từ khi được công nhận là giải thuật mã hóa tiên tiến, AES ngày càng được xã hội chấp nhận. Ban đầu AES chỉ được sử dụng để mã hóa các dữ liệu nhạy cảm. Về sau này, người ta đã dùng nó để mã hóa các thông tin bí mật. Giải thuật AES-192/256 được sử dụng để bảo vệ các thông tin mật và tối mật..

Ưu điểm: AES là giải thuật mã hóa có tốc độ xử lý nhanh, đã được chính phủ Hoa Kỳ tuyên bố là có độ an toàn cao, được sử dụng làm tiêu chuẩn mã hóa mới thay thế cho tiêu chuẩn DES đã lỗi thời. AES được sử dụng để mã hóa các thông tin mật đến tuyệt mật, kháng lại rất nhiều tấn công [1].

AES có cấu trúc đơn giản, rõ ràng và có mô tả toán học rất đơn giản.

Nhược điểm của AES:

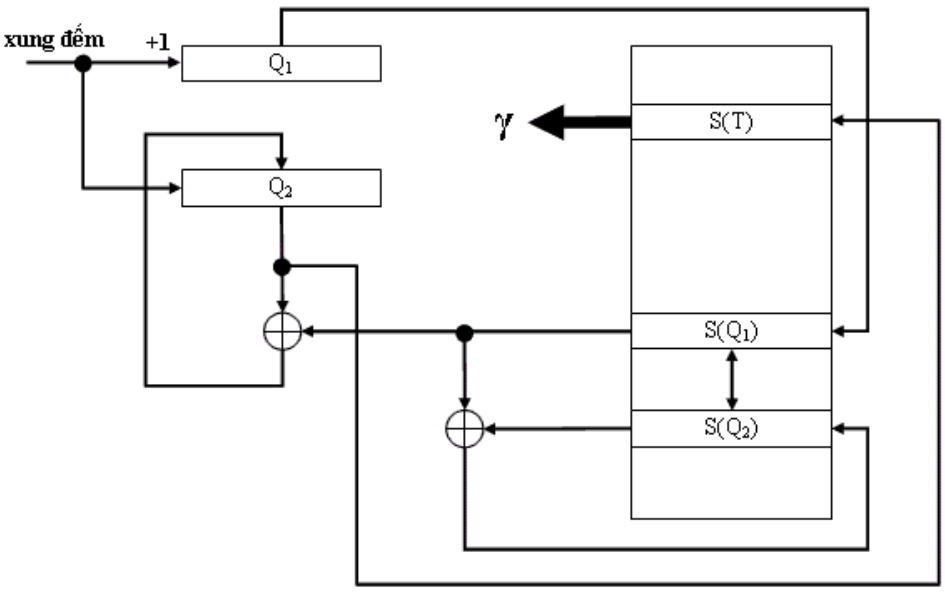
- Mặc dù AES được đánh giá là an toàn nhưng với phương pháp "*tấn công kênh biên*" thì nó chưa thực sự an toàn.
- Cấu trúc toán học của AES được mô tả khá đơn giản. Điều này có thể dẫn tới một số mối nguy hiểm trong tương lai.
- Ngoài ra, AES rất cồng kềnh và cần nhiều tài nguyên cho việc cài đặt [1].

2.3. Hệ mật RC4

2.3.1. Giới thiệu

RC4 là hệ mã dòng với chiều dài khóa biến đổi được nêu ra năm 1987, tác giả của RC4 là Ronald Rivest,.

Trong sơ đồ của RC4 có sử dụng 2 thanh ghi 8 bits (bộ đếm) là Q1 và Q2 và một khối thay thế (S-block) có kích thước 256x8 (256 phần tử, kích thước mỗi phần tử là 8 bit). Giá trị của khối S là một hoán vị nào đó của các số từ 0 đến 255.



Hình 2. 7. Sơ đồ tạo gama trong hệ mật RC4

Thủ tục cơ bản nhất trong một hệ mã dòng bất kỳ là thủ tục sinh Gama. Bởi khi đã có được chuỗi **gama** rồi thì phép mã hóa chỉ là phép cộng từng bit (XOR) bản rõ với chuỗi **gama** này. Ký hiệu S[i] là giá trị phần tử thứ i của khối S; γ là giá trị của kế tiếp (cần được sinh) của chuỗi Gama. Trong RC4, để sinh chuỗi Gama thì mỗi khi xuất hiện một xung cần thực hiện các thao tác sau đây:

1. Tăng Q_1 lên 1: $Q_1 = (Q_1 + 1) \bmod 256$
2. Thay đổi giá trị của Q_2: $Q_2 = (Q_2 + S[Q_1]) \bmod 256$
3. Hoán đổi giá trị của 2 phần tử: $S[Q_1] \leftrightarrow S[Q_2]$
4. Tính tổng T của 2 phần tử này: $T = (S[Q_1] + S[Q_2]) \bmod 256$
5. Gán giá trị cho γ: $\gamma = S[T]$

Trong quá trình sử dụng, bộ đếm Q_1 sẽ làm cho nội dung của khối S thay đổi chậm, còn bộ đếm Q_2 sẽ đảm bảo sự thay đổi này là ngẫu nhiên.

2.3.2. Thuật toán

2.3.2.1. Khởi tạo khối S

Giá trị của khối S là một hoán vị nào đó của 256 số từ 0…255. Sau đây là thuật toán để xác định hoán vị đó.

1. Gán cho mỗi phần tử giá trị bằng chỉ số của nó: S[i] = i; i=0…255
2. Tạo một mảng k gồm 256 phần tử, mỗi phần tử có kích thước 1 byte. Điền đầy bảng k bằng các byte của khóa K: k[0]=K[0], k[1]=K[1], ... Trong trường hợp cần thiết, khóa K được dùng lặp lại.
3. Khởi tạo biến đếm j: j=0;
4. Xáo trộn khối S:
    a. i = 0…255
    b. j = (j + S[i] + k[i]) mod 256

    Hoán đổi giá trị: S[i] ↔ S[j]

2.3.2.2. Mã hóa và Giải mã

Khi đã có được Gama rồi thì việc mã hóa và giải mã của RC4 diễn ra đơn giản. Nhận xét rằng Gama được tạo ra theo từng khối 8 bit nên kích thước của mỗi ký tự trong alphabet mà chúng ta sẽ sử dụng là 8. Quá trình mã hóa được thực hiện như sau:

- Sinh một giá trị Gama: γ
- Đọc một ký tự X_i từ bản tin.
- Thực hiện phép XOR giữa X_i và γ sẽ thu được một ký tự của bản mã Y_i: $Y_i = X_i \oplus \gamma$

Do tính chất đối xứng của phép XOR, quá trình giải mã sẽ hoàn toàn trùng với quá trình mã hóa. Trong thủ tục mã hóa ở trên, cho đầu vào là bản mã thì đầu ra sẽ thu được bản tin ban đầu.

2.3.3. Đánh giá

Ưu điểm của RC4 là thuật toán đơn giản, ý nghĩa của từng bước rõ ràng, logic.

- RC4 an toàn đối với cả 2 phương pháp thám cơ bản là thám tuyến tính và thám vi phân (chưa có công trình nào về thám RC4 được công bố). Số trạng thái mà RC4 có thể có là $256!\times256\times256 \approx 2^{1700}$.

- Tốc độ mã đạt rất cao, so với DES thì RC4 nhanh gấp 10 lần.

2.4. Hệ mã hóa RC5 [9]

2.4.1. Giới thiệu

Thuật toán mã hóa RC5 do giáo sư Ronald Rivest của đại học MIT công bố vào tháng 12 năm 1984

Đây là thuật toán mã hóa theo khóa bí mật. Mã hóa RC5 có yêu cầu công suất thấp và độ phức tạp thấp và độ trễ thấp, độ xử lý nhanh. RC5 được ứng dụng nhiều trong giao dịch mạng và thương mại điện tử.

2.4.2. Thuật toán

2.4.2.1. Định nghĩa các giá trị

+ w: kích thước khối cần được mã hóa (giá trị chuẩn là 32 bit, ngoài ra ta có thể chọn 16 hay 64 bit).

+ r: số vòng lặp (giá trị từ 0,1,...,255)

+ b: chiều dài khóa theo byte (0 đến 255)

Các giá trị thường dùng là: w = 32, r = 20, còn chiều dài khóa có thể 16, 24, hay 32 byte.

Đối với tất cả các biến, các thao tác *RC5-w-r-b* trên khối *w-bit* sử dụng các toán tử cơ bản sau:

a + b: phép cộng module 2^w

a - b: phép trừ module 2^w

a xor b: phép toán xor

a <<< b: phép toán quay trái a sang trái ít nhất $\log_2 w$ bit của b

Trong thuật toán RC5, quá trình mã hóa và giải mã đều cần qua một quá trình quan trọng là quá trình mở rộng khóa.

2.4.2.2. Mở rộng khóa

Để tăng độ an toàn cũng như việc bảo vệ khóa bí mật cho người dùng. Việc mở rộng khóa là một chiều nên không thể suy ngược lại giá trị của khóa K khi biết được các giá trị của khóa mở rộng. Đây cũng chính là một đặc điểm nổi bật của thuật toán RC5.

Thuật toán mở rộng cho khóa K của người sử dụng thành một tập gồm 2(r+1) các khóa trung gian. Các khóa trung gian này được điền vào một bảng khóa mở rộng S. Do vậy, S là một bảng của t = 2(r+1) các giá trị nhị phân ngẫu nhiên được quyết định bởi khóa K. Nó sử dụng hai hằng số lý tưởng được định nghĩa :

P_w = Odd ((e - 2)2^w)

Q_w = Odd ((Ø - 1)2^w

Trong đó :

e = 2.178281828459 (cơ số logarit tự nhiên)

Ø = 1.618033988749 (tỉ lệ vàng)

Odd (x) là số nguyên lẻ gần x nhất

Một số giá trị khác:

t = 2(r + 1) : số phần tử của bảng khóa mở rộng S.

u = w/8: u là số lượng các byte của khối w

c = b/u

Quá trình mở rộng khóa bao gồm các bước sau:

+ *Bước 1:*

Chép khóa bí mật K[0,...,b-1] vào mảng L[0,...,c-1].

Thao tác này sử dụng u byte liên tục nhau của khóa K để điền vào cho L theo thứ tự từ byte thấp đến byte cao. Các byte còn lại trong L được điền vào giá trị 0.

Trong trường hợp b = c = 0, chúng ta sẽ đặt c về 1 và L[0] về 0.

+ *Bước 2:*

Khởi tạo mảng S với một mẫu bit ngẫu nhiên đặc biệt, bằng cách dùng một phép tính số học module 2^w được quyết định bởi hằng số lý tưởng P_W và Q_w.

S[0] = P_w

For i = 1 to t - 1 do

S[i] = S[i-1] + Q_w

+ *Bước 3 :*

Trộn khóa bí mật của người sử dụng vào mảng L và S.

A = B = 0

i = j = 0

v = 3 * max{c,t}

For s=1 to v do {

A = S[i] = (S[i] + A + B) <<<3

B = L[j] = (L[j] + A + B) <<< (A + B)

i = (i + 1) mod (t)

j = (j + 1) mod (c)

}

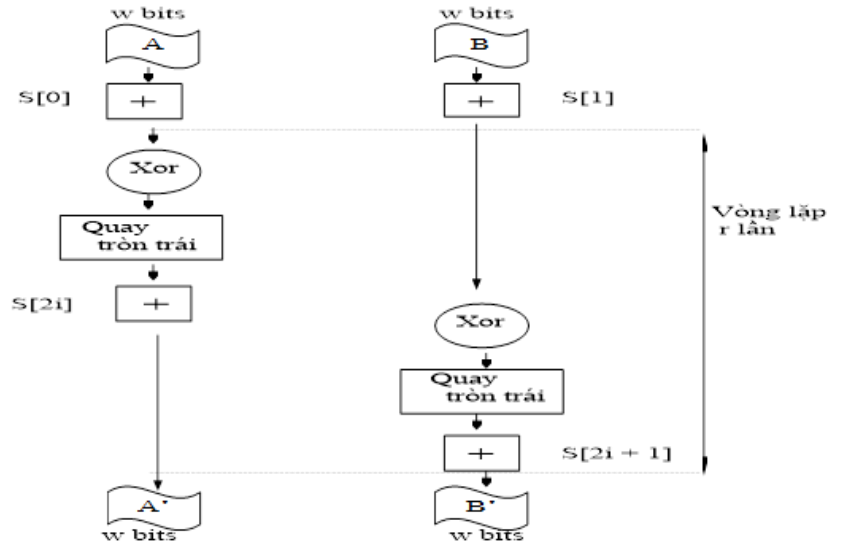
Lưu ý rằng: hàm mở rộng khóa là một chiều, do vậy không dễ dàng tìm ra khóa K từ S.

2.4.2.3. Quá trình mã hóa

Thuật toán mã hóa mỗi lần trên hai khối *w* bit, giả sử là A và B. Và sau quá trình mã hóa sẽ cho ra hai khối đã được mã hóa A' và B'.

Ban đầu A sẽ được cộng với giá trị khóa mở rộng S[0] và B sẽ được cộng với S[1]. Sau đó quá trình mã hóa sẽ thực hiện biến đổi A dựa vào giá trị của B bằng các phép toán XOR và quay tròn trái. Tiếp tục giá trị này sẽ được cộng tiếp với giá trị khóa mở rộng S[2]. Kết quả này được dùng để tiếp tục biến đổi giá trị của B giống như trên. Toàn bộ quá trình này sẽ được thực hiện r lần. Kết quả cuối cùng ở bước r sẽ là giá trị đã được mã hóa A', B'.

Quá trình mã hóa và giải mã có thể được minh họa như sau:



Hình 2. 8. Sơ đồ khối quá trình mã hóa và giải mã RC5

2.4.2.4. Quá trình giải mã :

Quá trình giải mã của RC5 đi ngược lại quá trình mã hóa để có được giá trị gốc.

Thuật toán giải mã như sau :

Input: giá trị mã được lưu trữ trong hai khối w-bit A', B'

Số vòng lặp r

w-bit khóa vòng lặp S[0,...,2r + 1]

Output: giá trị giải mã được lưu trong hai khối *w-bit* A, B

```
For i = r downto 1 do {
            B' = ((B' - S[2i + 1]) >>> A') XOR A'
            A' = ((A' - S[2i]) >>> B' XOR B'
}
B = B' - S[1]
A = A' - S[0]
```

2.4.3. Đánh giá

+ Theo kết quả đánh giá độ an toàn của các thuật toán, RC5 với 12 vòng lặp và mã hóa khối 64-bit cung cấp độ an toàn tương đương với thuật toán DES khi thử với phương pháp giả mã, 2^{44} cho RC5 và 2^{43} DES.

Ưu điểm:

+ RC5 là thuật toán mã hóa khối với tốc độ nhanh được thiết kế sử dụng dễ dàng cho cả phần cứng lẫn phần mềm.

+ Một đặc điểm nổi bật khác của RC5 là các thao tác quay sử dụng chặt chẽ các dữ liệu phụ thuộc với nhau nhằm tránh được các phép thám mã tuyến tính và vi phân.

+ Cơ chế mở rộng khóa của RC5 là một chiều, do vậy các hacker khó có thể phục hồi lại khóa chính ngay cả khi đã xác định được bộ khóa mở rộng.

+ Mỗi quá trình mã hóa và giải mã của RC5 được thực hiện trên hai khối *w* bit do vậy có thể tăng tốc độ mã hóa.

Nhược điểm:

Trên thực tế cho đến nay thì chưa có cách thám mã nào có thể giải mã được RC5. Tuy nhiên một số nghiên cứu lý thuyết đã cung cấp có một vài cách thám mã có thể thực thi, họ dựa vào đặc điểm là số lượng vòng lặp trong RC5 không phụ thuộc vào tất cả các bit trong một khối và thiết kế đơn giản.

2.5. Hệ mã hóa RC6 [19]

2.5.1. Giới thiệu

RC6 là một cải tiến của RC5, được thiết kế để giải quyết các yêu cầu về một chuẩn mã hóa cao cấp AES (Advanced Encryption Standard). Giống như RC5, RC6 sử dụng những vòng lặp. Đặc điểm mới của RC6 là chúng mã hóa một lần 4 khối w bit thay vì 2 khối của RC5, và sử dụng các phép tính tích các số nguyên như phép toán cộng các nguyên tố...

2.5.2. Thuật toán

2.5.2.1. Định nghĩa các giá trị

w: kích thước khối cần được mã hóa (giá trị chuẩn là 32 bit, ngoài ra ta có thể chọn 16 hay 64 bit).

r: số vòng lặp (giá trị từ 0,1,...,255)

b: chiều dài khóa theo byte (0 đến 255)

Các giá trị thường dùng là : w = 32, r = 20, còn chiều dài khóa có thể 16, 24, hay 32 byte.

