Khoa HTTT Kinh tế và THMĐT
Bộ môn Công nghệ thông tin

Bài giảng học phần

An toàn và bảo mật thông tin

1. Mục đích và yêu cầu

- Mục đích của học phần
  - Cung cấp những kiến thức cơ bản về an toàn và bảo mật thông tin cho HTTT doanh nghiệp
  - Cung cấp thông tin về các nguy cơ tấn công và phương pháp đảm bảo an toàn cho hệ thống thông tin doanh nghiệp
  - Giới thiệu một số ứng dụng của công nghệ trong đảm an toàn và bảo mật thông tin doanh nghiệp

1. Mục đích và yêu cầu (t)

- Yêu cầu cần đạt được
  - Nắm vững các kiến thức cơ bản về an toàn và bảo mật thông tin doanh nghiệp
  - Có kiến thức về các nguy cơ tấn công và và các phương pháp đảm bảo an toàn cho hệ thống thông tin doanh nghiệp
  - Sử dụng được một số ứng dụng đã có trong việc đảm bảo an toàn thông tin doanh nghiệp

2. Cấu trúc học phần

- Học phần gồm 3 tín chỉ (45 tiết) phân phối như sau:
  - Nội dung lý thuyết và thảo luận 45 tiết (15 buổi)
  - Thời gian: 10 buổi lý thuyết, 2 BT và KT, 3 Thảo luận
  - Email: hoint2002@gmail.com
  - Bài giảng: http://nguyenthihoi.com/baigiang

3. Nội dung học phần

- Chương 1. Tổng quan về an toàn và bảo mật thông tin
- Chương 2: Quy trình đảm bảo an toàn và bảo mật thông tin
- Chương 3: Các kiểu tấn công và các mối đe dọa đối với an toàn và bảo mật thông tin
- Chương 4: Mã hóa thông tin
- Chương 5: Sao lưu dữ liệu và phục hồi thông tin
- Chương 6: Đảm bảo an toàn cho hệ thống thông tin
- Chương 7: An toàn dữ liệu trong thương mại điện tử

4. Tài liệu tham khảo

1) Bộ môn CNTT, *Giáo trình An toàn dữ liệu trong thương mại điện tử*,, Đại học Thương Mại, NXB Thống kê, 2009.
2) Phan Đình Diệu, *Lý thuyết mật mã và an toàn thông tin,* Đại học Quốc gia Hà Nội, NXB ĐHQG, 1999.
3) William Stallings, *Cryptography and Network Security Principles and Practices, Fourth Edition,* Prentice Hall, 2008
4) Man Young Rhee. *Internet Security: Cryptographic principles, algorithms and protocols*. John Wiley & Sons, 2003.
5) David Kim, Michael G. Solomon, *Fundamentals of Information Systems Security,* Jones & Bartlettlearning, *2012.*
6) Michael E. Whitman, Herbert J. Mattord, *Principles of information security, 4th edition,* Course Technology, Cengage Learning, 2012.
7) Matt Bishop, *Introduction to Computer Security,* Prentice Hall, 2004.

Chương 1. Tổng quan về an toàn và bảo mật thông tin

- 1.1. GIỚI THIỆU CHUNG VỀ AN TOÀN VÀ BẢO MẬT THÔNG TIN
  - 1.1.1. Khái niệm an toàn và bảo mật thông tin
  - 1.1.2. Lịch sử phát triển của an toàn và bảo mật thông tin
  - 1.1.3. Vai trò của an toàn và bảo mật thông tin
- 1.2. MỤC TIÊU VÀ YÊU CẦU CỦA AN TOÀN VÀ BẢO MẬT THÔNG TIN
  - 1.2.1. Mục tiêu của an toàn và bảo mật thông tin
  - 1.2.2. Yêu cầu cho an toàn và bảo mật thông tin
  - 1.2.3. Các nguyên tắc an toàn và bảo mật thông tin
  - 1.2.4. Các mô hình đảm bảo an toàn và bảo mật thông tin
- 1.3. AN TOÀN VÀ BẢO MẬT THÔNG TIN THEO QUẢN TRỊ RỦI RO
  - 1.3.1. Tổng quan cề rủi ro và quản trị rủi ro
  - 1.3.2. Tổng quan về rủi ro cho thông tin và quản trị rủi ro trong hệ thống thông tin
  - 1.3.3. Mối quan hệ giữa quản trị rủi ro cho thông tin trong hệ thống thông tin và đảm bảo an toàn và bảo mật thông tin
- 1.4. CHÍNH SÁCH, PHÁP LUẬT VỀ AN TOÀN VÀ BẢO MẬT THÔNG TIN
  - 1.4.1. Các chính sách an toàn và bảo mật thông tin ở Việt Nam
  - 1.4.2. Các chính sách an toàn và bảo mật thông tin trên thế giới
- CÂU HỎI ÔN TẬP VÀ THẢO LUẬN CHƯƠNG 1

1.1. GIỚI THIỆU CHUNG VỀ ATBM TT

- 1.1.1. Khái niệm an toàn và bảo mật thông tin
- 1.1.2. Lịch sử phát triển của an toàn và bảo mật thông ti
- 1.1.3. Vai trò của an toàn và bảo mật thông tin

1.1.1. Khái niệm ATBM thông tin

- Khái niệm ATBM TT
  - ATTT là gì?
  - Bảo mật TT là gì?
- Ví dụ
  - Hỏng hóc máy tính
  - Sao chép dữ liệu trái phép
  - Giả mạo
  - …

1.1.1. Khái niệm ATBM thông tin

- Khái niệm HTTT An toàn
  - Đảm bảo an toàn thông tin
  - Đảm bảo hệ thống có khả năng hoạt động liên tục
  - Đảm bảo khả năng phục hồi khi gặp sự cố

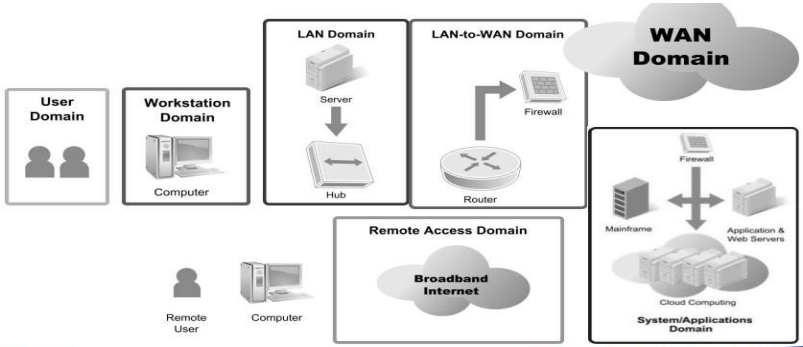
1.1.2. Lịch sử phát triển của ATBMTT

1.1.3. Vai trò của an toàn và bảo mật thông tin

- Bảo vệ chức năng hoạt động của tổ chức
- Tạo môi trường thuận lợi cho các ứng dụng trong tổ chức thực thi an toàn
- Bảo vệ dữ liệu mà tổ chức thu thập và sử dụng.
- Bảo vệ các tài sản có tính công nghệ trong các tổ chức

1.1.3. Vai trò của an toàn và bảo mật thông tin

Các vùng cần đảm bảo ATTT trong HTTT



Các vùng cần đảm bảo ATTT trong HTTT

- Vùng người dùng (User domain)
- Vùng máy trạm (Workstation domain)
- Vùng mạng LAN (LAN domain)
- Vùng LAN-to-WAN (LAN-to-WAN domain)
- Vùng WAN (WAN domain)
- Vùng truy nhập từ xa (Remote Access domain)
- Vùng hệ thống/ứng dụng (Systems/Applications domain)

1.2. MỤC TIÊU VÀ YÊU CẦU CỦA ATBM TT

- 1.2.1. Mục tiêu của an toàn và bảo mật thông tin
- 1.2.2. Yêu cầu cho an toàn và bảo mật thông tin
- 1.2.3. Các nguyên tắc an toàn và bảo mật thông tin
- 1.2.4. Các mô hình đảm bảo an toàn và bảo mật thông tin

1.2.1. Mục tiêu của ATBM TT

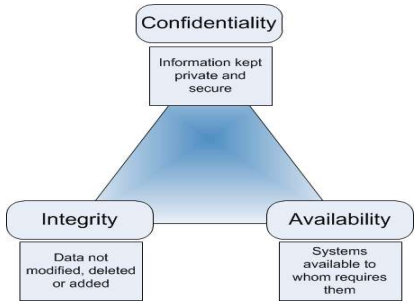
- (1) Phát hiện các lỗ hổng của hệ thống thông tin cũng như dự đoán trước những nguy cơ tấn công vào hệ thống thông tin của tổ chức gây mất an toàn và bảo mật thông tin.
- (2) Ngăn chặn những hành động gây mất an toàn thông tin và bảo mật thông tin từ bên trong cũng như từ bên ngoài của tổ chức.
- (3) Phục hồi các tổn thất trong trường hợp hệ thống thông tin bị tấn công gây mất an toàn và bảo mật thông tin, nhằm đưa hệ thống thông tin trở lại hoạt động bình thường trong thời gian sớm nhất

Nguyên tắc đánh giá HTTT an toàn

- (1) Có tìm và phát hiện được tất cả các khả năng mà đối tượng phá hoại có thể thâm nhập vào hệ thống thông tin ?
- (2) Có đảm bảo tất cả các tài sản của tổ chức phải được bảo vệ đến khi hết giá trị sử dụng?

1.2.2. Yêu cầu cho ATBM TT

- Yêu cầu cho ATBM TT (CIAA)
  - Có tính bí mật
  - Có tính toàn vẹn
  - Có tính sẵn sàng
  - Có tính xác thực
- Bảo mật HTTT là gì?
  - Các công cụ?
  - Các biện pháp?
  - Thực hiện như thế nào?

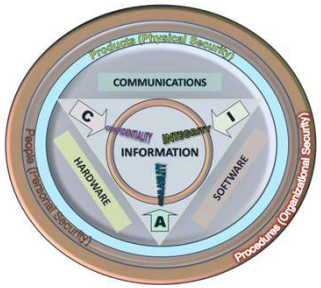


1.2.3. Các nguyên tắc ATBM TT

- Giới hạn quyền hạn tối thiểu (Last Privilege) cho người dùng trong hệ thống thông tin của tổ chức, doanh nghiệp.
- Cần triển khai mô hình bảo vệ theo chiều sâu (Defence In Depth).
- Việc kiểm soát trong hệ thống thông tin phải được thực hiện theo cơ chế nút thắt (Choke Point).
- Thường xuyên phát hiện và gia cố các điểm nối yếu nhất (Weakest Link) của hệ thống thông tin.
- Các giải pháp đảm bảo an toàn và bảo mật thông tin phải mang tính toàn cục (Global solutions)
- Cần đa dạng các biện pháp bảo vệ (Multi-methods)

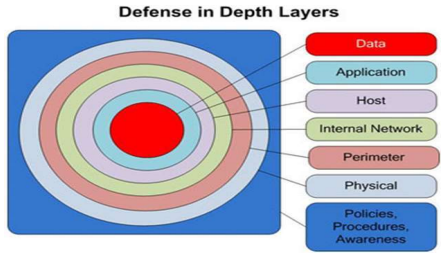
1.2.4. Các mô hình đảm bảo ATBMTT

- Yêu cầu:
  - Mức tổ chức ?
  - Mức cá nhân ?
  - Mức vật lý ?
  - Phần cứng ?
  - Phần mềm ?
  - Hệ thống mạng ?

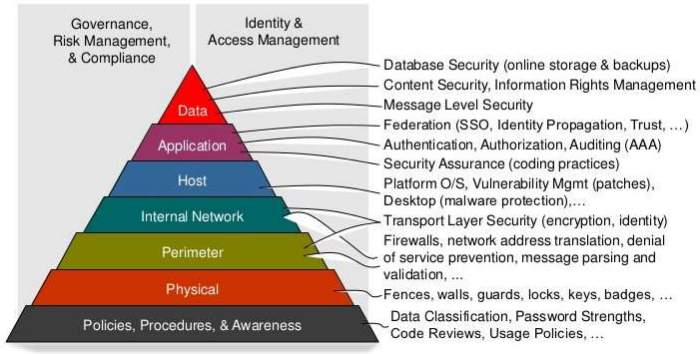


1.2.4. Các mô hình đảm bảo ATBMTT

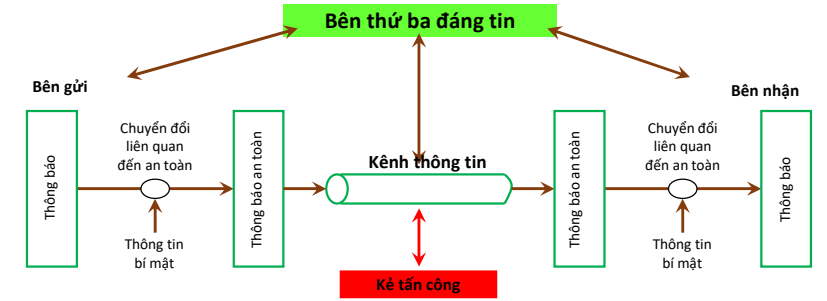
- Các mức bảo vệ trong mô hình theo chiều sâu
  - Các biện pháp?
  - Kỹ thuật?
  - Phương pháp thực hiện?
  - Chính sách của tổ chức?



Defense in Depth



1.2.4. Các mô hình đảm bảo ATBMTT

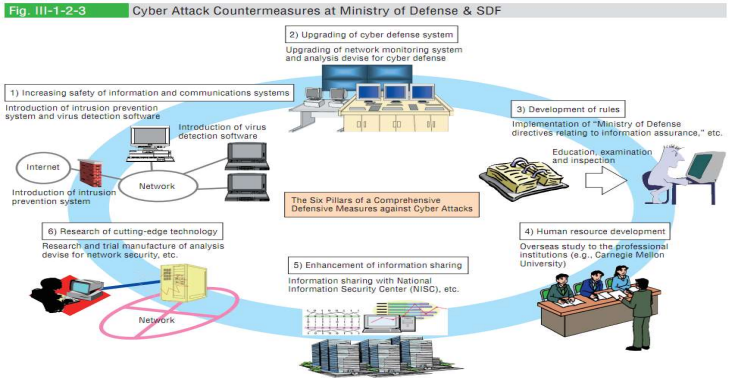


Mô hình an toàn trong truyền thông tin

1.2.4. Các mô hình đảm bảo ATBMTT

- Chính sách bảo mật theo lớp
  - Lớp an ninh cơ quan/tổ chức (Plant Security)
    - Lớp bảo vệ vật lý
    - Lớp chính sách & thủ tục đảm bảo ATTT
  - Lớp an ninh mạng (Network Security)
    - Lớp an ninh cho từng thành phần mạng
    - Tường lửa, mạng riêng ảo (VPN)
  - Lớp an ninh hệ thống (System Security)
    - Lớp tăng cường an ninh hệ thống
    - Lớp quản trị tài khoản và phân quyền người dùng
    - Lớp quản lý các bản vá và cập nhật phần mềm
    - Lớp phát hiện và ngăn chặn phần mềm độc hại.

1.2.4. Các mô hình đảm bảo ATBMTT



1.3. ATBMTT THEO QUẢN TRỊ RỦI RO

- 1.3.1. Tổng quan về rủi ro và quản trị rủi ro
- 1.3.2. Tổng quan về rủi ro cho thông tin và quản trị rủi ro trong HTTT
- 1.3.3. Mối quan hệ giữa QTRR cho thông tin trong HTTT và đảm bảo ATBM thông tin

1.3.1. Tổng quan về rủi ro và quản trị rủi ro

- *Rủi ro được hiểu là* một biến cố không chắc chắn mà nếu xảy ra thì sẽ gây tổn thất cho con người hoặc tổ chức nào đó.
- *Các đặc trưng cơ bản* là tần suất rủi ro và biên độ rủi ro.
  - Tần suất rủi ro biểu hiện số lần xuất hiện rủi ro trong một khoảng thời gian hay trong tổng số lần quan sát sự kiện.
  - Biên độ rủi ro thể hiện tính chất nguy hiểm, mức độ thiệt hại gây ra nghĩa là thể hiện hậu quả hay tổn thất do rủi ro gây ra về tài chính, nhân lực, …

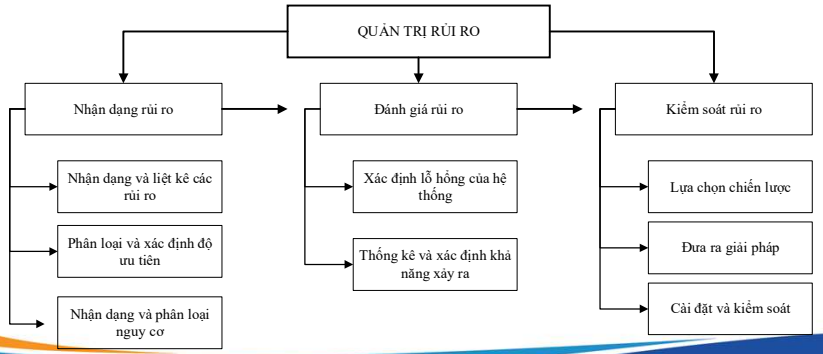
1.3.1. Tổng quan về rủi ro và quản trị rủi ro

- *Phân loại rủi ro*
  - Theo nguyên nhân gây ra rủi ro;
  - Theo kết quả hay hậu quả;
  - Theo nguồn gốc;
  - Theo đối tượng gánh chịu rủi ro;
  - Theo khả năng kiểm soát, giảm tổn thất;
  - Theo các giai đoạn phát triển của đối tượng chịu rủi ro.