Đối với tất cả các biến, các thao tác RC6-w-r-b trên khối w-bit sử dụng các toán tử cơ bản sau:

a + b	Số nguyên cộng modulo 2^w
a - b	Số nguyên trừ modulo 2^w
a $\oplus$ b	Bit độc quyền – or hoặc w-bit từ

a × b	Số nguyên nhân modulo 2^w
a <<< b	Xoay w-bit *a* sang trái bằng số lượng được cho bởi các bit quan ít trọng nhất của lg*w* bit của *b*
a >>> b	Xoay w-bit *a* sang phải bằng số lượng được cho bởi các bit có ít quan trọng nhất của lg*w* bit của *b*

2.5.2.2. Mở rộng khóa

Tương tự như RC5, RC6 cũng sử dụng cơ chế mở rộng khóa để đảm bảo an toàn và tăng thêm sự phức tạp. Tuy nhiên trong thuật toán RC6 thì khóa K của người sử dụng được mở rộng thành một tập hợp gồm 2(r + 2) và lưu vào bảng S. Do vậy, S là một mảng của t = 2(r + 2) các số ngẫu nhiên nhị phân được quyết định bởi khóa K. Nó sử dụng hai hằng số lý tưởng được định nghĩa:

P_w = Odd ((e -2)2^w)

Q_w = Odd ((0/ - 1)2^w)

Trong đó:

e = 2.178281828459 (cơ số logarithms tự nhiên)

Ø = 1.618033988749 (tỉ lệ vàng)

Odd (x) là số nguyên lẽ gần x nhất

Một số giá trị khác :

t = 2(r + 2): số phần tử của bảng khóa mở rộng S.

u = w/8: u là số lượng các byte của khối w

c = b/u

Quá trình mở rộng khóa bao gồm các bước sau:

Bước 1 :

- Chép khóa bí mật K[0,...,b-1] vào mảng L[0,...,c-1].
- Thao tác này sử dụng u byte liên tục nhau của khóa K để điền vào cho L, theo thứ tự từ byte thấp đến byte cao. Các byte còn lại trong L được điền vào giá trị 0.
- Trong trường hợp b = c = 0, chúng ta sẽ đặt c về 1 và L[0] về 0.

Bước 2 :

- Khởi tạo mảng S với một toán tử ngẫu nhiên đặc biệt, bằng cách dùng một phép tính số học module 2^w được quyết định bởi hằng số lý tưởng P_W và Q_w.

S[0] = P_w

For i = 1 to t - 1 do

S[i] = S[i-1] + Q_w

Bước 3:

- Trộn khóa bí mật của người sử dụng vào mảng L và S.

```
A = B = 0
i = j = 0
v = 3 * max{c, 2r + 4}
For s = 1 to v do {
    A = S[i] = (S[i] + A + B) <<<3
    B = L[j] = (L[j] + A + B) <<< (A + B)
    i = (i + 1) mod (t)
    j = (j + 1) mod (c)
}
```

Lưu ý rằng hàm mở rộng khóa là một chiều do vậy không dễ dàng tìm ra khóa K từ S.

2.5.2.3. Thuật toán mã hóa:

Input : giá trị gốc được lưu trữ trong bốn khối w-bit A, B,C, D
Số vòng lặp r
w-bit khóa vòng lặp S[0,...,2*r + 3]

Output : giá trị mã được lưu trong bốn khối w-bit A', B', C', D'

```
B = B + S[0]
D = D + S[1]
For i = 1 to r do {
        t = (B x (2B + 1)) <<< lgw
        u = (D x (2D +1)) <<< lgw
```

2.5.2.4. Thuật toán giải mã:

Quá trình giải mã của RC6 là quá trình đi ngược lại quá trình mã hóa để có được giá trị gốc.

Thuật toán giải mã như sau :

Input: giá trị mã được lưu trữ trong bốn khối *w-bit* A', B', C', D'
Số vòng lặp r
w-bit khóa vòng lặp S[0,...,2r + 3]

Output: giá trị giải mã được lưu trong bốn khối *w-bit* A, B, C, D

```
C' = C' - S[2r + 3]
A' = A' - S[2r + 2]
For i = r to 1 do {
        (A', B', C', D') = (D', A', B', C')
        u = (D' x (2D' + 1)) <<< lgw
        t = (B' x (2B' +1)) <<< lgw
        C' = ((C' - S[2i + 1]) >>> t) XOR u
        A' = ((A' - S[2i] >>> u) XOR t
        (A, B, C, D) = (B, C, D, A)
}
D' = D' - S[1]
B' = B' - S[0]
(A, B, C, D) = (A', B', C', D')
```

2.5.3 Đánh giá

RC6 được phát triển từ RC5 nên sẽ có tất cả những ưu điểm của RC5. Bên cạnh đó, RC6 còn có một số đặc tính sau :

+ RC6 tăng thêm sự phức tạp của quá trình mã hóa và giải mã bằng cách sử dụng các phép toán: cộng, trừ, nhân, exclusive-or, quay trái và quay phải.

+Một số đặc điểm nổi bật khác của RC6 so với RC5 là thao tác quay sử dụng chặt chẽ các dữ liệu phụ thuộc và được thao tác trên tất cả các bit.

+Tăng thêm độ an toàn của thuật toán bằng cách tăng số phần tử trong bảng khóa mở rộng là 2(r + 2) thay vì 2(r + 1) đối với RC5 (với r là số vòng lặp).

+Mỗi quá trình mã hóa và giải mã của RC6 được thực hiện trên 4 khối w bit. Do vậy, RC6 có thể tăng tốc độ mã hóa đồng thời cũng tăng thêm sự phức tạp.

+ Với những ưu điểm trên, RC6 được chọn vào danh sách một trong năm ứng cử viên lọt vào vòng chung kết của chuẩn mã hóa dữ liệu cao cấp AES (Advanced Encryption Standard).

2.6. Hệ mật RSA [9]

2.6.1. Giới thiệu

Khái niệm hệ mật mã RSA đã được ra đời năm 1977 bởi các tác giả R.Rivets, A.Shamir, và L.Adleman. Hệ mật này dựa trên cơ sở của bài toán phân tích thừa số nguyên tố.

Về mặt tổng quát RSA là một phương pháp mã hóa theo khối. Trong đó bản rõ M và bản mã C là các số nguyên từ 0 đến 2^i với i số bit của khối. Kích thước thường dùng của i là 2048 bit hoặc 3072 bit. RSA sử dụng hàm một chiều là bài toán phân tích một số thành thừa số nguyên tố.

2.6.2. Thuật toán

Để thực hiện mã hóa và giải mã, RSA dùng phép lũy thừa modulo của lý thuyết số. Các bước thực hiện như sau:

1) Chọn hai số nguyên tố lớn p và q và tính $N = pq$. Cần chọn p và q sao cho: $M < 2^{i-1} < N < 2^i$. Với $i = 1024$ thì N là một số nguyên dài khoảng 309 chữ số.
2) Tính $n = (p-1)(q-1)$
3) Tìm một số e sao cho e nguyên tố cùng nhau với n
4) Tìm một số d sao cho $e.d \equiv 1 \ mod \ n$ (d là nghịch đảo của e trong phép modulo n)
5) Hủy bỏ n, p và q. Chọn khóa công khai K_U là cặp (e, N), khóa riêng K_R là cặp (d, N)
6) Việc mã hóa thực hiện theo công thức:
   - Theo phương án 1, mã hóa bảo mật: $C = E(M, K_U) = M^e \ mod \ N$
   - Theo phương án 2, mã hóa chứng thực: $C = E(M, K_R) = M^d \ mod \ N$
7) Việc giải mã thực hiện theo công thức:

- Theo phương án 1, mã hóa bảo mật: $\overline{M} = D(C, K_R) = C^d \ Mod \ N$
- Theo phương án 2, mã hóa chứng thực: $\overline{M} = D(C, K_U) = C^e \ Mod \ N$

Để đảm bảo rằng RSA thực hiện đúng theo nguyên tắc của mã hóa khóa công khai, ta phải chứng minh hai điều sau:

a) Bản giải mã chính là bản rõ ban đầu: : $\overline{M} = M$, *xét phương án 1:*

Từ bước 4 ta suy ra:

$ed = kn+1$ với k là một số nguyên tố nào đó

Vậy: $\overline{M} = C^d \ mod \ N$

$= M^{ed} \ mod \ N$

$= M^{kn+1} \ mod \ N$

$= M^{k(p-1)(q-1)+1} \ mod \ N$

Trước tiên ta chứng minh: $M^{k(p-1)(q-1)+1} \equiv M \bmod p$. Xét hai trường hợp của M

- M chia hết cho p: M mod p = 0 do đó $M^{k(p-1)(q-1)+1} \equiv M \equiv 0 \ mod \ p$
- M không chia hết cho p vì p là số nguyên tố nên suy ra M nguyên tố cùng nhau với p. Vậy: $M^{k(p-1)(q-1)+1} \ mod \ p = M.(M^{p-1})^{k(q-1)} \ mod \ p$

  $= M.1^{k(q-1)} \ mod \ p$

  $= M \ mod \ p$

  Vậy $M^{k(p-1)(q-1)+1} - M \equiv 0 \ mod \ p$ với mọi M hay nói cách khác $M^{k(p-1)(q-1)+1} - M$ chia hết cho p. Chứng minh tương tự $M^{k(p-1)(q-1)+1} - M$ chia hết cho q. Vì p,q là hai số nguyên tố nên suy ra $M^{k(p-1)(q-1)+1} - M$ chia hết cho N = pq. Tóm lại

  $M^{k(p-1)(q-1)+1} \equiv M \ mod \ N$

  Suy ra $\overline{M} = M^{k(p-1)(q-1)+1} \ mod \ N = M$ (do $M<N$) (điều phải chứng minh)

  Vì e và d đối xứng nên có thể thấy trong phương án 2, ta cũng có $\overline{M} = M$

  b) Khó suy ra K_R từ K_U, nghĩa là tìm cặp (d,N) từ cặp (e,N):

Có *e* và *N*, muốn tìm *d*, ta phải dựa vào công thức: $e.d \equiv 1 \ mod \ n$. Do đó phải tính được *n*. Vì *n = (p-1)(q-1)* nên suy ra ta phải tính được *p* và *q*. Vì *N = pq* nên ta chỉ có thể tính được *p* và *q* từ *N*. Tuy nhiên điều này là khó khi N đủ lớn. Vậy khó có thể tính được K_R từ K_U.

Sơ đồ

Bước 1. ***Tạo cặp khóa*** **(*bí mật, công khai*) (a, b)**

Input: 2 số nguyên tố lớn phân biệt p và q.

Output: Cặp (n,b) là khóa công khai.

Cặp (n,a) là khóa bí mật.

Thuật toán

1. Chọn bí mật số nguyên tố lớn p và q.
2. Tính n = p * q, công khai n, đặt P=C = Zn.
3. Tính bí mật $\phi(n) = (p-1).(q-1)$.
4. Chọn khóa công khai $b < \phi(n)$, nguyên tố với $\phi(n)$.

Khóa bí mật a là phần tử nghịch đảo của b theo mod $\phi(n)$ tức là $a*b \equiv 1 (mod \ \phi(n))$.

5. Tập cặp khóa (bí mật, công khai) $K = \{(\mathbf{a}, \mathbf{b})/a,b \in Z_n , a*b \equiv 1 (mod \phi(n))\}$.

Bước 2. ***Ký số***:

Chữ ký trên $x \in P$ là $y = Sig\ k(x) = x^a \ (mod \ n), \ y \in A$.

Bước 3. ***Kiểm tra chữ ký***:

Verk (x,y) = đúng $\Leftrightarrow x \equiv y^b \ (mod \ n)$.

Ví dụ:

Bước 1. Tạo khoá (bí mật, công khai)

Chọn 2 số nguyên tố p = 2131, q = 1381

n = p*q = 2131*1381 = 2942911

$\phi(n) = (p-1) * (q-1) = 2130*1380 = 2939400$

1. Chọn b = 607 gcd (b, $\phi(n)$) = gcd (607, 2939400) = 1
2. Tính a:

$a = b^{-1} \ mod \ 1161216 = 585943$ (bằng thuật toán Euclide mở rộng)

5. Khóa công khai = (n,b) = (2942911,607)

Khoá bí mật = (n, a) = (2942911, 585943).

Bước 2. Mã hóa

Để mã hóa văn bản có giá trị x= 398, ta thự hiện phép tính:

$c = x^b \ (mod \ n) = 398^{607} \ mod \ 2942911 = 22411291$

Bước 3. **Giải mã**

Để giải mã văn bản có giá trị 22411291, ta thực hiện phép tính:

$y = c^a = 22411291^{585943} \ mod \ 2942911 = 398$

2.5.3. Đánh giá

Độ an toàn của hệ RSA

Sau đây ta sẽ xem xét một số các tấn công phương pháp RSA.

1) Vét cạn khóa: cách tấn công này thử tất cả các khóa *d* có thể có để tìm ra bản giải mã có ý nghĩa, tương tự như cách thử khóa *K* của mã hóa đối xứng, với *N* lớn, việc tấn công là bất khả thi.

2) Phân tích N thành thừa số nguyên tố N = pq: việc phân tích phải là khó khi N đủ lớn, đây cũng là nguyên tắc hoạt động của RSA. Tuy nhiên, nhiều thuật toán phân tích mới đã được đề xuất, cùng với tốc độ xử lý của máy tính ngày càng nhanh, đã làm cho việc phân tích *N* không còn quá khó khăn như trước đây. Năm 1977, các tác giả của RSA đã treo giải thưởng cho ai phá được RSA có kích thước của *N* vào khoảng 428 bit, tức 129 chữ số. Các tác giả này ước đoán phải mất 40 nghìn triệu triệu năm mới có thể giải được.

Bảng dưới đây cho biết các thời gian dự đoán, giả sử rằng mỗi phép toán thực hiện trong một micro giây.

Số các chữ số trong số được phân tích	**Thời gian phân tích**
50	4 giờ
75	104 giờ
100	74 năm
200	4.000.000 năm
300	5×10^{15} năm
500	4×10^{25} năm

Tuy nhiên vào năm 1994, câu đố này đã được giải chỉ trong vòng 8 tháng.

3) Đo thời gian: Đây là một phương pháp phá mã không dựa vào mặt toán học của thuật toán RSA, mà dựa vào một "hiệu ứng lề" sinh ra bởi quá trình giải mã RSA. Hiệu ứng lề là thời gian thực hiện giải mã. Giả sử người phá mã có thể đo được thời giải mã dùng thuật toán bình phương liên tiếp. Trong thuật toán bình phương liên tiếp, nếu một bit của *d* là 1 thì xảy ra hai phép modulo, nếu bit đó là 0 thì chỉ có một phép modulo, do đó thời gian thực hiện giải mã là khác nhau. Bằng một số phép thử chosen-plaintext, người phá mã có thể biết được các bit của *d* là 0 hay 1 và từ đó biết được *d*. Phương pháp phá mã này là một ví dụ cho thấy việc thiết kế một hệ mã an toàn rất phức tạp. Người thiết kế phải lường trước được hết các tình huống có thể xảy ra.

CHƯƠNG 3: MỘT SỐ GIẢI PHÁP ĐẢM BẢO ATTT CHO CÁC DNVVN

3.1. Nhóm giải pháp về Quản lý ATTT

3.1.1. Thiết lập hệ thống quản lý ATTT cho DNVVN theo tiêu chuẩn ISO 27001:2013

Hệ thống quản lý ATTT (ISMS) là nhu cầu thiết yếu của một doanh nghiệp, khi cần đảm bảo ATTT một cách toàn diện. Xây dựng hệ thống ISMS theo tiêu chuẩn ISO 27001: 2013 sẽ giúp hoạt động đảm bảo ATTT của doanh nghiệp được quản lý chặt chẽ.

Theo tiêu chuẩn ISO/IEC 27001: 2013, thông tin và các hệ thống, quy trình, cán bộ liên quan đều là tài sản của tổ chức. Tất cả các tài sản đều có giá trị quan trọng trong hoạt động của tổ chức và cần được bảo vệ thích hợp. Do thông tin tồn tại và được lưu trữ dưới nhiều hình thức khác nhau, nên tổ chức phải có các biện pháp bảo vệ phù hợp để hạn chế rủi ro.

Hệ thống quản lý ATTT sẽ giúp tổ chức thực hiện việc kiểm soát và định hướng cho các hoạt động đảm bảo ATTT. Việc Hệ thống vận hành tốt sẽ giúp công tác đảm bảo ATTT tại tổ chức được duy trì liên tục, được xem xét đánh giá định kỳ và không ngừng cải tiến để đối phó với các rủi ro mới phát sinh. Các hoạt động đảm bảo ATTT trong tổ chức sẽ mang tính hệ thống, giảm sự phụ thuộc vào cán bộ thực thi và luôn được xem xét, đánh giá để nâng cao hiệu quả.

Lợi ích triển khai áp dụng ISMS

Tiêu chuẩn ISO 27001: 2013 có thể áp dụng được cho mọi loại hình tổ chức có nhu cầu bảo vệ thông tin. Việc triển khai Hệ thống ISMS theo tiêu chuẩn ISO 27001 sẽ giúp tổ chức đạt được các lợi ích sau:

- Đảm bảo ATTT của tổ chức, đối tác và khách hàng, giúp cho hoạt động của tổ chức luôn thông suốt và an toàn.
- Giúp nhân viên tuân thủ việc đảm bảo ATTT trong hoạt động nghiệp vụ thường ngày; Các sự cố ATTT do người dùng dây ra sẽ được hạn chế tối đa khi nhân viên được đào tạo, nâng cao nhận thức ATTT.
- Giúp hoạt động đảm bảo ATTT luôn được duy trì và cải tiến. Các biện pháp kỹ thuật và chính sách tuân thủ được xem xét, đánh giá, đo lường hiệu quả và cập nhật định kỳ.
- Đảm bảo hoạt động nghiệp vụ của tổ chức không bị gián đoạn bởi các sự cố liên quan đến ATTT.
- Nâng cao uy tín của tổ chức, tăng sức cạnh tranh, tạo lòng tin với khách hàng, đối tác, thúc đẩy quá trình toàn cầu hóa và tăng cơ hội hợp tác quốc tế.

Cấu trúc Tiêu chuẩn ISO 27001: 2013

Khái quát về Tiêu chuẩn

Tiêu chuẩn quốc tế ISO/IEC 27001: 2013 cung cấp mô hình thiết lập, triển khai, vận hành, giám sát, xem xét, duy trì và nâng cấp Hệ thống ISMS.

ISO/IEC 27001 đặc tả các yêu cầu cần thiết cho việc thiết lập, vận hành và giám sát hoạt động của ISMS; đưa ra các nguyên tắc cơ bản cho việc khởi tạo, thực thi, duy trì và cải tiến ISMS. Tiêu chuẩn này đưa ra các quy tắc bảo mật thông tin và đánh giá sự tuân thủ đối với các bộ phận bên trong tổ chức, xây dựng các yêu cầu bảo mật thông tin mà đối tác, khách hàng cần phải tuân thủ khi làm việc với tổ chức.

Đây cũng là công cụ để các nhà lãnh đạo thực hiện giám sát, quản lý các Hệ thống thông tin, giảm thiểu rủi ro và tăng cường mức độ an toàn, bảo mật cho các tổ chức.

Tiêu chuẩn ISO/IEC 27001: 2013 gồm:

- 07 điều khoản chính (từ phần 4 đến phần 10 của Tiêu chuẩn): đưa ra yêu cầu bắt buộc về các công việc cần thực hiện trong việc thiết lập, vận hành, duy trì, giám sát và nâng cấp Hệ thống ISMS của các tổ chức. Bất kỳ vi phạm nào của tổ chức so với các quy định nằm trong 07 điều khoản này đều được coi là không tuân thủ theo tiêu chuẩn:

Điều khoản 4 - Phạm vi tổ chức: Đưa ra các yêu cầu cụ thể để tổ chức căn cứ trên quy mô, lĩnh vực hoạt động và các yêu cầu, kỳ vọng của các bên liên quan thiết lập phạm vi Hệ thống quản lý ATTT phù hợp.

Điều khoản 5 - Lãnh đạo: Quy định các vấn đề về trách nhiệm của Ban lãnh đạo mỗi tổ chức trong Hệ thống ISMS, bao gồm các yêu cầu về sự cam kết, quyết tâm của Ban lãnh đạo trong việc xây dựng và duy trì hệ thống; các yêu cầu về việc cung cấp nguồn lực, tài chính để vận hành hệ thống.

Điều khoản 6 - Lập kế hoạch: Tổ chức cần định nghĩa và áp dụng các quy trình đánh giá rủi ro, từ đó đưa ra các quy trình xử lý. Điều khoản này cũng đưa ra các yêu cầu về việc thiết lập mục tiêu ATTT và kế hoạch để đạt được mục tiêu đó.

Điều khoản 7 - Hỗ trợ: yêu cầu đối với việc tổ chức đào tạo, truyền thông, nâng cao nhận thức cho toàn thể cán bộ, nhân viên của tổ chức về lĩnh vực ATTT và ISMS, số hóa thông tin.

Điều khoản 8 - Vận hành hệ thống: Tổ chức cần có kế hoạch vận hành và quản lý để đạt được các mục tiêu đã đề ra. Đồng thời cần định kỳ thực hiện đánh giá rủi ro ATTT và có kế hoạch xử lý.

Điều khoản 9 - Đánh giá hiệu năng hệ thống: Quy định trách nhiệm của Ban lãnh đạo trong việc định kỳ xem xét, đánh giá Hệ thống ISMS của tổ chức. Phần này đưa ra yêu cầu đối với mỗi kỳ xem xét hệ thống, đảm bảo đánh giá được toàn bộ hoạt động của hệ thống, đo lường hiệu quả của các biện pháp thực hiện và có kế hoạch khắc phục, nâng cấp hệ thống cho phù hợp với những thay đổi trong hoạt động của tổ chức.

Điều khoản 10 - Cải tiến hệ thống: Giữ vững nguyên tắc Kế hoạch - Thực hiện - Kiểm tra - Hành động (P-D-C-A), tiêu chuẩn cũng đưa ra các yêu cầu đảm bảo Hệ thống ISMS không ngừng được cải tiến trong quá trình hoạt động. Gồm các quy định trong việc áp dụng các chính sách mới, các hoạt động khắc phục, phòng ngừa các điểm yếu đã xảy ra và tiềm tàng để đảm bảo hiệu quả của Hệ thống ISMS.

- Phụ lục A - Các mục tiêu và biện pháp kiểm soát: đưa ra 14 lĩnh vực kiểm soát nhằm cụ thể hóa các vấn đề mà tổ chức cần xem xét, thực hiện khi xây dựng và duy trì Hệ thống ISMS. Các lĩnh vực đưa ra xem xét bao gồm từ chính sách của lãnh đạo tổ chức, tới việc đảm bảo ATTT trong quản lý tài sản, nhân sự, các nguyên tắc căn bản để đảm bảo ATTT trong việc vận hành, phát triển, duy trì các hệ thống CNTT....

Tại Việt Nam, một số tiêu chuẩn quốc gia (TCVN) về ATTT đã được xây dựng, công bố trên cơ sở chấp nhận nguyên vẹn các tiêu chuẩn ISO/IEC.

Bộ tiêu chuẩn về hệ thông quản lý an toàn thông tin ISMS:

Công nghệ thông tin - Hệ thống quản lý an toàn thông tin - Các yêu cầu (TCVN ISO/IEC 27001:2009 ISO/IEC 27001:2005).

Công nghệ thông tin - Các kỹ thuật an toàn - Quy tắc thực hành Quản lý an toàn thông tin (TCVN ISO/IEC 27002:2011).

Công nghệ thông tin - Các kỹ thuật an toàn - Quản lý rủi ro an toàn thông tin (TCVN 10295:2014 ISO/IEC 27005:2011)

Bộ tiêu chuẩn về đánh giá ATTT:

Công nghệ thông tin - Các kỹ thuật an toàn - Các tiêu chí đánh giá an toàn CNTT - Phần 1: Giới thiệu và mô hình tổng quát (TCVN 8709-1:2011 ISO/IEC 15408-1:2009).

- Công nghệ thông tin - Các kỹ thuật an toàn - Các tiêu chí đánh giá an toàn CNTT - Phần 2: Các thành phần chức năng an toàn (TCVN 8709-2:2011 ISO/IEC 15408-2:2008).

Công nghệ thông tin - Các kỹ thuật an toàn - Các tiêu chí đánh giá an toàn CNTT - Phần 3: Các thành phần đảm bảo an toàn (TCVN 8709-3:2011 ISO/IEC 15408-3:2008).

Bộ tiêu chuẩn về an toàn mạng

TCVN 9801-1:2013 (ISO/IEC 27033-1:2009) Công nghệ thông tin - Kỹ thuật an ninh - An ninh mạng - Phần 1: Tổng quan và khái niệm

3.1.1.1. Chính sách về ATTT [10]

Chính sách ATTT là tài liệu cấp cao đặc thù, tập hợp các luật đặc biệt của Doanh nghiệp như những yêu cầu, quy định mà những người trong doanh nghiệp đó phải thực hiện để đạt được các mục tiêu về ATTT. Chính sách ATTT sẽ được người đứng đầu tổ chức, doanh nghiệp phê chuẩn và ban hành thực hiện. Nó được ví như bộ luật của tổ

chức, doanh nghiệp mà mọi thành viên trong tổ chức, các đối tác, khách hàng quan hệ đều phải tuân thủ. Chính sách ATTT sẽ là tiền đề để doanh nghiệp xây dựng các giải pháp bảo mật, xây dựng những quy trình đảm bảo an toàn hệ thống, đưa ra các hướng dẫn thực hiện, gắn kết yếu tố con người, quản trị, công nghệ để thực hiện mục tiêu an toàn hệ thống. Đồng thời chính sách ATTT cũng đưa ra nhận thức về an toàn thông tin, gán trách nhiệm về an toàn cho các thành viên của tổ chức doanh nghiệp, từ đó đảm bảo hệ thống được vận hành đúng quy trình, an toàn hơn.

Chính sách ATTT cần nêu rõ:

• Mục tiêu của công ty trong lĩnh vực ATTT;
• Khung quản lý ATTT;
• Vai trò và trách nhiệm của các nhân viên liên quan đến ATTT;
• Chiến lược và các ưu tiên trong việc thực hiện quy trình ATTT;
• Quan hệ với các tổ chức khác từ quan điểm ATTT.

Vậy làm thế nào để thiết lập một chính sách ATTT tốt?

Chính sách ATTT có thể có bất kỳ hình thức nào, có thể rất súc tích để có hiệu quả. Để thiết lập một chính sách ATTT tốt, trước tiên người thiết lập cần phải trả lời những câu hỏi về chính sách ATTT như:

• Ai trong công ty có quyền ban hành chính sách?
• Ai tham gia vào việc thiết lập chính sách?
• Ai chịu trách nhiệm theo dõi sự tuân thủ chính sách?
• Chính sách được phổ biến cho ai? Phổ biến như thế nào?
• Chính sách được cập nhật thường xuyên như thế nào? Các thông tin cập nhật được phổ biến và công nhận như thế nào?

Nội dung của một chính sách ATTT

Bảng dưới đây liệt kê các phần chính cần được nêu trong chính sách ATTT.

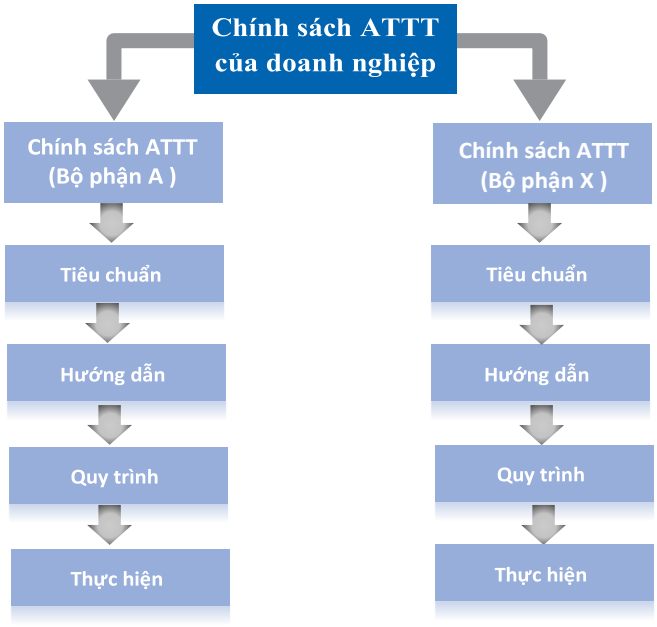
Bảng 3. 1. Các thành phần chính trong chính sách ATTT [10]

Tên thành phần	Mục tiêu
Mục tiêu của chính sách, phạm vi và quá trình quản lý	- Xác định mục tiêu kinh doanh của doanh nghiệp, phạm vi và khả năng áp dụng chính sách ATTT - Xác định quy trình quản lý của chính sách ATTT
Sự tuân thủ	Đảm bảo mọi nhân viên trong doanh nghiệp không được vi phạm các quy định trong hợp đồng trong việc thực hiện nhiệm vụ của mình
Nhân sự ATTT	- Đảm bảo mọi nhân viên có trách nhiệm bảo mật thông tin và trách nhiệm giải quyết sự cố trong khi thực hiện công việc, có những biện pháp xử lý nhân viên vi phạm chính sách ATTT. - Đảm bảo nhân viên được đào tạo về ATTT

Tên thành phần	Mục tiêu
Tổ chức ATTT	Đảm bảo nguyên tắc cơ bản về quản lý cơ sở hạ tầng ATTT và quyền truy cập bên thứ ba được xác định rõ ràng.
Phân loại tài sản và quản lý rủi ro	- Đảm bảo rằng tất cả nhân viên đều nhận thức được việc phân loại tài sản thông tin và phải có biện pháp phòng ngừa về an toàn thông tin, tính toàn vẹn của dữ liệu. - Đảm bảo có một hệ thống đánh giá rủi ro thích hợp, giảm thiểu rủi ro và quá trình kiểm soát rủi ro.
An toàn về khía cạnh vật lý và môi trường	Đảm bảo các khu vực an toàn và thiết bị được đáp ứng.
Quản lý về truyền thông và vận hành	- Đảm bảo tính tin cậy của thông tin trong việc trao đổi, tính toàn vẹn hệ thống đối với các phần mềm độc hại, tính sẵn sàng của dữ liệu. - Việc lập kế hoạch, quản lý mạng internet phải được phê duyệt. - Mọi nhân viên trong công ty đều được đào tạo về ATTT, sử dụng thành thạo Internet, email một cách an toàn.
Kiểm soát truy cập	Đảm bảo rằng có biện pháp quản lý người dùng chặt chẽ trong việc truy cập mạng, hệ thống và các ứng dụng tại văn phòng và thậm chí là từ xa.
Phát triển hệ thống và bảo trì	Đảm bảo việc nghiên cứu, phát triển hệ thống, quy trình hỗ trợ và kiểm soát hệ mật mã tuân theo yêu cầu của doanh nghiệp.
Thường xuyên quản lý kinh doanh	Đảm bảo việc quản lý kinh doanh và ứng phó với những sự cố luôn được ưu tiên

3.1.1.2 Thực hiện chính sách ATTT theo các tiêu chuẩn, quy trình và hướng dẫn

Tất cả các tiêu chuẩn, hướng dẫn và quy trình liên quan đến ATTT đều có nguồn gốc từ chính sách ATTT. Việc lập kế hoạch và triển khai nên tuân theo các tiêu chuẩn và quy trình. Chúng ta sẽ chỉ chọn một vài tài liệu về chính sách quản lý cơ bản để thảo luận như: Nhân sự, kiểm soát Truy cập và Chính sách sử dụng.



Hình 3. 1. Cấp bậc trong quản lý ATTT

3.1.1.3. Chính sách về an toàn đối với nhân sự trong doanh nghiệp

Chính sách này được ban hành bởi phòng quản lý nhân sự, bao gồm một số nội dung chính như sau:

- Quá trình tuyển dụng: Tài liệu tham khảo hỗ trợ cho ứng viên phải được xác nhận trước khi chấp nhận tuyển dụng;
- Vai trò và trách nhiệm trong việc đảm bảo ATTT:

+ Ứng viên phải ký cam kết đảm bảo ATTT cho công ty;

+ Cần đảm bảo rằng tất cả các tài sản thông tin, mật khẩu,… phải được trả lại công ty trước khi nhân sự không còn làm tại công ty nữa.

- Không nên sắp xếp những nhân viên làm việc có tính chất thời vụ vào những công việc nhạy cảm.
- Cần đưa ra những cách tuyên truyền hiệu quả về chính sách ATTT tới toàn thể nhân viên trong công ty.
- Cần tổ chức các khóa đào tạo nâng cao nhận thức về ATTT cho nhân viên

3.1.1.5. Chính sách quản lý truy cập

Chính sách này được ban hành bởi bộ phận kỹ thuật nhằm đảm bảo sự nhất quán trong việc quản lý truy cập mạng internet, hệ thống và các ứng dụng cho những người truy cập ở văn phòng cũng như từ xa. Chính sách bao gồm những điểm sau:

Định danh, xác thực và trách nhiệm giải trình trong việc quản lý người dùng.

- Tạo lập tài khoản riêng cho mỗi người dùng và có điều kiện ràng buộc để họ phải chịu trách nhiệm về những hành động của mình.
- Đưa ra cơ chế sử dụng mật khẩu mạnh trong việc xác thực.

- Thực hiện việc xác thực người dùng mạnh mẽ (ví dụ như sử dụng token hoặc sinh trắc học) trong các hệ thống quan trọng.
- Thực thi cơ chế đăng xuất và cảnh báo nội bộ để ngăn chặn các cuộc tấn công bằng mật khẩu.
- Kiểm soát việc chia sẻ tài khoản người dùng và mật khẩu

3.1.2. Đánh giá rủi ro về ATTT

Đánh giá rủi ro về ATTT là một quá trình xác định những nguồn lực thông tin tồn tại cần được bảo vệ, và để hiểu cũng như lưu tài liệu các rủi ro tiềm ẩn từ mối nguy CNTT có thể gây ra mất thông tin bí mật, tính toàn vẹn, hoặc tính sẵn có. Mục đích của việc đánh giá rủi ro là để giúp quản lý tạo ra các chiến lược và kiểm soát thích hợp cho quản lý của các tài sản thông tin. Bởi vì các điều kiện kinh tế, quản lý và điều hành sẽ tiếp tục thay đổi, các cơ chế cần thiết để xác định và đối phó với các rủi ro đặc biệt gắn liền với sự thay đổi.