1.3.1. Tổng quan về rủi ro và quản trị rủi ro

- Quản trị rủi ro
  - (1) Nhận biết các rủi ro có thể xảy ra trong hoạt động của tổ chức, phân tích nguồn gốc, tính chất và mức độ ảnh hưởng của các rủi ro đã được nhận dạng;
  - (2) Chỉ ra được những rủi ro cần và/có thể né tránh được và cách thức để tránh, cũng như chỉ ra những rủi ro nào có thể chấp nhận được;
  - (3) Chỉ ra cách thức, biện pháp cần áp dụng để phòng ngừa hay giảm thiểu hậu quả của các rủi ro khác;
  - (4) Dự tính được tổn thất nếu rủi ro sẽ xảy ra và đo lường được tổn thất trong trường hợp rủi ro đã xảy ra và phương thức, biện pháp khắc phục hậu quả, bù đắp tổn thất

1.3.2. Tổng quan về rủi ro cho thông tin và quản trị rủi ro trong hệ thống thông tin



Các mối đe dọa chính trong tổ chức

Threat	Example
Compromises to intellectual property	Piracy, copyright infringement
Espionage or trespass	Unauthorized access and/or data collection
Forces of nature	Fire, flood, earthquake, lightning
Human error or failure	Accidents, employee mistakes, failure to follow policy
Information extortion	Blackmail of information disclosure
Missing, inadequate, or incomplete controls	Software controls, physical security
Missing, inadequate, or incomplete organizational policy or planning	Training issues, privacy, lack of effective policy
Quality of service deviations from service providers	Power and WAN quality of service issues
Sabotage or vandalism	Destruction of systems or information
Software attacks	Viruses, worms, macros, denial of service
Technical hardware failures or errors	Equipment failure
Technical software failures or errors	Bugs, code problems, unknown loopholes
Technological obsolescence	Antiquated or outdated technologies
Theft	Illegal confiscation of property

Table 4-3 Threats to Information Security[5]

Source: ©2003 ACM, Inc., Included here by permission.

Bài tập về đánh giá rủi ro

- Phân loại các mối đe dọa
- Xác định rủi ro
- Đề xuất chiến lược?

Threat Category	Cost per Incident (SLE)	Frequency of Occurrence
Programmer mistakes	$5,000	1 per week
Loss of intellectual property	$75,000	1 per year
Software piracy	$500	1 per week
Theft of information (hacker)	$2,500	1 per quarter
Theft of information (employee)	$5,000	1 per six months
Web defacement	$500	1 per month
Theft of equipment	$5,000	1 per year
Viruses, worms, Trojan horses	$1,500	1 per week
Denial-of-service attacks	$2,500	1 per quarter
Earthquake	$250,000	1 per 20 years
Flood	$250,000	1 per 10 years
Fire	$500,000	1 per 10 years

Bài tập về đánh giá rủi ro

- Phân loại các mối đe dọa
- Xác định rủi ro
- Đề xuất chiến lược?

Threat Category	Cost per Incident	Frequency of Occurrence	Cost of Control	Type of Control
Programmer mistakes	$5,000	1 per month	$20,000	Training
Loss of intellectual property	$75,000	1 per 2 years	$15,000	Firewall/IDS
Software piracy	$500	1 per month	$30,000	Firewall/IDS
Theft of information (hacker)	$2,500	1 per 6 months	$15,000	Firewall/IDS
Theft of information (employee)	$5,000	1 per year	$15,000	Physical security
Web defacement	$500	1 per quarter	$10,000	Firewall
Theft of equipment	$5,000	1 per 2 years	$15,000	Physical security
Viruses, worms, Trojan horses	$1,500	1 per month	$15,000	Antivirus
Denial-of-service attacks	$2,500	1 per 6 months	$10,000	Firewall
Earthquake	$250,000	1 per 20 years	$5,000	Insurance/backups
Flood	$50,000	1 per 10 years	$10,000	Insurance/backups
Fire	$100,000	1 per 10 years	$10,000	Insurance/backups

Các nguyên tắc quản trị rủi ro trong HTTT

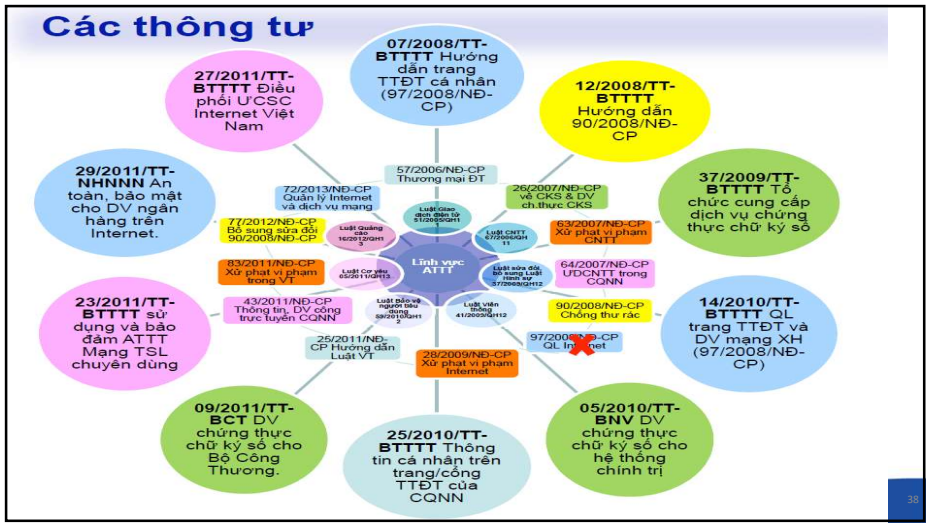
- *Nguyên tắc 1:* Không chấp nhận các rủi ro không cần thiết, chấp nhận rủi ro khi lợi ích thu được lớn hơn chi phí bỏ ra.
- *Nguyên tắc 2:* Các quyết định quản trị rủi ro phải được ra ở cấp quản trị thích hợp.
- *Nguyên tắc 3:* Hoạt động quản trị rủi ro trong hệ thống thông tin cần được thực hiện kết hợp với các hoạt động hoạch đinh cũng như vận hành ở tất cả các cấp trong hệ thống thông tin, cũng như trong tổ chức bởi quản trị rủi ro không phải và không thể là một hoạt động độc lập.

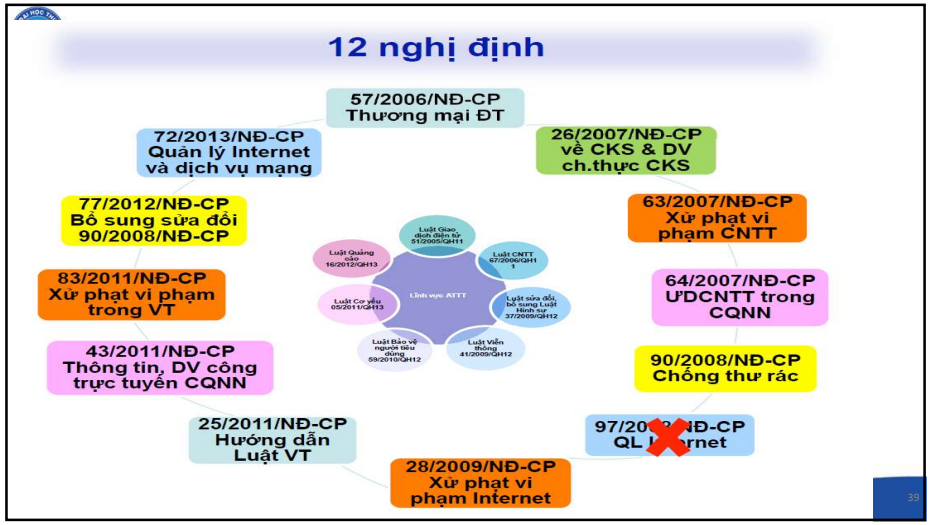
1.3.3. Mối quan hệ giữa QTRR cho thông tin trong HTTT và đảm bảo ATBMTT

- QTRR là quá trình nhận dạng, phân tích, đo lường, đánh giá rủi ro, để từ đó tìm các biện pháp kiểm soát, khắc phục các hậu quả của rủi ro đối với hoạt động kinh doanh nhằm sử dụng tối ưu các nguồn lực
- ATBMTT bao hàm các nội dung bảo vệ và bảo mật thông tin, an toàn dữ liệu, an toàn máy tính và an toàn mạng
- => Đảm bảo an toàn và bảo mật thông tin là một hoạt động cụ thể trong quy trình quản trị rủi ro của hệ thống thông tin doanh nghiệp. Nó đảm bảo cho thông tin trong hệ thống thông tin có tính bí mật, sẵn sàng và toàn vẹn khi hệ thống thông tin của doanh nghiệp hoạt động

1.4. CHÍNH SÁCH, PHÁP LUẬT VỀ ATBMTT

- 1.4.1. Các chính sách ATBM thông tin ở Việt Nam
- 1.4.2. Các chính sách ATBM thông tin trên thế giới





Một số Website

- 1. https://vnisa.org.vn
- 2. http://antoanthongtin.vn

Quy tắc quốc tế trong ứng xử về ATTTM

- Quy tắc 1: Quy tắc về lãnh thổ (The Territoriality Rule)
- Quy tắc 2: Quy tắc về trách nhiệm (The Responsibility Rule)
- Quy tắc 3: Quy tắc hợp tác (The Cooperation Rule)
- Quy tắc 4: Quy tắc tự vệ (The Self-Defence Rule)
- Quy tắc 5: Quy tắc bảo vệ dữ liệu (The Data Protection Rule)
- Quy tắc 6: Quy tắc nhiệm vụ xây dựng (The Duty of Care Rule)
- Quy tắc 7: Quy tắc cảnh báo sớm (The Early Warning Rule)
- Quy tắc 8: Quy tắc về quyền truy cập thông tin (The Access to Information Rule)
- Quy tắc 9: Quy tắc tố tụng hình sự (The Criminality Rule)
- Quy tắc 10: Quy tắc quyền ủy thác (The Mandate Rule)

Định hướng về phát triển ATBM TT của Việt Nam

- Định hướng về phát triển ATBM TT của Việt Nam
  - ATTTs là một trụ cột để phát triển CNTT, CPĐT…
  - ATTTs là một bộ phận của QPANQG
  - ATTTs là một ngành kinh tế công nghiệp, dịch vụ công nghệ cao
  - ATTTs là một lĩnh vực đặc thù ưu tiên sản phẩm, tổ chức nội địa
  - ATTTs là một lĩnh vực nóng trong đối ngoại
  - ATTTs là sự nghiệp của toàn xã hội

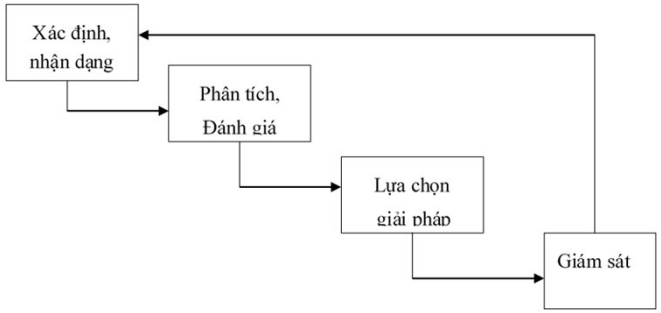
Câu hỏi chương 1

1. Trình bày khái niệm về an toàn thông tin? bảo mật hệ thống thông tin?
2. Vai trò của an toàn bảo mật thông tin trong hoạt động của các tổ chức, doanh nghiệp?
3. Nêu các nguy cơ gây mất an toàn thông tin? Các nguy cơ mất an toàn thông tin trong TMĐT?
4. Thế nào là tính bí mật? Tính toàn vẹn? Tính sẵn sàng? Tính không thể chối bỏ?
5. Mục tiêu của an toàn và bảo mật thông tin là gì? Hãy giải thích.
6. Yêu cầu chung của hệ thống đảm bảo an toàn thông tin? Hãy giải thích vì sao cần bảo vệ các tài sản của tổ chức, doanh nghiệp cho đến khi chúng bị loại bỏ khỏi hoạt động của tổ chức?
7. Quy trình chung đảm bảo an toàn thông tin cho tổ chức? Hãy giải thích các bước trong quy trình này?
8. Trình bày các mô hình đảm bảo an toàn và bảo mật thông tin? Cho ví dụ minh họa.
9. Trình bày mô hình bảo mật nhiều lớp trong hệ thống thông tin của tổ chức? Vì sao các hệ thống ISMS cần triển khai theo mô hình bảo mật nhiều lớp?
10. Trình bày và giải thích về mô hình truyền thông tin an toàn?

Chương 2. Quy trình đảm bảo ATBMTT

- 2.1. QUY TRÌNH CHUNG
  - 2.1.1. Xác định, nhận dạng các nguy cơ
  - 2.1.2. Phân tích, đánh giá các nguy cơ
  - 2.1.3. Lựa chọn giải pháp đảm bảo ATBMTT
  - 2.1.4. Giám sát an toàn và bảo mật thông tin
- 2.2. NHẬN DẠNG CÁC NGUY CƠ GÂY MẤT ATBTTT TRONG HTTT
  - 2.1.1. Khái niệm và tầm quan trọng của nhận dạng các nguy cơ
  - 2.1.2. Phân loại các nguy cơ
  - 2.1.3. Phương pháp nhận dạng các nguy cơ
- 2.3. PHÂN TÍCH, ĐÁNH GIÁ CÁC NGUY CƠ GÂY MẤT ATBMTT
  - 2.3.1. Khái niệm
  - 2.3.2. Nội dung phân tích, đánh giá các nguy cơ gây mất an toàn và bảo mật thông tin
- 2.4. KIỂM SOÁT ATBMTT
  - 2.4.1. Quy trình kiểm soát
  - 2.4.2. Chiến lược kiểm soát
- CÂU HỎI ÔN TẬP VÀ THẢO LUẬN CHƯƠNG 2

2.1. QUY TRÌNH CHUNG



2.2. NHẬN DẠNG CÁC NGUY CƠ GÂY MẤT ATBTTT

- 2.1.1. Khái niệm và tầm quan trọng của nhận dạng các nguy cơ
- 2.1.2. Phân loại các nguy cơ
- 2.1.3. Phương pháp nhận dạng các nguy cơ

2.1.1. Khái niệm và tầm quan trọng của nhận dạng các nguy cơ

- *Nhận dạng các nguy cơ gây mất an toàn và bảo mật thông tin được hiểu là* quá trình xác định một cách liên tục và có hệ thống các nguy cơ, các mối đe dọa có thể xảy ra gây mất an toàn và bảo mật thông tin trong các hoạt động liên quan đến thông tin bao gồm thu thập, xử lý, sử dụng, lưu trữ và truyền phát thông tin.

2.1.1. Khái niệm và tầm quan trọng của nhận dạng các nguy cơ

- *Mục đích của nhận dạng các nguy cơ*
  - (1) Các nguy cơ có thể xuất hiện;
  - (2) Các mối hiểm họa;
  - (3) Thời điểm nguy cơ có thể xuất hiện.

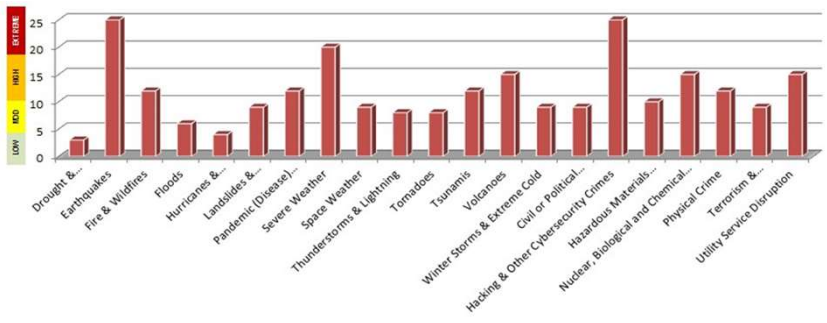
2.1.1. Khái niệm và tầm quan trọng của nhận dạng các nguy cơ

- **Nhận dạng nguy cơ giúp nhà quản trị**
  - Có thể chủ động trong việc ứng phó với các rủi ro, hiểm họa,
  - Làm cơ sở để đảm bảo hiệu quả của hoạt động đảm bảo an toàn và bảo mật thông tin
  - Hoạt động đảm bảo an toàn và bảo mật thông tin sẽ không thể được thực hiện hiệu quả nếu việc nhận dạng nguy cơ chưa được quan tâm đúng mức và tổ chức triển khai thực hiện một cách khoa học.

2.1.2. Phân loại các nguy cơ

- Các nguy cơ ngẫu nhiên
  - Lũ lụt, hỏa hoạn, động đất, song thần
  - Bệnh dịch
  - …
- Các nguy cơ có chủ định
  - Các nguy cơ từ thiết bị phần cứng;
  - Các nguy cơ từ phần mềm
  - Các nguy cơ từ con người (bao gồm cả người ở trong và ở ngoài tổ chức, doanh nghiệp).

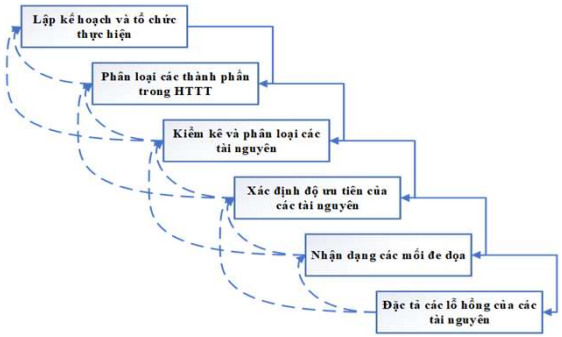
Một số nguy cơ



2.1.3. Phương pháp nhận dạng các nguy cơ

- Các bước trong quy trình nhận dạng các nguy cơ
  - (1) Bước 1: Lập kế hoạch và tổ chức quá trình thực hiện.
  - (2) Bước 2: Phân loại các thành phần của hệ thống thông tin.
  - (3) Bước 3: Kiểm kê và phân loại các tài nguyên.
  - (4) Bước 4: Phân loại các tài nguyên theo mức độ ưu tiên.
  - (5) Bước 5: Xác định các nguy cơ, mối đe dọa theo mức độ nguy hiểm.
  - (6) Bước 6: Chỉ định các mối đe dọa tấn công các lỗ hổng.

Quy trình nhận dạng nguy cơ



2.3. PHÂN TÍCH, ĐÁNH GIÁ CÁC NGUY CƠ

- 2.3.1. Khái niệm về nguy cơ
- 2.3.2. Nội dung phân tích, đánh giá các nguy cơ gây mất an toàn và bảo mật thông tin

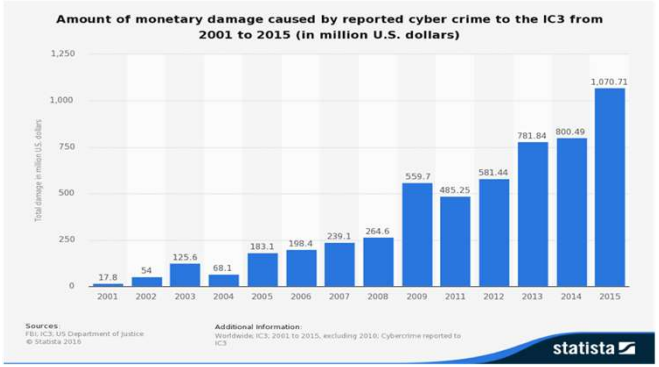
2.3.1. Khái niệm

- "Phân tích rủi ro là việc sử dụng kiến thức, kinh nghiệm, kỹ năng và ứng dụng công nghệ thông tin dựa theo tiêu chí quản lý rủi ro đã được xác định để dự đoán tần suất và hậu quả của rủi ro".
- Phân tích rủi ro là việc xác định, đánh giá và xác định mức độ ưu tiên các rủi ro với mục đích tiết kiệm các nguồn lực cũng như để giảm thiểu, giám sát và kiểm soát khả năng hoặc tác động của các sự kiện không may hoặc để tối đa hóa các cơ hội.
- Quá trình nghiên cứu những nguy cơ, hiểm họa đe dọa an toàn và bảo mật thông tin cũng như xác định những nguyên nhân, nguồn gốc của các nguy cơ, hiểm họa và phân tích, đo lường những tổn thất mà các nguy cơ, hiểm họa gây ra.

2.3.2. Nội dung phân tích, đánh giá các nguy cơ

- Liệt kê tất cả các nguy cơ, các mối đe dọa đã biết,
- Thu thập các thông tin liên quan đến các nguy cơ, mối đe dọa đã được xác định
- Xác định những hậu quả có thể xảy ra,
- Xây dựng các biện pháp có thể sử dụng để phòng ngừa và giảm nhẹ ảnh hưởng của các nguy cơ, các mối đe dọa,
- Tạo báo cáo phân tích, đánh giá.
- Cơ bản để đánh giá một rủi ro trong hệ thống thông tin thường sử dụng công thức sau đây:
  - Rủi ro = Xác suất/Khả năng xảy ra của (Mối đe dọa và Khai thác lỗ hổng) x Chi phí cho thiệt hại của tài sản.
  - (Risk =Probability (Threat + Exploit of Vulnerability) x Cost of Asset Damage)

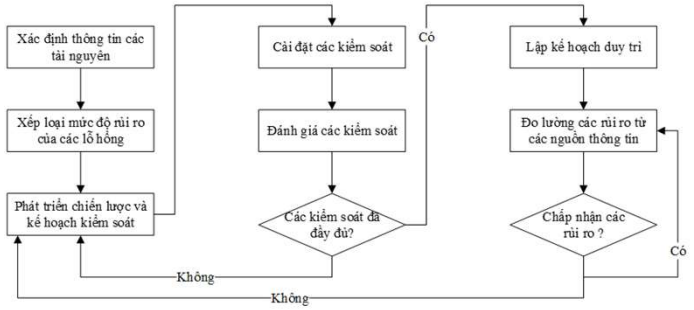
2.3.2. Nội dung phân tích, đánh giá các nguy cơ



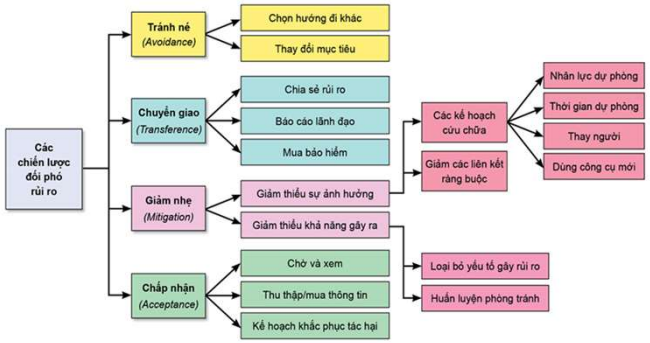
2.4. KIỂM SOÁT ATBMTT

- 2.4.1. Quy trình kiểm soát
- 2.4.2. Chiến lược kiểm soát

2.4.1. Quy trình kiểm soát



2.4.2. Chiến lược kiểm soát



Câu hỏi ôn tập chương 2

1. Trình bày khái niệm về rủi ro? Quản trị rủi ro trong hệ thống thông tin của tổ chức, doanh nghiệp?
2. Vai trò của quản trị rui ro trong hoạt động của các tổ chức, doanh nghiệp?
3. Trình bày quy trình chung trong quản trị rủi ro cho hệ thống thông tin của tổ chức, doanh nghiệp?
4. Mục tiêu của quản trị rủi ro trong quản trị tổ chức, doanh nghiệp? Hãy giải thích.
5. Yêu cầu chung của quy trình quản trị rủi ro trong hệ thống thông tin của tổ chức, doanh nghiệp? Hãy giải thích vì sao cần bảo vệ các tài sản của tổ chức, doanh nghiệp cho đến khi chúng bị loại bỏ khỏi hoạt động của tổ chức?
6. Trình bày các bước thực hiện trong quy trình kiểm soát rủi ro của tổ chức, doanh nghiệp? Cho ví dụ minh họa.
7. Tại sao an toàn và bảo mật thông tin là một bộ phận không thể thiếu được của quy trình quản trị rủi ro trong hệ thống thông tin của tổ chức, doanh nghiệp? Hãy giải thích.
8. Trên thực tế các tổ chức thường gặp những rủi ro gì khi hoạt động? Lấy ví dụ minh họa.

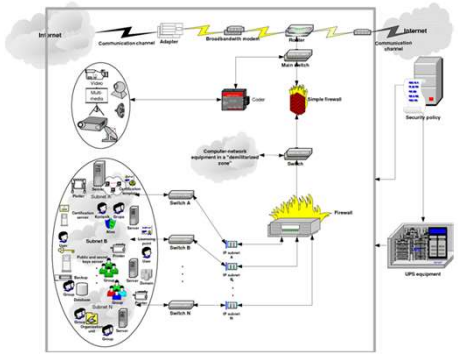
Chương 3. Các kiểu tấn công và các mối đe dọa đối với ATBMTT

3.1. CÁC MỐI ĐE DỌA (THREATS)

- 3.1.1. Mối đe dọa từ các thiết bị phần cứng
- 3.1.2. Mối đe dọa từ các phần mềm
- 3.1.3. Mối đe dọa từ con người

3.1.1. Mối đe dọa từ các thiết bị phần cứng

- Các máy tính
- Các thiết bị truyền thông
- Các thiết bị công nghệ
- Các thiết bị lưu trữ
- Các thiết bị nội thất, các hệ thống đánh giá, v.v...
- Các loại thẻ thanh toán, các loại cổ phiếu, thẻ ghi nợ, dữ liệu cá nhân lưu trữ trên giấy, điện thoại cá nhân, v.v...

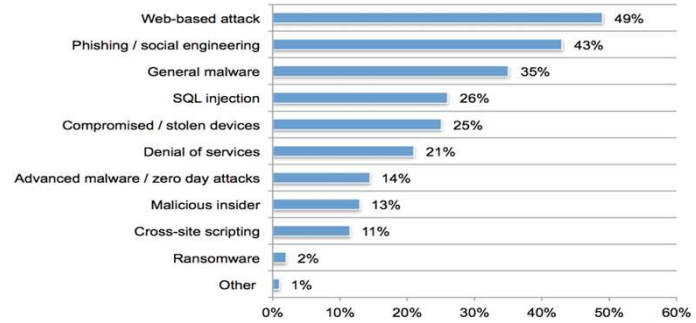


3.1.2. Mối đe dọa từ các phần mềm

- Hỏng hóc
- Virus
- Worm
- Trojan
- Malware
- …

3.1.2. Mối đe dọa từ các phần mềm

Figure 2. What types of attacks did your business experience?
More than one choice permitted



3.1.3. Mối đe dọa từ con người

- Các mối đe dọa ngẫu nhiên do con người gây ra
  - Đánh mất các thiết bị phần cứng (điện thoại, máy tính xách tay, v.v…),
  - Tiết lộ thông tin,
  - Làm hỏng hóc dữ liệu, các lỗi và thiếu sót của người dùng, v.v…
- Các mối đe dọa có chủ ý do con người gây ra
  - Cố ý gian lận và đánh cắp thông tin (Fraud and Theft),
  - Cố ý lây lan mã độc và các chương trình độc hại, gây ra các cuộc tấn công như tấn công từ chối dịch vụ (Denial-of-Service Attacks)
  - Cố ý sử dụng các kỹ thuật xã hội khác (Social Engineering) để tấn công

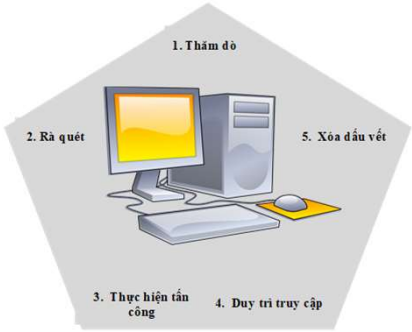
3.1.3. Mối đe dọa từ con người

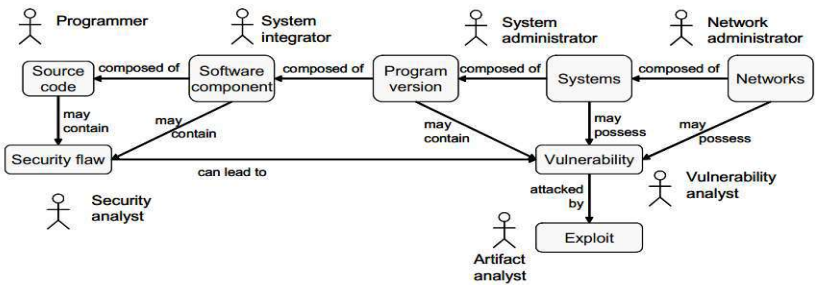
3.2. CÁC KIỂU TẤN CÔNG GÂY MẤT ATBMTT

- 3.2.1. Kịch bản của một cuộc tấn công
- 3.2.2. Tấn công thụ động
- 3.2.3. Tấn công chủ động
- 3.2.4. Tấn công từ chối dịch vụ
- 3.2.5. Một số kiểu tấn công khác

3.2.1. Kịch bản của một cuộc tấn công

- **Bước 1:** Chuẩn bị tấn công sẽ thực hiện các thao tác thăm dò và đánh giá mục tiêu
- **Bước 2:** Thực hiện quét, rà soát mục tiêu
- **Bước 3:** Thực thi tấn công
- **Bước 4:** Duy trì truy cập
- **Bước 5:** Xóa dấu vết





- Source code: mã nguồn
- Software component: thành phần phần mềm
- Program version: phiên bản chương trình
- Systems: các hệ thống
- Networks: các mạng
- Security flaw: khiếm khuyết an ninh
- Vulnerability: lỗ hổng an ninh
- Exploit: khai thác lỗ hổng an ninh

- Programmer: lập trình viên
- System integrator: nhân viên tích hợp hệ thống
- System administrator: nhân viên quản trị hệ thống
- Network administrator: nhân viên quản trị mạng
- Security analyst: nhân viên phân tích an ninh
- Vulnerability analyst: nhân viên phân tích lỗ hổng an ninh
- Artifact analyst: nhân viên phân tích hiện vật.

7 bước cơ bản của một cuộc tấn công hiện nay

Top 10 Black-Hat Hackers in the World

https://www.technotification.com/2014/12/top-10-best-black-hat-hackers-in-the-world.html

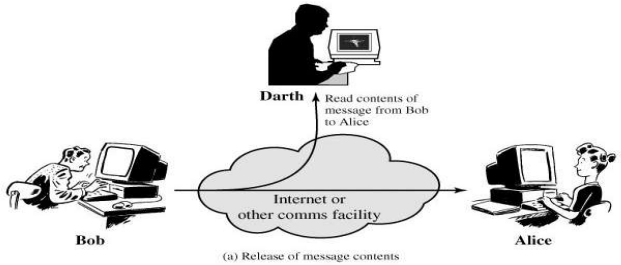
https://www.wondershare.com/top-10-black-hat-hackers/

3.2.2. Tấn công thụ động

- Khái niệm
- Đặc điểm
- Các phương thức thực hiện
- Ngăn chặn
- Môi trường

- Tấn công thụ động (Passive Attack) là kiểu tấn công mà đối tượng bị tấn công không biết mình đang bị tấn công, chúng không tác động trực tiếp đến hệ thống thông tin hay mục tiêu tấn công mà chỉ nghe, xem, đọc nội dung mà không làm thay đổi nội dung thông điệp.

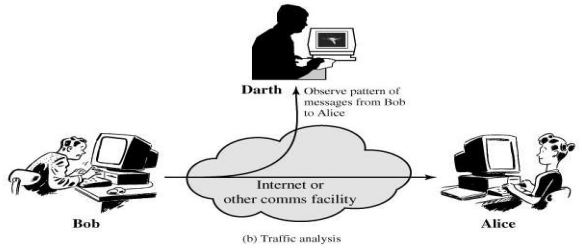
3.2.2. Tấn công thụ động



Nghe trộm đường truyền

Dữ liệu truyền từ Bob -> Alice , Darth nghe trộm được nhưng không thay đổi dữ liệu

3.2.2. Tấn công thụ động



Phân tích lưu lượng

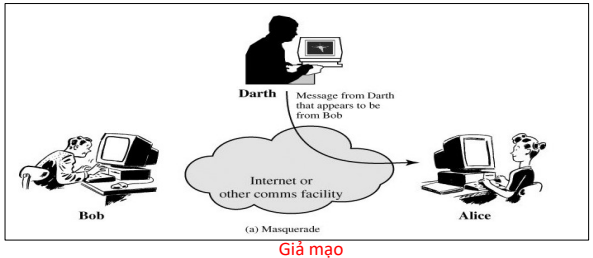
Dữ liệu truyền từ Bob -> Alice (Dữ liệu đã mã hóa), Darth lấy được dữ liệu nhưng không hiểu -> phân tích luồng thông tin để phán đoán

3.2.3. Tấn công chủ động

- Khái niệm
- Đặc điểm
- Các phương thức thực hiện
- Ngăn chặn
- Môi trường

- Tấn công chủ động là loại hình tấn công có chủ ý, có sự tác động trực tiếp lên nội dung của thông điệp bao gồm cả việc sửa đổi dữ liệu trong khi truyền từ người nhận đến người gửi.

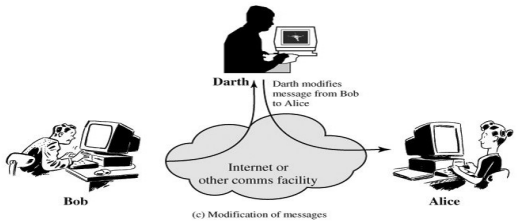
3.2.3. Tấn công chủ động



Giả mạo

Darth giả mạo thông điệp của Bob rồi gửi cho Alice, Chỉ áp dụng với mạng bảo mật kém, không có mã hóa hay xác thực

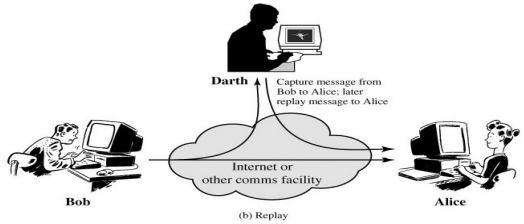
3.2.3. Tấn công chủ động



Thay đổi thông điệp

Thông điệp từ Bob bị Darth chặn lại, sửa đổi rồi mới gửi lại cho Alice => Alice không biết thông điệp đã bị sửa đổi

3.2.3. Tấn công chủ động



Tấn công làm trễ

Darth lấy được 1 gói tin từ Bob, đợi 1 thời gian nào đó rồi gửi lại cho Alice

3.2.3. Tấn công chủ động

- Một số công cụ và kỹ thuật hỗ trợ tấn công:
  - Công cụ quét lỗ hổng (Vulnerability scanners)
  - Công cụ quét cổng dịch vụ (Port scanners)
  - Công cụ nghe lén (Sniffers)
  - Công cụ ghi phím gõ (Keyloggers)

3.2.4. Tấn công từ chối dịch vụ

- Khái niệm
- Đặc điểm
- Phân loại
- Phòng tránh
- Khắc phục

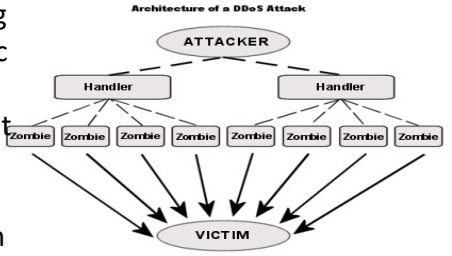
- Tấn công từ chối dịch vụ (Denial of Service- DoS) là tên gọi chung của kiểu tấn công làm cho một hệ thống nào đó bị quá tải dẫn tới không thể cung cấp dịch vụ, hoặc phải ngưng hoạt động

DoS

- Hàng loạt Client gửi request đến Server
- Server không reply được do nghẽn đường truyền
- => DoS cổ điển

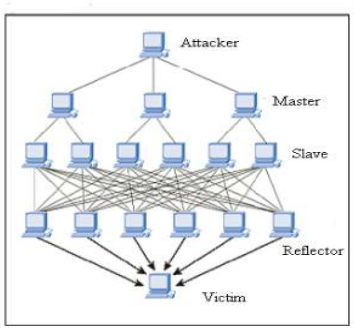
DDoS

- Kẻ tấn công tìm cách chiếm dụng và điều khiển nhiều máy tính hoặc mạng máy tính trung gian
⇒Từ nhiều nơi đồng loạt gửi ào ạt các gói tin với số lượng rất lớn
⇒ Mục đích chiếm dụng tài nguyên, làm quá tải đường truyền của một mục tiêu xác định nào đó.