Mục tiêu phải được thiết lập trước khi các quản trị viên có thể xác định và thực hiện các bước cần thiết để quản lý rủi ro. Mục tiêu hoạt động liên quan đến hiệu quả và hiệu quả của các hoạt động, bao gồm cả hiệu suất và mục tiêu tài chính và bảo vệ chống thất thoát nguồn tài nguyên. Mục tiêu của các báo cáo tài chính liên quan đến việc chuẩn bị các báo cáo tài chính được công bố một cách tin cậy, như phòng chống gian lận báo cáo tài chính. Mục tiêu phù hợp liên quan đến pháp luật và các quy định thiết lập đạt các tiêu chuẩn tối thiểu của hành vi trên.

Bộ phận ATTT với sự trợ giúp của các phòng ban khác, sẽ tiến hành một cuộc đánh giá rủi ro hàng năm hoặc phân tích tác động kinh doanh để:

- Lưu kho và xác định các bản chất tài nguyên thông tin của Doanh nghiệp.
- Có sự hiểu biết và lưu tài liệu các mối đe doạ từ các sự kiện có thể làm cho việc thất thoát tính bảo mật, tính toàn vẹn và sẵn sàng của dữ liệu.
- Xác định mức độ cần thiết của mối đe doạ an toàn để bảo vệ các nguồn tài nguyên

3.1.3. Chính sách phòng chống virus

Virus là một mối đe dọa cho các doanh nghiệp nếu như các máy tính bị nhiễm virus có thể truyền tải thông tin bí mật đến các bên thứ ba một cách trái phép, cung cấp một nền tảng cho việc truy cập hoặc sử dụng mạng nội bộ trái phép, lây nhiễm các thiết bị kết nối mạng khác, hoặc gây trở ngại với việc sử dụng các dịch vụ CNTT của Doanh nghiệp. Phần mềm diệt virus được cung cấp cho toàn thể cộng đồng doanh nghiệp để bảo vệ và chống lại các thiệt hại gây ra bởi tấn công từ virus. Người quản trị mạng có trách nhiệm tạo các quy trình trong việc cung cấp các phần mềm anti-virus luôn được cập nhật mới nhất và các thông tin về virus được cập nhật nhanh nhất.

Các Doanh nghiệp có quyền xem xét bất kỳ thiết bị truy cập vào hệ thống mạng (công cộng hoặc riêng tư). Doanh nghiệp cũng có quyền từ chối việc truy cập vào hệ

thống mạng của bất kỳ thiết bị nào đó được bảo vệ toàn diện hay các Doanh nghiệp có quyền vô hiệu hóa truy cập mạng với bất kỳ thiết bị được bảo vệ không đầy đủ, hoặc đang bị nhiễm virus. Truy cập mạng có thể được khôi phục khi thiết bị hiện tại đã được xoá sạch khỏi virus và phần mềm diệt virus và hệ thống điều hành và các ứng dụng bản vá lỗi được áp dụng đã được cập nhật mới nhất.

3.1.4. Chính sách sao lưu và phục hồi

Tất cả thông tin điện tử phải được sao lưu vào các phương tiện lưu trữ an toàn một cách thường xuyên (ví dụ: sao lưu dữ liệu), với mục đích khôi phục sau sự cố có thể xảy ra và hoạt động trở lại. Kế hoạch sao lưu và phục hồi dữ liệu đưa ra các yêu cầu tối thiểu cho việc tạo ra và duy trì các bản sao lưu.

Tất cả các bản sao lưu phải tuân theo các thủ tục sau đây:

• Tất cả dữ liệu và tiện ích phải có đầy đủ hệ thống sao lưu (đảm bảo bao gồm tất cả các bản vá lỗi, sửa lỗi và cập nhật)

• Lưu thông tin về những gì được sao lưu và lưu trữ ở đâu mà phải được bảo quản

• Hồ sơ về giấy phép của phần mềm cần được sao lưu

• Các phương tiện lưu trữ dự phòng phải được dán nhãn chính xác theo yêu cầu tối thiểu, các dấu hiệu nhận dạng sau đó có thể dễ dàng hiển thị bởi việc dán nhãn:

• Tên của hệ thống

• Ngày tạo ra

• Phân loại dữ liệu nhạy cảm (dựa trên quy định lưu giữ hồ sơ điện tử được áp dụng)

• Bản sao của các thiết bị lưu trữ, cùng với các bản lưu trữ sao lưu, nên được lưu trữ một cách an toàn ở một nơi cách xa vị trí hiện tại, ở một khoảng cách đủ xa để thoát khỏi bất kỳ thiệt hại từ thiên tai từ khu vực chính.

• Kiểm tra thường xuyên công việc của quá trình khôi phục dữ liệu / phần mềm từ các bản sao lưu cần được thực hiện để đảm bảo rằng các dữ liệu sau lưu này có thể sử dụng trong Doanh nghiệp hợp khẩn cấp. Lưu ý: Đối với các dữ liệu quan trọng nhất và mốc thời gian quan trọng, một hệ thống song song (mirror), hoặc ít nhất là dữ liệu song song có thể được ưu tiên phục hồi trước.

3.2. Nhóm giải pháp về công nghệ

3.2.1. Mã hóa dữ liệu trong lưu trữ

Mã hoá dữ liệu là biện pháp cần áp dụng để đảm bảo an toàn cho cơ sở dữ liệu của DNVVN, là lớp bảo vệ trong trường hợp các biện pháp kiểm soát truy cập đã bị vượt qua. Việc mã hoá này phải được thực hiện một cách đúng đắn để đảm bảo người dùng có toàn quyền trên hệ điều hành cũng không thể đọc được dữ liệu nếu không thông qua kiểm soát của ứng dụng. Yếu tố quan trọng đầu tiên cần xét đến trong quy trình mã hoá dữ liệu trong lưu trữ là quản lý khoá, nếu hệ thống quản lý khoá không đảm bảo thì tác dụng của mã hoá cũng giảm rất nhiều.

3.2.1.1. Quản lý khóa

Quản lý khóa [25] đóng một vai trò hết sức quan trọng trong mật mã, nó là cơ sở an toàn cho các kỹ thuật mật mã được sử dụng nhằm cung cấp tính bí mật, xác thực thực

thể, xác thực nguồn gốc dữ liệu, toàn vẹn dữ liệu và chữ ký số. Các thủ tục quản lý khóa phụ thuộc vào các cơ chế mật mã được dùng đến, ý định sử dụng khóa và chính sách an toàn được áp dụng. Quản lý khóa cũng bao gồm cả các chức năng được thi hành trong một thiết bị mật mã.

Theo xu thế phát triển, quản lý khóa dần được tiêu chuẩn hóa nhằm đưa đến các cơ chế sử dụng thống nhất đáp ứng vấn đề tương thích giữa các hệ thống sử dụng kỹ thuật mật mã, tại Việt Nam là tiêu chuẩn TCVN 7817: 2007, trong đó có phần 3: TCVN 7817-3: 2007 Công nghệ thông tin - Kỹ thuật mật mã - Quản lý khoá - Phần 3: Các cơ chế sử dụng kỹ thuật phi đối xứng - khuyến cáo 7 cơ chế thỏa thuận khóa bí mật, 6 cơ chế vận chuyển khóa bí mật và 3 cơ chế vận chuyển khóa công khai. Các cơ chế này đều dựa trên kỹ thuật mật mã phi đối xứng.

Với nhiều tính chất đặc biệt, kỹ thuật mật mã khóa công khai là phương tiện phù hợp với việc xây dựng các cơ chế thiết lập khóa: dùng mật mã khóa công khai có thể thiết lập khóa không cần giao tác, tạo chữ ký số để xác thực thực thể, nội dung thông tin, chống chối bỏ v.v.

Yếu tố cốt lõi trong kỹ thuật này là mỗi chủ thể A sử dụng một cặp khóa, khóa công khai E_A và khóa bí mật D_A. Hai khóa này được xác định theo cùng một thuật toán, liên quan nhau theo hệ thức $E_AD_A= I$ (với I là ánh xạ đồng nhất) và thỏa mãn tính chất có ý nghĩa quyết định đối với tính an toàn khi sử dụng mật mã khóa công khai: biết E không thể suy ra D. Khóa E được công khai và có khả năng truy cập đối với tất cả mọi người trong hệ thống. Khóa mật D được người dùng giữ bí mật. Kỹ thuật mật mã phi đối xứng sử dụng hai phép biến đổi là phép biến đổi công khai (phụ thuộc vào khóa công khai) và phép biến đổi bí mật (phụ thuộc vào khóa mật). Do tính chất đã nêu của cặp khóa, biết phép biến đổi công khai không thể tính toán ra được phép biến đổi bí mật.

3.2.1.2. Mã hóa dữ liệu theo tiêu chuẩn mã hóa tiên tiến – AES

Thuật toán mã dữ liệu AES được NIST ban hành thành FIPS PUB 197: ADVANCED ENCRYPTION STANDARD - AES (Tiêu chuẩn mã hóa dữ liệu tiên tiến - AES) ngày 26/11/2001 và ISO ban hành trong ISO/IEC 18033-3 Information technology- Security techniques- Encryption algorithms - Part 3: Block ciphers (Công nghệ thông tin - Kỹ thuật an toàn - Thuật toán mã hóa - Phần 3: Các hệ mã khối). Việc biên soạn Tiêu chuẩn mã hóa dữ liệu này tại Việt Nam được dựa trên việc tham khảo, kết hợp cả hai tài liệu trên nhưng chủ yếu dựa vào FIPS PUB 197.

Sau đây là một số chỉ dẫn để thực thi thuật toán:

Các chế độ hoạt động của AES

Khi cài đặt thuật toán mã AES người ta thường không sử dụng ở dạng nguyên gốc. AES thường hoạt động ở bốn chế độ cơ bản của mã khối n-bit (ECB, CBC, CFB và OFB) đặc tả bởi tiêu chuẩn ISO/IEC 10116:1997 Information technology– Security

techniques – Modes of operation for an n-bit cipher (Công nghệ thông tin- kỹ thuật an toàn- chế độ hoạt động của mã hóa nbit). Trên cơ sở bốn chế độ cơ bản ban đầu này người ta đã phát triển thêm một số chế độ khác (Có thể trong tương lai ISO/IEC sẽ công bố thêm một số chế độ hoạt động khác nữa cho mã khối. Hiện tại ISO/IEC mới quy định bốn chế độ cơ bản nói trên). Sau đây là những nét sơ lược của bốn chế độ này.

Chế độ sách mã điện tử ECB (Electronic Code Book): Trong chế độ ECB các khối rõ được mã hoá độc lập nhau và khối mã được giải mã độc lập: $C_i = E_k(M_i)$; $M_i = D_k(C_i)$, trong đó E_k và D_k là các phép mã hoá và giải mã theo khoá mật K.

Chế độ xích liên kết khối mã CBC (Cipher block Chaining): Trong chế độ này, đầu tiên người ta tạo ra một xâu nhị phân 64 bit được gọi là véc-tơ khởi đầu và thông báo cho nhau. Trong bước đầu tiên khối dữ liệu rõ M_1 được cộng với véc-tơ khởi đầu theo phép cộng bit, kết quả nhận được sẽ được biến đổi qua các phép mã hóa để được đầu ra là khối mã C_1. Ở các bước sau, mỗi khối Mi của bản rõ được cộng theo modulo 2 với bản mã trước đó C_{i-1} và được mã hoá:

$C_i = E_k(M_i \text{ r } C_{i-1})$

$M_i = D_k(C_i) \text{ r } C_{i-1}$

Chế độ mã liên kết ngược CFB (Cipher Feed Back): Chế độ này này khác với chế độ CBC, tại bước đầu tiên véc-tơ khởi đầu được mã hóa bằng Ek rồi cộng theo modulo 2 với khối rõ. Kết quả thu được lại làm véc-tơ khởi đầu cho bước tiếp theo, rồi lại thực hiện tương tự chế độ CBC:

$C_i = M_i \text{ r } E_k(C_{i-1})$

$Mi = C_i \text{ r } D_k(C_{i-1})$

Chế độ đầu ra liên kết ngược OFB (Output Feedback): Thực chất của chế độ OFB là tạo ra khóa dòng rồi cộng theo modulo 2 với bản rõ. Khóa dòng được tạo như sau: Đầu tiên lấy véc-tơ khởi đầu s_0 rồi mã hóa qua phép mã khối E_k được s_1. Tiếp đó, s_1 lại được mã hóa qua E_k để được s_2,.. và cứ thế thực hiện cho đến khi tạo được khóa dòng có độ dài bằng dữ liệu cần mã.

Mỗi chế độ sử dụng mã khối trên đây đều có ưu điểm và nhược điểm riêng. Tùy từng trường hợp cụ thể mà người ta lựa chọn một chế độ sử dụng phù hợp đáp ứng yêu cầu bảo mật đặt ra.

3.2.2. Phòng chống tấn công website

Để chống xâm nhập vào website, các DNVVN nên thực hiện một số giải pháp sau:

Không dùng share hosting

Hiện nay, rất nhiều website bị tấn công do hosting chung trên cùng máy chủ với các website khác. Với hiện trạng bảo mật còn yếu, khi tin tặc tấn công vào một website thì

sẽ thực hiện leo thang đặc quyền dùng website này làm "bàn đạp" để tấn công vào các website khác trong cùng máy chủ. Đây là một lỗ hổng rất phổ biến mà các tin tặc thường dùng để xâm nhập website hiệu quả.

Để tránh tình trạng này thì đội ngũ quản trị của DNVVN nên sử dụng máy chủ ảo (VPS). Với máy chủ ảo, website sẽ chạy trên một máy chủ độc lập, do đó tính bảo mật cao hơn, giảm thiểu khả năng bị tấn công từ các đối tượng khác.

Kiểm tra mã nguồn website thường xuyên

Website được công khai cho tất cả mọi người truy cập, do đó phải thường xuyên giám sát, kiểm tra mã nguồn. Trong trường hợp phát hiện những tệp tin bất thường thì phải tiến hành kiểm tra, vì đây có thể là các Trojan/Backdoor do tin tặc cài vào hệ thống website.

Quá trình kiểm tra chống xâm nhập được thực hiện như: kiểm thử xâm nhập hộp đen (đánh giá từ bên ngoài hệ thống), kiểm thử xâm nhập hộp trắng (đánh giá từ bên trong hệ thống), sửa chữa các lỗi tìm thấy, trang bị các hệ thống phát hiện và phòng chống xâm nhập như: ModSecurity, tường lửa....

Không cài thêm các plugin "lạ" vào website

Hiện nay, rất nhiều website được phát triển trên các mã nguồn mở miễn phí như Joomla, Wordpress… các mã nguồn này cho phép cài thêm các plugin để tăng tính năng của website. Tuy nhiên, rất nhiều plugin "lạ", được cung cấp miễn phí trên internet có chứa Trojan/Backdoor đính kèm. Khi người sử dụng cài đặt plugin này vào website thì Trojan/Backdoor cũng được cài đặt và nằm "âm thầm" bên trong hệ thống để chờ lệnh.

Sao lưu dữ liệu thường xuyên

Dữ liệu là một phần rất quan trọng của hệ thống website. Dữ liệu có thể bị mất do tin tặc xâm nhập và xóa mất, hoặc do bị thiên tai, hỏa hoạn, lũ lụt.... Thực tế đã chứng minh rằng, nhiều doanh nghiệp mất toàn bộ dữ liệu, thiệt hại kinh tế rất lớn do không thực hiện quy trình sao lưu dữ liệu. Do đó, công việc này phải được đưa vào danh sách công việc thường xuyên, có phân công nhân sự đảm trách.

3.2.3. Sử dụng chữ ký số trong các giao dịch điện tử [4, 12, 13]

Đối với các DNVVN hiện nay, hầu hết các thông tin đều được trao đổi qua mạng, giải pháp để đảm bảo thông tin có độ an toàn và tính xác thực cao là ứng dụng chữ ký số trong các giao dịch điện tử. Việc ứng dụng này được coi là yếu tố quan trọng giúp doanh nghiệp giữ vững và mở rộng thị trường, tăng tính cạnh tranh, và thực hiện các thỏa thuận thương mại với các nước trong khu vực và trên thế giới.

Chữ ký số giải quyết vấn đề đảm bảo độ an toàn thông tin, toàn vẹn dữ liệu và là bằng chứng chống chối bỏ trách nhiệm trên nội dung đã ký, giúp cho các DNVVN không phải gặp trực tiếp nhau mà vẫn có thể yên tâm mua bán, trao đổi, ký hợp đồng,… thông qua môi trường Internet".

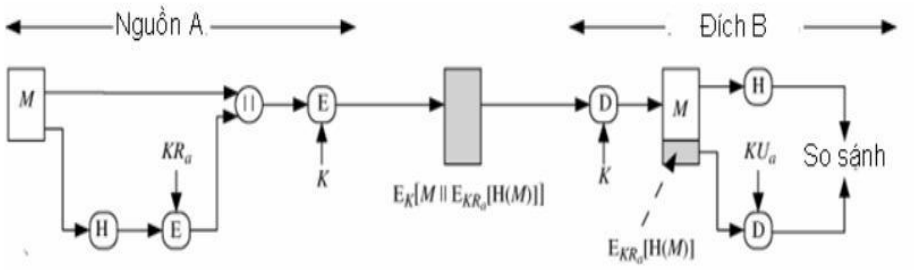
3.2.3.1. Khái niệm:

Chữ ký số khóa công khai (hay hạ tầng khóa công khai) [5] là mô hình sử dụng các kỹ thuật mật mã để gắn với mỗi người sử dụng một cặp khóa công khai - bí mật và qua đó có thể ký các văn bản điện tử cũng như trao đổi các thông tin mật. Khóa công khai thường được phân phối thông qua chứng thực khóa công khai. Quá trình sử dụng chữ ký số bao gồm 2 quá trình: tạo chữ ký và kiểm tra chữ ký.

3.2.3.2. Chức năng chữ ký số

- Xác minh tác giả và thời điểm ký thông tin được gửi
- Xác thực nội dung thông tin gửi
- Là căn cứ để giải quyết tranh chấp – không thể từ chối trách nhiệm

Giao thức của chữ ký số bao gồm thuật toán tạo chữ ký số và thuật toán để kiểm tra chữ ký số



Hình 3. 2. Minh họa chữ ký số của bên gửi cho thông báo M

KRa, KUa: khóa bí mật và công khai của bên A

K: khóa phiên đối xứng dùng chung của A và B

M: thông báo gửi

H: hàm băm

E: Mã hóa

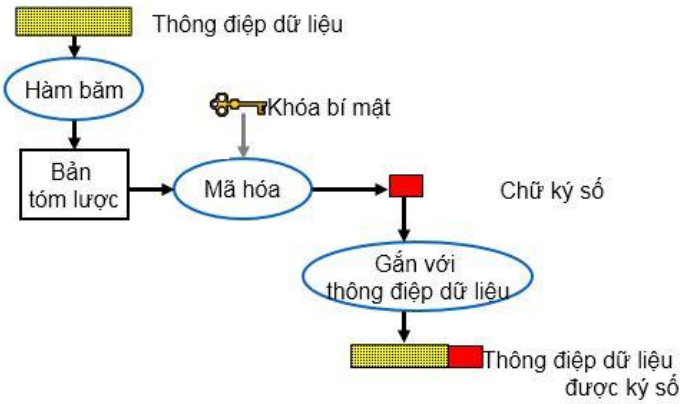
D: Giải mã

3.2.3.3. Mô hình chữ ký số RSA trong các hệ thống quản lý

Quá trình gửi và nhận các tệp văn bản phục vụ quản lý dựa vào thuật toán băm và thuật toán mã hóa RSA.

Quá trình ký và gửi các tệp văn bản

Từ file cần gửi ban đầu, chương trình sẽ sử dụng hàm băm để mã hóa chuỗi ký tự dài 128 bit. Chương trình sử dụng thuật toán RSA để mã hóa giá trị băm thu được với khóa riêng của người gửi được một giá trị gọi là chữ ký điện tử. Kết hợp file ban đầu với chữ ký điện tử thành một thông điệp đã ký và gửi đi cho người nhận



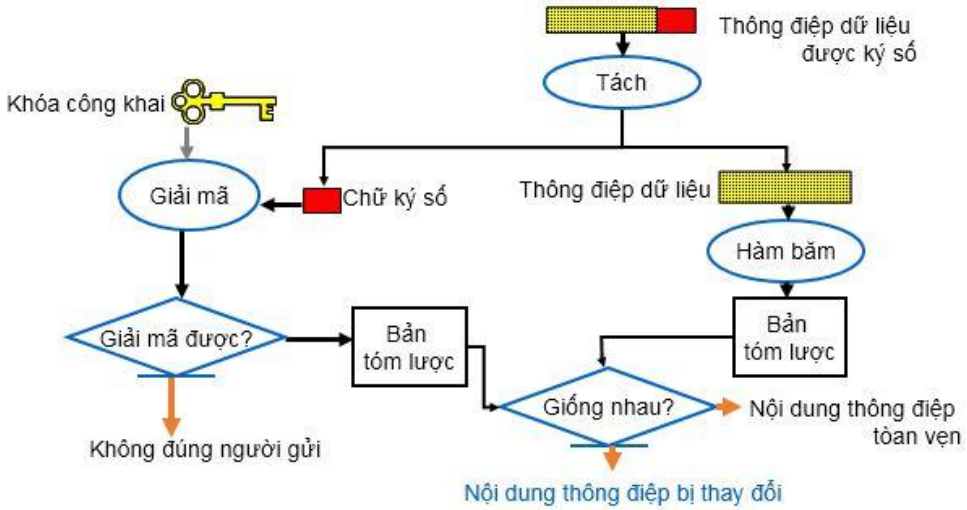
Hình 3. 3. Ký văn bản

Quá trình nhận các tệp văn bản

Sau khi người nhận nhận được văn bản, hệ thống sẽ tách thông điệp đã ký ra thành file và chữ ký điện tử. Đến giai đoạn này có 2 quá trình kiểm tra :

Kiểm tra file có đúng người gửi hay không: Sử dụng thuật toán RSA để giải mã chữ ký điện tử bằng khóa công khai của người gửi. Nếu giải mã không được file nhận được thì file nhận được không đúng người. Nếu giải mã thành công thì file nhận đuợc đúng người gửi và có giá trị băm 1 (bản tóm lược 1)

Kiểm tra file có bị thay đổi hay không: Từ file được tách ra ta sử dụng hàm băm mã hóa thành giá trị băm 2 (bản tóm lược 2). Kiểm tra giá trị băm 1 và giá trị băm 2 có giống nhau hay không? Nếu giống nhau thì file nhận được là toàn vẹn, không bị thay đổi, ngược lại là file đã bị thay đổi.



Hình 3. 4. Xác thực chữ ký

Đối với các DNVVN, chữ ký số có thể sử dụng trong các giao dịch thư điện tử, các e-mail, để mua hàng trực tuyến, đầu tư chứng khoán trực tuyến, chuyển tiền ngân hàng, thanh toán trực tuyến mà không sợ bị đánh cắp tiền như với các tài khoản Visa, Master. Ngoài ra, chữ ký số cũng có thể dùng để kê khai, nộp thuế trực tuyến, khai báo

hải quan và thông quan trực tuyến mà không phải mất thời gian đi in các tờ khai, đóng dấu đỏ của công ty rồi đến cơ quan thuế xếp hàng để nộp tờ khai này. Chữ ký số giúp cho các đối tác có thể ký hợp đồng làm ăn hoàn toàn trực tuyến không cần ngồi trực tiếp với nhau, chỉ cần ký vào file hợp đồng và gửi qua e-mail…

3.2.4 Xây dựng hệ thống mạng an toàn

Hệ thống mạng cung cấp các dịch vụ cốt lõi cho doanh nghiệp. Mọi người đều sử dụng phương tiện chia sẻ này để làm việc hiệu quả, bao gồm chia sẻ tệp, in ấn, gửi email và duyệt web. Sau đây là một số mô hình mạng an toàn mà doanh nghiệp có thể tham khảo, thiết lập.

Thiết kế an toàn về khía cạnh vật lý và môi trường cho hệ thống mạng

Đặt các tài sản thông tin quan trọng vào các phòng hoặc tủ khóa, bao gồm các đường dây truyền thông mạng, bộ định tuyến, thiết bị chuyển mạch, tường lửa, và các file của máy chủ.

Kiểm soát truy cập mạng.

Sử dụng sơ đồ địa chỉ IP riêng cho mạng nội bộ: Điều này sẽ ngăn không cho mạng nội bộ được truy cập bằng mạng bên ngoài. Chỉ sử dụng IP công cộng cho các máy truy cập công cộng.

Thiết kế bảo mật mạng internet bằng tổ chức mô hình mạng hợp lý [15]

Việc tổ chức mô hình mạng hợp lý có ảnh hưởng lớn đến sự an toàn cho các hệ thống mạng và các cổng thông tin điện tử. Đây là cơ sở đầu tiên cho việc xây dựng các hệ thống phòng thủ và bảo vệ. Ngoài ra, việc tổ chức mô hình mạng hợp lý có thể hạn chế được các tấn công từ bên trong và bên ngoài một cách hiệu quả.

Các thành phần trong mô hình:

Vùng mạng nội bộ: Còn gọi là mạng LAN (Local area network), là nơi đặt các thiết bị mạng, máy trạm và máy chủ thuộc mạng nội bộ của đơn vị.

Vùng mạng DMZ: Vùng DMZ là một vùng mạng trung lập giữa mạng nội bộ và mạng Internet, là nơi chứa các thông tin cho phép người dùng từ Internet truy xuất vào và chấp nhận các rủi ro tấn công từ Internet. Các dịch vụ thường được triển khai trong vùng DMZ là: máy chủ Web, máy chủ Mail, máy chủ DNS, máy chủ FTP,…

Vùng mạng Server: Vùng mạng Server hay Server Farm, là nơi đặt các máy chủ không trực tiếp cung cấp dịch vụ cho mạng Internet. Các máy chủ triển khai ở vùng mạng này thường là Database Server, LDAP Server,…

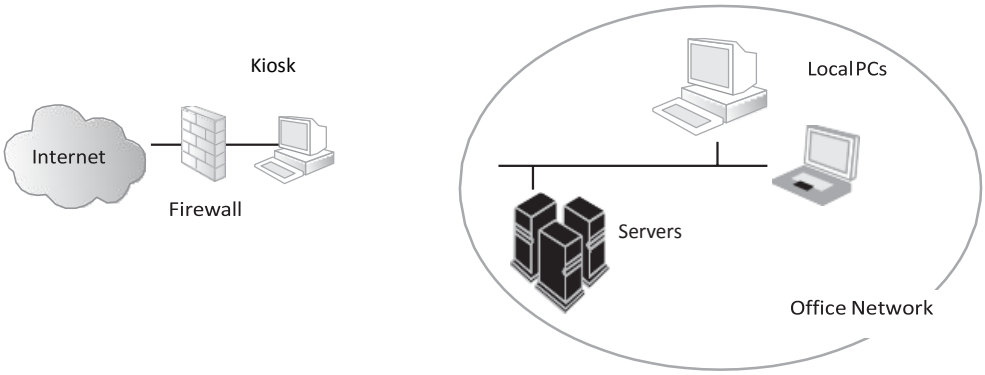
Vùng mạng Internet: Còn gọi là mạng ngoài, kết nối với mạng Internet toàn cầu.

- ***Các DNVVN có thể chọn từ một trong mô hình truy cập Internet sau[10]***:

(1) Mô hình Kiosk

- Trong mô hình này, một máy tính kiosk chuyên dụng được kết nối với Internet. Mạng văn phòng hoàn toàn tách biệt khỏi Internet. Mọi người phải đi đến máy tính kiosk để truy cập Internet.

- Đây là mô hình an toàn nhất vì mạng văn phòng không có các cuộc tấn công từ Internet. Tuy nhiên, hiệu suất của mô hình này thấp nhất.



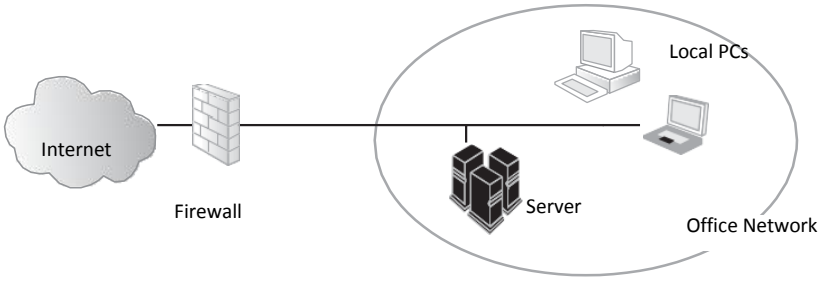
Hình 3. 5. Mô hình Kiosk

(2) Mô hình Office-Internet

- Trong mô hình này, các máy chủ và máy tính của doanh nghiệp được đặt phía sau tường lửa bảo vệ chống lại các cuộc tấn công từ Internet.

- Rủi ro bảo mật tồn tại khi một máy chủ truy cập công cộng có lỗ hổng bị khai thác bởi hacker, hacker có thể truy cập vào mạng văn phòng.

- Mô hình này hữu ích khi máy chủ email công ty được lưu trữ tại ISP và không có máy chủ truy cập công cộng trong văn phòng



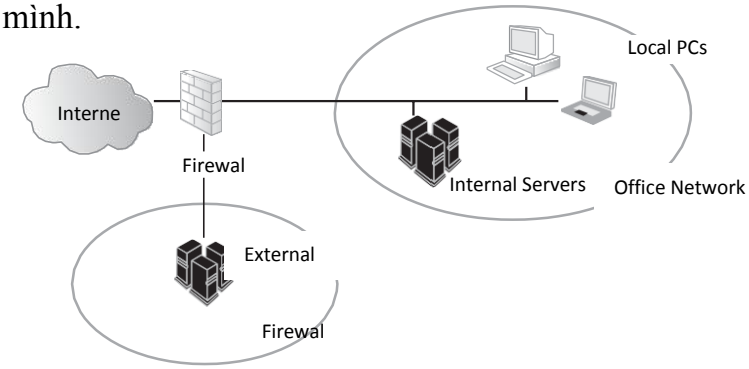
Hình 3. 6. Mô hình Office-Internet

(3) Mô hình Office-DMZ-Internet

- Mô hình này tương tự như mô hình Office-Internet nhưng có thêm dịch vụ mạng (DMZ). Các máy chủ của công ty được chia thành 2 nhóm với các máy chủ có thể truy cập công cộng đưa vào mạng DMZ.

- Nếu máy chủ bên ngoài bị xâm nhập, chỉ các máy chủ trong mạng DMZ bị phơi nhiễm. Mạng lưới văn phòng vẫn an toàn.

- Mô hình này rất hữu ích khi công ty cần lưu trữ máy chủ email và máy chủ web của chính mình.



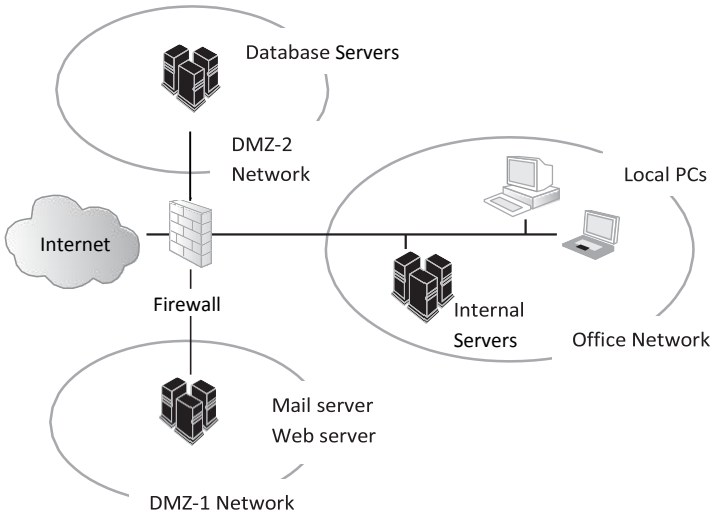
Hình 3. 7. Mô hình Office-DMZ-Internet

(4) Mô hình Office-MultiDMZ-Internet

- Mô hình này là một phần mở rộng của mô hình Office-DMZ-Internet, với nhiều hơn một mạng DMZ. Các máy chủ công cộng được chia thành 2 nhóm, mỗi nhóm được đặt trong một mạng DMZ riêng biệt.

- Máy chủ (email và web) trong mạng DMZ-1 được truy cập công cộng. Máy chủ cơ sở dữ liệu trong DMZ-2 phục vụ dữ liệu cho máy chủ web và không được truy cập trực tiếp bởi công cộng. Nếu mail hoặc máy chủ web bị xâm nhập, máy chủ cơ sở dữ liệu vẫn an toàn.

- Mô hình này rất hữu ích khi công ty cần lưu trữ máy chủ web của mình với máy chủ dữ liệu và muốn bảo vệ máy chủ cơ sở dữ liệu khỏi bị tấn công trên Internet.



Hình 3. 8. Mô hình Office-MultiDMZ-Internet

3.3. Các biện pháp giảm nhẹ rủi ro về ATTT cho các DNVVN [10]

3.3.1. Vai trò của giảm nhẹ rủi ro về ATTT

Giảm nhẹ rủi ro về ATTT giúp cho doanh nghiệp giảm thiểu thiệt hại về kinh doanh và mức độ bồi thường cho khách hàng;

- Giảm thiểu tác động có thể xảy ra do sự thiếu hiểu biết làm rò rỉ thông tin, mất mát và gián đoạn hệ thống,…;
- Đảm bảo hệ thống phục hồi nhanh chóng khi bị xâm nhập;
- Đảm bảo các nguồn lực cần thiết sẵn có để đối phó với sự cố, bao gồm nhân lực, công nghệ,…;
- Ngăn chặn các cuộc tấn công tiếp theo và giảm thiểu thiệt hại;
- Xử lý các vấn đề pháp lý có liên quan.