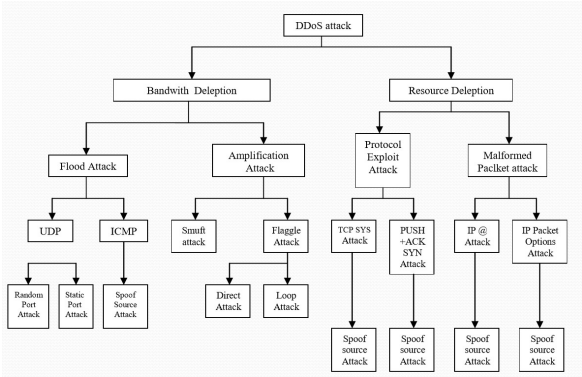


RDoS

- Attacker => chiếm quyền điều khiển các Master
- Các Master => chiếm quyền điều khiển các Slave => các Master sẽ yêu cầu Slave gửi các gói tin => các Reflector
- Các gói tin không có địa chỉ máy gửi chỉ có địa chỉ máy nhận.
- Reflector nhận các gói tin => trả lời theo địa chỉ trong gói tin => vô tình trở thành kẻ trung gian tiếp tay => tấn công từ chối dịch vụ vào Victim



Tóm tắt các kiểu DDoS



3.2.5. Một số kiểu tấn công khác

- Tấn công bằng mã độc
- Tấn công vào các loại mật khẩu
- Tấn công từ chối dịch vụ
- Tấn công giả mạo địa chỉ, nghe trộm
- Tấn công kiểu phát lại và người đứng giữa
- Tấn công bằng bom thư và thư rác
- Tấn công sử dụng cửa hậu Trojan
- Tấn công kiểu Social Engineering
- Tấn công phising, pharming

CYBER ATTACK TRENDS 2020

Cybersecurity Trends Table of Contents

1. User Awareness
2. Attacks on the Healthcare Sector
3. Machine Learning
4. Geo-Targeted Phishing Threats
5. Cloud Security
6. GDPR Compliance
7. Threats to Higher Education
8. Vulnerability of IoT
9. Mobile Devices as Attack Vectors
10. Financial Services Cyberattacks

1 Leading cyberthreats targeting organizations (scale 1 to 5)

Source: Imperva

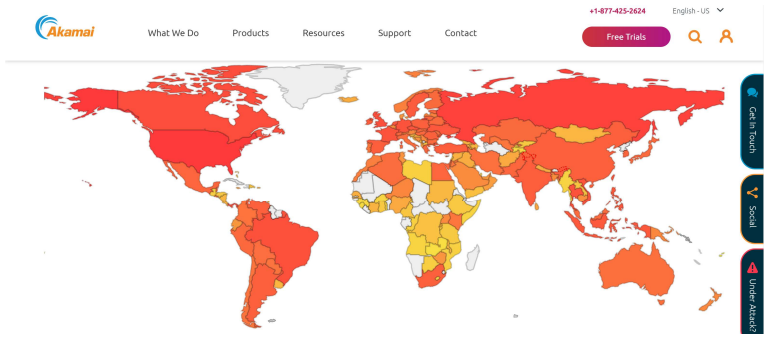
malware (viruses, worms, trojans)	3.74
phishing/spear-phishing attacks	3.71
ransomware	3.68
account takeover / credential abuse attacks	3.68
denial of service (DoS / DDoS) attacks	3.63
web application attacks (buffer overflows, SQL injection, cross-site scripting)	3.62
SSL-encrypted threats	3.61
advanced persistent threats (APTs) / targeted attacks	3.61
insider threats / data alteration by employees	3.60
zero-day attacks (against publicly unknown vulnerabilities)	3.60

2 Leading organizations impersonated by phishers worldwide

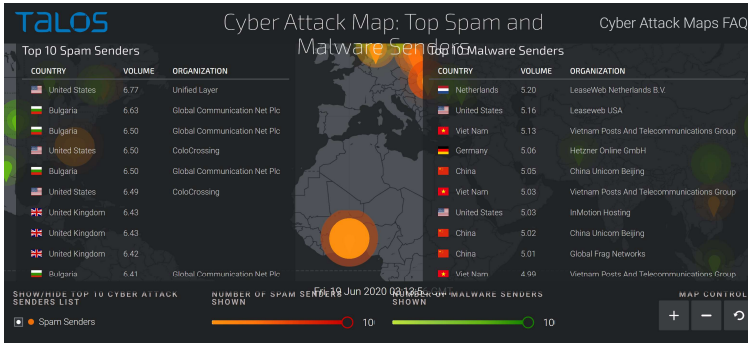
Source: Statista

13%	11%	10%	10%	6%
Microsoft	Google	Facebook	Apple	PayPal

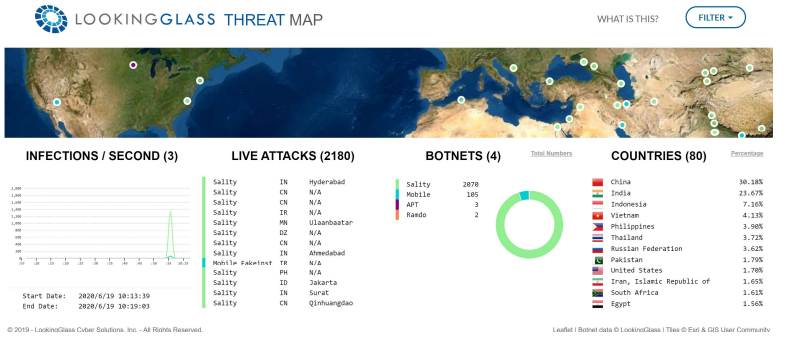
Bản đồ lây nhiễm mã độc và virus trên thế giới quý II/2020



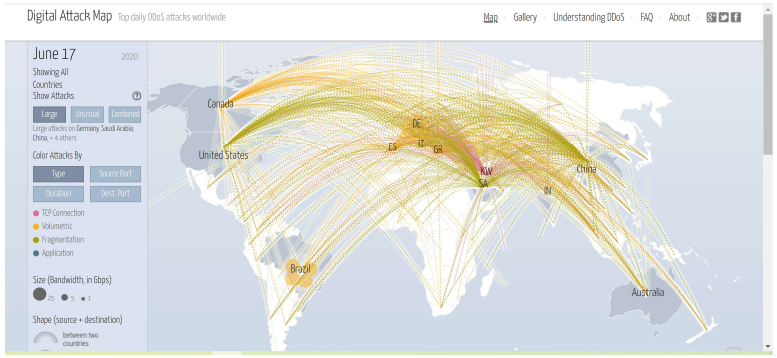
https://talosintelligence.com/



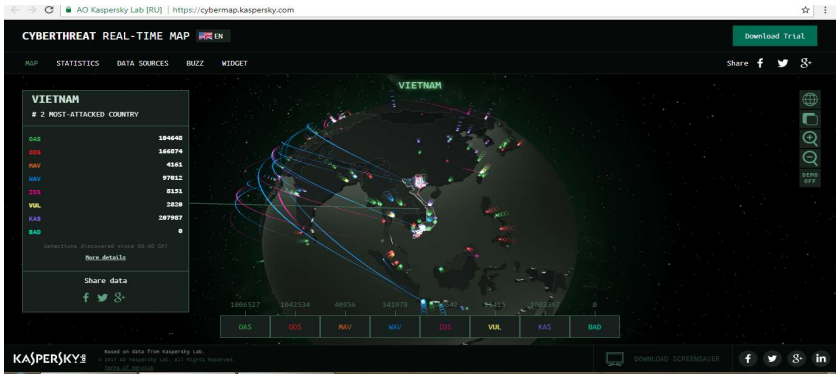
https://map.lookingglasscyber.com/



https://www.digitalattackmap.com/



Map of Kasper



Câu hỏi ôn tập chương 3

1. Tấn công là gì? Trình bày kịch bản của một cuộc tấn công thông thường?
2. Có những kiểu phân loại hình thức tấn công như thế nào?
3. Mối đe dọa là gì? Phân loại và giải thích các mối đe dọa gây mất an toàn thông tin trong hệ thống thông tin của tổ chức doanh nghiệp?
4. Trình bày khái niệm, đặc điểm và lấy ví dụ minh họa về tấn công thụ động
5. Trình bày khái niệm, đặc điểm và lấy ví dụ minh họa về tấn công chủ động
6. Tấn công từ chối dịch vụ là gì? Trình bày và phân loại các kiểu tấn công từ chối dịch vụ hiện nay?
7. Tấn công thăm dò thường được thực hiện khi nào? Vì sao hiện nay lại phổ biến? Hãy giải thích
8. Tấn công truy cập là gì? Vì sao hệ thống mạng doanh nghiệp và mạng Internet phát triển thì tấn công truy cập càng tăng nhanh? Hãy giải thích.

Chương 4. MÃ HÓA THÔNG TIN

- 4.1. TỔNG QUAN VỀ MÃ HÓA
  - 4.1.1. Khái niệm hệ mã hóa
  - 4.1.2. Vài nét về lịch sử mã hóa
  - 4.1.3. Vai trò của mã hóa và quy trình mã hóa
  - 4.1.4. Các yêu cầu của hệ mã hóa
  - 4.1.5. Các kỹ thuật phá mã phổ biến
- 4.2. HỆ MÃ HÓA ĐỐI XỨNG
  - 4.2.1. Khái niệm về hệ mã hóa đối xứng
  - 4.2.2. Ưu điểm và nhược điểm của hệ mã hóa đối xứng
  - 4.2.3. Hệ mã hóa đối xứng cổ điển
  - 4.2.4. Hệ mã hóa đối xứng hiện đại
- 4.3. HỆ MÃ HÓA KHÔNG ĐỐI XỨNG
  - 4.3.1. Khái niệm về hệ mã hóa không đối xứng
  - 4.3.2. Ưu điểm và nhược điểm của hệ mã hóa không đối xứng
  - 4.3.3. Hệ mã hóa RSA
  - 4.3.4. Một số hệ mã hóa khóa công khai khác
- CÂU HỎI ÔN TẬP VÀ BÀI TẬP CHƯƠNG 4

4.1. TỔNG QUAN VỀ MÃ HÓA

- 4.1.1. Khái niệm hệ mã hóa
- 4.1.2. Vài nét về lịch sử mã hóa
- 4.1.3. Vai trò của mã hóa và quy trình mã hóa
- 4.1.4. Các yêu cầu của hệ mã hóa
- 4.1.5. Các kỹ thuật phá mã phổ biến

4.1.1. Khái niệm hệ mã hóa

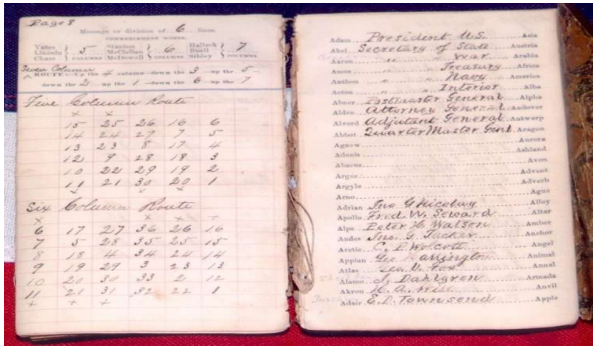
- Khái niệm mã hóa
- Mục đích của việc mã hóa
- Quy trình mã hóa
- Ứng dụng của mã hóa

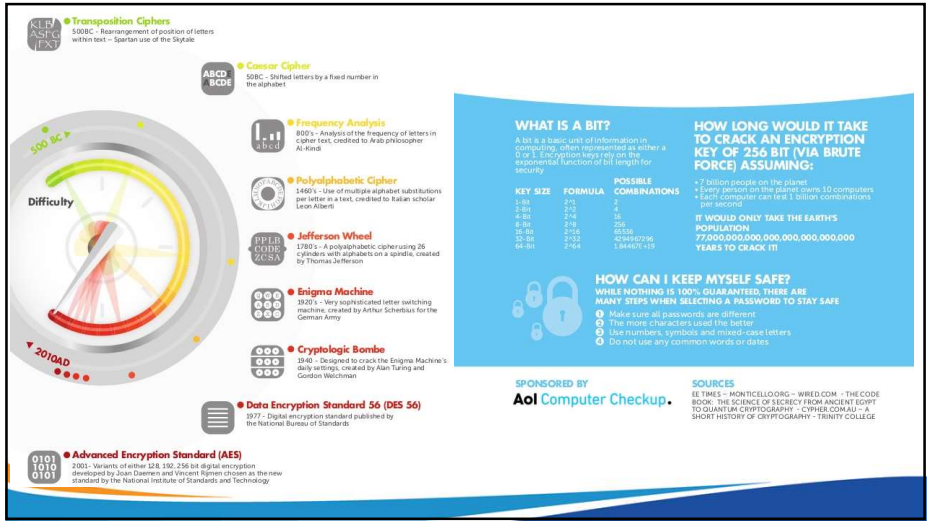
Mã hóa và giải mã

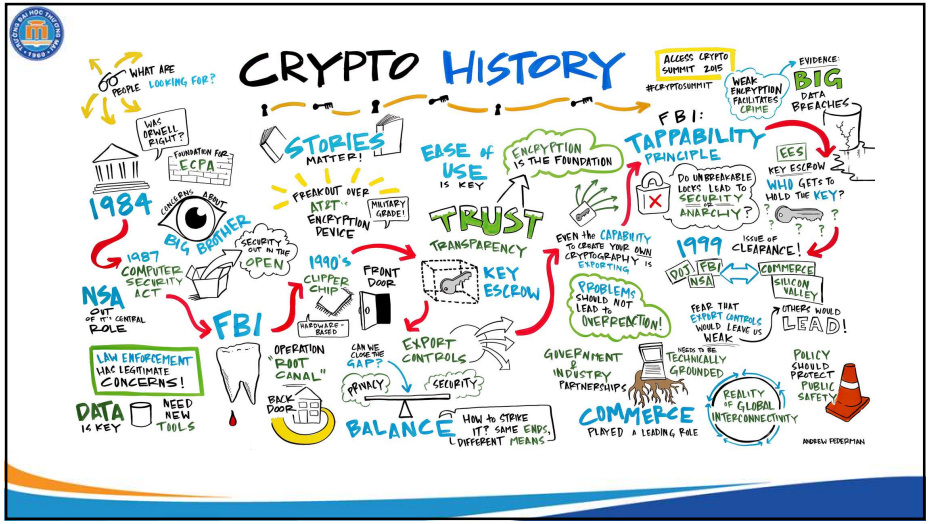
4.1.1. Khái niệm hệ mã hóa

- Mã hóa
  - Phương thức biến đổi thông tin từ định dạng thông thường (văn bản, hình ảnh, …) thành một định dạng khác không giống như ban đầu nhưng có thể khôi phục lại được, (việc khôi phục này gọi là giải mã).
- Mục đích
  - Đảm bảo tính bí mật của thông tin khi chúng được truyền trong những môi trường không đảm bảo an toàn

4.1.2. Vài nét về lịch sử mã hóa







Các thuật ngữ

- Plaintext: Bản rõ, bản gốc, nội dung thông điệp gốc
- Ciphertext: Bản mã, bản mật, bản kết quả sau khi mã hóa
- Encryption: Mật mã hóa, mã hóa, quá trình chuyển bản rõ thành bản mã
- Decryption: Giải mã, quá trình biến đổi bản mã thành bản rõ
- Cryptosystem: Hệ mã, hệ mã hóa
- Cryptanalysis: Phá mã, quá trình cố gắng chuyển đổi bản mật thành bản rõ mà không có khóa
- Không gian khóa (Keyspace) : tổng số khóa có thể có của một hệ mã hóa
- Hàm băm (Hash function)

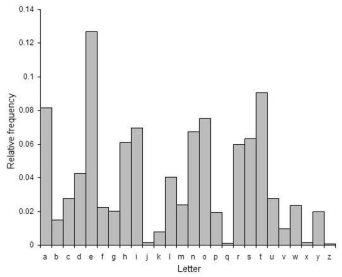
4.1.4. Các yêu cầu của hệ mã hóa

- Yêu cầu với hệ mã hóa
  - (1) Tính hỗn loạn (Confusion):
  - (2) Tính khuếch tán (Diffusion):
  - Nguyên lý Kerckhoff:
    - *"Tính an toàn của một hệ mã hoá không nên phục thuộc vào việc giữ bí mật giải thuật mã hoá, mã chỉ nên phục thuộc vào việc giữ bí mật khoá mã".*
- Độ an toàn của hệ mã hóa
  - An toàn vô điều kiện
  - An toàn tính toán
  - Thực tế thỏa mãn hai điều kiện
    - Không có nhược điểm
    - Khóa có quá nhiều giá trị không thể thử hết được

4.1.5. Các kỹ thuật phá mã phổ biến

- Phá mã là gì?
- Các biện pháp phá mã phổ biến
  - Vét cạn
    - Thử tất cả các khả năng có thể có của khóa
  - Thám mã
    - Dựa trên các lỗ hổng và điểm yếu của giải thuật mã hóa

Cracking Caesar-cipher



So this is the relative frequency distribution of letters in an english text

Frequency analysis cracking:

1.) calculate the relative frequency distribution of the ciphertext's letters

2.) get the most frequent letter in the ciphertext (or the second because the most frequent one may be white-spaces)

3.) we can get the key based on a simple formula

key = value of ciphertext's most frequent letter – value of E

Vigenere cipher cracking

plain text: help me i am under attack! these weasels won't stop biting me!!!
password: keykeykeykeykeykeykeykeykeykeykeykeykeykeykeykeykeykeykeykeykeyke
cipher: riJz[Ko[GieK;yLniP;eRDeAu%h;xFowC;ACkwCvwhGsL?xhCxMz[zsxGxkhwik=%

group 1 group 2 group 3

Let's call these three groups **group 1, 2, and 3**.

group 1: "rzo;;n;Du;o;kvG?Czsxw="

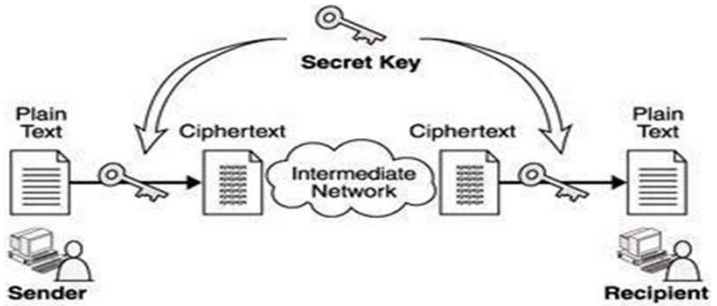
We know all letters in this group were encoded with the same rotation amount.

Can we do a brute force attack to decode *only* group 1?

4.2. HỆ MÃ HÓA ĐỐI XỨNG

- 4.2.1. Khái niệm về hệ mã hóa đối xứng
- 4.2.2. Ưu điểm và nhược điểm của hệ mã hóa đối xứng
- 4.2.3. Hệ mã hóa đối xứng cổ điển
- 4.2.4. Hệ mã hóa đối xứng hiện đại

4.2.1. Khái niệm về hệ mã hóa đối xứng



4.2.2. Ưu điểm và nhược điểm của hệ mã hóa đối xứng

- *Ưu điểm*
  - Mô hình khá đơn giản.
  - Dễ dàng tạo ra được một thuật toán mã hóa đối xứng.
  - Đơn giản và rõ ràng của mình, dễ cài đặt và hoạt động hiệu quả.
- *Nhược điểm*
  - Dùng chung khóa
  - Việc bảo mật và phân phối khóa là công việc khó khăn, phức tạp
  - Dễ bị bẻ khóa

4.2.3. Hệ mã hóa đối xứng cổ điển

- Mã hóa thay thế
- Mã hóa dịch chuyển
  - Ceasar
  - Nhân
  - Vigenere
  - Tự động
- Mã hóa hoán vị
  - Hàng rào
  - Hàng
- Mã hóa khối

4.2.3. Hệ mã hóa đối xứng cổ điển

- **Mã hóa thay thế**
- Ví dụ:
  - Bản chữ cái tiếng Anh,
  - Bản mã nhị phân,
  - Bản ký tự số, …

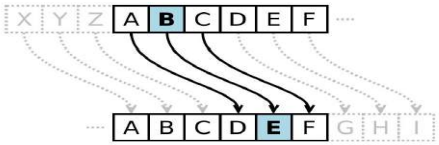
Với bảng chữ cái tiếng Anh:

Ký tự cần mã	a	b	c	d	…….	x	y	z
Ký tự thay thế	F	G	N	T	…….	K	P	L

Với thuật toán mã hoá này, ta có:
Văn bản gốc: a Bad day
Văn bản sau khi mã hóa: F GFT TFP

4.2.3. Hệ mã hóa đối xứng cổ điển

- **Mã hóa Ceasar**
  - Nguyên tắc: Dịch chuyển xoay vòng theo thứ tự chữ cái
  - Khóa k gọi là bước dịch chuyển
  - Với mỗi chữ cái của văn bản
  - Đặt p = 0 nếu chữ cái là a, p = 1 nếu chữ cái là b,...
  - Mã hóa : C = E(p) = (p + k) mod 26



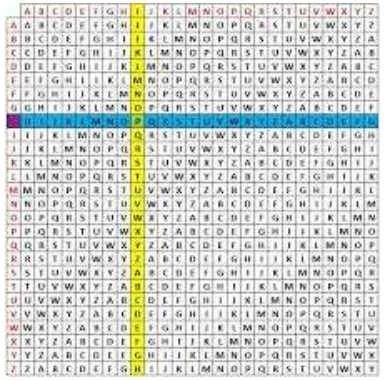
4.2.3. Hệ mã hóa đối xứng cổ điển

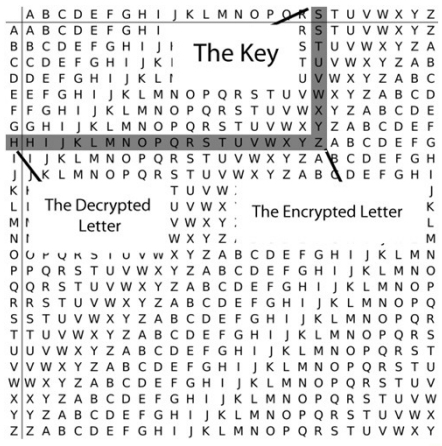
- **Mã hóa nhân**
  - Nguyên tắc: Dịch chuyển xoay vòng theo thứ tự chữ cái
  - Khóa k gọi là bước dịch chuyển
  - Với mỗi chữ cái của văn bản
  - Đặt p = 0 nếu chữ cái là a, p = 1 nếu chữ cái là b,...
  - Mã hóa : C = E(p) = (p*k) mod 26

4.2.3. Hệ mã hóa đối xứng cổ điển

- **Mã hóa Vigenère**
  - Nguyên tắc: Dịch chuyển xoay vòng theo thứ tự chữ cái
  - Khóa D= $k_1k_2...k_d$ là khóa của hệ mã hóa
  - Với mỗi chữ cái của văn bản
  - Đặt p = 0 nếu chữ cái là a, p = 1 nếu chữ cái là b,...
  - Mã hóa : C = E(p) = (p + i) mod 26 với i là kí tự thứ i trong khóa D
- Nguyên tắc mã hóa/ giải mã
  - Các ký tự bản rõ viết thành các cột
  - Các ký tự khóa viết thành các hàng
  - Bản mã là các ký tự nằm giao của hàng và cột

Hình vuông Vigenere





Thứ tự các kí tự trong bảng chữ cái

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

4.2.3. Hệ mã hóa đối xứng cổ điển

- **Mã hóa khóa tự động**
  - Cải tiến từ Vigenère
  - Gắn khóa D vào đầu nguyên bản tạo D'
  - Mã hóa theo Vigenère dựa trên khóa D'

4.2.3. Hệ mã hóa đối xứng cổ điển

- **Mã hóa hoán vị hàng rào (Row fence)**
- Nguyên tắc:
  - Viết các kí tự trong nguyên bản P theo đường chéo trên k hàng
  - Viết lại các kí tự trên từng hàng một để được bản mã
  - Ví dụ:
    - Nguyên bản : ATTACK AT MIDNIGHT
    - Mã hóa với độ cao hàng rào là k= 2
      - A T C A M D I H
      - T A K T I N G T
    - Bản mã : ATCAMDIHTAKTINGT
    - Giải mã: ATCAMDIH/TAKTINGT

4.2.3. Hệ mã hóa đối xứng cổ điển

- **Mã hóa hoán vị hàng (Column fence)**
- Nguyên tắc:
  - Viết các kí tự trong nguyên bản P theo hàng ngang trên k cột, k là khóa
  - Viết lại các kí tự trên từng cột theo thứ tự xuất hiện trong khóa k

Nguyên bản: ATTACK POSTPONED UNTIL TWO AM

Khóa K= 4 3 1 2 5 6 7

- **4 3 1 2 5 6 7**
- a t t a c k p
- o s t p o n e
- d u n t i l t
- w o a m x y z
- Bản mã : TTNAAPTMTSUOAODWCOIXKNLYPETZ
- Giải mã: TTNA/APTM/TSUO/AODW/COIX/KNLY/PETZ

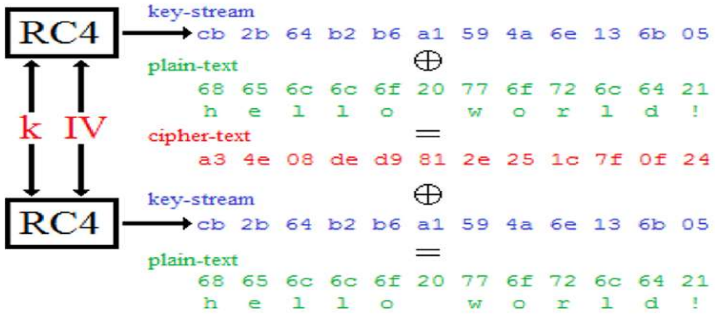
4.2.3. Hệ mã hóa đối xứng cổ điển

- **Mã hóa tích hợp**
  - Các hệ mã hóa thay thế và hoán vị không an toàn vì những đặc điểm của ngôn ngữ
  - Kết hợp sử dụng nhiều hệ mã hóa sẽ khiến việc phá mã khó hơn
  - Là cầu nối từ các hệ mã hóa cổ điển đến các hệ mã hóa hiện đại

4.2.4. Hệ mã hóa đối xứng hiện đại

- Chia thành 2 nhóm
  - Mã hóa luồng (stream ciphers): Tiny RC4, RC4, …
  - Mã hóa khối (block ciphers): DES, AES, Triple DES

4.2.4. Hệ mã hóa đối xứng hiện đại



4.2.4. Hệ mã hóa đối xứng hiện đại

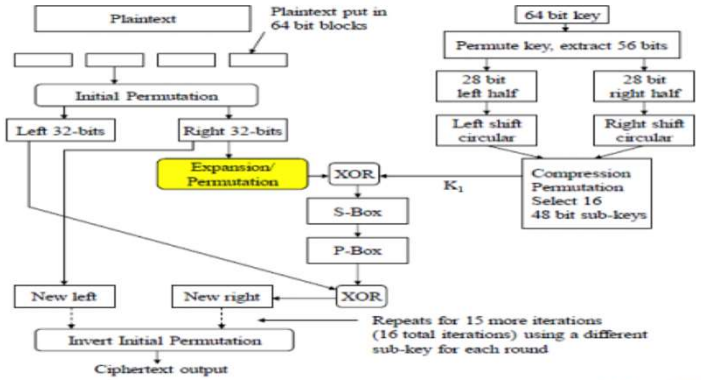
- Mã hóa khối
  - Mã hóa các khối kí tự
  - Chia theo cơ chế lấy lũy thừa của 2
  - Độ dài của khối là độ dài của đơn vị mã hóa
  - Kích thước khóa là độ dài của chuỗi dùng để mã hóa

4.2.4. Hệ mã hóa đối xứng hiện đại

Khóa	000	001	010	011	100	101	110	111
0	001	111	110	000	100	010	101	011
1	001	110	111	100	011	010	000	101
2	001	000	100	101	110	111	010	011
3	100	101	110	111	000	001	010	011
4	101	110	100	010	011	001	011	111

- Chuỗi plaintext: 010 100 110 111
=> Sử dụng khóa 1 ta được → 111 011 000 101
=> Sử dụng khóa 4 ta đươc → 100 011 011 111

4.2.4. Hệ mã hóa đối xứng hiện đại



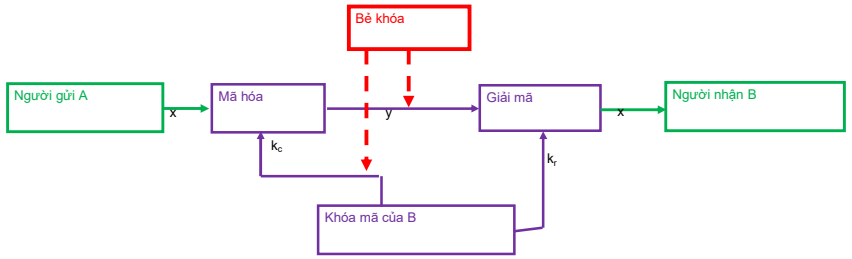
4.3. HỆ MÃ HÓA KHÔNG ĐỐI XỨNG

- 4.3.1. Khái niệm về hệ mã hóa không đối xứng
- 4.3.2. Ưu điểm và nhược điểm của hệ mã hóa không đối xứng
- 4.3.3. Hệ mã hóa RSA
- 4.3.4. Một số hệ mã hóa khóa công khai khác

4.3.1. Khái niệm về hệ mã hóa không đối xứng

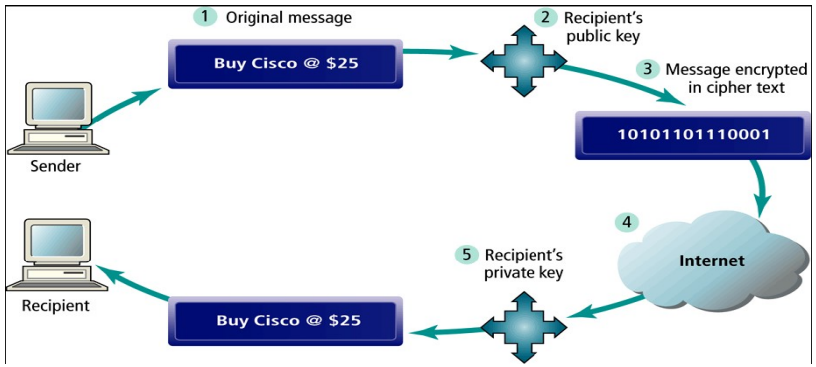
- Mã hóa khóa công khai là một dạng mã hóa cho phép người sử dụng trao đổi các thông tin mật mà không cần phải trao đổi các khóa bí mật trước đó, điều này được thực hiện bằng cách sử dụng một cặp khóa có quan hệ toán học với nhau là khóa công khai (Public key) và khóa riêng (Private key) hay khóa bí mật (Secret key).

4.3.1. Khái niệm về hệ mã hóa không đối xứng



- B sinh cặp khóa : Khóa công khai Kc và khóa bí mật Kr
- B gửi Kc cho A và ai cũng có thể biết
- A dùng Kc mã hóa thông điệp và gửi lại cho B
- B dùng Kr để giải mã thông điệp của A

4.3.1. Khái niệm về hệ mã hóa không đối xứng

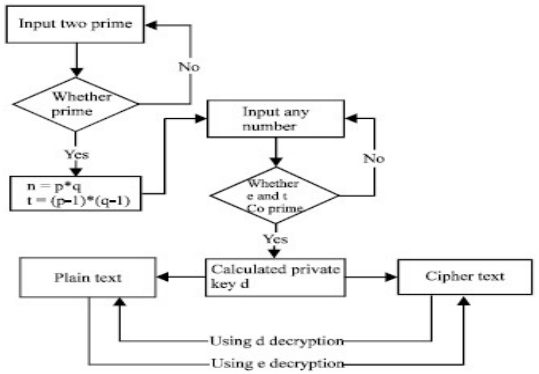


4.3.2. Ưu điểm và nhược điểm của hệ mã hóa không đối xứng

- **Ưu điểm của hệ thống mã hóa khóa công khai**
  - Đơn giản trong việc lưu chuyển khóa
  - Mỗi người chỉ cần một cặp khóa công khai – khóa bí mật là có thể trao đổi thông tin với tất cả mọi người,
  - Là tiền đề cho sự ra đời của chữ ký số và các phương pháp chứng thực số
- **Hạn chế của hệ mã hóa khóa công khai**
  - Tốc độ xử lý tốn nhiều thời gian
  - Cơ chế xác thực cần nhiều không gian trống.

4.3.3. Hệ mã hóa RSA

- Sinh khóa
- Mã hóa
- Giải mã



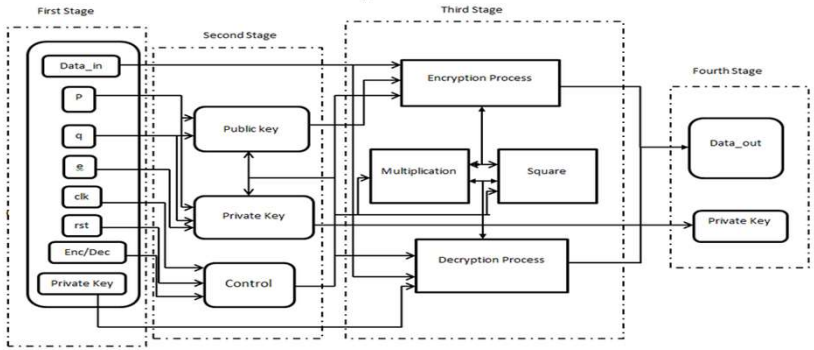
4.3.3. Hệ mã hóa RSA

- Thủ tục sinh khóa RSA:
  - Tạo 2 số nguyên tố p và q;
  - Tính n = p x q
  - Tính $\Phi(n) = (p-1) \times (q-1)$
  - Chọn số e sao cho $0 < e < \Phi(n)$ và $\gcd(e, \Phi(n)) = 1$
  - Chọn số d sao cho $d \equiv e^{-1} \bmod \Phi(n)$,
    hoặc $(d \times e) \bmod \Phi(n) = 1$
    (d là molulo nghịch đảo của e)
- Ta có (n, e) là khóa công khai, (n, d) là khóa riêng.

4.3.3. Hệ mã hóa RSA

- Thủ tục mã hóa RSA:
  - Thông điệp m đã được chuyển thành số, m<n
  - Bản mã $c = m^e \bmod n$
- Thủ tục giải mã RSA:
  - Bản mã c, c<n
  - Bản rõ $m = c^d \bmod n$

4.3.3. Hệ mã hóa RSA



4.3.3. Hệ mã hóa RSA

- Chọn 2 số ngtố: p = 17 ; q = 11
- Tính n = pq = $17 \times 11 = 187$
- Tính $\Phi(n) = (p-1)(q-1) = 16 \times 10 = 160$
- Chọn e : $\gcd(e, 160) = 1$ và $1 < e < 160$; lấy e = 7
- Xác định d: $de \equiv 1 \bmod 160$ và $d \leq 187$
- Giá trị d = 23 vì $23 \times 7 = 161 = 1 \times 160 + 1$
- Công bố khóa công khai KC = {7, 187}
- Giữ bí mật khóa riêng KR = {23, 187}
- Hủy bỏ các giá trị bí mật p = 17 và q = 11

4.3.4. Một số hệ mã hóa khóa công khai khác

- Hệ mật mã ElGamal là một thuật toán được xây dựng trên bài toán logarit rời rạc
- Mật mã xếp ba lô Merkle-Hellman do Ralph Merkle và Martin Hellman phát minh vào năm 1978 khá giống RSA

Câu hỏi ôn tập chương 4

- 1. Thế nào là mã hóa? Thế nào là giải mã ? Hãy nêu sự khác biệt giữa quá trình giải mã và phá mã một bản mã ?
- 2. Vì sao mã hóa được lựa chọn là biện pháp bảo vệ sâu nhất trong mô hình bảo mật nhiều lớp?
- 3. Trình bày và phân tích vai trò của mã hóa trong các hoạt động của tổ chức, doanh nghiệp?
- 4. Trình bày và phân tích các yêu cầu của một hệ mã hóa? Một hệ mã hóa đạt được những yêu cầu gì thì được coi là an toàn?
- 5. Trình bày các biện pháp phá mã phổ biến? Các thuật toán mã hóa đạt được điều kiện gì thì không thể phá mã ?
- 6. Trình bày mô hình mã hóa đối xứng?
- 7. Trình bày mô hình mã hóa không đối xứng?
- 8. So sánh hệ mã hóa đối xứng và hệ mã hóa không đối xứng?