Có hai cách tiếp cận nhằm giảm thiểu rủi ro ATTT là:

- **Kiểm soát**: môi trường an toàn của công ty được liên tục theo dõi và hành động khắc phục được thực hiện khi cần thiết.
- **Kiểm định**: thông tin được thu thập và được phân tích bằng một quy trình riêng để xác định xem tình trạng an toàn hiện tại trong một khu vực cụ thể có đáp ứng các mục tiêu quản lý của doanh nghiệp hay không.

3.3.2. Kiểm soát và kiểm định [10]

Kiểm soát ATTT

Kiểm soát ATTT bao gồm việc giám sát và thực hiện các hành động khắc phục cần thiết đối với các khu vực ATTT trọng yếu, bao gồm:

- Chính sách ATTT, các tiêu chuẩn, hướng dẫn và thủ tục;
- Nhiệm vụ và trách nhiệm của các nhân viên trong công ty;
- Kiểm soát truy cập như ID người dùng và mật khẩu, quyền truy cập,…
- An toàn về khía cạnh vật lý;
- Thay đổi quản lý kiểm soát;
- Đào tạo nâng cao nhận thức về ATTT;
- Phản ứng và xử lý các sự cố ATTT.

Doanh nghiệp nên thực hiện một số kiểm soát về ATTT, ngoài ra nên thực hiện việc giám sát, đo lường để phát hiện vi phạm chính sách ATTT, chẳng hạn như:

- Các cửa an toàn cho những khu vực mở;
- Không đăng nhập vào máy trạm;
- Các cổng quá tải;
- Các thiết bị không được kiểm tra đầu vào và đầu ra;
- Chia sẻ mật khẩu;
- Khách viếng thăm truy cập vào các khu vực, dữ liệu, hệ thống nhạy cảm.

Máy tính và mạng nên được cấu hình một cách tự động để ghi lại các sự kiện có liên quan đến ATTT. Bản ghi các sự kiện này rất quan trọng và là tài sản vô giá đối với doanh nghiệp bởi nó có thể cung cấp các cảnh báo sớm về tình hình thực tế hoặc cố tình lạm dụng hệ thống bởi người dùng:

- Đưa ra cảnh báo sớm về hoạt động của các hacker hoặc tấn công bằng mã độc hại như:

+ Truy cập hệ thống vào những giờ bất thường;

+ Các nỗ lực để dò mật khẩu;

+ Các nỗ lực đột nhập vào hệ thống mạng;

- Cung cấp thông tin chẩn đoán liên quan đến sự cố ATTT.

- Cung cấp bằng chứng về hoạt động bất hợp pháp.

Các bản ghi này cung cấp một hồ sơ về tình hình sử dụng máy tính và mạng. Người Quản lý ATTT của doanh nghiệp nên thường xuyên phân tích các bản ghi, kèm theo báo cáo và hành động khắc phục. Dưới đây là một số lưu ý:

+ Chỉ giữ các bản ghi có giá trị, chẳng hạn như các bản ghi về đánh giá truy cập ảnh hưởng đến ATTT;

+ Kiểm tra nhật ký thường xuyên và báo cáo sự cố ngay khi phát hiện những điều bất thường, sử dụng các công cụ để tự động hóa quá trình xem xét đăng nhập;

+ Lưu các tệp nhật ký ở nơi an toàn nhằm đảm bảo các đối tượng truy cập trái phép không thể đọc hoặc thay đổi, có thể lưu tại máy chủ đảm bảo an toàn, đảm bảo lưu trữ trong khoảng thời gian từ 6 tháng trở lên;

+ Mã hóa các tệp nhật ký nhạy cảm.

Kiểm định

Kiểm định ATTT là một phần quan trọng của chương trình đảm bảo rủi ro, mục tiêu của việc kiểm định ATTT bao gồm:

- Rà soát các kiểm soát ATTT hiện có về các vấn đề hoạt động, hành chính và quản lý, và đảm bảo tuân thủ chính sách ATTT của doanh nghiệp;

- Xác định các lỗ hổng hiện có;

- Xem xét tính hiệu quả và sự thiếu sót của chính sách, tiêu chuẩn, hướng dẫn, thủ tục và sự triển khai về ATTT;

- Cung cấp các khuyến nghị và hành động khắc phục về các biện pháp ATTT sau khi đánh giá.

Có hai loại kiểm định: kiểm định an toàn và kiểm định chính sách:

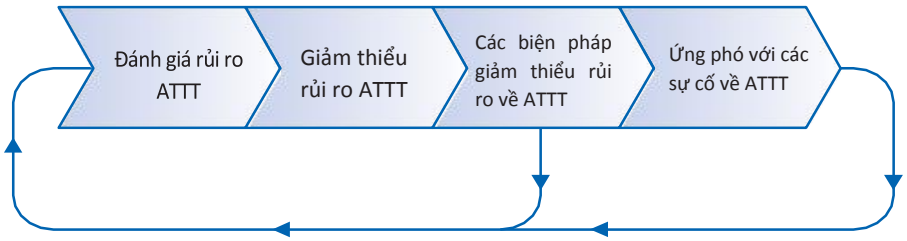
+ *Kiểm định an toàn*: xem xét lại hệ thống an toàn đối với các chính sách, thủ tục ATTT và tìm kiếm những điểm yếu, tính dễ bị tổn thương của hệ thống.

+ *Kiểm định chính sách*: kiểm tra và xác nhận các hệ thống chính sách ATTT đã được xác lập trong doanh nghiệp, đảm bảo rằng chính sách này phản ánh chính xác các quy tắc và quyền của hệ thống.

3.3.3. Đánh giá quy trình ATTT [10]

Đánh giá quy trình ATTT của doanh nghiệp nên được tiến hành tuần tự theo các giai đoạn: đánh giá rủi ro, giảm thiểu rủi ro, các biện pháp giảm thiểu rủi ro, giải quyết các sự cố về ATTT.

Quản lý ATTT hiệu quả quả đòi hỏi chuyên môn và kinh nghiệm về ATTT từ người quản lý doanh nghiệp và nhân viên kỹ thuật; Kinh nghiệm thu được từ đánh giá rủi ro, giảm thiểu rủi ro và các biện pháp giảm thiểu rủi ro sẽ điều kiện thuận lợi cho việc giải quyết các sự cố về ATTT.



Hình 3. 9. Đánh giá quy trình ATTT theo các giai đoạn

Báo cáo đánh giá quy trình ATTT nên được lập bởi bộ phận quản lý, khuyến nghị về nội dung của báo cáo bao gồm những phần sau:

- Tài liệu bảo mật hiện có;
- Báo cáo kiểm tra sự cố và báo cáo kiểm định;
- Chi tiết về việc thực hiện các khuyến nghị trong báo cáo phản hồi và báo cáo kiểm định;
- Nội dung chi tiết, đề xuất về những thay đổi được trong hệ thống, dịch vụ, hoạt động hoặc môi trường của doanh nghiệp;
- Chi tiết về những thay đổi môi trường bên ngoài có ảnh hưởng đến ATTT:

+ Công nghệ mới;

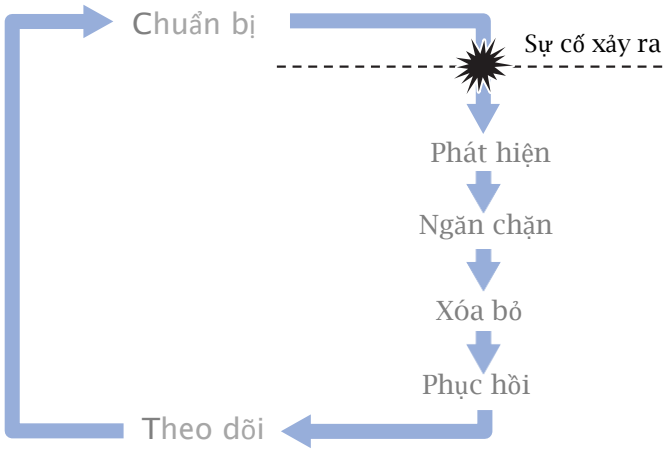
+ Quan điểm an toàn của đối thủ cạnh tranh;

+ Luật và những quy định mới;

3.4. Ứng phó sự cố về ATTT

Khi các cuộc tấn công mạng có chiều hướng phát triển ngày càng chuyên nghiệp và có tổ chức thì hoạt động ứng phó sự cố càng trở nên cần thiết. Hoạt động này sẽ cung cấp cho doanh nghiệp những thông tin cần thiết thu thập được trong quá trình xử lý sự cố để chuẩn bị tốt hơn cho việc xử lý những sự cố tương tự trong tương lai và củng cố các giải pháp an toàn cho hạ tầng hệ thống CNTT

Có 6 bước ứng phó các sự cố về ATTT cho doanh nghiệp như sau[10]:



Hình 3. 10. Các bước ứng phó với sự cố về ATTT

3.4.1. Chuẩn bị

Ở bước này doanh nghiệp cần lập kế hoạch giải quyết sự cố một cách tối ưu nhằm đảm bảo chất lượng và thời gian giải quyết, nội dung của kế hoạch cần tập trung vào các vấn đề sau:

- Xác định các chính sách ATTT của doanh nghiệp, đảm bảo kế hoạch giải quyết sự cố phù hợp với chính sách.
- Xác định vai trò và trách nhiệm của các bộ phận, nhân viên tham gia vào quá trình xử lý sự cố ATTT.
- Thiết lập danh sách các tài sản/dịch vụ thông tin, mức độ ưu tiền cần phải giải quyết và xác lập thời gian giải quyết
- Thiết lập các báo cáo, quy trình, thủ tục trả lời sự cố. Các thủ tục này được thông báo cho tất cả nhân viên trong công ty, bao gồm cả nhân viên quản lý, để tham khảo và tuân thủ.
- Lập chiến lược sao lưu dữ liệu.
- Thực hiện đào tạo nhân viên, đảm bảo rằng tất cả cán bộ quản lý và các nhân viên có liên quan đều có khả năng xử lý sự cố ATTT.
- Tuyên truyền cho người sử dụng về những cảnh báo khẩn cấp và các địa chỉ nghi ngờ.

Thiết lập cơ chế đồng bộ hóa theo thời gian hệ thống cho các hệ thống máy tính.

Thiết lập cơ chế theo dõi, báo động cho hệ thống máy tính, chẳng hạn như cài đặt hệ thống chống xâm nhập, chống vi rút, các công cụ lọc nội dung,…

3.4.2. Phát hiện

Khi phát hiện sự cố ATTT, doanh nghiệp nên dành thời gian để đánh giá sự cố, tìm hiểu trước khi đưa ra kết luận, đồng thời theo dõi những biểu hiện bất thường như: các thông báo lỗi, bản ghi đáng ngờ,…

- Xác định vấn đề của và mức độ ảnh hưởng.
- Bắt đầu ghi chép sự cố theo mẫu đã chuẩn bị.

- Thực hiện sao lưu toàn bộ hệ thống đã bị xâm nhập ngay khi phát hiện ra sự cố và lưu trữ ở nơi an toàn.

- Thiết lập hồ sơ về sự cố: nhật ký, sổ sách, vv

3.4.3. Ngăn chặn

Các hoạt động trong giai đoạn này bao gồm:

- Tiến hành đánh giá tác động của sự cố trên dữ liệu và thông tin của hệ thống để xác định các dữ liệu có liên quan, các thông tin đã bị hư hỏng hay mới bị nhiễm;

- Thực hiện bảo vệ các thông tin và hệ thống nhạy cảm hoặc quan trọng bằng cách di chuyển các thông tin quan trọng đến các các hệ thống khác và đảm bảo hệ thống này đã được tách ra khỏi hệ thống bị xâm nhập;

- Xác định tình trạng hoạt động của hệ thống bị xâm nhập;

- Lưu trữ lại hình ảnh của hệ thống bị xâm nhập cho mục đích điều tra và làm bằng chứng;

- Ghi chép về tất cả các hành động được thực hiện trong giai đoạn này;

- Kiểm tra toàn bộ hệ thống liên quan đến hệ thống bị xâm nhập thông qua các dịch vụ dựa trên những thông tin được chia sẻ hoặc qua bất kỳ mối quan hệ tin tưởng nào.

Một trong những quyết định quan trọng cần thực hiện là có nên tiếp tục hay đình chỉ các hoạt động và dịch vụ của hệ thống bị xâm nhập hay không. Điều này phụ thuộc vào loại và mức độ nghiêm trọng của sự cố bởi nó tác động đến hình ảnh của công ty.

Những hành động cần thực hiện bao gồm:

- Tắt hoặc tạm ngừng hoạt động của máy chủ hay hệ thống bị xâm nhập để ngăn ngừa các hư hỏng cho các hệ thống kết nối khác;

- Tắt một số chức năng của hệ thống;

- Loại bỏ quyền truy cập của người dùng hoặc đăng nhập vào hệ thống;

- Trong trường hợp sự cố không nghiêm trọng, có thể tiếp tục duy trì hoạt động của hệ thống nhưng phải xử lý cẩn thận và theo dõi chặt chẽ để thu thập chứng cứ cho vụ việc.

3.4.4. Xóa bỏ

Mục đích của giai đoạn này là loại bỏ hoặc giảm nhẹ nguyên nhân của sự cố ATTT. Trong giai đoạn này, các hành động sau có thể cần được thực hiện tùy thuộc vào mức độ, tính chất của sự cố cũng như yêu cầu của hệ thống:

- Ngừng hoặc xóa tất cả các quy trình hoạt động của hacker.

- Xoá tất cả các tệp tin giả mạo do hacker tạo ra. Có thể phải lưu trữ các tập tin giả mạo trước khi xóa để điều tra về sự cố.

- Loại bỏ tất cả các backdoor và các chương trình độc hại do hacker cài đặt.

- Áp dụng bản vá lỗi cho các lỗ hổng trên tất cả các hệ điều hành, máy chủ và các thiết bị mạng,…Các bản vá lỗi hoặc bản sửa lỗi được áp dụng cần được kiểm tra kỹ lưỡng trước khi đưa hệ thống trở lại hoạt động bình thường.

- Chỉnh sửa bất kỳ cài đặt không phù hợp nào trong hệ thống và mạng, ví dụ: Cấu hình sai trong tường lửa và router.

- Trong trường hợp xảy ra sự cố nhiễm vi rút, cần phải diệt toàn bộ vi rút từ các hệ thống bị nhiễm.

Cần đảm bảo rằng các bản sao lưu được diệt vi rút và có biện pháp tái nhiễm ở giai đoạn sau khi khôi phục hệ thống.

- Sử dụng một số công cụ bảo mật nhằm hỗ trợ quá trình loại bỏ, ví dụ như các công cụ quét an toàn để phát hiện bất kỳ sự xâm nhập nào, các công cụ này phải được cập nhật phiên bản mới nhất.

- Cập nhật mật khẩu truy cập của tất cả các tài khoản đăng nhập.

Trong một số trường hợp, bộ phận xử lý sự cố phải định dạng và cài đặt lại hệ thống, đặc biệt là khi họ không chắc chắn về mức độ thiệt hại hoặc rất khó để làm sạch hoàn toàn Hệ thống.

3.4.5. Phục hồi

Mục đích của giai đoạn này là khôi phục hệ thống hoạt động bình thường, một số nhiệm vụ cần thực hiện như sau:

- Đánh giá những thiệt hại sau sự cố.

- Cài đặt lại các tập tin bị xóa/hư hỏng hoặc toàn bộ hệ thống.

- Sắp xếp các ứng dụng/dịch vụ trở lại hoạt động theo các giai đoạn, một cách có kiểm soát, có thể sắp xếp ưu tiên theo thứ tự nhu cầu như: Các dịch vụ thiết yếu nhất hoặc những dịch vụ phục vụ nhiều người.

- Xác minh rằng hoạt động khôi phục đã thành công và hệ thống đã trở lại hoạt động bình thường.

- Thông báo cho tất cả các bên liên quan: người điều hành, quản trị viên, quản lý cấp cao, và các bên khác liên quan về việc khôi phục lại hoạt động của hệ thống.

- Tắt các dịch vụ không cần thiết.

- Lưu giữ một bản ghi về tất cả các hành động được thực hiện.

- Lưu ý: trước khi đưa hệ thống trở lại hoạt động bình thường, cần tiến hành kiểm tra an toàn đảm bảo rằng hệ thống và các thành phần liên quan của nó được đảm bảo.

3.4.6. Theo dõi

Mục tiêu của giai đoạn này là rút ra bài học từ sự cố, việc theo dõi nên bắt đầu càng sớm càng tốt, các nhiệm vụ cần thực hiện bao gồm:

- Tiến hành phân tích sau sự cố để cải tiến những biện pháp phòng tránh:

+ Kiểm tra toàn bộ cấu hình hiện tại của hệ thống.

+ Kiểm tra sự cần thiết phải đào tạo người dùng.

+ Xác định xem sự cố đó có cần phải có những hành động mạng tính pháp lý hay không.

- Mời các bên liên quan cùng tham gia bình luận và phân tích sự cố: một bản báo cáo về cuộc họp cùng với những đề xuất cải tiến các biện pháp phòng tránh cần được soạn lập và gửi tới ban điều hành công ty.

- Ban điều hành công ty nên đánh giá bản báo cáo và lựa chọn các khuyến nghị để cải tiến sẽ được thực hiện. Những người báo cáo về sự cố và những người tham gia khắc phục sự cố thành công sẽ được khen thưởng.