Chương 5. Sao lưu dữ liệu và phục hồi thông tin

- 5.1. TỔNG QUAN VỀ SAO LƯU VÀ PHỤC HỒI THÔNG TIN
  - 5.1.1 Xác định và tổ chức dữ liệu của tổ chức
  - 5.1.2. Xác định các thiết bị lưu trữ trong tổ chức, doanh nghiệp
- 5.2. SAO LƯU DỰ PHÒNG DỮ LIỆU
  - 5.2.1. Khái niệm về sao lưu dự phòng
  - 5.2.2. Các cơ chế sao lưu và phân loại
  - 5.2.3. Một số công cụ sao lưu dự phòng
- 5.3. PHỤC HỒI SAU SỰ CỐ
  - 5.3.1. Dữ liệu bị hỏng hóc và việc khôi phục dữ liệu
  - 5.3.2. Phục hồi bằng phần mềm
- CÂU HỎI ÔN TẬP CHƯƠNG 5

5.1. TỔNG QUAN VỀ SAO LƯU VÀ PHỤC HỒI THÔNG TIN

- 5.1.1 Xác định và tổ chức dữ liệu của tổ chức
- 5.1.2. Xác định các thiết bị lưu trữ trong tổ chức, doanh nghiệp

5.1.1 Xác định và tổ chức dữ liệu của tổ chức

- Trả lời các câu hỏi:
  - Những thông tin hay dữ liệu nào cần sao lưu?
  - Cần sao lưu vào đâu?
  - Các biện pháp sao lưu nào cần thực hiện?
  - Sao lưu bao nhiêu lần trong một ngày thì phù hợp? Một tuần? Một tháng? Một quý? Một năm? …

5.1.1 Xác định và tổ chức dữ liệu của tổ chức

Phân loại thông tin và nơi lưu trữ

Kiểu dữ liệu	Bản sao chủ/ bản sao lại	Thiết bị lưu trữ	Vị trí
Tài liệu điện tử	Bản chính	Ổ cứng máy tính	Văn phòng
Một ít tài liệu điện tử	Bản sao lại	Thẻ nhớ USB	Mang theo người
Chương trình cơ sở dữ liệu (ảnh, liên lạc, lịch, vv)	Bản chính	Ổ cứng máy tính	Văn phòng
Một ít tài liệu điện tử	Bản sao lại	Đĩa CD	Ở nhà
Thư điện tử và địa chỉ liên lạc	Bản chính	Tài khoản Gmail	Internet
Tin nhắn và liên lạc điện thoại	Bản chính	Máy điện thoại	Mang theo người
Tài liệu văn bản giấy (hợp đồng, hóa đơn, vv.)	Bản chính	Trong ngăn kéo	Văn phòng

5.1.2. Xác định các thiết bị lưu trữ trong TC,DN

Phân loại dữ liệu cần lưu trữ

Loại dữ liệu	Bản chính/ Bản sao	Thiết bị lưu trữ	Vị trí
Tài liệu điện tử	Bản chính	Ổ cứng máy tính	Văn phòng
	Bản sao lại	Đĩa CD	Ở nhà
Một số tài liệu điện tử quan trọng	Bản sao lại	Thẻ nhớ USB	Mang theo người
Cơ sở dữ liệu Chương trình	Bản chính	Ổ cứng máy tính	Văn phòng
	Bản sao lại	Đĩa CD	Ở nhà
Thư điện tử và danh sách địa chỉ email	Bản sao lại	Máy chủ Gmail	Internet
	Bản chính	Thunderbird cài đặt trên máy tính	Văn phòng
Tin nhắn và danh sách liên lạc điện thoại	Bản chính	Máy điện thoại	Mang theo người
	Bản sao lại	Ổ cứng máy tính	Văn phòng
	Bản sao lại	SIM card dự phòng	Ở nhà
Tài liệu văn bản trên giấy	Bản chính	Ngăn kéo	Văn phòng
Scanned documents	Bản sao lại	Đĩa CD	Ở nhà

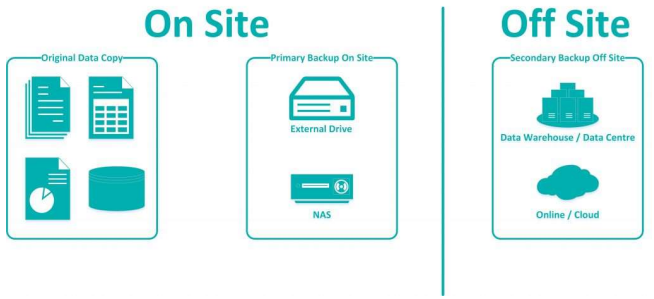
5.2. SAO LƯU DỰ PHÒNG DỮ LIỆU

- 5.2.1. Khái niệm về sao lưu dự phòng
- 5.2.2. Các cơ chế sao lưu và cách phân loại
- 5.2.3. Một số công cụ sao lưu dự phòng của Windows

5.2.1. Khái niệm về sao lưu dự phòng

- Sao lưu và phục hồi là một quá trình tạo và lưu trữ các bản sao của dữ liệu để tránh sự mất mát dữ liệu
- Vì sao cần sao lưu dự phòng?
  - Sao lưu dữ liệu (Data backup) là việc tạo ra các bản sao của dữ liệu gốc, cất giữ ở một nơi an toàn để có thể lấy ra sử dụng (restore) khi hệ thống gặp sự cố.
  - Sao lưu (backup) dữ liệu là cách tốt nhất hiện nay để bảo vệ dữ liệu của hệ thống tránh các sự cố hoặc tránh việc hỏng hóc khi bị tấn công.

5.2.2. Các cơ chế và phân loại



5.2.2. Các cơ chế và phân loại

- **Onsite Backup**
- Là loại hình sao lưu dữ liệu mà bản sao lưu được lưu trong cùng facility (cơ sở hạ tầng lưu trữ) với dữ liệu gốc. Phương pháp cổ điển thường dùng là sử dụng tape.
- Tape backup là kiểu sao lưu định kỳ dữ liệu từ thiết bị chính sang hộp băng
- Ưu điểm:
  - Băng thông dùng để sao lưu lớn nên tốc độ sao lưu, khôi phục nhanh
- Nhược điểm
  - Có thể mất dữ liệu khi có vấn đề xảy ra với facility, hoặc bị hack/chiếm quyền.

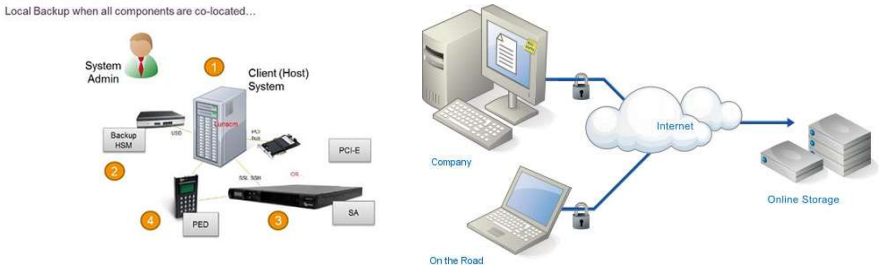
- **Offsite Backup**
- Dữ liệu backup được lưu khác facility với dữ liệu gốc, hoặc ở một nơi khác, hoặc được lưu trữ trên cloud.
- Ưu điểm:
  - Offsite backup có độ an toàn dữ liệu cao.
  - Có thể thuê các hệ thống Cloud để lưu trữ
- Nhược điểm
  - Offsite Backup là tốc độ sao lưu, khôi phục phụ thuộc vào băng thông kết nối giữa hệ thống chính và hệ thống dự phòng.

5.2.2. Các cơ chế và phân loại

- Local Backup:
  - Local Backup là hình thức backup cục bộ. Các này sử dụng các thiết bị nhớ rời như ổ cứng, ổ cứng di động, USB hay thậm chí là đĩa CD và DVD để lưu trữ.
- Ưu điểm:
  - Thực hiện lưu trữ khá nhanh
  - Có thể thực hiện mọi thời điểm
- Nhược điểm;
  - Độ an toàn chưa cao.

- Online Backup
  - Lưu trữ dữ liệu trên Internet bằng cách sử dụng một nhà cung cấp dịch vụ lưu trữ, thay vì lưu trữ dữ liệu cục bộ trên một đĩa vật lý, ổ cứng máy tính.
- Ưu điểm
  - Độ an toàn và tin cậy cao
  - Có thể thực hiện mọi thời điểm, mọi địa điểm từ nhiều thiết bị khác nhau
- Nhược điểm
  - Phụ thuộc vào mạng Internet
  - Phụ thuộc vào đường truyền, kết nối

5.2.3. Các cơ chế và phân loại



5.3. Phục hồi và phân loại

- Phục hồi
  - Phục hồi là công đoạn đưa dữ liệu, ứng dụng hoặc hệ thống trở lại trạng thái sẵn sàng sử dụng
- Phân loại:
  - Phục hồi dữ liệu
  - Phục hồi ứng dụng
  - Phục hồi hệ thống

Phục hồi dữ liệu

- Là quá trình lấy lại dữ liệu từ trạng thái bị hư hỏng, bị lỗi hoặc không thể tiếp cận được trên các thiết bị lưu trữ thứ cấp hoặc trên các phương tiện truyền thông nhằm đưa về trạng thái có thể sử dụng được
- Phục hồi bằng phần mềm
  - Sử dụng các phần mềm chuyên dụng
- Sử dụng các bản sao lưu
  - Sử dụng từ các bản sao lưu dự phòng của dữ liệu

Phục hồi ứng dụng

- Là quá trình đưa trạng thái không hoạt động hoặc không sử dụng được của ứng dụng về trạng thái có thể sử dụng được hay có thể hoạt động bình thường
- Sử dụng các công cụ để sửa lỗi, vá các lỗ hổng hoặc cập nhật các phiên bản mới của ứng dụng
- Cài đặt lại ứng dụng

Phục hồi hệ thống

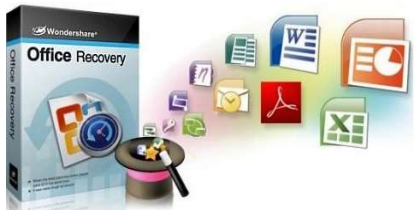
- Là quá trình đưa trạng thái không hoạt động hoặc không sử dụng được các ứng dụng trong hệ thống về trạng thái có thể sử dụng được hay có thể hoạt động bình thường

- Sử dụng các công cụ để sửa lỗi, vá lỗi hoặc cài đặt lại các thông số
- Cài đặt lại hệ thống

Phục hồi dữ liệu

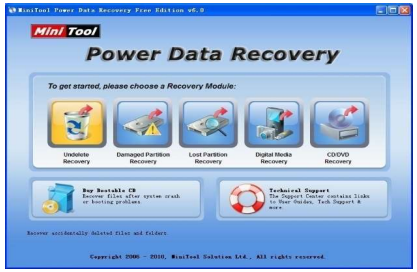
- Hard drive, camera card, USB, Zip, floppy disk, iPod and other media
- Emptied from the Recycle Bin
- Accidental format, reinstalled Windows.
- Hard disk crash
- Partitioning error
- RAW hard drives
- Documents, photos, video music, email.
- Recovers NTFS, AT(12/16/32), exFAT, HFS, HFS+

Phục hồi dữ liệu văn bản



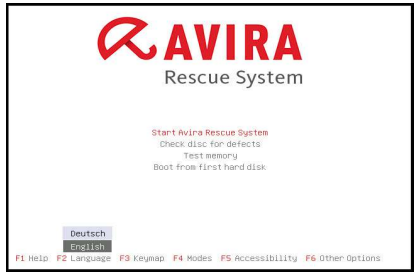
- Phục hồi dữ liệu văn phòng
  - Các file tài liệu có trong bộ pm văn phòng
  - Word, excel, ppt, access, visio, …

Phục hồi nhiều kiểu dữ liệu



- MiniTool Power Data Recovery phục hồi dữ liệu bị mất trong các phân hoạch FAT12, FAT16, FAT32, FAT64 và NTFS
- Chạy tốt trên Windows 98, Windows 2000, Windows 2003, Windows XP, Windows 7, Windows 2008, vv.
- MiniTool Power Data Recovery là miễn phí cho gia đình và người dùng gia đình.

Phục hồi hệ thống



- Cho phép truy cập vào máy tính không khởi động được
- Sửa chữa hệ thống
- Phát hiện sai sót trên ổ đĩa
- Boot máy
- Cứu dữ liệu
- Quét hệ thống để tìm virus.
- Chỉ cần ghi vào CD / DVD. Sau đó sử dụng đĩa CD / DVD để khởi động máy tính

Một số công cụ phổ biến

1. Acronis True Image
2. NovaBACKUP
3. EaseUS Todo Backup
4. AOMEI Backupper
5. Macrium Reflect
6. Genie Backup Manager
7. Paragon Backup & Recovery
8. Backup4all
9. NTI Backup Now
10. O&O DiskImage

Câu hỏi ôn tập chương 5

1. Sao lưu là gì? Vì sao cần sao lưu thông tin và dữ liệu trong hệ thống thông tin của tổ chức, doanh nghiệp? Hãy giải thích và lấy ví dụ minh họa
2. Các kiểu sao lưu thông tin và dữ liệu trong hệ thống thông tin của tổ chức, doanh nghiệp? Lấy ví dụ minh họa
3. So sánh sự giống nhau và khác nhau của sao lưu và dự phòng? Khi nào thì gọi là sao lưu? Khi nào thì gọi là dự phòng? Hãy giải thích.
4. Các kiểu sao lưu dự phòng phổ biến? Minh họa thực tế
5. Hãy trình bày các công cụ sao lưu dự phòng phổ biến của Windows?

Chương 6: Đảm bảo an toàn cho HTTT

- 6.1. ĐẢM BẢO AN TOÀN BẰNG MÔ HÌNH NHIỀU LỚP
  - 6.1.1. Bảo vệ mức quy trình và chính sách
  - 6.1.2. Bảo vệ hệ thống thông tin theo nhiều mức
- 6.2. CÁC KIẾN TRÚC AN TOÀN CHO HỆ THỐNG THÔNG TIN
  - 6.2.1. Bộ ISO 27001 và mô hình an toàn cho HTTT (ISMS)
  - 6.2.2. Khung bảo mật của NIST (NIST Security Framework)
- 6.3. MỘT SỐ GIẢI PHÁP AN TOÀN CHO HỆ THỐNG THÔNG TIN
  - 6.3.1. Phân quyền người sử dụng
  - 6.3.2. Bảo mật kênh truyền
  - 6.3.3. Sử dụng tường lửa
- 6.4. MỘT SỐ GIẢI PHÁP AN TOÀN CHO NGƯỜI DÙNG TRONG HỆ THỐNG THÔNG TIN
  - 6.4.1. Sử dụng phần mềm diệt virus
  - 6.4.2. Sử dụng mật khẩu mạnh.
  - 6.4.3. Xác minh thiết lập bảo mật phần mềm
  - 6.4.4. Cập nhật các sản phẩm bảo vệ
  - 6.4.5. Xây dựng tường lửa cá nhân
  - 6.4.6. Thường xuyên sao lưu dự phòng
  - 6.4.7. Có cơ chế bảo vệ chống lại các nguy cơ

6.1. ĐẢM BẢO AN TOÀN BẰNG MÔ HÌNH NHIỀU LỚP

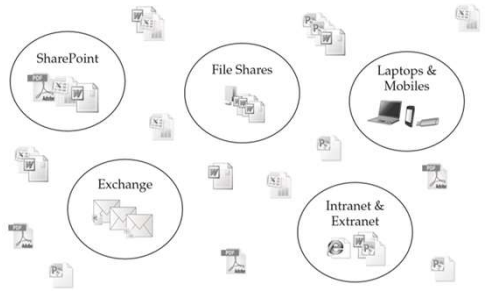
- 6.1.1. Bảo vệ mức quy trình và chính sách
- 6.1.2. Bảo vệ hệ thống thông tin theo nhiều mức

6.1.1. Bảo vệ mức quy trình và chính sách

- **Một chính sách an ninh thông tin bao gồm:**
  - Xác định được phạm vi;
  - Phân loại các nhóm thông tin;
  - Có mục tiêu quản lý rõ rang;
  - Xác định được ngữ cảnh/ bối cảnh;
  - Có tài liệu hỗ trợ;
  - Có hướng dẫn cụ thể;
  - Có trách nhiệm rõ ràng.
  - Xác định/Dự đoán được hậu quả.

6.1.2. Bảo vệ hệ thống thông tin theo nhiều mức

- Mức dữ liệu
  - Dữ liệu có cấu trúc
  - Dữ liệu phi cấu trúc



6.1.2. Bảo vệ hệ thống thông tin theo nhiều mức

- Mức ứng dụng
  - Ứng dụng offline
    - Ứng dụng trên máy cá nhân
    - Ứng dụng trên LAN
  - Ứng dụng online
    - Ứng dụng riêng
    - Ứng dụng chung
- Giải pháp
  - Cơ chế truy cập và kiểm soát
  - Bảo mật và lưu trữ các phiên truy cập
  - Quản lý các cấu hình và khung nhìn
  - Bảo vệ mã nguồn các ứng dụng

6.1.2. Bảo vệ hệ thống thông tin theo nhiều mức

- Mức vật lý
  - Tại tổ chức, doanh nghiệp
  - Tại nhà
  - Khi sử dụng các thiết bị di động
- Giải pháp
  - Xây dựng thói quen sử dụng các thiết bị an toàn
  - Sử dụng các thiết bị có nguồn gốc rõ rang
  - Sử dụng các biện pháp và chính sách bảo vệ thiết bị

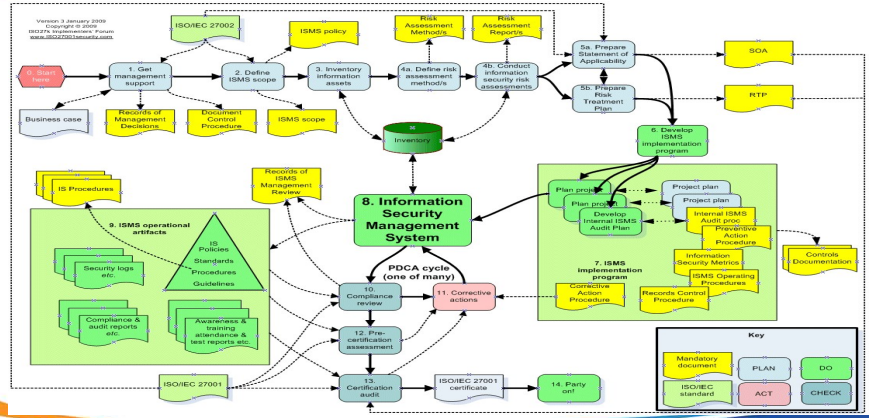
6.2. CÁC KIẾN TRÚC AN TOÀN CHO HTTT

- 6.2.1. Bộ ISO 27001 và mô hình an toàn cho HTTT (ISMS)
- 6.2.2. Khung bảo mật của NIST (NIST Security Framework)

6.2.1. Bộ ISO 27001 và mô hình an toàn cho HTTT (ISMS)

- Hệ thống quản lý an toàn thông tin (Information Security Management System - ISMS) hỗ trợ
  - Thực hiện việc giám sát,
  - Quản lý hệ thống thông tin,
  - Tăng cường mức độ an toàn, bảo mật, giảm thiểu rủi ro cho hệ thống thông tin,
  - Đáp ứng được mục tiêu của doanh nghiệp, tổ chức.
- ISO 27001 là tiêu chuẩn quốc tế đặc tả cho các hệ thống quản lý ATTT (ISMS) cung cấp:
  - Một mô hình thống nhất để thiết lập, vận hành, duy trì và cải tiến hệ thống quản lý ATTT cho các tổ chức, đơn vị
  - Tuân thủ theo một hệ thống quản lý ISMS

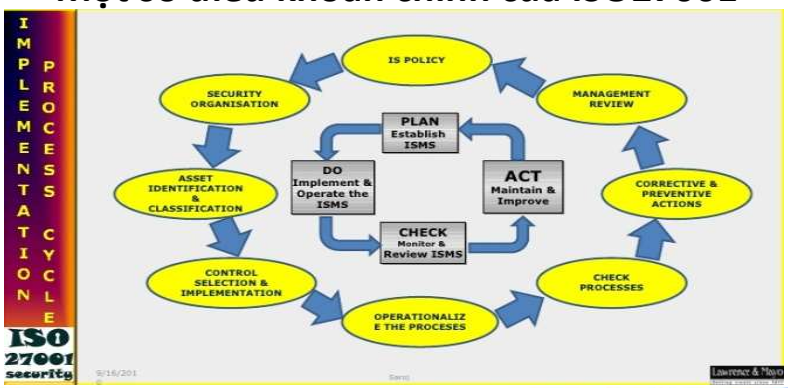
ISMS và ISO27001



Một số điều khoản chính của ISO27001

- Cấu trúc tiêu chuẩn ISO/IEC 27001: 2013 gồm có 07 điều khoản chính (từ phần 4 đến phần 10 của Tiêu chuẩn):
- *Điều khoản 4 - Phạm vi tổ chức*
- *Điều khoản 5 - Lãnh đạo*
- *Điều khoản 6 - Lập kế hoạch*
- *Điều khoản 7 - Hỗ trợ*
- *Điều khoản 8 - Vận hành hệ thống*
- *Điều khoản 9 - Đánh giá hiệu năng hệ thống*
- *Điều khoản 10 - Cải tiến hệ thống*: Giữ vững nguyên tắc 4 bước
  - Lập kế hoạch - Thực hiện - Kiểm tra - Hành động (P-D-C-A: Plan – Do – Check - Action),

Một số điều khoản chính của ISO27001



6.2.2. Khung bảo mật của NIST

- NIST sử dụng một số dạng tài liệu để công bố, phổ biến các tiêu chuẩn và hướng dẫn mật mã.
  - Các tiêu chuẩn xử lý thông tin liên bang (Federal Information Processing Standards - FIPS),
  - Các ấn phẩm đặc biệt (NIST Special Publications - NIST SP)
  - Các báo cáo nội bộ/liên ngành (NIST Internal/Interagency Reports).
- Khung bảo mật NIST
  - FIPS PUB 197 mô tả thuật toán mã khối AES;
  - FIPS PUB 186-4 mô tả các tiêu chuẩn về chữ ký số (Digital Signature Standard - DSS), bao gồm lược đồ chữ ký số: DSA, RSA, ECDSA. Ngoài ra, trong FIPS 186-4 cũng đưa ra các tiêu chuẩn an toàn và thuật toán sinh các bộ tham số cho các lược đồ chữ ký số nêu trên;
  - FIPS PUB 180-4 mô tả tiêu chuẩn về hàm băm bao gồm các hàm băm: SHA-1, SHA-256, SHA-224, SHA-384 và SHA-512;
  - FIP PUB 198-1 mô tả tiêu chuẩn mã xác thực thông báo hàm băm có khóa.

6.2.2. Khung bảo mật của NIST (NIST Security Framework)

- NIST SP 800-185 mô tả các hàm dẫn xuất SHA-3: cSHAKE, KMAC, TupieHash, ParallelHash;
- NIST SP 800-184 hướng dẫn khôi phục sự kiện an toàn mạng;
- NIST SP 800-163 mô tả việc kiểm định, đánh giá an toàn ứng dụng di động;
- NIST SP 800-145 mô tả các khái niệm điện toán đám mây;
- NIST SP 800-133 đưa ra các khuyến cáo về sinh khóa mật mã;
- NIST SP 800-132 đưa ra các khuyến cáo về dẫn xuất khóa dựa trên mật khẩu;
- NIST SP 800-131 mô tả về các thuật toán và độ dài khóa mật mã;
- NIST SP 800-130 mô tả khung hình chung cho việc thiết kế các hệ thống quản lý khóa mật mã;
- NIST SP 800-95 hướng dẫn các dịch vụ web an toàn.
- Các ấn phẩm NIST SP khác có thể tham khảo tại địa chỉ https://csrc.nist.gov/publications.

Các bước triển khai NIST

Hình 6.3: Các bước triển khai NIST

Đánh giá hiện trạng

	Các lĩnh vực chức năng riêng Các chuyên gia của riêng lĩnh vực đánh giá dựa trên cấu trúc tổ chức và cho điểm mỗi chức năng, lớp và lớp phụ			Điểm số Điểm cho bởi chuyên gia so sánh với nhóm nòng cốt độc lập		Kết quả Tổng hợp điểm số và so sánh với mục tiêu tổ chức đặt ra. Khoảng cách rủi ro tính được cần được giải quyết.		
	Lĩnh vực 1 (Chính sách)	Lĩnh vực 2 (Mạng)	Lĩnh vực 3 (Ứng dụng)	Điểm trung bình của chuyên gia	Điểm của nhóm nòng cốt	Tổng hợp	Mục tiêu cấp độ	Khoảng cách rủi ro
Xác định								
Kinh doanh	3	3	2	3	3	3	3	0
Tài sản	2	1	2	1	2	2	3	1
Quản trị	2	2	4	2	2	2	2	0
Đánh giá rủi ro	2	2	2	2	2	2	2	0
Quản lý rủi ro	2	2	2	2	2	2	3	1
Bảo vệ	2	1	1	1	1	1	3	2
Phát hiện	2	2	2	2	2	2	3	1
Ứng phó	1	1	2	1	2	1	3	2
Phục hồi	2	4	3	3	3	3	4	1

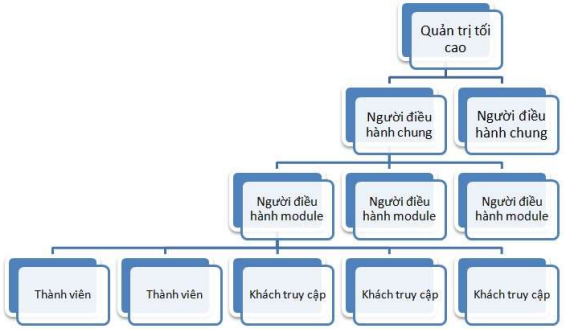
6.3. MỘT SỐ GIẢI PHÁP AN TOÀN CHO HTTT

- 6.3.1. Phân quyền người sử dụng
- 6.3.2. Bảo mật kênh truyền
- 6.3.3. Sử dụng tường lửa

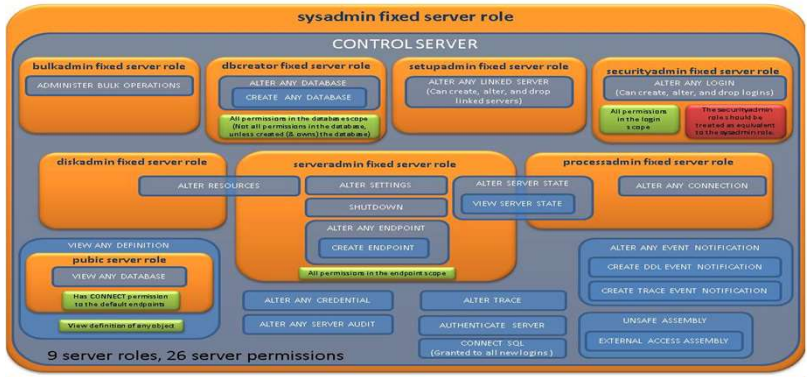
6.3.1. Phân quyền người sử dụng

- Người dùng
  - Những người được quyền đăng nhập và sử dụng tài nguyên của hệ thống trong phạm vi quyền hạn của mình
- Phân loại
  - Người dung cục bộ
  - Người dung toàn cục
- Phân quyền người dùng
  - Những biện pháp giúp phân chia rõ ràng quyền hạn, cách thức thao tác đối với hệ thống theo những yêu cầu khác nhau nhằm đảm bảo được sự an toàn của hệ thống cũng như đảm bảo tính riêng tư của mỗi người.

6.3.1. Phân quyền người sử dụng



6.3.1. Phân quyền người sử dụng

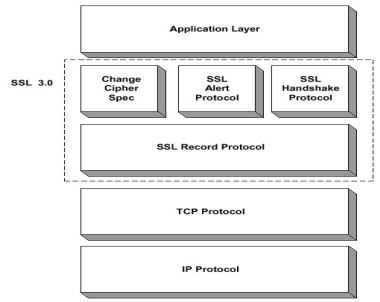


6.3.2. Bảo mật kênh truyền dữ liệu

- Bảo mật kênh truyền
  - Bảo mật kênh truyền dữ liệu là việc bảo mật các dữ liệu khi chúng được truyền trên kênh truyền thông
- Giải pháp
  - Mã hóa kênh truyền
    - SSL
    - SET
    - Bảo mật mạng không dây
  - Sử dụng các chứng chỉ an toàn
    - Chứng chỉ cá nhân
    - Chứng chỉ cho tổ chức, doanh nghiệp
    - Giao thức an toàn chung

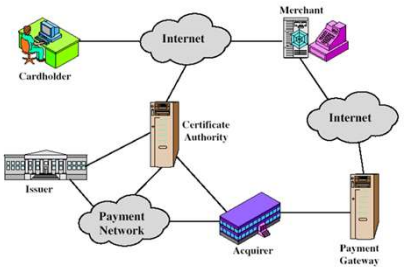
6.3.2. Bảo mật kênh truyền dữ liệu

- SSL
  - SSL là giao thức đa mục đích được thiết kế để tạo ra các giao tiếp giữa hai chương trình ứng dụng trên một cổng định trước (Socket 443) nhằm mã hoá toàn bộ thông tin đi/đến
  - Giao thức SSL được xây dựng trên tầng giao vận của mô hình TCP/IP
  - Có 4 tầng
    - Alert
    - Change Cipher Spec
    - Handshake
    - Record



6.3.2. Bảo mật kênh truyền dữ liệu

- SET
  - Mục đích:
    - (1) Đảm bảo về độ chính xác của thông tin nhận/gửi
    - (2) Đảm bảo tính toàn vẹn của thông tin khi được truyền
    - (3) Tạo ra cơ chế chứng thực cả người mua hàng/bán
  - Hoạt động



6.3.2. Bảo mật kênh truyền dữ liệu

- Bảo mật mạng không dây
  - Wifi (Wireless Fidelity)
  - WEP (Wired Equivalent Privacy)
- Giải pháp
  - (1) Sử dụng khóa WEP có độ dài 128 bit
  - (2) Thực thi chính sách thay đổi khóa WEP định kỳ
  - (3) Sử dụng các công cụ theo dõi số liệu thống kê dữ liệu trên đường truyền không dây
- Cơ chế
  - WEP cung cấp bảo mật cho dữ liệu trên mạng không dây qua phương thức mã hóa sử dụng thuật toán đối xứng RC4, được Ron Rivest - Thuộc hãng RSA Security Inc nổi tiếng - phát triển

6.4. MỘT SỐ GIẢI PHÁP AN TOÀN CHO NGƯỜI DÙNG TRONG HỆ THỐNG THÔNG TIN

- Sử dụng phần mềm diệt virus
- Sử dụng mật khẩu mạnh.
- Xác minh thiết lập bảo mật phần mềm
- Cập nhật các sản phẩm bảo vệ
- Xây dựng tường lửa cá nhân
- Thường xuyên sao lưu dự phòng
- Có cơ chế bảo vệ chống lại các nguy cơ

Câu hỏi chương 6

1. Vì sao cần bảo vệ thông tin của hệ thống thông tin bằng nhiều lớp và nhiều phương pháp khác nhau? Hãy giải thích và lấy ví dụ minh họa
2. Trình bày chi tiết các mức cần bảo vệ cho thông tin trong hệ thống thông tin của tổ chức, doanh nghiệp?
3. Nguyên tắc của ISO 27001 là gì? Vì sao mỗi tổ chức, doanh nghiệp cần khảo sát thực trạng trước khi triển khai quy trình ISO 27001?
4. Thực trạng triển khai ISO 27001 ở Việt Nam và trên thế giới? Vì sao bộ tiêu chuẩn đều có phần tùy chỉnh cho mỗi quốc gia?
5. Hãy trình bày các thành phần trong khung bảo mật NIST?
6. Trình bày các bản đặc biệt của NIST? Lấy ví dụ minh họa.
7. Người dùng là gì? Vì sao phải phân quyền người dùng trong hệ thống thông tin của tổ chức, doanh nghiệp? Hãy giải thích
8. Có những kiểu người dùng nào trong hệ thống thông tin của doanh nghiệp? Quyền và nghĩa vụ của mỗi nhóm người dùng? Hãy lấy ví dụ minh họa.

CHƯƠNG 7: AN TOÀN DỮ LIỆU TRONG TMĐT

7.1. CHỮ KÝ SỐ

- 7.1.1. Một số khái niệm
- 7.1.2. Cơ chế hoạt động của chữ ký số
- 7.1.3. Phân loại chữ ký số
- 7.1.4. Ưu và nhược điểm của chữ ký số

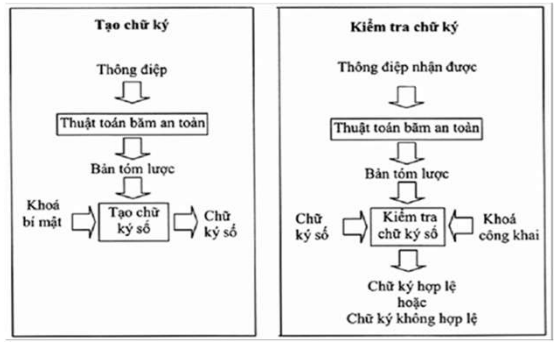
7.1.1. Một số khái niệm

- *Luật giao dịch điện tử* (ngày 29/11/2005)
  - "Chữ ký số được tạo lập dưới dạng từ, chữ, số, ký hiệu, âm thanh hoặc các hình thức khác bằng phương tiện điện tử, gắn liền hoặc kết hợp một cách logic với thông điệp dữ liệu, có khả năng xác nhận người ký thông điệp dữ liệu và xác nhận sự chấp thuận của người đó đối với nội dung thông điệp dữ liệu được ký" (Điều 21, Khoản 1).
- Tính chất
  - (1) Có khả năng kiểm tra được người ký và thời gian ký,
  - (2) Có khả năng xác thực các nội dung tại thời điểm ký
  - (3) Các thành viên thứ ba có thể kiểm tra chữ ký để giải quyết các tranh chấp (nếu có).

7.1.1. Một số khái niệm

- Yêu cầu:
  - (1) Phải là một mẫu bit phụ thuộc chặt chẽ vào văn bản được ký,
  - (2) Việc tạo ra chữ ký phải đơn giản, thuận tiện, dễ dàng,
  - (3) Dễ dàng cho việc kiểm tra (người nhận/ người gửi/ người xác minh)
  - (4) Khó giả mạo chữ ký
  - (5) Phải lưu giữ được một bản sao của chữ ký số

7.1.2. Cơ chế hoạt động của chữ ký số



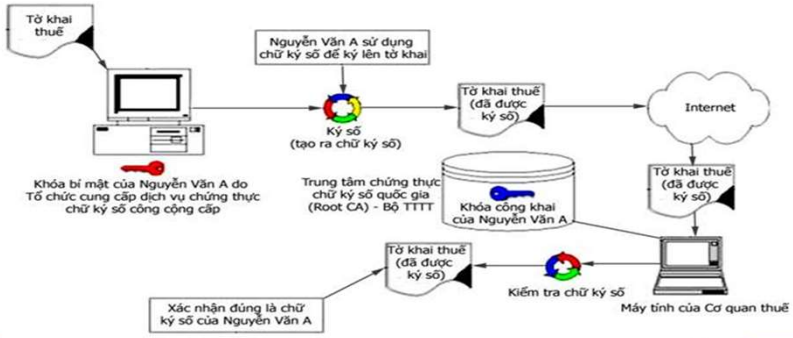
7.1.3. Phân loại chữ ký số

- Chữ ký số trực tiếp
  - Chữ ký số trực tiếp là hệ thống chữ ký trong đó chỉ có sự tham gia của người gửi và người nhận.
  - Chữ ký số được tạo ra bằng cách mã hóa toàn bộ thông điệp hoặc chuỗi băm của thông điệp bằng khóa riêng của người gửi
- Chữ ký của bên thứ ba
  - Chữ ký số của bên thứ ba đóng vai trò một trọng tài viên.
- Kịch bản
  - Giả sử X muốn gửi một thông điệp cần bảo mật cho Y:
  - (1) X ký thông điệp => thành viên thứ ba M trước khi gửi cho Y,
  - (2) M kiểm tra nguồn gốc, nội dung thông điệp và chữ ký của thông điệp => gắn tem thời gian và gửi cho Y
- Với sự tham gia của M có thể giải quyết vấn đề chống chối bỏ của X trong sử dụng chữ ký trực tiếp.