CHƯƠNG 4: CÀI ĐẶT VÀ THỬ NGHIỆM CHỮ KÝ SỐ ĐẢM BẢO ATTT TRONG VIỆC KÝ KẾT HỢP ĐỒNG ĐIỆN TỬ CỦA DNVVN

4.1. Tổng quan về hợp đồng điện tử

4.1.1. Khái niệm

Theo Điều 11, mục 1, Luật mẫu về Thương mại điện tử UNCITRAL 1996: *"Hợp đồng điện tử được hiểu là hợp đồng được hình thành thông qua việc sử dụng thông điệp dữ liệu"*

Theo Luật giao dịch điện tử của Việt Nam 2005: *"Hợp đồng điện tử là hợp đồng được thiết lập dưới dạng thông điệp dữ liệu theo quy định của Luật này"*

Thông điệp dữ liệu: "Thông tin được tạo ra, được gửi đi, được nhận và lưu trữ bằng phương tiện điện tử"

Các hình thức thể hiện thông điệp dữ liệu: Thông điệp dữ liệu được thể hiện dưới dạng hình thức trao đổi dữ liệu điện tử, chứng từ điện tử, thư điện tử, điện tín, điện báo, fax và các hình thức tương tự khác (webpage, file âm thanh, file văn bản…)[2]

4.1.2. Một số hợp đồng điện tử

Hợp đồng truyền thống được đưa lên web

Một số hợp đồng truyền thống đã được sử dụng thường xuyên và chuẩn hóa về nội dung, do một bên soạn thảo và đưa lên website để các bên tham gia ký kết. Hợp đồng điện tử loại này thường được sử dụng trong một số lĩnh vực như dịch vụ viễn thông, internet, điện thoại, du lịch, vận tải, bảo hiểm, tài chính, ngân hàng… Các hợp đồng được đưa toàn bộ nội dung lên web và phía dưới thường có nút **"Đồng ý"** hoặc **"Không đồng ý"** để các bên tham gia lựa chọn và xác nhận sự đồng ý với các điều khoản của hợp đồng.

Hợp đồng điện tử hình thành qua giao dịch tự động

Ở hình thức này nội dung hợp đồng không được soạn sẵn mà được hình thành trong giao dịch tự động. Máy tính tự tổng hợp nội dung và xử lý trong quá trình giao dịch dựa trên các thông tin do người mua nhập vào. Một số giao dịch điện tử kết thúc bằng hợp đồng, một số khác kết thúc bằng đơn đặt hàng điện tử, cuối quá trình giao dịch, hợp đồng điện tử được tổng hợp và hiển thị để người mua xác nhận sự đồng ý với các nội dung của hợp đồng. Sau đó, người bán sẽ được thông báo về hợp đồng và gửi xác nhận đối với hợp đồng đến người mua qua nhiều hình thức, có thể bằng email hoặc các phương thức khác như điện thoại, fax…

Hợp đồng hình thành qua nhiều giao dịch bằng email

Đây là hình thức hợp đồng điện tử được sử dụng phổ biến trong các giao dịch điện tử giữa các doanh nghiệp với doanh nghiệp (B2B), đặc biệt là trong các giao dịch thương mại điện tử quốc tế. Trong hình thức này, các bên sử dụng thư điện tử để tiến hành các giao dịch, các bước phổ biến thường bao gồm: chào hàng, hỏi hàng, đàm phán về các

điều khoản của hợp đồng như quy cách phẩm chất, giá cả, số lượng, điều kiện cơ sở giao hàng…

Hợp đồng điện tử sử dụng chữ ký số

Đặc điểm nổi bật là các bên phải có chữ ký số để ký vào các thông điệp dữ liệu trong quá trình giao dịch. Chính vì có sử dụng chữ ký số nên loại hợp đồng điện tử này có **độ bảo mật và ràng buộc trách nhiệm các bên cao hơn các hình thức trên.**

4.1.3. Lợi ích của hợp đồng điện tử

Thứ nhất, hợp đồng điện tử giúp các bên tiết kiệm thời gian, chi phí giao dịch, đàm phán và ký kết hợp đồng.

Thứ hai, sử dụng hợp đồng điện tử giúp các doanh nghiệp giảm chi phí bán hàng.

Thứ ba, sử dụng hợp đồng điện tử giúp quá trình giao dịch, mua bán nhanh và chính xác hơn.

Thứ tư, sử dụng hợp đồng điện tử giúp các doanh nghiệp nâng cao năng lực cạnh tranh và khả năng hội nhập kinh tế quốc tế. Hợp đồng điện tử không chỉ đem lại lợi ích cho các nhà sản xuất mà còn đem lại nhiều lợi ích cho các công ty thương mại..

4.1.4. Một số điểm cần lưu ý khi ký kết và thực hiện hợp đồng điện tử

Những hợp đồng nào có thể ký dưới dạng dữ liệu điện tử ?

- Điều 24 Luật thương mại 2005: quy định HĐ mua bán hàng hóa được thể hiện bằng văn bản, lời nói, hành vi
- Điều 27: Quy định HĐ mua bán hàng hóa quốc tế phải được thực hiện trên cơ sở hợp đồng bằng văn bản hoặc hình thức khác có giá trị tương đương
- Điều12 Luật giao dịch điện tử: Trường hợp pháp luật yêu cầu thông tin phải được thể hiện bằng văn bản thì thông điệp dữ liệu được xem là đáp ứng yêu cầu này nếu thông tin chứa trong thông điệp dữ liệu đó có thể truy cập và sử dụng được để tham chiếu khi cần thiết.

Giá trị tương đương bản gốc

Hợp đồng điện tử được forward (gửi chuyển tiếp) vào một hộp thư điện tử chuyên dùng để lưu trữ có giá trị như bản gốc hay không?

Điều 15. Lưu trữ thông điệp dữ liệu

- Nội dung của thông điệp dữ liệu đó có thể truy cập và sử dụng được để tham chiếu khi cần thiết;
- Nội dung của thông điệp dữ liệu đó được lưu trong chính khuôn dạng mà nó được khởi tạo, gửi, nhận hoặc trong khuôn dạng cho phép thể hiện chính xác nội dung dữ liệu đó;
- Thông điệp dữ liệu đó được lưu trữ theo một cách thức nhất định cho phép xác định nguồn gốc khởi tạo, nơi đến, ngày giờ gửi hoặc nhận thông điệp dữ liệu.

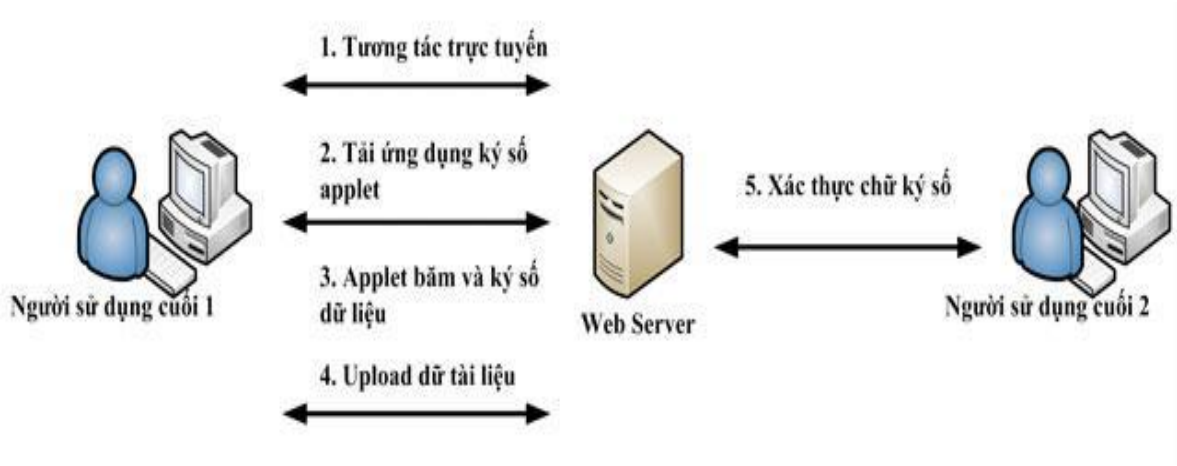
4.2. Quy trình cơ bản để ký kết hợp đồng điện tử có sử dụng chữ ký số

4.2.1. Những khía cạnh cần thiết về an toàn thông tin

Các yêu cầu trong giao dịch thương mại điện tử nói chung và hợp đồng điện tử nói riêng gồm:

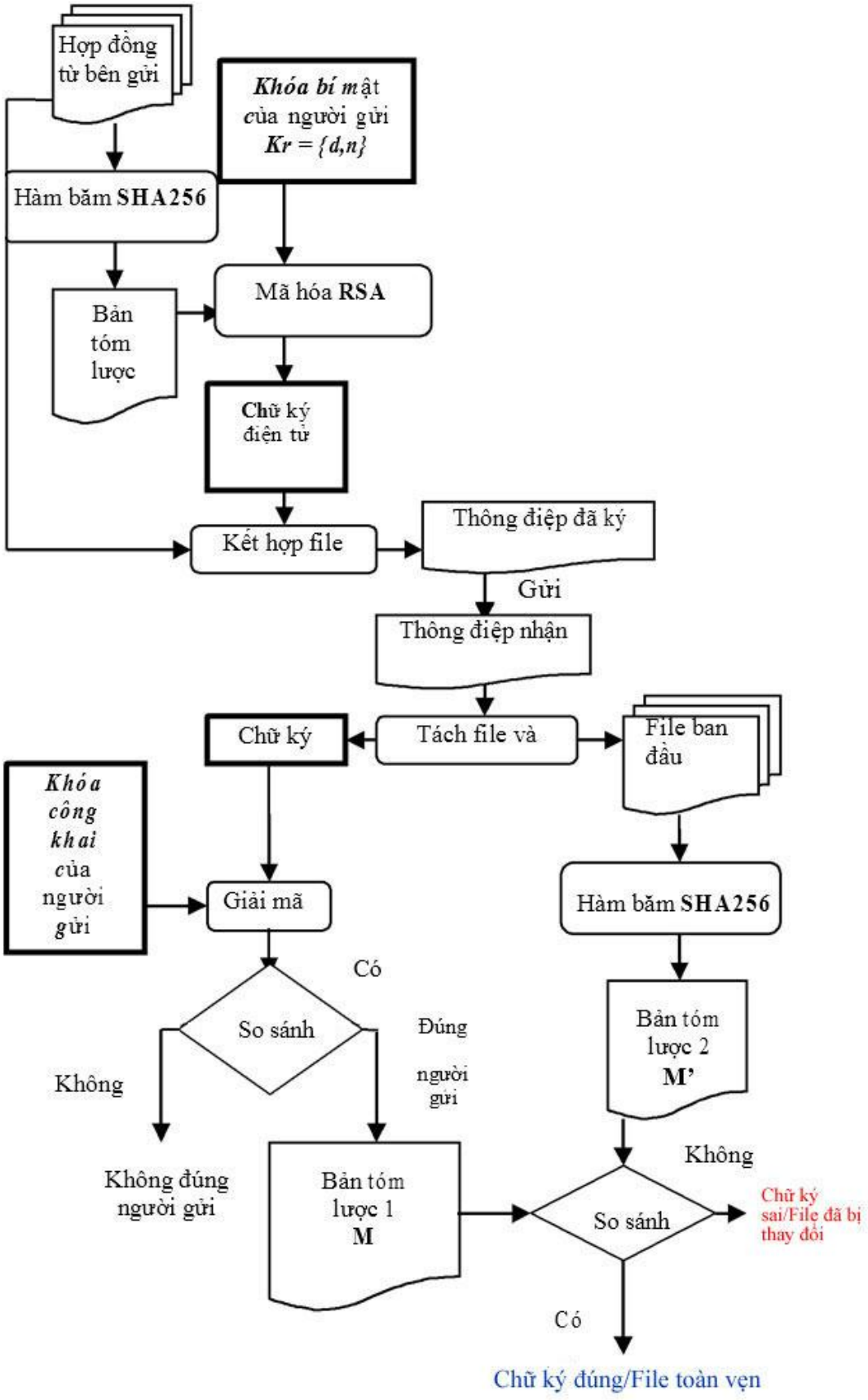
• **Đảm bảo tính bí mật**: tính bí mật nội dung thông điệp truyền đi được thực hiện bằng mã hóa trước khi gửi đi.

• **Đảm bảo tính toàn vẹn và nguồn gốc người gửi thông điệp**: thực hiện nhờ chữ ký số dựa trên mã hóa khóa công khai.



Hình 4. 1. Vai trò của xác thực người dùng

Trong quá trình ký kết hợp đồng điện tử, việc truyền thông điệp được đảm bảo an toàn qua việc mô tả quá trình ký và kiểm tra chữ ký trong chương trình như sau:



Hình 4. 2. Sơ đồ quá trình ký số hợp đồng điện tử

4.2.1.1. Quá trình ký và gửi hợp đồng

- Bên gửi soạn thảo hợp đồng, sau đó chương trình sử dụng hàm băm SHA256 để mã hóa thành chuỗi ký tự dài 256 bit gọi là bản tóm lược. Quy trình này còn được gọi là quy trình rút gọn hợp đồng (Hash-Value).

- Sử dụng thuật toán RSA để mã hóa khóa mật (private key) và bản tóm lược được chữ ký điện tử.

- Kết hợp bản hợp đồng với chữ ký điện tử thành một thông điệp đã ký và gửi đi cho người nhận.

4.2.1.2. Quá trình nhận hợp đồng

Sau khi bên nhận đăng nhập vào hệ thống và thực hiện việc nhận các tệp văn bản, hệ thống sẽ tách thông điệp đã ký thành ra file và chữ ký điện tử. Đến giai đoạn này sẽ có 2 quá trình kiểm tra :

a. Kiểm tra file có đúng người gửi hay không?

- Chương trình sử dụng thuật toán RSA để giải mã chữ ký điện tử bằng khóa công khai của người gửi.
- Nếu giải mã không được thì file nhận được không đúng người gửi.
- Nếu giải mã thành công thì file nhận được đúng người gửi và có được Bản tóm lược 1.

b. Kiểm tra file có bị thay đổi hay không?

- Từ file được tách ra, chương trình sử dụng hàm băm SHA256 mã hóa thành Bản tóm lược 2.
- Kiểm tra Bản tóm lược 1 và Bản tóm lược 2 có giống nhau hay không? Nếu giống nhau thì file nhận được là vẹn toàn (không bị thay đổi hay tác động), ngược lại là file đã bị thay đổi.

4.2.2 Cài đặt thử nghiệm

4.2.2.1. Xây dựng chương trình

Chương trình được xây dựng bằng ngôn ngữ lập trình C#, sử dụng hàm băm SHA256 và hệ mật RSA.

Hàm băm SHA256 là hàm băm phù hợp với tiêu chuẩn quốc gia Việt Nam về chữ ký số (TCVN 7635:2007)

SHA-256 có thể được sử dụng để băm một thông điệp M có chiều dài l bit với $0 \leq l < 2^{64}$. Thuật toán sử dụng một thông điệp lịch trình với 64 chữ 32-bit, 8 biến làm việc với 32 bit mỗi biến và giá trị băm với 8 chữ 32-bit. Kết quả cuối cùng của SHA-256 là một thông điệp tóm lược 256-bit.

Các chữ trong thông điệp lịch trình được gắn nhãn W_0, W_1,…, W_{63}. Tám biến làm việc được dán nhãn ***a***, ***b***, ***c***, ***d***, ***e***, ***f***, ***g*** và ***h***. Các chữ của giá trị băm được dán nhãn $H_0^{(i)}$, $H_1^{(i)}, \ldots, H_7^{(i)}$ để giữ lại giá trị băm ban đầu $H^{(0)}$ đã được thay thế bởi các giá trị băm trung

gian liên tiếp (sau khi mỗi khối thông điệp được xử lý) $H^{(i)}$ và kết thúc với giá trị băm cuối cùng $H^{(N)}$. SHA-256 sử dụng hai chữ tạm thời T_1 và T_2.

Giá trị băm ban đầu H(0) gồm 8 chữ 32-bit, trong hex như sau:

H_0^((0)) = c1059ed8
H_0^((0)) = 6a09e667
H_1^((0)) = bb67ae85
H_2^((0)) = 3c6ef372
H_3^((0)) = a54ff53a
H_4^((0)) = 510e527f
H_5^((0)) = 9b05688c
H_6^((0)) = 1f83d9ab
H_7^((0)) = 5be0cd19

Thuật toán băm SHA256

Phép cộng (+) được thực hiện theo modulo 2^{32}.

Mỗi khối thông điệp $M^{(1)}$, $M^{(2)}$,…, $M^{(N)}$ được xử lý theo thứ tự theo các bước sau đây :

For *i*=1 to *N*:

{

1. Chuẩn bị thông điệp lịch trình $\{W_t\}$:

$$W_t = \begin{cases} M_t^{(i)} & 0 \le t \le 15 \\ \sigma_1^{\{256\}}(W_{t-2}) + W_{t-7} + \sigma_0^{\{256\}}(W_{t-15}) + W_{t-16} & 15 \le t \le 63 \end{cases}$$

2. Khởi tạo tám biến làm việc ***a, b, c, d, e, f, g, h*** với (*i*-1)st giá trị :

a = $H_0^{(i-1)}$
b = $H_1^{(i-1)}$
c = $H_2^{(i-1)}$
d = $H_3^{(i-1)}$
e = $H_4^{(i-1)}$
f = $H_5^{(i-1)}$
g = $H_6^{(i-1)}$
h = $H_7^{(i-1)}$

3. For *t*=0 to 63:

{

$$T_1 = h + \sum_1^{\{256\}}(e) + Ch(e,f,g) + K_t^{\{256\}} + W_t$$

$$T_2 = \sum_0^{\{256\}}(a) + Maj(a,b,c)$$

$h = g$

$g = f$

$f = e$

$e = d + T_1$

$d = c$

$c = b$

$b = a$

$a = T_1 + T_2$

}

4. Tính toán lần thứ *i* giá trị băm trung gian $H^{(i)}$:

$H_0^{(i)} = a + H_0^{(i-1)}$

$H_1^{(i)} = b + H_1^{(i-1)}$

$H_2^{(i)} = c + H_2^{(i-1)}$

$H_3^{(i)} = d + H_3^{(i-1)}$

$H_4^{(i)} = e + H_4^{(i-1)}$

$H_5^{(i)} = f + H_5^{(i-1)}$

$H_6^{(i)} = g + H_6^{(i-1)}$

$H_7^{(i)} = h + H_7^{(i-1)}$

}

Sau khi lặp đi lặp lại các bước 1 đến 4 *N* lần (tức là sau khi xử lý $M^{(N)}$), thông điệp tóm lược 256-bit của thông điệp M là:

$$H_0^{(N)} || H_1^{(N)} || H_2^{(N)} || H_3^{(N)} || H_4^{(N)} || H_5^{(N)} || H_6^{(N)} || H_7^{(N)}$$

SHA-256 được sử dụng trong quá trình chứng thực gói phần mềm Debian GNU/ Linux và trong DKIM (chuẩn xác thực Email);

Hiện nay, Bộ Thông tin và Truyền thông đã có Quyết định số 1411/QĐ-BTTTT ngày 14/8/2016 về việc chuyển đổi chứng thư số sử dụng hàm băm an toàn SHA1 sang SHA256 trước ngày 31/12/2016

4.2.2.2. Các bước thử nghiệm chương trình:

Bước1: Bên gửi soạn thảo hợp đồng.

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM

Độc lập – Tự do – Hạnh phúc

HỢP ĐỒNG HỢP TÁC

V/v: Ươm tạo doanh nghiệp Công nghệ

Số:……/2017/ RISME

- Căn cứ Luật Khoa học và Công nghệ;
- Chức năng, nhiệm vụ của các bên;
- Căn cứ kết quả tiền ươm tạo và đơn đăng ký tham gia ươm tạo của doanh nghiệp.

Hôm nay, ngày 06 tháng 3 năm 2017, tại Văn phòng Viện Nghiên cứu doanh vừa và nhỏ, chúng tôi gồm:

BÊN A: VIỆN NGHIÊN CỨU DOANH NGHIỆP VỪA VÀ NHỎ (Cơ sở ươm tạo)

Đại diện: TS Phạm Thế Hưng - Chức vụ: Viện trưởng

Địa chỉ: Phòng 415-416E1, Khu ngoại giao đoàn Trung Tự, số 6 Đặng Văn Ngữ, Đống Đa, Hà Nội

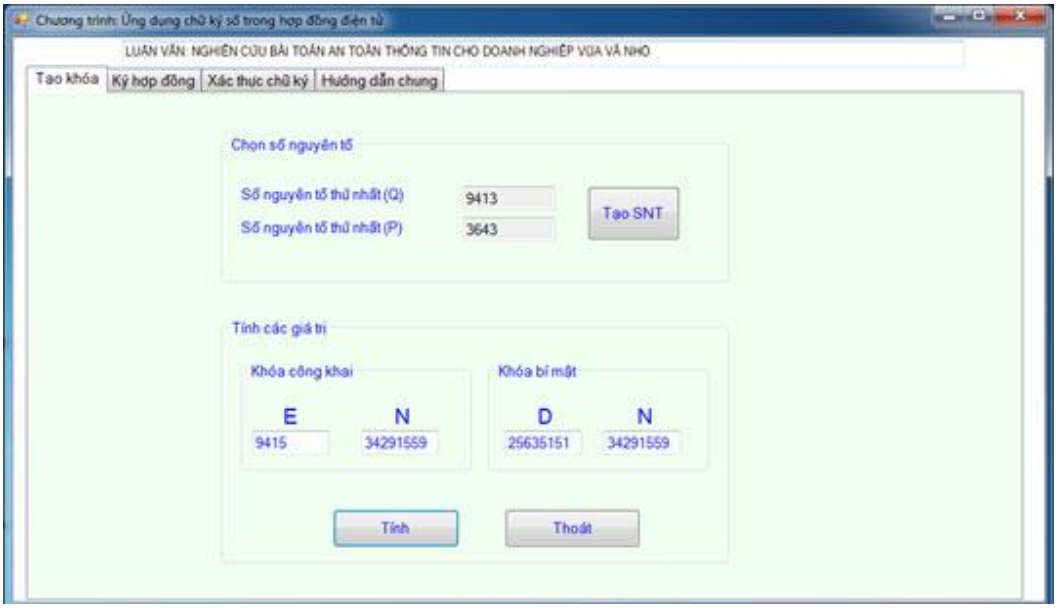
Hình 4. 3. Mẫu hợp đồng

Bước 2*: *Quy trình ký số và gửi hợp đồng

Tạo khóa

- Nhấn nút "Tính" để tạo ra cặp khóa bí mật (Pravite key) - (D,N), khóa công khai (Public key) - (E,N).

- Cất giữ khóa bí mật (D,N) để ký văn bản, công bố khóa công khai (E,N) để xác nhận chữ ký.



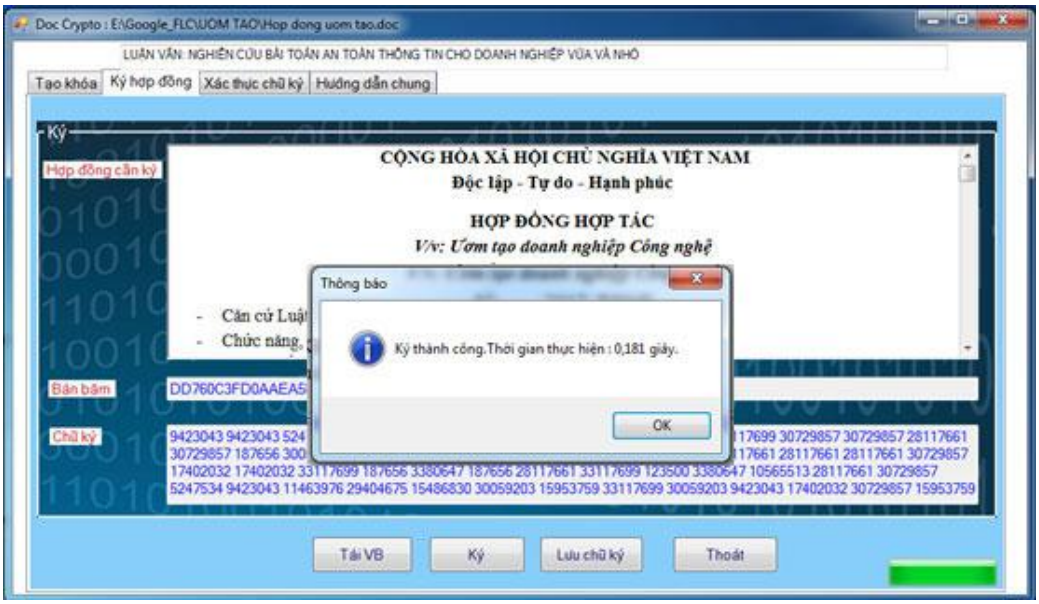
Hình 4. 4. Tạo cặp khóa RSA cho người dùng

Ký hợp đồng

- Tải hợp đồng cần ký bằng cách chọn nút "Tải VB"

- Nhấn nút "Ký" để ký văn bản, hàm băm SHA256 tóm lược hợp đồng chuỗi 256 bit (bản băm hay bản tóm lược).

- Thuật toán RSA mã hóa khóa mật (private key) và bản tóm lược được chữ ký điện tử



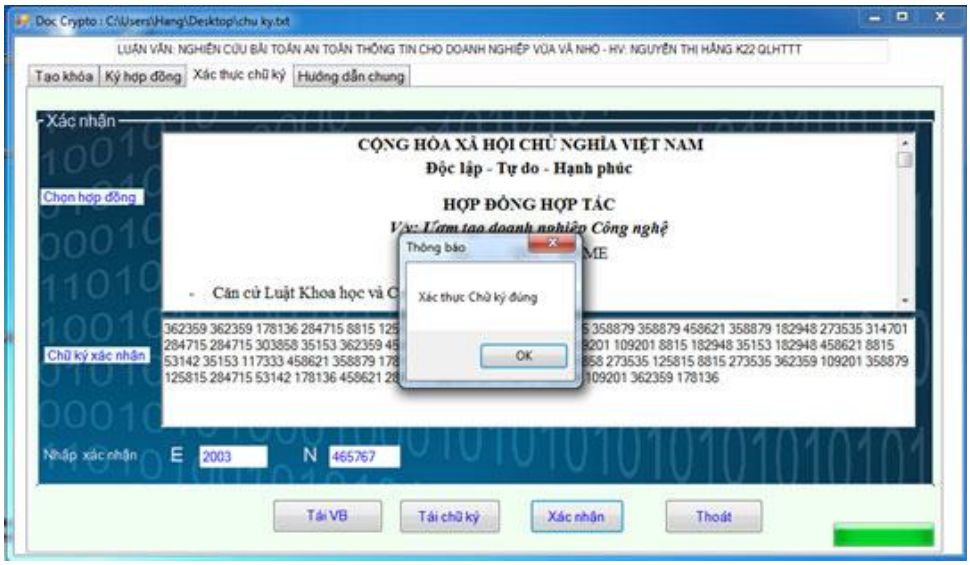
Hình 4. 5. ký hợp đồng bằng chữ ký điện tử

- Nhấn nút "Lưu chữ ký" để lưu giữ chữ ký điện tử dưới dạng file .txt.

Bên gửi gửi cho bên nhận bao gồm: Chữ ký điện tử và văn bản gốc cần ký

Bước 3: Quá trình nhận hợp đồng và xác thực chữ ký

- Bên nhận sử dụng chương trình, chọn cửa sổ "Xác thực chữ ký"
- Tải hợp đồng nhận được để xác nhận.
- Tải chữ ký điện tử của người gửi để xác nhận.
- Nhập khóa công khai (E,N) của người gửi để xác nhận.
- Nhấn nút "Xác nhận" để xác thực chữ ký của văn bản điện tử.



Hình 4. 6. Quá trình kiểm tra chữ ký

KẾT LUẬN

1. Các kết quả đạt được

a. Về lý thuyết

Để nghiên cứu bài toán an toàn thông tin cho doanh nghiệp vừa và nhỏ, học viên đã tập trung nghiên cứu cơ sở lý luận về an toàn thông tin, tìm hiểu đặc điểm hệ thống thông tin, thực trạng ATTT của các DNVVN, những tổn thất của DNVVN trước những nguy cơ mất ATTT để có thể đưa ra một số giải pháp đảm bảo ATTT phù hợp.

Bên cạnh đó, học viên cũng nghiên cứu, tìm hiểu một số hệ mật mã đảm bảo ATTT được dùng phổ biến hiện nay như: AES, RC4, RC5, RC6, RSA, đề xuất một số giải pháp đảm bảo ATTT cho DNVVN về mặt công nghệ ứng dụng một số hệ mật mã này như: Mã hóa dữ liệu cho DNVVN, ứng dụng chữ ký số trong các giao dịch điện tử đang phổ biến tại các DNVVN hiện nay.

Cùng với nhóm giải pháp về công nghệ, học viên cũng đề xuất nhóm giải pháp về quản lý ATTT đối với các DNVVN trong đó tập trung vào việc hướng dẫn các DNVVN thiết lập các Chính sách ATTT một cách bài bản, xây dựng kế hoạch đánh giá rủi ro, các biện pháp giảm thiểu rủi ro, cách ứng phó khi xuất hiện các mối de dọa ATTT.

b. Về thực nghiệm

Xuất phát từ yêu cầu thực tế cần phải đảm bảo tính bí mật, toàn vẹn nội dung thông điệp và xác định được nguồn gốc dữ liệu trong việc ký kết hợp đồng điện tử, học viên đã xây dựng ứng dụng chữ ký số trong việc ký kết hợp đồng điện tử dựa trên sơ đồ chữ ký số RSA và hàm băm SHA256.

2. Hướng nghiên cứu tiếp theo

Học viên sẽ tiếp tục tìm hiểu và thực nghiệm với một số phương pháp mã hoá khoá đối xứng như IDEA, một số hệ mật mã dòng, mật mã khối; các phương pháp mã hoá khoá công khai như Elgamal, Rabin, Knapsack, Eliptic Curve,…

Về phần thực nghiệm, học viên sẽ tìm hiểu, phát triển thêm phần chứng thực số và ứng dụng chữ ký số dùng trên các thiết bị thông minh như điện thoại, máy tính bảng,… giúp các DNVVN ký kết hợp đồng điện tử một cách thuận lợi nhất.

Hoàn thiện luận văn này, học viên mong muốn đóng góp một phần kiến thức của mình vào vấn đề ATTT cho các DNVVN hiện nay. Tuy nhiên, do hạn chế về nguồn số liệu và kiến thức, luận văn không tránh khỏi những thiếu sót nhất định. Hơn nữa, do tình hình ATTT còn nhiều bất ổn và khó dự đoán nên trong tương lai học viên sẽ tiếp tục nghiên cứu để tìm ra những giải pháp phù hợp nhất, đảm bảo an toàn thông tin cho các DNVVN.

TÀI LIỆU THAM KHẢO

Tiếng Việt

[1] Lê Phê Đô, Mai Mạnh Trừng, Lê Trung Thực, Nguyễn Thị Hằng, Vương Thị Hạnh, Nguyễn Khắc Hưng, Đinh Thị Thúy, Lê Thị Len, *Nghiên cứu một số hệ mật mã hạng nhẹ và ứng dụng IoT,* Tạp chí Nghiên cứu Khoa học và Công nghệ Quân sự số Đặc san 05-2017, từ trang 134-147.

[2] Luật Giao dịch điện tử ban hành ngày 29 tháng 11 năm 2005.

[3] Cục thương mại điện tử và Công nghệ thông tin*, Báo cáo thương mại điện tử năm 2015.*

[4] Nguyễn Văn Minh, Trần Hoài Nam, (2002*), Giao dịch thương mại điện tử - Một số vấn đề căn bản*, NXB Chính trị quốc gia Hà Nội

[5] TS. Hồ Văn Hương, KS. Hoàng Chiến Thắng, *Ký số và xác thực trên nền tảng web*, Tạp chí An toàn thông tin, số 2 (026) năm 2013.

[6] TS. Hồ Văn Hương, KS. Hoàng Chiến Thắng, KS. Nguyễn Quốc Uy *Giải pháp bảo mật và xác thực thư điện tử*, Tạp chí An toàn thông tin số 04 (028), 2013.

[7] PGS.TS. Trịnh Nhật Tiến, GV. Lý Hùng Sơn, *"Giáo trình an toàn dữ liệu và mã hóa"*, Trường Đại học Công nghệ - Đại học Quốc Gia Hà Nội, 5/2006

[8] Vnisa, *Báo cáo hiện trạng ATTT tại Việt Nam 2015*.

[9] Trần Minh Văn, Khoa Công nghệ thông tin - Trường đại học Nha Trang, Bài giảng: *An toàn và bảo mật thông tin, 2008*

Tiếng Anh

[10] The Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT): *Information Security Guide for Small Business*

[11] FIPS (1993), *Data Encryption Standard (DES)*

[12] Warwick Ford, Secure Electronic Commerce*: Building the Infrastructure for Digital Signatures and Encryption (2nd Edition) Paperback, Ed. Michael S. Baum, 2014*

[13] Addison Wesley, *Understanding PKI: Concepts, Standards, and Deployment Considerations*, Second Edition, 2002.

[14] Oreilly, *Web Security, Privacy & Commerce 2nd*

[15] Dr. Eric Cole, Dr. Ronald Krutz, and James W.Conley, *Network Security Bible*, Wiley Publishing, Jan 2005.

[16] T. Dierks, E. Rescorla (August 2008). *The Transport Layer Security (TLS) Protocol, Version 1.2*.

[17] Holly Lynne McKinley, SANS Institude. *SSL and TLS: A Beginners' Guide.*

[18] O. Goldreich, S. Goldwasser, and S. Micali, *"How to Construct Random Functions,"* Journal of the ACM, vol. 33, no. 4, pp.210–217, 1986

[19] S. Contini, R.L. Rivest, M.J.B. Robshaw and Y.L. Yin. *The Security of the RC6TM Block Cipher*. Version 1.0. August 20, 1998.