7.1.4. Ưu và nhược điểm của chữ ký số

- Ưu điểm
  - (1) Chữ ký số đảm bảo tính không thể chối cãi.
  - (2) Có thể sử dụng chữ ký số để thiết lập một kênh truyền tin có xác nhận
- Nhược điểm
  - (1) Thuật toán sinh chữ ký số tiêu tốn nhiều thời gian
  - (2) Dung lượng của chữ ký số hoàn toàn phụ thuộc vào dung lượng của thông điệp.

Sử dụng chữ ký điện tử trong kê khai thuế ở Việt Nam



7.2. CHỨNG THỰC SỐ

- 7.2.1. Khái niệm chứng thực số
- 7.2.2. Sơ đồ chứng thực số sử dụng khóa công khai

7.2.1. Khái niệm chứng thực số

- Chứng thực số (Digital Certificate) là một giải pháp trong bảo mật an toàn thông tin.
- Là hoạt động chứng thực danh tính của những người tham gia vào việc gửi và nhận thông tin qua kênh truyền,
- Một giải pháp cung cấp cho người dùng những công cụ, dịch vụ cần thiết để thực hiện việc bảo mật thông tin, chứng thực nguồn gốc và nội dung thông tin.
- Chứng thực số là một loại "giấy tờ" điện tử dùng để chứng thực bạn là ai khi chúng ta tham gia vào mạng Internet.
- Chứng thực số được cấp bởi một cơ quan chứng thực có uy tin trên thế giới.

7.2.1. Khái niệm chứng thực số

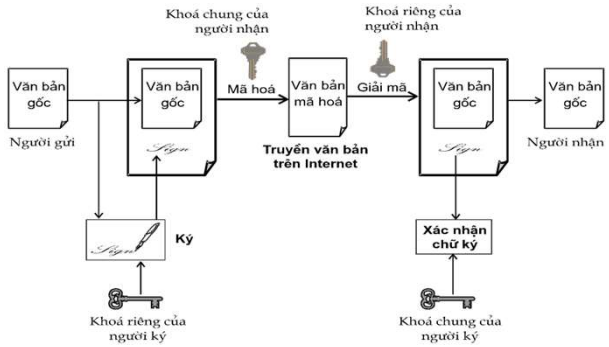
- Một chứng thực số bao gồm:
  - Khóa công khai của người sở hữu chứng thực số này,
  - Các thông tin riêng của người sở hữu chứng thực,
  - Hạn sử dụng,
  - Tên cơ quan cấp chứng thực điện tử,
  - Số hiệu của chứng thực,
  - Chữ ký của nhà cung cấp.
- Phân loại
  - (1) Chứng thực cho máy chủ Web (Server Certificate)
  - (2) Chứng thực cho các phần mềm
  - (3) Chứng thực cá nhân
  - (4) Chứng thực của các nhà cung cấp chứng thực điện tử

Qui trình tạo một chứng thực số

- (1) Tạo ra một cặp khóa công khai và khóa bí mật của riêng người dùng
- (2) Gửi yêu cầu xin cấp chứng thực điện tử
- (3) CA nhận được các thông tin cần thiết cho chứng thực, CA kiểm tra sự chính xác của các thông tin nhận được này
- (4) Xác định tính chính xác của các thông tin, CA sẽ tạo ra một chứng thực số
- (5) CA phân chia chứng thực này thành các đoạn băm sau đó tiến hành mã hóa từng đoạn bằng khóa bí mật của mình và trên mỗi phần sử dụng chữ ký riêng của mình để ký lên đó và gửi trở lại cho đơn vị đăng ký chứng thực điện tử.
- (6) Một bản sao của chứng thực được chuyển tới thuê bao (tổ chức/cá nhân) và có thể thông báo lại tới CA là đã nhận được,
- (7) CA có thể lưu giữ bản sao của chứng thực số,
- (8) CA ghi lại các chi tiết của quá trình tạo chứng chỉ vào nhật ký kiểm toán

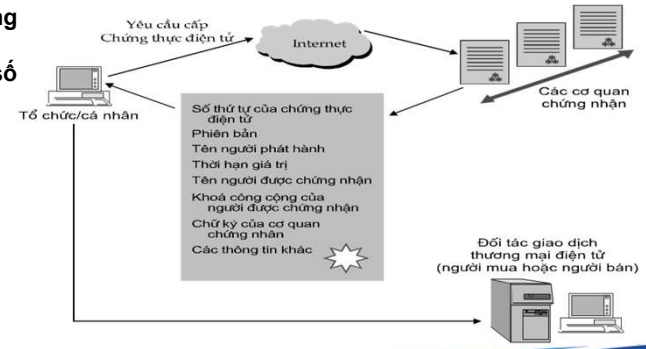
7.2.2. Sơ đồ chứng thực số sử dụng khóa công khai

Bước 1: Chữ ký số tạo bởi khóa công khai

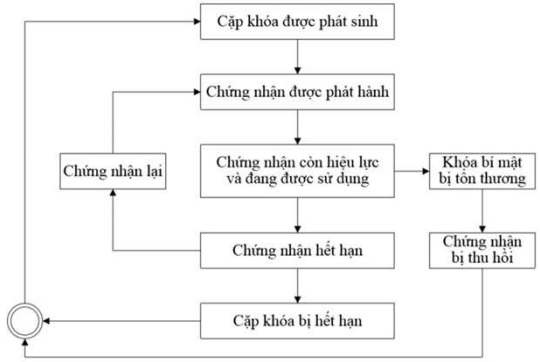


7.2.2. Sơ đồ chứng thực số sử dụng khóa công khai

Bước 2: Chứng thực số sử dụng chữ ký số



Chu kỳ sống của chứng thực số



7.3. AN TOÀN DỮ LIỆU THANH TOÁN ĐIỆN TỬ

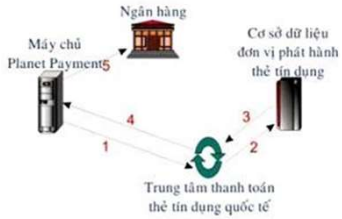
- 7.3.1. Tổng quan về thanh toán điện tử
- 7.3.2. Các đặc trưng của hệ thống thanh toán điện tử
- 7.3.3. An toàn thông tin trong thanh toàn điện tử

7.3.1. Tổng quan về thanh toán điện tử

- Thanh toán điện tử là hệ thống cho phép các bên tham gia mua và bán tiến hành thanh toán với nhau tương tự như trong các phương thức thanh toán truyền thống đã có.
- Mô tả hoạt động của một hệ thống có nhiều bên tham gia.
  - Người mua (người trả tiền) và người bán (người được trả tiền).
  - Người mua và người bán được đại diện bởi các máy tính và các máy tính này được nối với nhau thông qua mạng máy tính để thực hiện các giao thức thanh toán điện tử.
- Có sự tham gia của các tổ chức tài chính như là các ngân hàng đại diện cho mỗi bên:
  - Cung cấp các hình thức của tiền (một vật thể mang giá trị trao đổi thanh toán)
  - Đồng tiền số (Digital Coin), tiền điện tử (Electronic Cash) hoặc séc điện tử (Electronic Cheque).

7.3.2. Các đặc trưng của hệ thống TTĐT

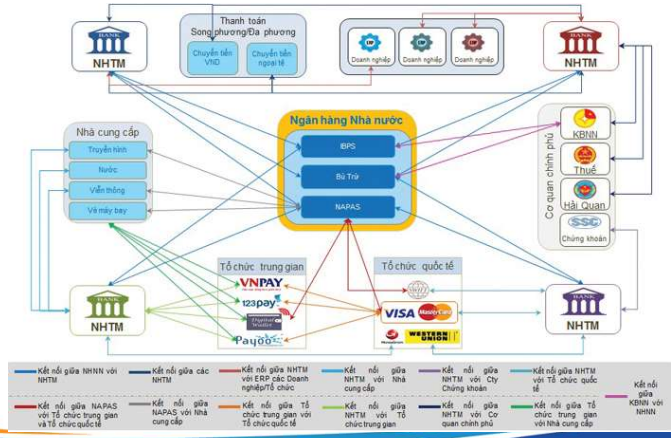
- Các thành phần tham gia trong HTTTĐT gồm:
  - (1) Máy chủ Web Server
  - (2) Máy chủ cơ sở dữ liệu (Database Server)
  - (3) Máy chủ Billing (Billing Server)
  - (4) Người mua hàng (User)



7.3.2. Các đặc trưng của hệ thống TTĐT

- Tính chất
  - (1) Độc lập vật lý
  - (2) An toàn
  - (3) Riêng tư
  - (4) Thanh toán ngoại tuyến
  - (5) Chuyển nhượng
  - (6) Phân chia

Thanh toán của Vietinbank



Thanh toán điện tử khác

7.3.3. An toàn thông tin trong TTĐT

- Vấn đề
  - Là mảnh đất mầu mỡ cho tội phạm công nghệ cao
  - Tỷ lệ tấn công cao, thiệt hại lớn
  - Có nhiều nguy cơ, lỗ hổng
  - …
- Giải pháp
  - Người dùng
  - Tổ chức cung cấp dịch vụ
  - Hạ tầng pháp lý

7.4. BẢO MẬT WEB

- 7.4.1. Một vài khái niệm
- 7.4.2. Các nguy cơ đối với Website
- 7.4.3. Các biện pháp bảo mật cho Website

7.4.1. Một vài khái niệm

- Vai trò của website trong nền kinh tế số
  - Công cụ để thu thập thông tin, cải thiện chất lượng sản phẩm, dịch vụ, cũng như hiệu quả của các chiến dịch truyền thông;
  - Giúp doanh nghiệp bán hàng và thanh toán trực tuyến, tiết kiệm chi phí mặt bằng và nhân công
  - Là một kênh để phân phối phần mềm trực tiếp tới khách hàng
  - Có nhiều ứng dụng thiết thực khác như giao dịch tài chính, tiền điện tử, thanh toán, kết nối, mạng xã hội, v.v.

7.4.1. Một vài khái niệm

- Bảo mật Web là một hình thức bảo vệ các thông tin và tài nguyên của hệ thống website
  - (1) Cơ sở dữ liệu của trang Web
  - (2) Thông tin cá nhân của khách hàng và thông tin của tổ chức
  - (3) Tài nguyên của hệ thống website

Vai trò của bảo mật Website

- Khi Website bị tấn công:
  - Gây gián đoạn hoạt động kinh doanh;
  - Có thể bị lộ dữ liệu khách hàng và thông tin quan trọng của tổ chức
  - Ảnh hưởng đến SEO
  - Ảnh hưởng tới uy tín thương hiệu;
  - Không thể thực hiện các chiến lược trên Website
- => Có vai trò quan trọng trong hoạt động SX, KD của tổ chức

7.4.2. Các nguy cơ đối với Website

- (1) Tấn công vào hệ thống website của TC, DN và cá nhân
- (2) Tấn công vào hệ thống máy chủ lấy cắp thông tin
- (3) Tấn công làm tê liệt hoạt động của hệ thống máy chủ Web
- (4) Giả mạo người dùng để thực hiện các giao dịch giả.
- (5) Nghe lén thông tin trên đường truyền

7.4.3. Các biện pháp bảo mật cho Website

- Bảo mật Server
- Xây dựng chính sách hoạt động cho máy chủ Web
  - Phân quyền người dung
  - Sao lưu định kỳ
  - Cơ chế mã hóa
- Kiểm soát truy cập và xác thực danh tính
- Bảo vệ tài nguyên máy khách và đường truyền

7.5. BẢO MẬT TRÊN CÁC PHƯƠNG TIỆN TTXH

- 7.5.1. Giới thiệu về các phương tiện TTXH
- 7.5.2. Các nguy cơ trên các phương tiện TTXH
- 7.5.3. Một số biện pháp an toàn trên các phương tiện TTXH

7.5.1. Giới thiệu về các phương tiện TTXH

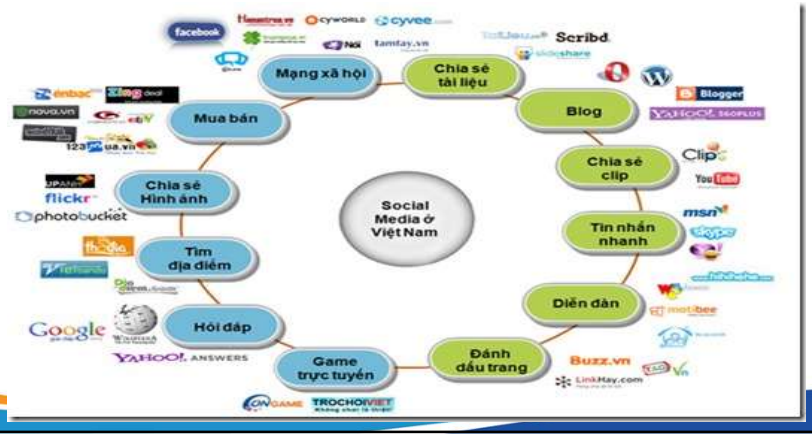
- Phương tiện truyền thông chính là phương thức cụ thể giúp doanh nghiệp có thể truyền tải thông điệp, nội dung của chiến lượng marketing của mình tới khách hàng
- Các phương tiện truyền thông phổ biến hiện nay có thể kể đến bao gồm báo chí, truyền hình, internet, phát thanh sách, quảng cáo, băng đĩa, điện thoại trực tiếp.
- Phương tiện truyền thông xã hội là các phương tiện truyền thông sử dụng các nền tảng công nghệ dựa trên mạng Internet

Phân loại

- Thứ nhất là Social Community: Nhóm này sẽ tập trung vào việc phát triển các mạng lưới quan hệ và gắn kết những người có cùng mối quan tâm và sở thích.
  - Facebook, Twitter, …
- Thứ hai là Social Publishing: Đây là các trang website truyền tải và phổ biến nội dung trên mạng.
  - Blog; trang tin tức; microsite; các trang đăng tải tài liệu, nhạc, video, hình ảnh v.v..
- Thứ ba là Social Commerce: Đây là nhóm phục vụ cho mục đích hỗ trợ việc giao dịch, mua bán. Social Commerce là một phần của thương mại điện tử, nơi người bán, người mua có thể chủ động và linh hoạt hơn trong việc tương tác, phản hồi ý kiến.

- Thứ tư là Social Entertainment: Đúng như tên gọi, nhóm này chủ yếu dùng để phục vụ người dùng với mục đích vui chơi, giải trí.
  - Trang website chơi game trực tuyến, social game v.v

Phân loại



7.5.2. Các nguy cơ trên các phương tiện TTXH

- Có khả năng bị tin tặc tấn công, đánh cắp tài khoản người dùng và công khai các tài khoản này lên mạng Internet để trao đổi, mua bán hoặc giả mạo
- Có thể bị kiểm soát quyền truy cập tài khoản, rò rỉ thông tin cá nhân
- Có thể bị nhiễm mã độc
- Mất an toàn qua mạng
  - Các tin nhắn nhanh / hòm thư điện tử do bị kẻ xấu lợi dụng các phương tiện truyền thông xã hội để lừa đảo qua mạng (social engineering) hoặc qua các email.
  - Các trò chơi xã hội như rò rỉ thông tin cá nhân hoặc khi người dùng sử dụng một số phần mềm miễn phí qua các phương tiện truyền thông xã hội.
  - Bị lộ thông tin vị trí/ bị theo dõi theo địa chỉ IP hoặc bị đánh cắp thông tin

7.5.3. Một số biện pháp an toàn trên các phương tiện TTXH

- Đối với các ban ngành chức năng, cơ quan, tổ chức, doanh nghiệp
  - Tuyên truyền, giáo dục
  - Xây dựng chính sách pháp luật
  - Sử dụng các biện pháp kỹ thuật
  - Có cơ chế xác thực người dung
  - Khuyến cáo người dung khi đăng nhập
- Đối với cá nhân người dung
  - Tạo thói quen kiểm tra và sử dụng mạng Internet an toàn
  - Hạn chế chia sẻ thông tin cá nhân
  - Sử dụng mật khẩu đủ mạnh
  - Cài đặt các cơ chế xác thực và kiểm tra
  - …

Câu hỏi ôn tập chương 7

1. Trình bày khái niệm về chữ ký số? Nguyên tắc xây dựng chữ ký số và quy trình hoạt động của chữ ký số? Lấy ví dụ minh họa
2. Chứng thực số là gì? Trình bày các thành phần trong một chứng thực số? Trình bày sự giống nhau và khác nhau giữa chữ ký số và chứng thực số?
3. Thanh toán điện tử là gì? Các thành phần tham gia trong một giao dịch điện tử có thành toán? Hãy lấy ví dụ minh họa. Các nguy cơ của một giao dịch điện tử có thanh toán? Lấy ví dụ minh họa
4. Hãy trình bày một số giải pháp nhằm đảm bảo an toàn cho các giao dịch điện tử và giao dịch điện tử có thanh toán?
5. Bảo mật website là gì? Hãy trình bày các nguy cơ đối với website thông thường và website thương mại điện tử?
6. Hãy trình bày một số giải pháp đảm bảo an toàn cho một website thương mại điện tử? Lấy ví dụ minh họa
7. Phương tiện truyền thông xã hội là gì? Vai trò của các phương tiện truyền thông xã hội trong hoạt động của các doanh nghiệp thương mại điện tử?
8. Trình bày các nguy cơ đối với người dùng và các tổ chức, doanh nghiệp khi sử dụng các phương tiện truyền thông xã hội trong hoạt động kinh doanh?